Crown Commercial Service

G-Cloud 13 Call-Off Contract

This Call-Off Contract for the G-Cloud 13 Framework Agreement (RM1557.13) includes:

G-Cloud 13 Call-Off Contract

Part A: Order Form

Buyers must use this template order form as the basis for all Call-Off Contracts and must refrain from accepting a Supplier's prepopulated version unless it has been carefully checked against template drafting.

Platform service ID number	633643680068275
Call-Off Contract reference	Project_25292 Application Performance Monitoring – G-Cloud 13
Call-Off Contract title	Dynatrace Full Stack Observability for the Enterprise Cloud
Call-Off Contract description	Application Performance Monitoring (APM) Strategic Tooling
Start date	31 December 2024
Expiry date	30 December 2027
Call-Off Contract value	The Call-Off Contract Value for an initial three year committed contract term is £6,169,349.52 (excluding non-recoverable VAT @ £1,233,869.90) Buyer has the opportunity to exercise 1 year extension to 30 December 2028, further increasing non-committed contract value to £15,651,200 (excluding non-recoverable VAT @ £3,130,240)
Charging method	Supplier invoicing via BAC's

Purchase order number	To be shared with Supplier once approvals received.

This Order Form is issued under the G-Cloud 13 Framework Agreement (RM1557.13).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Services offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

From the Buyer	The Department for Work and Pensions Caxton House, 6 – 12 Tothill Street, London SW1H 9NA
To the Supplier	Dynatrace Limited REDACTED REDACTED REDACTED
Together the 'Parties'	

1. Principal contact details

1.1 For the Buyer:

Title:REDACTED

Name: REDACTED

Email:REDACTED

REDACTED

1.2 For the Supplier:

Title:REDACTED

Name:REDACTED

Email: REDACTED

Phone: REDACTED

2. Call-Off Contract term

2.1 Start date	This Call-Off Contract Starts on **31 December 2024** and is valid for **3 years to 30 December 2027**
2.2 Ending (termination)	The notice period for the Supplier needed for Ending the Call-Off Contract is at least **90** Working Days from the date of written notice for undisputed sums (as per clause 18.6). The notice period for the Buyer is a maximum of **30** days from the date of written notice for Ending without cause (as per clause 18.1) provided that the Buyer will remain obligated for payment of any unpaid fees and expenses covering the remainder of the term including any fees incurred relating to on-demand usage.

2.3 Extension period	This Call-Off Contract can be extended by the Buyer for **one** period of up to 12 months, by giving the Supplier **3 months** written notice before its expiry. The extension period is subject to clauses 1.3 and 1.4 in Part B below. Extensions which extend the Term beyond 36 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8. If a buyer is a central government department and the contract Term is intended to exceed 24 months, then under the Spend Controls process, prior approval must be obtained from the Government Digital Service (GDS). Further guidance: https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service

3 Buyer contractual details

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

3.1 G-Cloud Lot	This Call-Off Contract is for the provision of Services Under: ● Lot 2: Cloud software
3.2 G-Cloud Services required	The Services to be provided by the Supplier under the above Lot are listed in Framework Schedule 4 and outlined in Annexes 1 and 2: **Service ID: 633643680068275**

3.3 Additional Services	REDACTED [redacted]
3.4 Location	Services will be delivered remotely.
3.5 Quality Standards	The quality standards required for this Call-Off Contract are **included in Suppliers G-Cloud Service documents and available on the Digital Marketplace.**
3.6 Technical Standards:	The technical standards used as a requirement for this Call-Off Contract are included in Suppliers Service documents and available on the Digital Marketplace.
3.7 Service level agreement:	The service level and availability criteria required for this Call-Off Contract are included in Supplier's Service documents and Schedule 1 to this Call-Off Contract and available on the Digital Marketplace.
3.8 Onboarding	No On-boarding requirement for this Call-Off contract

3.9 Offboarding	In relation to off-boarding, the following will be required but not be limited to: • All /Authority data belonging to the Buyer and relating to the scope of Services (Schedule 1) will be handed over to the Buyer at the time of off-boarding without any cost implications or IPR restriction. • Appropriate deletion of any Buyer data • Agreed knowledge transfer in terms of understanding the capabilities and requirements for future activities. At the end of the off-boarding and handover period - removal of any security clearance and site/system access for the Supplier by the Buyer.

3.10 Collaboration agreement	Not Applicable
3.11 Limit on Parties' liability	Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets or equipment but excluding any loss or damage to Buyer Data) of the other Party will not exceed £5,000,000 per year or 125% of the cumulative charges payable buy the Buyer to the Supplier during the Call-Off Contract Term. (Whichever is the greater) The annual total liability of the Supplier for Buyer Data Defaults resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data will not exceed £5,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Call-Off Contract Term (whichever is the greater). The annual total liability of the Supplier for all other Defaults will not exceed £2,000,000.

3.12 Insurance	The Supplier insurance(s) required will be: ● a minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract ● professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) ● employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
3.13 Buyer's responsibilities	Not relevant for the purpose of this Call-Off Contract
3.14 Buyer's equipment	Not relevant for the purpose of this Call-Off Contract

4 Supplier's information

4.1 Subcontractors or partners	Not relevant for the purpose of this Call-Off Contract

5 Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

5.1 Payment method	The payment method for this Call-Off Contract is **via invoice and BACS**
5.2 Payment profile	REDACTED

5.3 Invoice details	The Supplier will issue electronic invoices annually, at the start of each contract year. The Buyer will pay the Supplier within 30 days of receipt of a valid undisputed invoice.
5.4 Who and where to send invoices to	REDACTED
5.5 Invoice information required	All invoices must include PO number and Buyers reference details. The invoice format will follow the standard Supplier invoice format mirroring the necessary information in clause 7 of the Call-Off Contract.
5.6 Invoice frequency	Invoice will be sent to the Buyer Annually or by exception via agreed Variation procedure.
5.7 Call-Off Contract value	The Call-Off Contract Value for an initial three year committed contract term is £6,169,349.52 (excluding non-recoverable VAT @ £1,233,869.90) Buyer has the opportunity to exercise 1 year extension to 30 December 2028, further increasing non-committed contract value to £15,651,200 (excluding non-recoverable VAT @ £3,130,240)

5.8 Call-Off Contract charges	REDACTED

6. Additional Buyer terms

6.1 Performance of the Service	As per Schedule 1 and any agreed Variations
6.2 Guarantee	Not applicable for the purpose of the G-Cloud Call-Off Contract
6.3 Warranties, representations	As per the incorporated Framework Agreement clause 2.3**.**
6.4 Supplemental requirements in addition to the Call-Off terms	Special Terms to apply to this agreement with DWP. The following clauses in the Dynatrace Subscription Agreement at Annex 5, will **not** apply. REDACTED

	REDACTED **12.2 Order Form and SOW. Each Order Form or SOW begins on its effective date and continues in effect through the end date of the Term or the Service Period thereof. Except as expressly provided under the Agreement, Order Forms and SOWs may not be terminated, cancelled or reduced during the Term or Service Period, payment obligations are non-cancellable, and fees are non-refundable. Each Dynatrace Platform and Support subscription will automatically renew for additional periods equal to the greater of the expiring subscription term or one (1) year unless either party gives the other written notice at least sixty (60) days before the expiration thereof. Notice to Dynatrace should be provided via** REDACTED [redacted]
6.5 Alternative clauses	These Alternative Clauses, relating to DWP Minimum Security Requirements will apply to this contract: MINIMUM SECURITY REQUIREMENTS GENERAL The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with the Authority's security requirements as set out in the Contract which include the requirements set out in this section 6.5 The Authority's Security Requirements include, but are not limited to, requirements regarding the confidentiality, integrity and availability of Authority Assets, the Authority's Systems Environment and the Contractor's Systems Environment.

Terms used in this section 6.5 which are not defined below shall have the meanings given to them in clause A1 (Definitions and Interpretations) of the Contract.

1. DEFINITIONS

1.1 In this section 6.5, the following definitions shall apply:

“Authority Personnel”

shall mean all persons employed by the Authority including directors, officers, employees together with the Authority’s servants, agents, consultants, contractors and suppliers but excluding the Contractor and any Sub-contractor (as applicable).

“Availability Test” shall mean the activities performed by the Contractor to confirm the availability of any or all components of any relevant ICT system as specified by the Authority.

“CHECK” shall mean the scheme for authorised penetration tests which scheme is managed by the NCSC.

“Cloud” shall mean an off-premise network of remote ICT servers on the Internet to store, process, manage and transmit data.

“Cyber Essentials”

shall mean the Government-backed, industry-supported scheme managed by the NCSC to help organisations to protect themselves against online threats or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.

“Cyber Security Information Sharing Partnership” or “CiSP” shall mean the cyber security information sharing partnership established by the NCSC or the relevant successor or replacement scheme which is published and/or formally recommended by the NCSC.

“Good Security Practice” shall mean:

a) the technical and organisational measures and practices that are required by, or recommended in, nationally or internationally accepted management standards and codes of practice relating to Information Security (such as published by the International Organization for Standardization or the National Institute of Standards and Technology);

b) security standards and guidelines relating to Information Security (including generally accepted principles regarding the segregation of the duties of governance, implementation and control) provided to the general public or Information Security practitioners and stakeholders by generally recognised authorities and organisations; and

c) the Government’s security policies, frameworks, standards and guidelines relating to Information Security.

“Information Security” shall mean:

a) the protection and preservation of:

i) the confidentiality, integrity and availability of any Authority Assets, the Authority's Systems Environment (or any part thereof) and the Contractor's Systems Environment (or any part thereof);

ii) related properties of information including, but not limited to, authenticity, accountability, and non-repudiation; and

b) compliance with all Law applicable to the processing, transmission, storage and disposal of Authority Assets.

"Information Security Manager" shall mean the person appointed by the Contractor with the appropriate experience, authority and expertise to ensure that the Contractor complies with the Authority's Security Requirements.

"Information Security Management System ("ISMS")" shall mean the set of policies, processes and systems designed, implemented and maintained by the Contractor to manage Information Security Risk as specified by ISO/IEC 27001.

"Information Security Questionnaire" shall mean the Authority's set of questions used to audit and on an ongoing basis assure the Contractor's compliance with the Authority's Security Requirements.

"Information Security Risk"shall mean any risk that might adversely affect Information Security including, but not limited to, a Breach of Security.

"ISO/IEC 27001, ISO/IEC 27002 and ISO 22301" shall mean

a) ISO/IEC 27001;

b) ISO/IEC 27002/IEC; and

c) ISO 22301

in each case as most recently published by the International Organization for Standardization or its successor entity (the "ISO") or the relevant successor or replacement information security standard which is formally recommended by the ISO.

"NCSC" shall mean the National Cyber Security Centre or its successor entity (where applicable).

"Penetration Test" shall mean a simulated attack on any Authority Assets, the Authority's Systems Environment (or any part thereof) or the Contractor's Systems Environment (or any part thereof).

"PCI DSS" shall mean the Payment Card Industry Data Security Standard as most recently published by the PCI Security Standards Council, LLC or its successor entity (the "PCI").

"Risk Profile"

shall mean a description of any set of risk. The set of risks can contain those that relate to a whole organisation, part of an organisation or as otherwise applicable.

"Security Test" shall include, but not be limited to, Penetration Test, Vulnerability Scan, Availability Test and any other security related test and audit.

“Tigerscheme” shall mean a scheme for authorised penetration tests which scheme is managed by USW Commercial Services Ltd.

“Vulnerability Scan” shall mean an ongoing activity to identify any potential vulnerability in any Authority Assets, the Authority’s Systems Environment (or any part thereof) or the Contractor’s Systems Environment (or any part thereof).

1.2 Reference to any notice to be provided by the Contractor to the Authority shall be construed as a notice to be provided by the Contractor to the Authority’s Representative.

2. PRINCIPLES OF SECURITY

2.1 The Contractor shall at all times provide a level of security which is in accordance with the Security Policies and Standards, Good Security Practice and Law.

3. ISO/IEC 27001 COMPLIANCE AND AUDIT

3.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, comply with ISO/IEC 27001 in relation to the Services during the Contract Period.

3.2 The Contractor shall appoint an Information Security Manager and shall notify the Authority of the identity of the Information Security Manager on the Commencement Date.

3.3 The Contractor shall ensure that it operates and maintains the Information Security Management System during the Contract Period and that the Information Security

Management System meets the Security Policies and Standards, Good Security Practice and Law and includes:

a) a scope statement (which covers all of the Services provided under this Contract);

b) a risk assessment (which shall include any risks specific to the Services);

c) a statement of applicability;

d) a risk treatment plan; and

e) an incident management plan

in each case as specified by ISO/IEC 27001.

The Contractor shall provide the Information Security Management System to the Authority upon request within 10 Working Days from such request.

3.4 The Contractor shall carry out regular Security Tests in compliance with ISO/IEC 27001.

3.5 Notwithstanding the provisions of paragraph 3.1 to paragraph 3.4, the Authority may notify the Contractor that it is not in compliance with the Authority's Security Requirements and provide details of such non-compliance. The Contractor shall undertake those actions required in order to comply with the Authority's Security Requirements within a reasonable timeframe or on a date as agreed by the Parties.

4. CYBER ESSENTIALS SCHEME

4.1 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, obtain and maintain certification to Cyber Essentials (the "Cyber Essentials

	Certificate”) in relation to the Services during Contract Period. The Cyber Essentials Certificate shall be provided by the Contractor to the Authority annually on the dates as agreed by the Parties. 4.2 The Contractor shall notify the Authority of any failure to obtain, or the revocation of, a Cyber Essentials Certificate within 2 Working Days of confirmation of such failure or revocation. The Contractor shall, at its own expense, undertake those actions required in order to obtain a Cyber Essentials Certificate following such failure or revocation. For the avoidance of doubt, any failure to obtain and/or maintain a Cyber Essentials Certificate during the Contract Period after the first date on which the Contractor was required to provide a Cyber Essentials Certificate in accordance with paragraph 4.1 (regardless of whether such failure is capable of remedy) shall constitute a Material Breach entitling the Authority to exercise its rights under clause F5.2A. 5. RISK MANAGEMENT 5.1 The Contractor shall operate and maintain policies and processes for risk management (the Risk Management Policy) during the Contract Period which includes standards and processes for the assessment of any potential risks in relation to the Services and processes to ensure that the Authority’s Security Requirements are met (the Risk Assessment). The Contractor shall provide the Risk Management Policy to the Authority upon request within 10 Working Days of such request. 5.2 The Contractor shall carry out a Risk Assessment (i) at least annually, (ii) in the event of a material change in the Contractor’s Systems Environment or in the threat landscape or (iii) at the request of the Authority. The Contractor shall provide the report of the Risk Assessment to the Authority upon request, The Contractor shall notify the Authority within 5 Working Days if the Risk Profile in relation to the Services

has changed materially, for example, but not limited to, from one risk rating to another risk rating.

5.3 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, co-operate with the Authority in relation to the Authority’s own risk management processes regarding the Services.

6. SECURITY AUDIT AND ASSURANCE

6.1 The Contractor shall complete the information security questionnaire in the format stipulated by the Authority (the “Information Security Questionnaire”) at least annually or at the request by the Authority. The Contractor shall provide the completed Information Security Questionnaire to the Authority within one calendar month from the date of request.

6.2 The Contractor shall conduct Security Tests to assess the Information Security of the Contractor’s Systems Environment and, if requested, the Authority’s Systems Environment. In relation to such Security Tests, the Contractor shall appoint a third party which i) in respect of any Penetration Test, is duly accredited by CHECK, CREST (International), or Tigerscheme and, ii) in respect of any Security Test to which PCI DSS apply, is an approved scanning vendor duly accredited by the PCI. Such Security Test shall be carried out (i) at least annually, (ii) in the event of a material change in the Contractor’s Systems Environment or in the Authority’s System Environment. The Contractor shall provide any report of such Security Tests upon request by the Authority.

6.3 Where the Contractor provides code development services to the Authority, the Contractor shall comply with the Authority’s Security Requirements in respect of code

	development within the Contractor's Systems Environment and the Authority's Systems Environment. **SDLC Standard** Dynatrace has aligned its SDLC with the ISO 27034-1 standard and has published the Dynatrace SDL at https://www.dynatrace.com/support/help/how-to-use-dynatrace/data-privacy-and-security/data-security/secure-development-controls/ **Version Control** All code changes are managed with a central version control system (Git). REDACTED

	REDACTED

	REDACTED Read more about Dynatrace secure development controls at https://www.dynatrace.com/support/help/how-to-use-dynatrace/data-privacy-and-security/data-security/secure-development-controls/ 6.4 The Authority, or an agent appointed by it, may undertake Security Tests in respect of the Contractor’s Systems Environment after providing advance notice to the Contractor. If any Security Test identifies any non-compliance with the Authority’s Security Requirements, the Contractor shall, at its own expense, undertake those actions required in order to rectify such identified non-compliance in the manner and timeframe as stipulated by the Authority at its absolute discretion. The Contractor shall provide all such co-operation and assistance in relation to any Security Test conducted by the Authority as the Authority may reasonably require. Any audits shall be limited to no more than once per year, conducted during Dynatrace’s business hours, and subject to 30 days’ prior notice. Before the commencement of any audit, the parties shall agree on a detailed audit plan, including fees, timing, scope, evidence to be produced, and duration. Dynatrace may reasonably limit the proposed scope so as not to compromise the security or confidentiality of Dynatrace's other customers’ data, the security of its systems, or Dynatrace's proprietary interests. Customer shall not be

permitted to access any of Dynatrace’s networks, servers, scan summaries, or audit logs.

6.5 The Authority shall schedule regular security governance review meetings which the Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, attend.

Any audits shall be limited to no more than once per year, conducted during Dynatrace’s business hours, and subject to 30 days’ prior notice. Before the commencement of any audit, the parties shall agree on a detailed audit plan, including fees, timing, scope, evidence to be produced, and duration. Dynatrace may reasonably limit the proposed scope so as not to compromise the security or confidentiality of Dynatrace's other customers’ data, the security of its systems, or Dynatrace's proprietary interests. Customer shall not be permitted to access any of Dynatrace’s networks, servers, scan summaries, or audit logs.

7. SECURITY POLICIES AND STANDARDS

7.1 Notwithstanding the foregoing, the Authority’s Security Requirements applicable to the Services may be subject to change following any material change in the delivery of the Services. Where any such change constitutes a Contract Change, any reasonable change in the Authority’s Security Requirements resulting from such Contract Change (if any) shall be agreed by the Parties in accordance with the Contract Change Procedure. Where any such change constitutes an Operational Change, any reasonable change in the Authority’s Security Requirements resulting from such Operational Change (if any) shall be agreed by the Parties and documented in the relevant Operational Change Confirmation.

7.2 The Contractor shall, and shall procure that any Sub-contractor (as applicable) shall, maintain appropriate records and is otherwise able to demonstrate compliance with Dynatrace Security Policies and Procedures.

8. CYBER SECURITY INFORMATION SHARING PARTNERSHIP

8.1 The Supplier may require a nominated representative of the Supplier to join the Cyber Security Information Sharing Partnership on behalf of the Supplier during the Term, in which case the Supplier's nominated representative shall participate in the Cyber Security Information Sharing Partnership for the exchange of cyber threat information.

8.2 If the Supplier elects a nominated representative to join the Cyber Security Information Sharing Partnership in accordance with Paragraph 9.1 above, it shall review the NCSC weekly threat reports on a weekly basis and implement recommendations in line with the Supplier's Risk Management Policy.

ANNEX A – AUTHORITY SECURITY POLICIES AND STANDARDS

The Security Policies are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards unless specified otherwise:

a) Acceptable Use Policy

b) Information Security Policy

c) Personnel Security Policy

d) Physical Security Policy

e) Information Management Policy

	f) Email Policy g) Technical Vulnerability Management Policy h) Remote Working Policy i) Social Media Policy j) Forensic Readiness Policy k) Microsoft Teams recording and transcription policy l) SMS Text Policy m) Privileged Users Security Policy n) Protective Monitoring Security Policy o) User Access Control Policy p) Security Classification Policy q) Cryptographic Key Management Policy r) HMG Personnel Security Controls – May 2018

(published on https://www.gov.uk/government/publications/hmg-personnel-security-controls)

s) NCSC Secure Sanitisation of Storage Media (published on https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media)

ANNEX B – SECURITY STANDARDS

The Security Standards are published on:

https://www.gov.uk/government/publications/dwp-procurement-security-policies-and-standards:

a) SS-001 - Part 1 - Access & Authentication Controls

b) SS-001 - Part 2 - Privileged User Access Controls

c) Security Standard Physical and Electronic Security (Part 1)

d) SS-002 - PKI & Key Management

e) SS-003 - Software Development

f) SS-005 - Database Management System

g) SS-006 - Security Boundaries

h) SS-007 - Use of Cryptography

i) SS-008 - Server Operating System

j) SS-009 - Hypervisor

k) SS-010 - Desktop Operating System

l) SS-011 - Containerisation

m) SS-012 - Protective Monitoring Standard for External Use

n) SS-013 - Firewall Security

o) SS-014 - Security Incident Management

p) SS-015 - Malware Protection

q) SS-016 - Remote Access

r) SS-017 - Mobile Devices

s) SS-018 - Network Security Design

t) SS-019 - Wireless Network

u) SS-022 - Voice & Video Communications

v) SS-023 - Cloud Computing

w) SS-025 - Virtualisation

x) SS-027 - Application Security Testing

y) SS-028 - Microservices Architecture

z) SS-029 - Securely Serving Web Content

aa) SS-030 - Oracle Database

bb) SS-031 - Domain Management

cc) SS-033 – Security Patching

dd) SS-035 – Backup and Recovery

ee) SS-036 – Secure Sanitisation and Destruction

Protection of Information

The Contractor and any of its Sub-contractors, shall not access, process, host or transfer Authority Data outside the United Kingdom without the prior written consent of the Authority, and where the Authority gives consent, the Contractor shall comply with any reasonable instructions notified to it by the Authority in relation to the Authority Data in question. The provisions set out in this paragraph shall apply to Landed Resources.

	Where the Authority has given its prior written consent to the Contractor to access, process, host or transfer Authority Data from premises outside the United Kingdom: - a) the Contractor must notify the Authority (in so far as they are not prohibited by Law) where any Regulatory Bodies seek to gain or has gained access to such Authority Data; b) the Contractor shall take all necessary steps in order to prevent any access to, or disclosure of, any Authority Data to any Regulatory Bodies outside the United Kingdom unless required by Law without any applicable exception or exemption. Signature of this Call-Off Contract shall count as the Authority giving prior written consent to the Contractor transferring Authority Data outside of the United Kingdom solely for the purpose of providing single sign-on, follow-the-sun support and if applicable, Insights, and the Contractor shall take all reasonable steps to ensure that the data transferred is the minimum necessary to provide this support. For the purpose of interpreting paragraph 9.1 of the Data Processing Agreement referenced form the Subscription Agreement, this is the sole purpose for which the Authority authorises the Contractor to transfer Authority Data across international borders.
6.6 Buyer specific amendments to/refinements of the Call-Off Contract terms	Not applicable for the purpose of the G-Cloud Call-Off Contract

6.7 Personal Data and Data Subjects	Personal data is shared but limited to account data - emails addresses and any data that may be shared in a support ticket.
6.8 Intellectual Property	Clause 11 applies
6.9 Social Value	To support the delivery of Social Value through Governmental contracts, the Supplier will work with the Buyer and provide a quarterly update at any arranged governance review meeting. This will include the steps the Supplier is taking (as an organisation) and, to the extent applicable to the Services, as part of the delivery of this contract, to support the following theme: Theme 4 to “Tackle economic inequality” with the required policy outcome being to “Create New Business, New Jobs and New Skills”, more specifically: • To support the creation of employment opportunities for historically underrepresented and under-recognized communities across regions we conduct business • To support the creation of training opportunities for people in industries with limited access and resources

7. Formation of contract

7.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.

7.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.

7.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.

7.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

8. Background to the agreement

8.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.13.

8.2 The Buyer provided an Order Form for Services to the Supplier.

REDACTED

Customer Benefits

For each Call-Off Contract please complete a customer benefits record, by following this link:

G-Cloud 13 Customer Benefit Record

Part B: Terms and conditions

1. Call-Off Contract Start date and length

1.1 The Supplier must start providing the Services on the date specified in the Order Form.

1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 36 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.

1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 1 period of up to 12 months.

1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to set the Term at more than 24 months.

2. Incorporation of terms

2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:

- 2.3 (Warranties and representations)
- 4.1 to 4.6 (Liability)
- 4.10 to 4.11 (IR35)
- 10 (Force majeure)
- 5.3 (Continuing rights)
- 5.4 to 5.6 (Change of control)
- 5.7 (Fraud)
- 5.8 (Notice of fraud)
- 7 (Transparency and Audit)
- 8.3 (Order of precedence)
- 11 (Relationship)
- 14 (Entire agreement)
- 15 (Law and jurisdiction)
- 16 (Legislative change)
- 17 (Bribery and corruption)
- 18 (Freedom of Information Act)
- 19 (Promoting tax compliance)
- 20 (Official Secrets Act)
- 21 (Transfer and subcontracting)
- 23 (Complaints handling and resolution)
- 24 (Conflicts of interest and ethical walls)
- 25 (Publicity and branding)
- 26 (Equality and diversity)
- 28 (Data protection)
- 31 (Severability)

- 32 and 33 (Managing disputes and Mediation)
- 34 (Confidentiality)
- 35 (Waiver and cumulative remedies)
- 36 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement Schedule 3

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the ‘Framework Agreement’ will be a reference to the ‘Call-Off Contract’

2.2.2 a reference to ‘CCS’ or to ‘CCS and/or the Buyer’ will be a reference to ‘the Buyer’

2.2.3 a reference to the ‘Parties’ and a ‘Party’ will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 7 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause ‘XX’, where ‘XX’ is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier’s Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer’s acceptance criteria, as defined in the Order Form.

4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.

4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.

4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.

4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.

4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.

4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

5. Due diligence

5.1 Both Parties agree that when entering into a Call-Off Contract they:

5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party

5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms

5.1.3 have raised all due diligence questions before signing the Call-Off Contract

5.1.4 have entered into the Call-Off Contract relying on their own due diligence

6. Business continuity and disaster recovery

6.1 The Supplier will have a clear business continuity and disaster recovery plan in their Service Descriptions.

6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.

6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

7. Payment, VAT and Call-Off Contract charges

7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.

7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.

7.3 The Call-Off Contract Charges include all Charges for payment processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.

7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.

7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.

7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.

7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.

7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.

7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.

7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoices under the Late Payment of Commercial Debts (Interest) Act 1998.

7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.

7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

8. Recovery of sums due and right of set-off

8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

9. Insurance

9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

9.2 The Supplier will ensure that:

9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

9.2.2 the third-party public and products liability insurance contains an ‘indemnity to principals’ clause for the Buyer’s benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly
9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

10. Confidentiality

10.1 The Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under incorporated Framework Agreement clause 34. The indemnity doesn’t apply to the extent that the Supplier breach is due to a Buyer’s instruction.

11. Intellectual Property Rights

11.1 Save for the licences expressly granted pursuant to Clauses 11.3 and 11.4, neither Party shall acquire any right, title or interest in or to the Intellectual Property Rights (“IPR”s) (whether pre-existing or created during the Call-Off Contract Term) of the other Party or its licensors unless stated otherwise in the Order Form.

11.2 Neither Party shall have any right to use any of the other Party's names, logos or trade marks on any of its products or services without the other Party's prior written consent.

11.3 The Buyer grants to the Supplier a royalty-free, non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Buyer’s or its relevant licensor’s Buyer Data and related IPR solely to the extent necessary for providing the Services in accordance with this Contract, including the right to grant sub-licences to Subcontractors provided that:

11.3.1 any relevant Subcontractor has entered into a confidentiality undertaking with the Supplier on substantially the same terms as set out in Framework Agreement clause 34 (Confidentiality); and

11.3.2 the Supplier shall not and shall procure that any relevant Sub-Contractor shall not, without the Buyer’s written consent, use the licensed materials for any other purpose or for the benefit of any person other than the Buyer.

11.4 The Supplier grants to the Buyer the licence taken from its Supplier Terms which licence shall, as a minimum, grant the Buyer a non-exclusive, non-transferable licence during the Call-Off Contract Term to use the Supplier's or its relevant licensor's IPR solely to the extent necessary to access and use the Services in accordance with this Call-Off Contract.

11.5 Subject to the limitation in Clause 24.3, the Buyer shall:

11.5.1 defend the Supplier, its Affiliates and licensors from and against any third-party claim:

(a) alleging that any use of the Services by or on behalf of the Buyer and/or Buyer Users is in breach of applicable Law;

(b) alleging that the Buyer Data violates, infringes or misappropriates any rights of a third party;

(c) arising from the Supplier's use of the Buyer Data in accordance with this Call-Off Contract; and

11.5.2 in addition to defending in accordance with Clause 11.5.1, the Buyer will pay the amount of Losses awarded in final judgment against the Supplier or the amount of any settlement agreed by the Buyer, provided that the Buyer's obligations under this Clause 11.5 shall not apply where and to the extent such Losses or third-party claim is caused by the Supplier's breach of this Contract.

11.6 The Supplier will, on written demand, fully indemnify the Buyer for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:

11.6.1 rights granted to the Buyer under this Call-Off Contract

11.6.2 Supplier's performance of the Services

11.6.3 use by the Buyer of the Services

11.7 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:

11.7.1 modify the relevant part of the Services without reducing its functionality or performance

11.7.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer

11.7.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer

11.8 Clause 11.6 will not apply if the IPR Claim is from:

11.8.1 the use of data supplied by the Buyer which the Supplier isn’t required to verify under this Call-Off Contract

11.8.2 other material provided by the Buyer necessary for the Services

11.9 If the Supplier does not comply with this clause 11, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer’s written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer’s instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

13. Buyer data

13.1 The Supplier must not remove any proprietary notices in the Buyer Data.

13.2 The Supplier will not store or use Buyer Data except if necessary to fulfil its obligations.

13.3 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.4 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.5 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.6 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

13.6.1 the principles in the Security Policy Framework: https://www.gov.uk/government/publications/security-policy-framework and the Government Security - Classification policy: https:/www.gov.uk/government/publications/government-security-classifications

13.6.2 guidance issued by the Centre for Protection of National Infrastructure on Risk Management: https://www.npsa.gov.uk/content/adopt-risk-management-approach and Protection of Sensitive Information and Assets: https://www.npsa.gov.uk/sensitive-information-assets

13.6.3 the National Cyber Security Centre's (NCSC) information risk management guidance: https://www.ncsc.gov.uk/collection/risk-management-collection

13.6.4 government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint: https://www.gov.uk/government/publications/technologycode-of-practice/technology-code-of-practice

13.6.5 the security requirements of cloud services using the NCSC Cloud Security Principles and accompanying guidance: https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles

13.6.6 Buyer requirements in respect of AI ethical standards.

13.7 The Buyer will specify any security requirements for this project in the Order Form.

13.8 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.

13.9 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.

13.10 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

14. Standards and quality

14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.

14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at: https://www.gov.uk/government/publications/technologycode-of-practice/technology -code-of-practice

14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.

14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.

14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

15. Open source

15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.

15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

16. Security

16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.

16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.

16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.

16.4 Responsibility for costs will be at the:

16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided

16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control

16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information. Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.

16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

17. Guarantee

17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:

17.1.1 an executed Guarantee in the form at Schedule 5

17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period are reasonable compensation and cover all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.

19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the ordered G-Cloud Services until the dates set out in the notice.

19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.

19.4 Ending or expiry of this Call-Off Contract will not affect:

19.4.1 any rights, remedies or obligations accrued before its Ending or expiration

19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry

19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses

- 7 (Payment, VAT and Call-Off Contract charges)
- 8 (Recovery of sums due and right of set-off)
- 9 (Insurance)
- 10 (Confidentiality)
- 11 (Intellectual property rights)
- 12 (Protection of information)
- 13 (Buyer data)
- 19 (Consequences of suspension, ending and expiry)
- 24 (Liability); and incorporated Framework Agreement clauses: 4.1 to 4.6, (Liability), 24 (Conflicts of interest and ethical walls), 35 (Waiver and cumulative remedies)

19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires.

19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:

19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it

19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer

19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer

19.5.4 destroy all copies of the Buyer Data when they receive the Buyer’s written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law

19.5.5 work with the Buyer on any ongoing work

19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.

19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

20. Notices

20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

- Manner of delivery: email
- Deemed time of delivery: 9am on the first Working Day after sending
- Proof of service: Sent in an emailed letter in PDF format to the correct email address without any error message

20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

21. Exit plan

21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.

21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.

21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 36 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 30 month anniversary of the Start date.

21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.

21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.

21.6 The Supplier acknowledges that the Buyer's right to take the Term beyond 36 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

22. Handover to replacement supplier

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

23. Force majeure

23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than 30 consecutive days, the other Party may End this Call-Off Contract with immediate effect by written notice.

24. Liability

24.1 Subject to incorporated Framework Agreement clauses 4.1 to 4.6, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract shall not exceed the greater of five hundred thousand pounds (£500,000) or one hundred and twenty-five per cent (125%) of the Charges paid and/or committed to be paid in that Year (or such greater sum (if any) as may be specified in the Order Form).

24.2 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Supplier's liability:

24.2.1 pursuant to the indemnities in Clauses 7, 10, 11 and 29 shall be unlimited; and

24.2.2 in respect of Losses arising from breach of the Data Protection Legislation shall be as set out in Framework Agreement clause 28.

24.3 Notwithstanding Clause 24.1 but subject to Framework Agreement clauses 4.1 to 4.6, the Buyer's liability pursuant to Clause 11.5.2 shall in no event exceed in aggregate five million pounds (£5,000,000).

24.4 When calculating the Supplier's liability under Clause 24.1 any items specified in Clause 24.2 will not be taken into consideration.

25. Premises

25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

29.2.1 the activities they perform
29.2.2 age
29.2.3 start date
29.2.4 place of work
29.2.5 notice period
29.2.6 redundancy payment entitlement
29.2.7 salary, benefits and pension entitlements
29.2.8 employment status
29.2.9 identity of employer
29.2.10 working arrangements
29.2.11 outstanding liabilities
29.2.12 sickness absence
29.2.13 copies of all relevant employment contracts and related documents
29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.

29.3 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.

29.4 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.

29.5 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:

29.5.1 its failure to comply with the provisions of this clause

29.5.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer

29.6 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.

29.7 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

30. Additional G-Cloud services

30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.

30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

31. Collaboration

31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.

31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:

31.2.1 work proactively and in good faith with each of the Buyer's contractors

31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

32. Variation process

32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.

32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.

32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call-Off Contract by giving 30 days notice to the Supplier.

33. Data Protection Legislation (GDPR)

33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clause 28 of the Framework Agreement is incorporated into this Call-Off Contract. For reference, the appropriate UK GDPR templates which are required to be completed in accordance with clause 28 are reproduced in this Call-Off Contract document at Schedule 7.

Schedule 1: Services

The Services to be provided by the Supplier are outlined in Annexes 1 and 2

Service ID: 633643680068275

Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Platform pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term are detailed in Annex 6 (G-Cloud 13 Pricing Document)

The agreed Licence and Service price points are held for the duration of the Term and Extension period if exercised as per section 2.3 of the Call-Off Contract.

The Buyer may purchase additional quantities of Licences via agreed Variation Procedure to the Call-Off Contract. Additional licences may be purchased at any time during the Term at a pro-rated unit price charge to allow for co-termination with other term licences.

Schedule 3: Collaboration agreement

Not applicable for this call-off contract

Schedule 4: Alternative clauses

1. Introduction

1.1 This Schedule specifies the alternative clauses that may be requested in the Order Form and, if requested in the Order Form, will apply to this Call-Off Contract.

2. Clauses selected

2.1 The Customer may, in the Order Form, request the following alternative Clauses:

2.1.1 Scots Law and Jurisdiction

2.1.2 References to England and Wales in incorporated Framework Agreement clause 15.1 (Law and Jurisdiction) of this Call-Off Contract will be replaced with Scotland and the wording of the Framework Agreement and Call-Off Contract will be interpreted as closely as possible to the original English and Welsh Law intention despite Scots Law applying.

2.1.3 Reference to England and Wales in Working Days definition within the Glossary and interpretations section will be replaced with Scotland.

2.1.4 References to the Contracts (Rights of Third Parties) Act 1999 will be removed in clause 27.1. Reference to the Freedom of Information Act 2000 within the defined terms for ‘FoIA/Freedom of Information Act’ to be replaced with Freedom of Information (Scotland) Act 2002.

2.1.5 Reference to the Supply of Goods and Services Act 1982 will be removed in incorporated Framework Agreement clause 4.1.

2.1.6 References to “tort” will be replaced with “delict” throughout

2.2 The Customer may, in the Order Form, request the following Alternative Clauses:

2.2.1 Northern Ireland Law (see paragraph 2.3, 2.4, 2.5, 2.6 and 2.7 of this Schedule)

2.3 Discrimination

2.3.1 The Supplier will comply with all applicable fair employment, equality of treatment and anti-discrimination legislation, including, in particular the:

- Employment (Northern Ireland) Order 2002
- Fair Employment and Treatment (Northern Ireland) Order 1998
- Sex Discrimination (Northern Ireland) Order 1976 and 1988
- Employment Equality (Sexual Orientation) Regulations (Northern Ireland) 2003
- Equal Pay Act (Northern Ireland) 1970
- Disability Discrimination Act 1995
- Race Relations (Northern Ireland) Order 1997
- Employment Relations (Northern Ireland) Order 1999 and Employment Rights (Northern Ireland) Order 1996

- Employment Equality (Age) Regulations (Northern Ireland) 2006
- Part-time Workers (Prevention of less Favourable Treatment) Regulation 2000
- Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002
- The Disability Discrimination (Northern Ireland) Order 2006
- The Employment Relations (Northern Ireland) Order 2004
- Equality Act (Sexual Orientation) Regulations (Northern Ireland) 2006
- Employment Relations (Northern Ireland) Order 2004 ● Work and Families (Northern Ireland) Order 2006

and will use his best endeavours to ensure that in his employment policies and practices and in the delivery of the services required of the Supplier under this Call-Off Contract he promotes equality of treatment and opportunity between:

. persons of different religious beliefs or political opinions
. men and women or married and unmarried persons
. persons with and without dependants (including women who are pregnant or on maternity leave and men on paternity leave)
. persons of different racial groups (within the meaning of the Race Relations (Northern Ireland) Order 1997)
. persons with and without a disability (within the meaning of the Disability Discrimination Act 1995)
. persons of different ages
. persons of differing sexual orientation

2.3.2 The Supplier will take all reasonable steps to secure the observance of clause 2.3.1 of this Schedule by all Supplier Staff.

2.4 Equality policies and practices

2.4.1 The Supplier will introduce and will procure that any Subcontractor will also introduce and implement an equal opportunities policy in accordance with guidance from and to the satisfaction of the Equality Commission. The Supplier will review these policies on a regular basis (and will procure that its Subcontractors do likewise) and the Customer will be entitled to receive upon request a copy of the policy.

2.4.2 The Supplier will take all reasonable steps to ensure that all of the Supplier Staff comply with its equal opportunities policies (referred to in clause 2.3 above). These steps will include:

a. the issue of written instructions to staff and other relevant persons
b. the appointment or designation of a senior manager with responsibility for equal opportunities
c. training of all staff and other relevant persons in equal opportunities and harassment matters
d. the inclusion of the topic of equality as an agenda item at team, management and staff meetings

The Supplier will procure that its Subcontractors do likewise with their equal opportunities policies.

2.4.3 The Supplier will inform the Customer as soon as possible in the event of:

A. the Equality Commission notifying the Supplier of an alleged breach by it or any Subcontractor (or any of their shareholders or directors) of the Fair Employment and Treatment (Northern Ireland) Order 1998 or

B. any finding of unlawful discrimination (or any offence under the Legislation mentioned in clause 2.3 above) being made against the Supplier or its Subcontractors during the Call-Off Contract Period by any Industrial or Fair Employment Tribunal or court,

The Supplier will take any necessary steps (including the dismissal or replacement of any relevant staff or Subcontractor(s)) as the Customer directs and will seek the advice of the Equality Commission in order to prevent any offence or repetition of the unlawful discrimination as the case may be.

2.4.4 The Supplier will monitor (in accordance with guidance issued by the Equality Commission) the composition of its workforce and applicants for employment and will provide an annual report on the composition of the workforce and applicants to the Customer. If the monitoring reveals under-representation or lack of fair participation of particular groups, the Supplier will review the operation of its relevant policies and take positive action if appropriate. The Supplier will impose on its Subcontractors obligations similar to those undertaken by it in this clause 2.4 and will procure that those Subcontractors comply with their obligations.

2.4.5 The Supplier will provide any information the Customer requests (including Information requested to be provided by any Subcontractors) for the purpose of assessing the Supplier’s compliance with its obligations under clauses 2.4.1 to 2.4.5 of this Schedule.

2.5 Equality

2.5.1 The Supplier will, and will procure that each Subcontractor will, in performing its/their obligations under this Call-Off Contract (and other relevant agreements), comply with the provisions of Section 75 of the Northern Ireland Act 1998, as if they were a public authority within the meaning of that section.

2.5.2 The Supplier acknowledges that the Customer must, in carrying out its functions, have due regard to the need to promote equality of opportunity as contemplated by the Northern Ireland Act 1998 and the Supplier will use all reasonable endeavours to assist (and to ensure that relevant Subcontractor helps) the Customer in relation to same.

2.6 Health and safety

2.6.1 The Supplier will promptly notify the Customer of any health and safety hazards which may arise in connection with the performance of its obligations under the Call-Off Contract. The Customer will promptly notify the Supplier of any health and safety hazards which may exist or arise at the Customer premises and which may affect the Supplier in the performance of its obligations under the Call-Off Contract.

2.6.2 While on the Customer premises, the Supplier will comply with any health and safety measures implemented by the Customer in respect of Supplier Staff and other persons working there.

2.6.3 The Supplier will notify the Customer immediately in the event of any incident occurring in the performance of its obligations under the Call-Off Contract on the Customer premises if that incident causes any personal injury or damage to property which could give rise to personal injury.

2.6.4 The Supplier will comply with the requirements of the Health and Safety at Work (Northern Ireland) Order 1978 and any other acts, orders, regulations and codes of practice relating to health and safety, which may apply to Supplier Staff and other persons working on the Customer premises in the performance of its obligations under the Call-Off Contract.

2.6.5 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work (Northern Ireland) Order 1978) is made available to the Customer on request.

2.7 Criminal damage

2.7.1 The Supplier will maintain standards of vigilance and will take all precautions as advised by the Criminal Damage (Compensation) (Northern Ireland) Order 1977 or as may be recommended by the police or the Northern Ireland Office (or, if replaced, their successors) and will compensate the Customer for any loss arising directly from a breach of this obligation (including any diminution of monies received by the Customer under any insurance policy).

2.7.2 If during the Call-Off Contract Period any assets (or any part thereof) is or are damaged or destroyed by any circumstance giving rise to a claim for compensation under the provisions of the Compensation Order the following provisions of this clause 2.7 will apply.

2.7.3 The Supplier will make (or will procure that the appropriate organisation make) all appropriate claims under the Compensation Order as soon as possible after the CDO Event and will pursue any claim diligently and at its cost. If appropriate, the Customer will also make and pursue a claim diligently under the Compensation Order. Any appeal against a refusal to meet any claim or against the amount of the award will be at the Customer’s cost and the Supplier will (at no additional cost to the Customer) provide any help the Customer reasonably requires with the appeal.

2.7.4 The Supplier will apply any compensation paid under the Compensation Order in respect of damage to the relevant assets towards the repair, reinstatement or replacement of the assets affected.

Schedule 5: Guarantee

[A Guarantee should only be requested if the Supplier’s financial standing is not enough on its own to guarantee delivery of the Services. This is a draft form of guarantee which can be used to procure a Call Off Guarantee, and so it will need to be amended to reflect the Beneficiary’s requirements]

This deed of guarantee is made on [**insert date, month, year]** between:

() [**Insert the name of the Guarantor]** a company incorporated in England and Wales with number [insert company number] whose registered office is at [i**nsert details of the guarantor's registered office**] [or a company incorporated under the Laws of [**insert country**], registered in [**insert country**] with number [**insert number**] at [**insert place of registration**], whose principal office is at [**insert office details**]]('Guarantor'); in favour of
and

() The Buyer whose offices are [**insert Buyer’s official address**] (‘Beneficiary’) **Whereas:**

() The guarantor has agreed, in consideration of the Buyer entering into the Call-Off Contract with the Supplier, to guarantee all of the Supplier's obligations under the Call-Off Contract.

() It is the intention of the Parties that this document be executed and take effect as a deed.

[Where a deed of guarantee is required, include the wording below and populate the box below with the guarantor company's details. If a deed of guarantee isn’t needed then the section below and other references to the guarantee should be deleted.

Suggested headings are as follows:

- Demands and notices
- Representations and Warranties
- Obligation to enter into a new Contract
- Assignment
- Third Party Rights
- Governing Law
- This Call-Off Contract is conditional upon the provision of a Guarantee to the Buyer from the guarantor in respect of the Supplier.]

Guarantor company	[**Enter Company name**] **‘Guarantor’**

Guarantor company address	[**Enter Company address**]
Account manager	[**Enter Account Manager name]**
	Address: [**Enter Account Manager address]**
	Phone: [**Enter Account Manager phone number]**
	Email: [**Enter Account Manager email**]
	Fax: [**Enter Account Manager fax** if applicable]

In consideration of the Buyer entering into the Call-Off Contract, the Guarantor agrees with the Buyer as follows:

Definitions and interpretation

In this Deed of Guarantee, unless defined elsewhere in this Deed of Guarantee or the context requires otherwise, defined terms will have the same meaning as they have for the purposes of the Call-Off Contract.

Term	**Meaning**

Call-Off Contract	Means [the Guaranteed Agreement] made between the Buyer and the Supplier on [insert date].
Guaranteed Obligations	Means all obligations and liabilities of the Supplier to the Buyer under the Call-Off Contract together with all obligations owed by the Supplier to the Buyer that are supplemental to, incurred under, ancillary to or calculated by reference to the Call-Off Contract.
Guarantee	Means the deed of guarantee described in the Order Form (Parent Company Guarantee).

References to this Deed of Guarantee and any provisions of this Deed of Guarantee or to any other document or agreement (including to the Call-Off Contract) apply now, and as amended, varied, restated, supplemented, substituted or novated in the future.

Unless the context otherwise requires, words importing the singular are to include the plural and vice versa.

References to a person are to be construed to include that person's assignees or transferees or successors in title, whether direct or indirect.

The words ‘other’ and ‘otherwise’ are not to be construed as confining the meaning of any following words to the class of thing previously stated if a wider construction is possible.

Unless the context otherwise requires:

- reference to a gender includes the other gender and the neuter
- references to an Act of Parliament, statutory provision or statutory instrument also apply if amended, extended or re-enacted from time to time
- any phrase introduced by the words ‘including’, ‘includes’, ‘in particular’, ‘for example’ or similar, will be construed as illustrative and without limitation to the generality of the related general words

References to Clauses and Schedules are, unless otherwise provided, references to Clauses of and Schedules to this Deed of Guarantee.

References to liability are to include any liability whether actual, contingent, present or future.

Guarantee and indemnity

The Guarantor irrevocably and unconditionally guarantees that the Supplier duly performs all of the guaranteed obligations due by the Supplier to the Buyer.

If at any time the Supplier will fail to perform any of the guaranteed obligations, the Guarantor irrevocably and unconditionally undertakes to the Buyer it will, at the cost of the Guarantor:

- fully perform or buy performance of the guaranteed obligations to the Buyer

- as a separate and independent obligation and liability, compensate and keep the Buyer compensated against all losses and expenses which may result from a failure by the Supplier to perform the guaranteed obligations under the Call-Off Contract

As a separate and independent obligation and liability, the Guarantor irrevocably and unconditionally undertakes to compensate and keep the Buyer compensated on demand against all losses and expenses of whatever nature, whether arising under statute, contract or at common Law, if any obligation guaranteed by the guarantor is or becomes unenforceable, invalid or illegal as if the obligation guaranteed had not become unenforceable, invalid or illegal provided that the guarantor's liability will be no greater than the Supplier's liability would have been if the obligation guaranteed had not become unenforceable, invalid or illegal.

Obligation to enter into a new contract

If the Call-Off Contract is terminated or if it is disclaimed by a liquidator of the Supplier or the obligations of the Supplier are declared to be void or voidable, the Guarantor will, at the request of the Buyer, enter into a Contract with the Buyer in the same terms as the Call-Off Contract and the obligations of the Guarantor under such substitute agreement will be the same as if the Guarantor had been original obligor under the Call-Off Contract or under an agreement entered into on the same terms and at the same time as the Call-Off Contract with the Buyer.

Demands and notices

Any demand or notice served by the Buyer on the Guarantor under this Deed of Guarantee will be in writing, addressed to:

[**Enter Address of the Guarantor in England and Wales**]

[**Enter Email address of the Guarantor representative**]

For the Attention of [**insert details**]

or such other address in England and Wales as the Guarantor has notified the Buyer in writing as being an address for the receipt of such demands or notices.

Any notice or demand served on the Guarantor or the Buyer under this Deed of Guarantee will be deemed to have been served if:

- delivered by hand, at the time of delivery
- posted, at 10am on the second Working Day after it was put into the post

- sent by email, at the time of despatch, if despatched before 5pm on any Working Day, and in any other case at 10am on the next Working Day

In proving Service of a notice or demand on the Guarantor or the Buyer, it will be sufficient to prove that delivery was made, or that the envelope containing the notice or demand was properly addressed and posted as a prepaid first class recorded delivery letter, or that the fax message was properly addressed and despatched.

Any notice purported to be served on the Buyer under this Deed of Guarantee will only be valid when received in writing by the Buyer.

Beneficiary's protections

The Guarantor will not be discharged or released from this Deed of Guarantee by:

- any arrangement made between the Supplier and the Buyer (whether or not such arrangement is made with the assent of the Guarantor)
- any amendment to or termination of the Call-Off Contract
- any forbearance or indulgence as to payment, time, performance or otherwise granted by the Buyer (whether or not such amendment, termination, forbearance or indulgence is made with the assent of the Guarantor)
- the Buyer doing (or omitting to do) anything which, but for this provision, might exonerate the Guarantor

This Deed of Guarantee will be a continuing security for the Guaranteed Obligations and accordingly:

- it will not be discharged, reduced or otherwise affected by any partial performance (except to the extent of such partial performance) by the Supplier of the Guaranteed Obligations or by any omission or delay on the part of the Buyer in exercising its rights under this Deed of Guarantee
- it will not be affected by any dissolution, amalgamation, reconstruction, reorganisation, change in status, function, control or ownership, insolvency, liquidation, administration, appointment of a receiver, voluntary arrangement, any legal limitation or other incapacity, of the Supplier, the Buyer, the Guarantor or any other person
- if, for any reason, any of the Guaranteed Obligations is void or unenforceable against the Supplier, the Guarantor will be liable for that purported obligation or liability as if the same were fully valid and enforceable and the Guarantor were principal debtor
- the rights of the Buyer against the Guarantor under this Deed of Guarantee are in addition to, will not be affected by and will not prejudice, any other security, guarantee, indemnity or other rights or remedies available to the Buyer

The Buyer will be entitled to exercise its rights and to make demands on the Guarantor under this Deed of Guarantee as often as it wishes. The making of a demand (whether effective, partial or defective) relating to the breach or non-performance by the Supplier of any Guaranteed Obligation will not preclude the Buyer from making a further demand relating to the same or some other Default regarding the same Guaranteed Obligation.

The Buyer will not be obliged before taking steps to enforce this Deed of Guarantee against the Guarantor to:

- obtain judgment against the Supplier or the Guarantor or any third party in any court
- make or file any claim in a bankruptcy or liquidation of the Supplier or any third party
- take any action against the Supplier or the Guarantor or any third party
- resort to any other security or guarantee or other means of payment

No action (or inaction) by the Buyer relating to any such security, guarantee or other means of payment will prejudice or affect the liability of the Guarantor.

The Buyer's rights under this Deed of Guarantee are cumulative and not exclusive of any rights provided by Law. The Buyer's rights may be exercised as often as the Buyer deems expedient. Any waiver by the Buyer of any terms of this Deed of Guarantee, or of any Guaranteed Obligations, will only be effective if given in writing and then only for the purpose and upon the terms and conditions on which it is given.

Any release, discharge or settlement between the Guarantor and the Buyer will be conditional upon no security, disposition or payment to the Buyer by the Guarantor or any other person being void, set aside or ordered to be refunded following any enactment or Law relating to liquidation, administration or insolvency or for any other reason. If such condition will not be fulfilled, the Buyer will be entitled to enforce this Deed of Guarantee subsequently as if such release, discharge or settlement had not occurred and any such payment had not been made. The Buyer will be entitled to retain this security before and after the payment, discharge or satisfaction of all monies, obligations and liabilities that are or may become due owing or incurred to the Buyer from the Guarantor for such period as the Buyer may determine.

Representations and warranties

The Guarantor hereby represents and warrants to the Buyer that:

- the Guarantor is duly incorporated and is a validly existing company under the Laws of its place of incorporation
- has the capacity to sue or be sued in its own name
- the Guarantor has power to carry on its business as now being conducted and to own its Property and other assets
- the Guarantor has full power and authority to execute, deliver and perform its obligations under this Deed of Guarantee and no limitation on the powers of the Guarantor will be exceeded as a result of the Guarantor entering into this Deed of Guarantee
- the execution and delivery by the Guarantor of this Deed of Guarantee and the performance by the Guarantor of its obligations under this Deed of Guarantee including entry into and performance of a Call-Off Contract following Clause 3) have been duly authorised by all necessary corporate action and do not contravene or conflict with:
  - the Guarantor's memorandum and articles of association or other equivalent constitutional documents, any existing Law, statute, rule or Regulation or any judgment, decree or permit to which the Guarantor is subject

  - the terms of any agreement or other document to which the Guarantor is a party or which is binding upon it or any of its assets

○ all governmental and other authorisations, approvals, licences and consents, required or desirable

This Deed of Guarantee is the legal valid and binding obligation of the Guarantor and is enforceable against the Guarantor in accordance with its terms.

Payments and set-off

All sums payable by the Guarantor under this Deed of Guarantee will be paid without any set-off, lien or counterclaim, deduction or withholding, except for those required by Law. If any deduction or withholding must be made by Law, the Guarantor will pay that additional amount to ensure that the Buyer receives a net amount equal to the full amount which it would have received if the payment had been made without the deduction or withholding.

The Guarantor will pay interest on any amount due under this Deed of Guarantee at the applicable rate under the Late Payment of Commercial Debts (Interest) Act 1998, accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgment.

The Guarantor will reimburse the Buyer for all legal and other costs (including VAT) incurred by the Buyer in connection with the enforcement of this Deed of Guarantee.

Guarantor’s acknowledgement

The Guarantor warrants, acknowledges and confirms to the Buyer that it has not entered into this Deed of Guarantee in reliance upon the Buyer nor been induced to enter into this Deed of Guarantee by any representation, warranty or undertaking made by, or on behalf of the Buyer, (whether express or implied and whether following statute or otherwise) which is not in this Deed of Guarantee.

Assignment

The Buyer will be entitled to assign or transfer the benefit of this Deed of Guarantee at any time to any person without the consent of the Guarantor being required and any such assignment or transfer will not release the Guarantor from its liability under this Guarantee.

The Guarantor may not assign or transfer any of its rights or obligations under this Deed of Guarantee.

Severance

If any provision of this Deed of Guarantee is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision will be severed and the remainder of the provisions will continue in full force and effect as if this Deed of Guarantee had been executed with the invalid, illegal or unenforceable provision eliminated.

Third-party rights

A person who is not a Party to this Deed of Guarantee will have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Deed of Guarantee. This Clause does not affect any right or remedy of any person which exists or is available otherwise than following that Act.

Governing law

This Deed of Guarantee, and any non-Contractual obligations arising out of or in connection with it, will be governed by and construed in accordance with English Law.

The Guarantor irrevocably agrees for the benefit of the Buyer that the courts of England will have jurisdiction to hear and determine any suit, action or proceedings and to settle any dispute which may arise out of or in connection with this Deed of Guarantee and for such purposes hereby irrevocably submits to the jurisdiction of such courts.

Nothing contained in this Clause will limit the rights of the Buyer to take proceedings against the Guarantor in any other court of competent jurisdiction, nor will the taking of any such proceedings in one or more jurisdictions preclude the taking of proceedings in any other jurisdiction, whether concurrently or not (unless precluded by applicable Law).

The Guarantor irrevocably waives any objection which it may have now or in the future to the courts of England being nominated for this Clause on the ground of venue or otherwise and agrees not to claim that any such court is not a convenient or appropriate forum.

[The Guarantor hereby irrevocably designates, appoints and empowers [**enter the Supplier name**] [or a suitable alternative to be agreed if the Supplier's registered office is not in England or Wales] either at its registered office or on fax number [**insert fax number**] from time to time to act as its authorised agent to receive notices, demands, Service of process and any other legal summons in England and Wales for the purposes of any legal action or proceeding brought or to be brought by the Buyer in respect of this Deed of Guarantee. The Guarantor hereby irrevocably consents to the Service of notices and demands, Service of process or any other legal summons served in such way.]

IN WITNESS whereof the Guarantor has caused this instrument to be executed and delivered as a Deed the day and year first before written.

EXECUTED as a DEED by

[**Insert name of the Guarantor**] acting by [**Insert names**]

Director

Director/Secretary

Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	**Meaning**
Additional Services	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Clause 2 (Services) which a Buyer may request.
Admission Agreement	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
Application	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Platform).
Audit	An audit carried out under the incorporated Framework Agreement clauses.
Background IPRs	For each Party, IPRs: ● owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes ● created by the Party independently of this Call-Off Contract, or For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.

Buyer	The contracting authority ordering services as set out in the Order Form.
Buyer Data	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
Buyer Personal Data	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
Buyer Representative	The representative appointed by the Buyer under this Call-Off Contract.
Buyer Software	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
Call-Off Contract	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.

Charges	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
Collaboration Agreement	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
Commercially Sensitive Information	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.
Confidential Information	Data, Personal Data and any information, which may include (but isn't limited to) any: ● information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above ● other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').
Control	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.

Controller	Takes the meaning given in the UK GDPR.
Crown	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.

Data Loss Event	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Call-Off Contract and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
Data Protection Impact Assessment (DPIA)	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
Data Protection Legislation (DPL)	(i) the UK GDPR as amended from time to time; (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy; (iii) all applicable Law about the Processing of Personal Data and privacy.
Data Subject	Takes the meaning given in the UK GDPR

Default	Default is any: • breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term) • other default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.
DPA 2018	Data Protection Act 2018.
Employment Regulations	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) (‘TUPE’) .
End	Means to terminate; and Ended and Ending are construed accordingly.
Environmental Information Regulations or EIR	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
Equipment	The Supplier’s hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.

ESI Reference Number	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
Employment Status Indicator test tool or ESI tool	The HMRC Employment Status Indicator test tool. The most up-todate version must be used. At the time of drafting the tool may be found here: https://www.gov.uk/guidance/check-employment-status-fortax
Expiry Date	The expiry date of this Call-Off Contract in the Order Form.

Force Majeure	A force Majeure event means anything affecting either Party's performance of their obligations arising from any: ● acts, events or omissions beyond the reasonable control of the affected Party ● riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare ● acts of government, local government or Regulatory Bodies ● fire, flood or disaster and any failure or shortage of power or fuel ● industrial dispute affecting a third party for which a substitute third party isn’t reasonably available The following do not constitute a Force Majeure event: ● any industrial dispute about the Supplier, its staff, or failure in the Supplier’s (or a Subcontractor's) supply chain ● any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure ● the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into ● any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans
Former Supplier	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
Framework Agreement	The clauses of framework agreement RM1557.13 together with the Framework Schedules.

Fraud	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
Freedom of Information Act or FoIA	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
G-Cloud Services	The cloud services described in Framework Agreement Clause 2 (Services) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
UK GDPR	The retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679).
Good Industry Practice	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.

Government Procurement Card	The government's preferred method of purchasing and payment for low value goods or services.
Guarantee	The guarantee described in Schedule 5.
Guidance	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
Implementation Plan	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
Indicative test	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
Information	Has the meaning given under section 84 of the Freedom of Information Act 2000.
Information security management system	The information security management system and process developed by the Supplier in accordance with clause 16.1.

Inside IR35	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

Insolvency event	Can be: ● a voluntary arrangement ● a winding-up petition ● the appointment of a receiver or administrator ● an unresolved statutory demand ● a Schedule A1 moratorium ● a Dun & Bradstreet rating of 10 or less
Intellectual Property Rights or IPR	Intellectual Property Rights are: ● copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information ● applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction ● all other rights having equivalent or similar effect in any country or jurisdiction
Intermediary	For the purposes of the IR35 rules an intermediary can be: ● the supplier's own limited company ● a service or a personal service company ● a partnership It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).

IPR claim	As set out in clause 11.5.
IR35	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
IR35 assessment	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.

Know-How	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or Buyer's possession before the Start date.
Law	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
Loss	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and '**Losses**' will be interpreted accordingly.

Lot	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
Malicious Software	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
Management Charge	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
Management Information	The management information specified in Framework Agreement Schedule 6.
Material Breach	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
Ministry of Justice Code	The Ministry of Justice’s Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

New Fair Deal	The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.
Order	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
Order Form	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
Ordered G-Cloud Services	G-Cloud Services which are the subject of an order by the Buyer.
Outside IR35	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
Party	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.

Personal Data	Takes the meaning given in the UK GDPR.
Personal Data Breach	Takes the meaning given in the UK GDPR.
Platform	The government marketplace where Services are available for Buyers to buy.
Processing	Takes the meaning given in the UK GDPR.
Processor	Takes the meaning given in the UK GDPR.

Prohibited act	To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to: ● induce that person to perform improperly a relevant function or activity ● reward that person for improper performance of a relevant function or activity ● commit any offence: ○ under the Bribery Act 2010 ○ under legislation creating offences concerning Fraud ○ at common Law concerning Fraud ○ committing or attempting or conspiring to commit Fraud

Project Specific IPRs	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
Property	Assets and property including technical infrastructure, IPRs and equipment.
Protective Measures	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

PSN or Public Services Network	The Public Services Network (PSN) is the government's high performance network which helps public sector organisations work together, reduce duplication and share resources.
Regulatory body or bodies	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
Relevant person	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
Relevant Transfer	A transfer of employment to which the employment regulations applies.
Replacement Services	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call- Off Contract, whether those services are provided by the Buyer or a third party.

Replacement supplier	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).
Security management plan	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.

Services	The services ordered by the Buyer as set out in the Order Form.
Service data	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
Service definition(s)	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Clause 2 (Services) of the Framework Agreement.
Service description	The description of the Supplier service offering as published on the Platform.

Service Personal Data	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.
Spend controls	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see https://www.gov.uk/service-manual/agile-delivery/spend-controlsche ck-if-you-need-approval-to-spend-money-on-a-service
Start date	The Start date of this Call-Off Contract as set out in the Order Form.
Subcontract	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
Subcontractor	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.

Subprocessor	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
Supplier	The person, firm or company identified in the Order Form.
Supplier Representative	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
Supplier staff	All persons employed by the Supplier together with the Supplier’s servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
Supplier Terms	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier’s Application.
Term	The term of this Call-Off Contract as set out in the Order Form.

Variation	This has the meaning given to it in clause 32 (Variation process).
Working Days	Any day other than a Saturday, Sunday or public holiday in England and Wales.
Year	A contract year.

Schedule 7: UK GDPR Information

This schedule reproduces the annexes to the UK GDPR schedule contained within the Framework Agreement and incorporated into this Call-off Contract and clause and schedule references are to those in the Framework Agreement but references to CCS have been amended.

Annex 1: Processing Personal Data

Not applicable for this call-off contract – no PII data will be accessed or processed by the Supplier.

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Buyer at its absolute discretion.

1.1 The contact details of the Buyer’s Data Protection Officer are: [Insert Contact details]

1.2 The contact details of the Supplier’s Data Protection Officer are: [Insert Contact details]

1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

1.4 Any such further instructions shall be incorporated into this Annex.

Description	**Details**
Identity of Controller for each Category of Personal Data	**The Buyer is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with paragraphs 2 to paragraph 15 of Schedule 7 and for the purposes of the Data Protection Legislation, Buyer is the Controller and the Supplier is the Processor of the Personal Data recorded below ***[Insert** the scope of Personal Data which the purposes and means of the Processing by the Supplier is determined by the Buyer]* **The Supplier is Controller and the Buyer is Processor**

	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with paragraph 2 to paragraph 16 of the following Personal Data: ● *[Insert the scope of Personal Data which the purposes and means of the Processing by the Buyer is determined by the Supplier]* **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: ● *[Insert the scope of Personal Data which the purposes and means of the Processing is determined by both Parties together]* **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: ● *Business contact details of Supplier Personnel for which the Supplier is the Controller,* ● *Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier*

	Personnel) engaged in the performance of the Buyer's duties under the Contract) for which the Buyer is the Controller,

	● ***[Insert*** *the scope of other Personal Data provided by one Party who is Controller to the other Party who will separately determine the nature and purposes of its Processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Buyer cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Buyer]* ***[Guidance*** *where multiple relationships have been identified above, please address the below rows in the table in respect of each relationship identified]*
Duration of the Processing	*[Clearly set out the duration of the Processing including dates]*
Nature and purposes of the Processing	*[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the Processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.* *The purpose might include: employment processing, statutory obligation, recruitment assessment etc]*

Type of Personal Data	*[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]*

Categories of Data Subject	*[*Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under Union or Member State law to preserve that type of data	*[Describe how long the data will be retained for, how it be returned or destroyed]*

Annex 2: Joint Controller Agreement

1. Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 2 (Joint Controller Agreement) in replacement of paragraphs 2 to 15 of Schedule 7 (Where one Party is Controller and the other Party is Processor) and paragraphs 17 to 27 of Schedule 7 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the [**select: Supplier or Buyer**]:

(a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

(b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;

(c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

(d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and

(e) shall make available to Data Subjects the essence of this Annex (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the [**select: Supplier's or Buyer's**] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of clause 1.2, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Controller.

2. Undertakings of both Parties

2.1 The Supplier and the Buyer each undertake that they shall:

(a) report to the other Party every [**insert number**] months on:

() the volume of Data Subject Request (or purported Data Subject Requests) from Data Subjects (or third parties on their behalf);

() the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

() any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;

() any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

() any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law, that it has received in relation to the subject matter of the Contract during that period;

(b) notify each other immediately if it receives any request, complaint or communication made as referred to in Clauses 2.1(a)(i) to (v);

(c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Clauses 2.1(a)(iii) to (v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation;

(d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under the Contract or is required by Law) ensure consent has been obtained from the Data Subject prior to disclosing or transferring the Personal Data to the third party. For the avoidance of doubt the third party to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex;

(e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information;

(f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful Processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data;

(g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:

() are aware of and comply with their 's duties under this Annex 2 (Joint Controller Agreement) and those in respect of Confidential Information

() are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

() have undergone adequate training in the use, care, protection and handling of Personal Data as required by the applicable Data Protection Legislation;

(h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;
() harm that might result from a Data Loss Event;
() state of technological development; and
() cost of implementing any measures;

(i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that it holds; and

(i) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.

2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex in such a way as to cause the other Joint Controller to breach any of its obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations

3. Data Protection Breach

3.1 Without prejudice to Paragraph 3.2, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:

(a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation; and

(b) all reasonable assistance, including:

() co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

() co-operation with the other Party including taking such reasonable steps as are directed by the other Party to assist in the investigation, mitigation and remediation of a Personal Data Breach;

() co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach; and/or

() providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Clause 3.2.

3.2 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within 48 hours of the Personal Data Breach relating to the Personal Data Breach, in particular:

(a) the nature of the Personal Data Breach;

(b) the nature of Personal Data affected;

(c) the categories and number of Data Subjects concerned;

(d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

(e) measures taken or proposed to be taken to address the Personal Data Breach; and

(f) describe the likely consequences of the Personal Data Breach.

4. Audit

4.1 The Supplier shall permit:

(a) the Buyer, or a third-party auditor acting under the Buyer's direction, to conduct, at the Buyer's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 2 and the Data Protection Legislation; and/or

(b) the Buyer, or a third-party auditor acting under the Buyer's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

4.2 The Buyer may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Clause 4.1 in lieu of conducting such an audit, assessment or inspection.

5. Impact Assessments

5.1 The Parties shall:

(a) provide all reasonable assistance to the each other to prepare any data protection impact assessment as may be required (including provision of detailed information and assessments in relation to Processing operations, risks and measures); and

(b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with the Contract, in accordance with the terms of Article 30 UK GDPR.

6. ICO Guidance

6.1 The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Buyer may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7. Liabilities for Data Protection Breach

[Guidance: This clause represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions]

7.1 If financial penalties are imposed by the Information Commissioner on either the Buyer or the Supplier for a Personal Data Breach ("Financial Penalties") then the following shall occur:

(a) if in the view of the Information Commissioner, the Buyer is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Buyer, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Buyer, then the Buyer shall be responsible for the payment of such Financial Penalties. In this case, the Buyer will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such Personal Data Breach. The Supplier shall provide to the Buyer and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach;

(b) if in the view of the Information Commissioner, the Supplier is responsible for thePersonal Data Breach, in that it is not a Personal Data Breach that the Buyer is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Buyer and its auditors, on request and at the Supplier’s sole cost, full cooperation and access to conduct a thorough audit of such Personal Data Breach; or

(c) if no view as to responsibility is expressed by the Information Commissioner,then the Buyer and the Supplier shall work together to investigate the relevant Personal Data Breach and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any Financial Penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the procedure set out in clause 32 of the Framework Agreement (Managing disputes).

7.2 If either the Buyer or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“Court”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the Court to be responsible for the Personal Data Breach shall be liable for the losses arising from such Personal Data Breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.

7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “Claim Losses”):

(a) if the Buyer is responsible for the relevant Personal Data Breach, then the Buyer shall be responsible for the Claim Losses;

(b) if the Supplier is responsible for the relevant Personal Data Breach, then the Supplier shall be responsible for the Claim Losses: and

(c) if responsibility for the relevant Personal Data Breach is unclear, then the Buyer and the Supplier shall be responsible for the Claim Losses equally.

7.4 Nothing in either clause 7.2 or clause 7.3 shall preclude the Buyer and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the Personal Data Breach and the legal and financial obligations of the Buyer.

8. Termination

8.1 If the Supplier is in material Default under any of its obligations under this Annex 2 (Joint Controller Agreement), the Buyer shall be entitled to terminate the Contract by issuing a Termination Notice to the Supplier in accordance with Clause 5.1.

9. Sub-Processing

9.1 In respect of any Processing of Personal Data performed by a third party on behalf of a Party, that Party shall:

(a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by the Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

(b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10. Data Retention

10.1 The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and their privacy policy (save to the extent (and for the limited period) that such information needs to be retained by the a Party for statutory compliance purposes or as otherwise required by the Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Annex 1 – Dynatrace Service Description

Dynatrace Limited
Dynatrace Full Stack Observability for the Enterprise Cloud
Gartner magic quadrant leader for Observability. Grail unifies logs, metrics, and events in the context of traces, topology, and user sessions. Single agent delivers AI-powered full stack Application Performance Monitoring, automated root cause analysis with integrated digital experience management, enhanced with run-time Application Security. Available as SaaS or on-premises.
Features
• Automated Discovery and Mapping Out of all Cloud Components
• AIOps Driven
• Massive Automation of Deployment and Maintenance of Solution
• Full Stack Visibility into your hybrid Multi-Cloud Environment
• Automated Troubleshooting Down to Code Level
• Continuous runtime vulnerability detection and AI-powered automatic risk assessment
• Unify and contextually analyze your data with Grail
Benefits
• Automation enables Rapid Deployment with Minimal Manual Configuration
• Automated Root Case Analysis significantly reduces MTTR
• Significantly Reduces the Operational Costs of Supporting Cloud Apps
• Enhance Collaboration Across Developers, Testers and Operations
• Understand the Business Impact of Application Performance Issues
• Deliver better software faster with Dynatrace Autonomous Cloud
• Lower enterprise risk with automatic vulnerability management and protection
Pricing
£800.00 to £1600.00 a unit a year
• Education pricing available
• Free trial available
Service documents
• Pricing document
PDF
• Skills Framework for the Information Age rate card
PDF
• Service definition document
PDF
• Terms and conditions
PDF
• Modern Slavery statement
PDF

Request an accessible format
Framework
G-Cloud 13
Service ID
633643680068275
633643680068275
Contact
REDACTED
Service scope
Software add-on or extension
No
Cloud deployment model
• Public
• Hybrid
Service constraints
There are no constraints with this service being delivered
System requirements
• Systems Requirements are listed at help.dynatrace.com
User support
Email or online ticketing support
Yes
Support response times
Dynatrace offers two levels of support for its customers: Standard and Premium. Standard support is available for customers that are current on their maintenance renewals and SaaS subscriptions. Premium Support is an additional cost. Please visit the following URL for a comprehensive description of these two service levels and the response times to questions. www.dynatrace.com/company/trust-center/support/policy/
User can manage status and priority of support tickets
Yes
Online ticketing support accessibility

None
Phone support
Yes
Phone support availability
9 to 5 mon to fri
Web chat support
Yes
Web chat support availability
24 7
Web chat support accessibility standard
None or not sure
How the web chat support is accessible
Dynatrace's Live Chat is an in-product, always on, instant access to Dynatrace product specialists. You will need to log into your Dynatrace account to access the Live Chat function.
Web chat accessibility testing
Dynatrace product management are aware there is a need to continually improve accessibility with our product and a strategy is being actively worked on to deliver these improvements. recent developments have seen the following improvements delivered in the product: - use of angular components within the ui - better keyboard support and aria labels for screen readers. - typographic hierarchy has recently been rolled out through the product from a design operations perspective improved colour contrasts and legibility are re-designed into the product as a design principle when new versions are developed. in addition, dynatrace has started a student project with linz university to elevate our approach to accessibility testing in the future.
Onsite support
Yes extra cost
Support levels
DynatraceOne (Standard Support) - Mon-Fri, 9am-5pm local time and requires an active maintenance or subscription contract. DynatraceOne Premium (Premium Support) - 24/7 x 365 - priority response times and a dedicated product specialist and customer success manager. Premium Support has an entry level price of £40,000 for annual license revenue below £250K. For license revenue above £250K the Premium Support costs are calculated at 20% of the annual licenses revenue and decrease on a sliding scale to no less than 10% as annual license revenue increases. Full Service Descriptions of DynatraceOne and DynatraceOne Premium are available at www.dynatrace.com/services-support/#

Support available to third parties
Yes
Onboarding and offboarding
Getting started
Extensive on-boarding services, self paced training, access to the Dynatrace Community and and professional services are available to ensure the successful implementation and adoption of the Dynatrace Service
Service documentation
Yes
Documentation formats
• HTML
• PDF
End-of-contract data extraction
Dynatrace provides an API that enables the end user to extract the performance metrics and specific data they require before ending the contract. Our services team are able to advise and support the end user through the data extraction process.
End-of-contract process
For SaaS customers if the Software licence is terminated or expires, the rights and licence granted to the customer, including the service, shall immediately terminate. For customers that have deployed our solution own premise with a TERM license the license will automatically expire on the contractually agreed end date. The customer will then have 30 business days to remove the Dynatrace software from their environment and either return it to Dynatrace or destroy it. For Customers with a perpetual license they simply stop paying the maintenance on perpetual licenses. They can continue to use the software but it will no longer be supported by Dynatrace.
Using the service
Web browser interface
Yes
Supported browsers
• IE11
• EDGE

- FIREFOX
- CHROME
- SAFARI
- OPERA

Application to install

Yes

Compatible operating systems

- Linux Or Unix
- Windows

Designed for use on mobile devices

Yes

Differences between the mobile and desktop service

There are no differences in functionality between the Dynatrace Mobile and desktop Browser User Interfaces other than the User Interface is optimised for the device on which the User Interface is being accessed.

Service interface

No

API

Yes

What users can and can't do using the API

API's are an important part of the of the Dynatrace solution.
The following URL provides everything you need to know about how you can set-up and make changes changes through the API's available in the Dynatrace ecosystem.

www.dynatrace.com/support/help/dynatrace-api/

API documentation

Yes

API documentation formats

- Html
- Pdf

API sandbox or test environment

Yes

Customisation available

Yes

Description of customisation

The customisation of the Dynatrace service is limited to the configuration of the User Interface such as Dashboard views and specific views of the enterprise cloud depending on the User's role. For example, developers, testers and operational people can customise their views based on the the information and data relevant to their role. Additional customisation can also be used in extending the capabilities of Dynatrace through the Software Development Kit, or SDK, to enables users to monitor a technology for which their is currently no code module available. A more detailed description can be found at www.dynatrace.com/support/help/extend-dynatrace/

Scaling

Independence of resources

Artificial Intelligence is built into the heart of the solution and this AL has industry leading predictive capabilities that ensure our service auto-scales based on demand placed on the service.

In addition each customer has their own Dynatrace tenet that is independent of any others tenets supported by Dynatrace.

Analytics

Service usage metrics

Yes

Metrics types

Dynatrace delivers a rich set of services metrics that cover end user experience, infrastructure, applications and databases.

Please review the Full Service Description to better understand the full service metric capabilities of Dynatrace.

Reporting types

- API
- REAL-TIME
- ON-REQUEST

Resellers

Supplier type
Not reseller
Staff security
Staff security clearance
STAFF SCREENING TO BS7858 2019
Government security clearance
SC
Asset protection
Knowledge of data storage and processing locations
Yes
Data storage and processing locations
• UK
User control over data storage and processing locations
Yes
Datacentre security standards
Recognised standard
Penetration testing frequency
At least every 6 months
Penetration testing approach
Other penetration testing organisation
Protecting data at rest
• Other standard
• Encrypted media
• Other
Data sanitisation process
Yes
Data sanitisation type
• No access

Equipment disposal approach
Recognised standard
Data importing and exporting
Data export approach
Data export is delivered through APIs. More detailed information is available at the following URL www.dynatrace.com/support/help/dynatrace-api/
Data export formats
• CSV
• ODF
Other data export formats
Data import formats
• CSV
• ODF
Other data import formats
Data-in-transit protection
Data protection between buyer and supplier networks
• IPSEC_OR_VPN
Other protection between networks
Data protection within supplier network
• IPSEC_OR_VPN
Other protection within supplier network
Availability and resilience
Guaranteed availability
Dynatrace will use commercially reasonable efforts to make the Dynatrace SaaS Monitoring Service available with a Monthly Uptime Percentage (defined below) of at least 99.5%. SLA Definitions, Service Credits and Credit Request and Payment procedures are available to read at www.dynatrace.com/company/terms-and-conditions/sla/
Approach to resilience

Dynatrace is hosted in the AWS cloud. High availability architecture: Each cluster uses multiple data centers for redundancy and over-provisions required capacity. If a server fails, another server in the same or a different data center can take over, while the fail-over process recreates the failed instance. Data is replicated to other data centers, too. The architecture even allows for failure of the entire data center. We constantly monitor the health of our systems. Fail-over is handled automatically. Critical data is backed-up to other regions at short intervals for disaster recovery. Backups are encrypted. We test the recovery process at regular intervals.

Outage reporting

Dynatrace communicates outages by a combination of email alerts to the affected customers and posting the outage to the Dynatrace community where affected users can track the resolution of the issue. The information provided includes service impacted, site location, start and end times, current status, description of service outage and customer impact. Once the problem has been resolved the Senior Director or Vice President responsible for the service issues a "reason for outage" report that is emailed to those customers affected by the outage.

Identity and authentication

User authentication needed

Yes

User authentication

- USERNAME OR PASSWORD

- OTHER

Access restrictions in management interfaces and support channels

Our customers control access to their data in Dynatrace individually. Only users who are members of a monitoring environment's administrative groups are able to grant/revoke access to collected data. How these roles can be managed and what possibilities for managing access control Dynatrace offers is explained in detail at the following URL - www.dynatrace.com/support/help/get-started/introduction/how-do-i-set-up-user-groups-and-permissions/

If support from Dynatrace is required by a customer, authorized Dynatrace employees (specifically, 2nd and 3rd level support representatives) can be granted access to view customer data, restricted by a strong "need to access" policy. All such authorized Dynatrace employees are bound by strict confidentiality agreements.

Access restriction testing frequency

At least every 6 months

Management access authentication

- Username or password

Audit information for users
Access to user activity audit information
Real-time
How long user audit data is stored for
User defined
Access to supplier activity audit information
Real time
How long supplier audit data is stored for
User defined
How long system logs are stored for
At least 12 months
Standards and certifications
ISO/IEC 27001 certification
Yes
Who accredited the ISO/IEC 27001
Covered through AWS's 27001 certification
ISO/IEC 27001 accreditation date
Dec. 11th 2011 and re-certified Dec 15th 2017
What the ISO/IEC 27001 doesn’t cover
Risk Management or-though this is addressed by Dynatrace through independently audited annual SOC2 Type 1 & 2 reports by an accredited AICPA accredited organisation. Dynatrace SOC2 Type II report is available to Dynatrace customers (after signing a Non-Disclosure Agreement).
ISO 28000:2007 certification
No
CSA STAR certification
No
PCI certification
No
Other security certifications

Yes

Any other security certifications

- SOC2 Type 1 and 2
- Dynatrace operates in AWS cloud with ISO 27017 and 27018

Security governance

Named board-level person responsible for service security

Yes

Security governance certified

Yes

Security governance standards

- ISO IEC 27001

Other security governance standards

Information security policies and processes

ISO 27002:2013 reference model

Operational security

Configuration and change management standard

Recognised standard

Configuration and change management approach

Proper change control procedure are in place. These include notification, testing, signoff and backout procedures. Access controls are modified to reflect changes in organizational structure and processes. Evidence can be provided upon request. This is attested to in our SOC 2 Type II certification.

Vulnerability management type

Recognised standard

Vulnerability management approach

Critical bugs and security vulnerabilities are triaged by senior support engineers (if reported by a customer) and the effected senior software engineers, managed by the development management and the chief software architects. Once the root cause is identified, it gets fixed in the current developed release and back ported to all effected versions. Test and test plans are adopted to prevent a regression in future.

A detailed description of how Dynatrace does this is available on Request.

Protective monitoring type
Recognised standard
Protective monitoring approach
Dynatrace continuously monitors the security of our environments. Breach detection: We are alerted if a user modifies the payload of a request. Important logs are transmitted to a third party service for review. We use intrusion detection. In the event of a detected breach, we publish details at status.ruxit.com. Unauthorized access: We use an additional Dynatrace cluster for monitoring clusters with customer data. This server detects unauthorized access. Forensics: We save logs to 3rd party systems so that an attacker can't wipe their trail. We use CloudTrail logs to track and report infrastructure changes.
Incident management type
Recognised standard
Incident management approach
Security and availability incidents, including logical and physical security breaches, failures, concerns, and other complaints are identified, reported to appropriate personnel, and acted on in accordance within and as part of our Incident Response plan including the results and synopsis of security invents is reflected in updates and modifications to the Incident Response. Dynatrace adheres to the pre-defined process for common events, controls and reporting of incidences as defined by the SCO2 Type 2 certification. Dynatrace is audited on an annual basis by an independent certified third party. The annual report is available under NDA.
Secure development
Approach to secure software development best practice
Independent review
Public sector networks
Connection to public sector networks
No
Social Value
Fighting climate change
Minimizing our carbon footprint is important to our customers, employees, and shareholders. We’re committed to protecting the environment by monitoring and managing our business operations to better understand and continuously improve our impact on the environment. Dynatrace's Environmental Sustainability priorities can be found at the following URL - https://www.dynatrace.com/company/sustainability/#environmental-sustainability
Covid-19 recovery

Following the onset of COVID-19, Dynatrace successfully transitioned all employees to work fully remote. Dynatrace is currently implementing a flexible work model where employees may choose whether they would like to work from home or from their respective office.
Equal opportunity
Diversity, Equity and Inclusion Our people are our most valued asset, and our focus on fostering an inclusive and supportive environment drives our culture and helps us attract, maintain, and invest in the development of our employees. • To further our goal of being a more diverse, inclusive, and equitable workplace we have launched a team dedicated to diversity, equity, and inclusion, including but not limited to establishing hiring goals focused on increasing Black, Indigenous, and people of color representation company-wide, and anti-racism training for employees and managers. In addition, we continue to establish active new employee resource groups, such as Women of Dynatrace and the Black Employee Network to support unique interests and initiatives throughout the organization. We plan to disclose gender and race/ethnicity metrics in Fiscal 2023 as part of our initial materiality assessment. More information, detailing our priorities, can be found at the following URL - https://www.dynatrace.com/company/sustainability/#diversity-equity-and-inclusion
Wellbeing
• Providing a safe, productive, and healthy workplace for our employees is of paramount importance. We comply with applicable safety and health laws and regulations at all our office locations globally and work with our employees to address and remediate identified risks of accidents, injury, or other health impacts. • We do not tolerate disrespectful or inappropriate behavior, unfair treatment, or retaliation of any kind. Harassment is not tolerated in the work environment and in any work-related situations outside the work environment. • We are committed to maintaining a workplace that is free from violence, harassment, intimidation and other unsafe or disruptive conditions due to internal and external threats. Security safeguards for employees are provided, as needed, and are maintained with respect for employee privacy and dignity. • For more information, please refer to our Human Rights Policy.
Pricing
Price
£800.00 to £1600.00 a unit a year
Discount for educational organisations
Yes
Free trial available
Yes
Description of free trial

Free Trials are offered for SaaS or on-premise deployments. Typical free trial period is 15 days but can be extended on request. Pre-Sales Technical resource is available - free of charge - throughout the trial period.
Link to free trial
https://www.dynatrace.com/

Annex 2 – Service Definition Document

Dynatrace Solution Overview

dynatrace

Our Mission, Purpose, and Vision

We have leveraged these conversations to update our mission, purpose, and vision — simple yet powerful tenets that establish a common understanding of who we are, what differentiates us, and where we are heading. These principles unite us around our shared goals as well as our approach to current and future strategies. They also help elevate our conversations to not just what we do, but also why we do it and how this enhances people's lives. Here is an overview of each of them:

Mission is what we do every day in service of our purpose — it is our differentiator. Purpose is why we exist and the impact we have on the world — it illuminates our passion. Vision is the outcome we seek to deliver to the world — it fulfills our mission and purpose.

Our Mission — We deliver answers and intelligent automation from data

Dynatrace products go well beyond getting data into dashboards. Our platform combines broad and deep observability and continuous runtime application security with advanced AIOps to provide answers and intelligent automation from data at an enormous scale. The Dynatrace platform provides situational awareness of your cloud ecosystem at all times and in real time to give you the confidence that your organization is operating as you expect it to.

Our Purpose — To enable flawless and secure digital interactions

Digital transformation is now ubiquitous. It combines people, technology, and processes to enable organizations to innovate faster and execute with more agility. Such transformation, however, also brings monumental complexity in the connections between people and machines as well as machine to machine. At Dynatrace, we want to facilitate billions of flawless and secure interactions despite this complexity through instant learning to enable software to become self-healing. We want to deliver a world that keeps data safe and applications and clouds running as expected, which requires end-to-end causal and contextual understanding for zero-moment response.

Our Vision — A world where software works perfectly

Only when we fulfill our purpose, without exception and with zero downtime, will we realize our vision of a world in which software works perfectly. This level of perfection is aspirational, but it is precisely what is expected, both by those providing software as well as those consuming it. We're investing aggressively to produce the most advanced software intelligence platform on the planet to enable bulletproof software delivery.

I am inspired by our mission, purpose, and vision, and I am excited about their positive impact on the message we deliver to our customers and other stakeholders. Only Dynatrace can provide the degree of observability, precision of answers and application security, and scale of automation needed to power today's modern cloud ecosystems.

Our future has never been brighter, and our ability to contribute meaningfully to the success of our customers is upon us — right now.

It's an exciting time to be engaged with Dynatrace!

Solution Overview

Dynatrace has redefined the way to monitor today's digital ecosystems. The solution is **AI-powered**, full stack and completely automated and is the only solution that provides answers, not just data, based on deep insight into every user, every transaction, across every application. The world's leading brands trust Dynatrace to optimize customer experiences, innovate faster and to modernize IT operations with absolute confidence.

Dynatrace offers the market-leading software intelligence platform, purpose-built for the enterprise cloud. As enterprises embrace the cloud to effect their digital transformation, our all-in-one intelligence platform is designed to address the growing complexity faced by technology and digital business teams. 6 years ago, we decided to re-write the entire APM platform to deliver a Software Intelligence Solution to meet the new requirements of digital transformation, cloud adoption and micro-service architectures. At the center of this we built an **AI engine** to help IT operations in providing **root cause**; the first step to making the journey to AIOps and NoOps.

Our platform utilizes **artificial intelligence** at its core and **advanced automation** to provide answers, not just data, about the performance of applications, the underlying hybrid cloud infrastructure, and the experience of our customers' users. We designed our software intelligence platform to allow our customers to modernize and automate IT operations, develop, and release high quality software faster, and improve user experiences for better business outcomes. Our products are trusted by more than 2,700 customers in over 90 countries in diverse industries such as banking, insurance, telecom, retail, manufacturing & travel.

Dynatrace is the only vendor to be in the top-right of the Gartner magic quadrant for all 11 years since the inception of the APM Quadrant. We recently became the only APM vendor to lead in both categories of "completeness of vision" and "ability to execute."

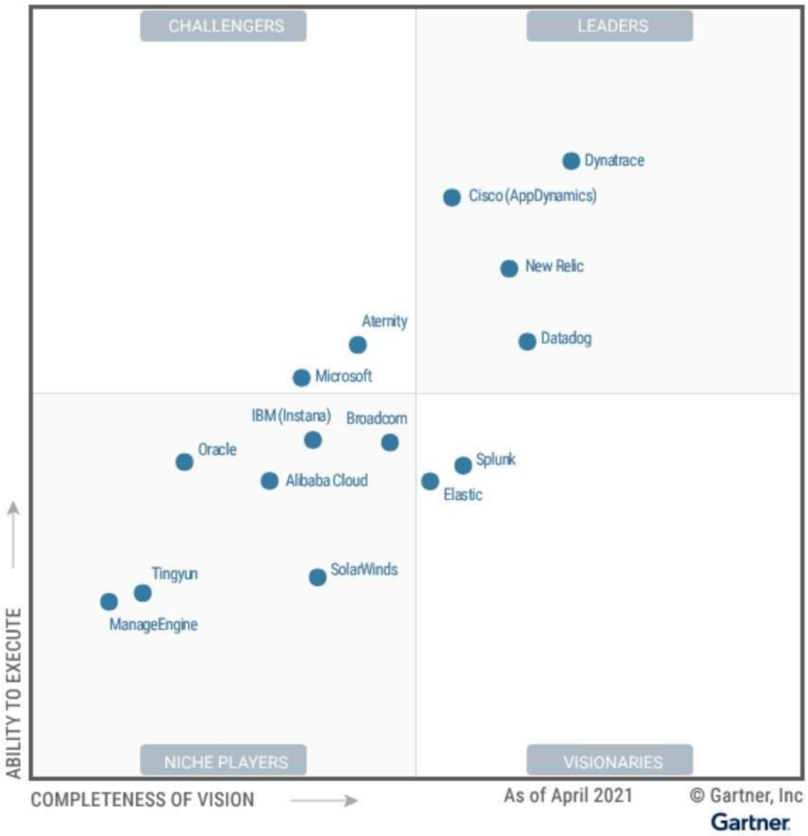
Recognized as a Leader in the Gartner Magic Quadrant for Application Performance Monitoring, 2021, with the furthest overall position for Completeness of Vision. This marks the 11th consecutive time Dynatrace has been positioned in the Leaders' quadrant for its Completeness of Vision and Ability to Execute.

Dynatrace named a Leader for 11th consecutive time, positioned highest for Ability to Execute and furthest for Completeness of Vision.

2021 GARTNER CRITICAL CAPABILITIES FOR APM
Dynatrace received the highest score in 4 of 5 uses cases
dynatrace
Gartner

Gartner 2021 Critical Capabilities for Application Performance Monitoring.

The Gartner APM Quadrant:



Source: Gartner (April 2021)

Disclaimer: Gartner, Magic Quadrant for Application Performance Monitoring, Charley Rich, Federico De Silva 22 April 2020. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

The Gartner 2021 Magic Quadrant for Application Performance Monitoring report can be found here: https://www.dynatrace.com/gartner-magic-quadrant-for-application-performance-monitoring/

Today’s Challenges

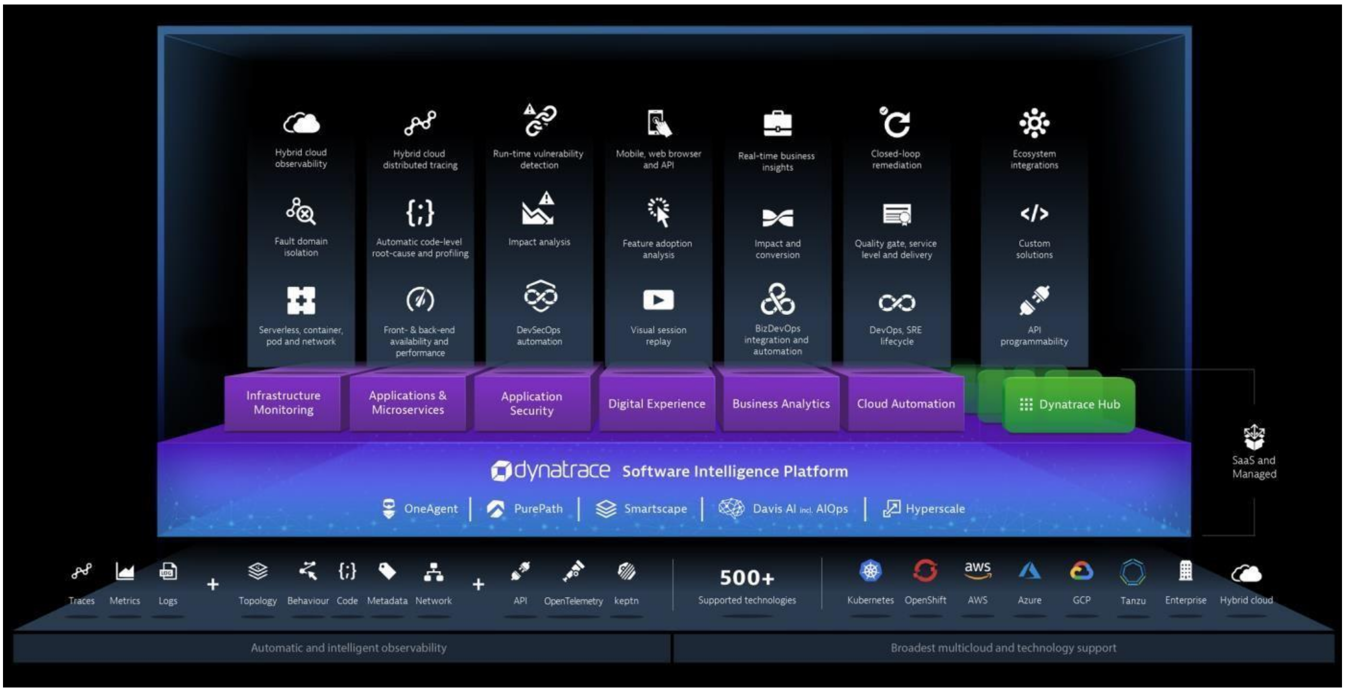
Our customers and other industry-leading companies are striving to deliver innovative digital services that exceed expectations and expand market opportunities. However, developing and operating new applications is growing more difficult than ever, largely driven by:

- **User Experience**: User expectations for software performance have rapidly increased and enterprises are focused on advancing branded experiences to maximize revenue, differentiate offerings, and retain competitive positions.
- **Cloud Transformation**: Enterprises are building and deploying software across multiple public and on-premises platforms, creating significant visibility challenges across all an enterprise’s hosted environments.
- **Application Complexity**: Applications are increasingly complex and deployed as microservices-based architectures that are written in multiple different programming languages with hundreds of loosely coupled service connections. The scale of this complexity is heightened by the advent of the Internet of Things, which increases the number of potential sources of application failure.
- **DevOps**: Ensuring that software updates work without issues has grown more challenging due to the increased frequency of software releases, reduced testing time, and the use of independent development teams.

The Dynatrace Difference

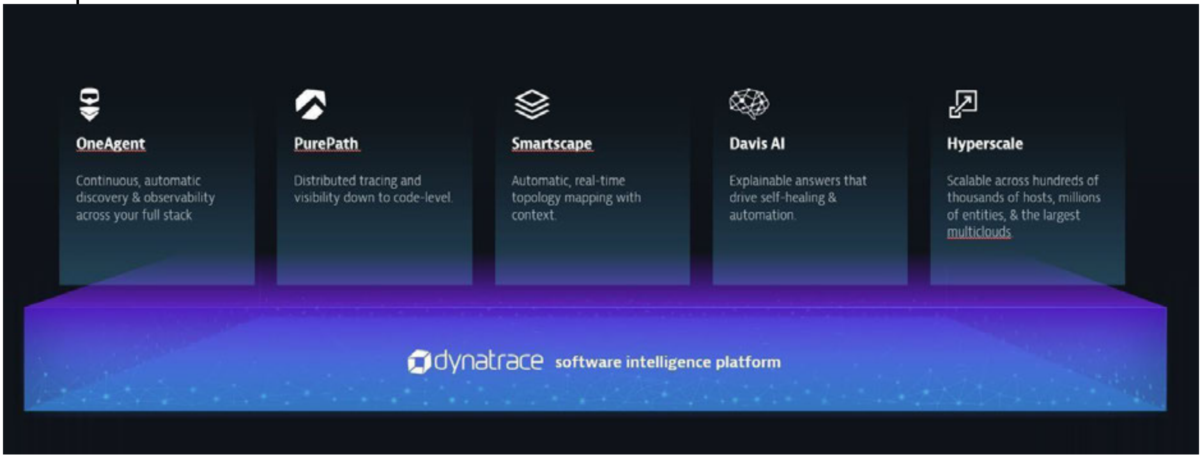
Dynatrace offers the market-leading software intelligence platform, purpose-built for complex enterprise environments and the challenges involved with digital experience management and application performance monitoring.

The Dynatrace software intelligence platform


Hybrid cloud observability
Hybrid cloud distributed tracing
Run-time vulnerability detection
Mobile, web browser and API
Real-time business insights
Closed-loop remediation
Ecosystem integrations
Fault domain isolation
Automatic code-level root-cause and profiling
Impact analysis
Feature adoption analysis
Impact and conversion
Quality gate, service level and delivery
Custom solutions
Serverless, container, pod and network
Front- & back-end availability and performance
DevSecOps automation
Visual session replay
BizDevOps integration and automation
DevOps, SRE lifecycle
API programmability
Infrastructure Monitoring
Applications & Microservices
Application Security
Digital Experience
Business Analytics
Cloud Automation
Dynatrace Hub
SaaS and Managed
dynatrace Software Intelligence Platform
OneAgent | PurePath | Smartscape | Davis AI incl. AIOps | Hyperscale
Traces
Metrics
Logs
+
Topology
Behaviour
Code
Metadata
Network
+
API
OpenTelemetry
keptn
500+
Supported technologies
Kubernetes
OpenShift
aws
AWS
Azure
GCP
Tanzu
Enterprise
Hybrid cloud
Automatic and intelligent observability
Broadest multicloud and technology support

As organizations embrace new technologies and the cloud to rapidly enable digital transformation, they are driven to re-think their monitoring strategies. Traditional

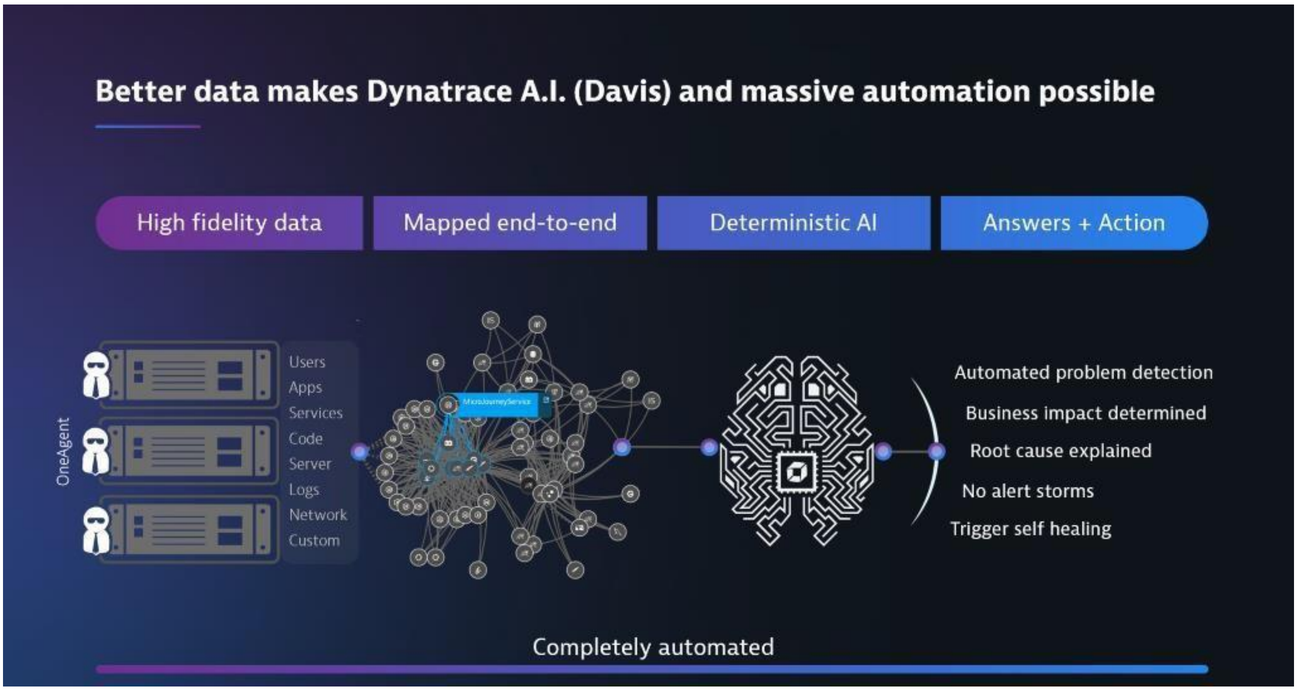
monitoring solutions are difficult to deploy (manual by nature), narrow in scope, and designed to operate in a simpler, siloed environment. They struggle to keep up with the dynamic nature of new applications and cloud technologies.
While Dynatrace has maintained the leadership role in the APM market for many years, we knew change was required to navigate modern IT goals. Several years ago, we anticipated that the new emerging enterprise hybrid-cloud would create new challenges throughout the application and infrastructure landscape. To stay ahead of the market and help our customers succeed in a modern digital age, we rebuilt our solution from the ground-up as a new platform intended to fit the new requirements of dynamic, web-scale cloud monitoring. Today, Dynatrace is the industry's only 3rd-generation monitoring platform that seamlessly brings together digital experience management, application performance management, infrastructure monitoring, and AIOps into an all-in-one, automated solution
with artificial intelligence powering its core. The platform, which we simply call "Dynatrace", fundamentally changes how end users are monitored, applications are managed and help bring together development, operations, and business teams to drive performance results.


OneAgent
Continuous, automatic discovery & observability across your full stack
PurePath
Distributed tracing and visibility down to code-level
Smartscape
Automatic, real-time topology mapping with context
Davis AI
Explainable answers that drive self-healing & automation
Hyperscale
Scalable across hundreds of thousands of hosts, millions of entities, & the largest multiclouds
dynatrace software intelligence platform

One platform, five groundbreaking capabilities

Dynatrace® simplifies the complexity of the enterprise hybrid cloud for architects, application teams, operations teams, and product owners, while providing actionable insights that accelerate cloud migrations, cloud adoption, and DevOps success. Our solution provides full stack observability and advanced automation at the core:

- OneAgent – Automatic instrumentation technology which discovers all processes running on the host and automatically activates instrumentation specifically for your stack
- PurePath - Our transaction-centric code analysis technology
- Smartscape – Provides real-time dependency mapping system
- Davis – Our open artificial intelligence, or AI, engine that we call Davis provides instant answers to degradations in service, anomalies in behavior, and user impact
- Hyperscale - Scalable across hundreds of thousands of hosts, millions of entities, & the largest multiclouds



Better data makes Dynatrace A.I. (Davis) and massive automation possible

High fidelity data | Mapped end-to-end | Deterministic AI | Answers + Action

OneAgent

Users
Apps
Services
Code
Server
Logs
Network
Custom

Automated problem detection
Business impact determined
Root cause explained
No alert storms
Trigger self healing

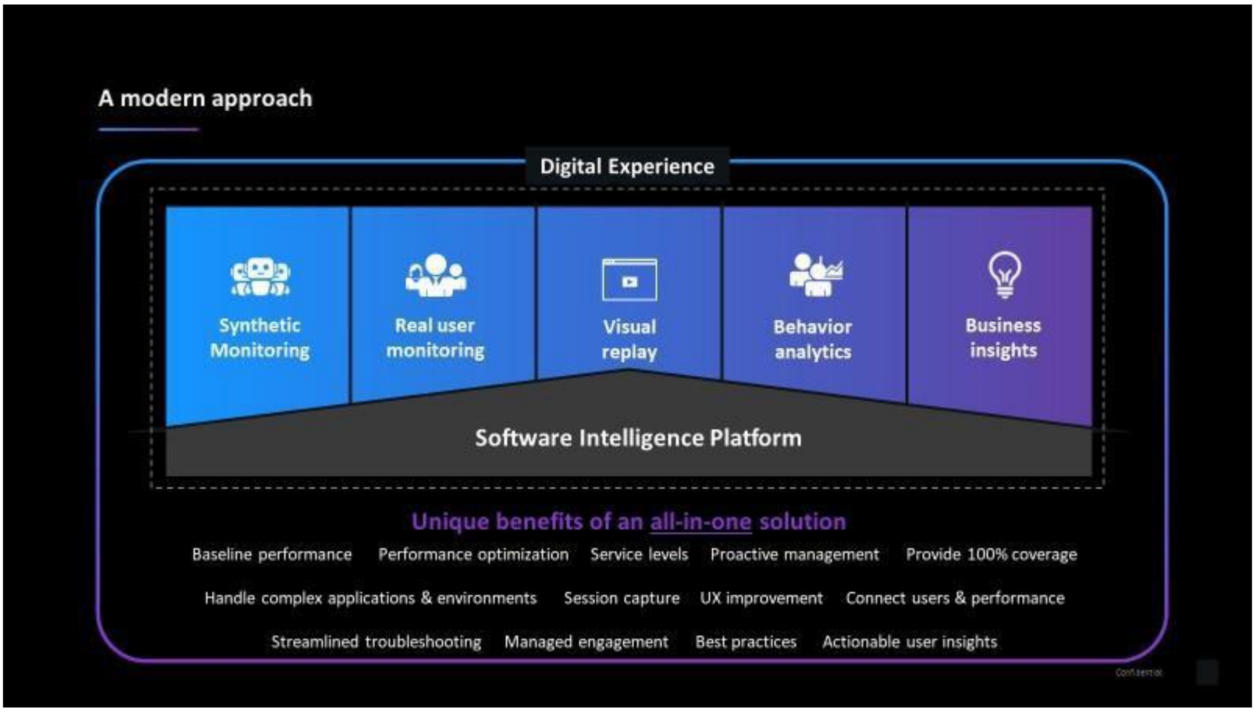
Completely automated

Dynatrace has been integrated with key components of the enterprise cloud ecosystem to support dynamic cloud orchestration, including AWS, Azure, Google Cloud Platform, Pivotal Cloud Foundry, Red Hat OpenShift, and Kubernetes. In these environments, Dynatrace automatically launches and monitors the full cloud stack and all the applications and containers running anywhere in the stack, including applications and workloads that may traverse multiple cloud and hybrid environments. Our ability to integrate Dynatrace with cloud platforms simplifies development and operational efforts, to improve situational awareness for our customers. Additional advantages include:

Key Advantages for your company

1. **Single Agent**: High fidelity data collection (no sampling or data gaps). Dynatrace OneAgent has complex applications and large-scale deployment in mind.
2. **Fully Automated**: No manual configuration required out of the box.
3. **All-in-One Open Platform Support**: Dynatrace provides a single view across your entire hybrid-cloud environment from on-prem to cloud.
4. **Native AI-Davis**: Delivers analysis of millions+ of dependencies for root-cause analysis and eliminates alert-storms.
5. **Web Scale**: Dynatrace can scale to 100,000+ hosts per deployment & analyzes 55B causations per minute.
6. **New Stack Ready**: Microservices, containers and functions are automatically instrumented.

7. **Innovation**: Dynatrace is an agile product that has 26 automated releases per year to keep up with our customer's rapidly changing environment and business needs.



A modern approach

Unique benefits of an all-in-one solution

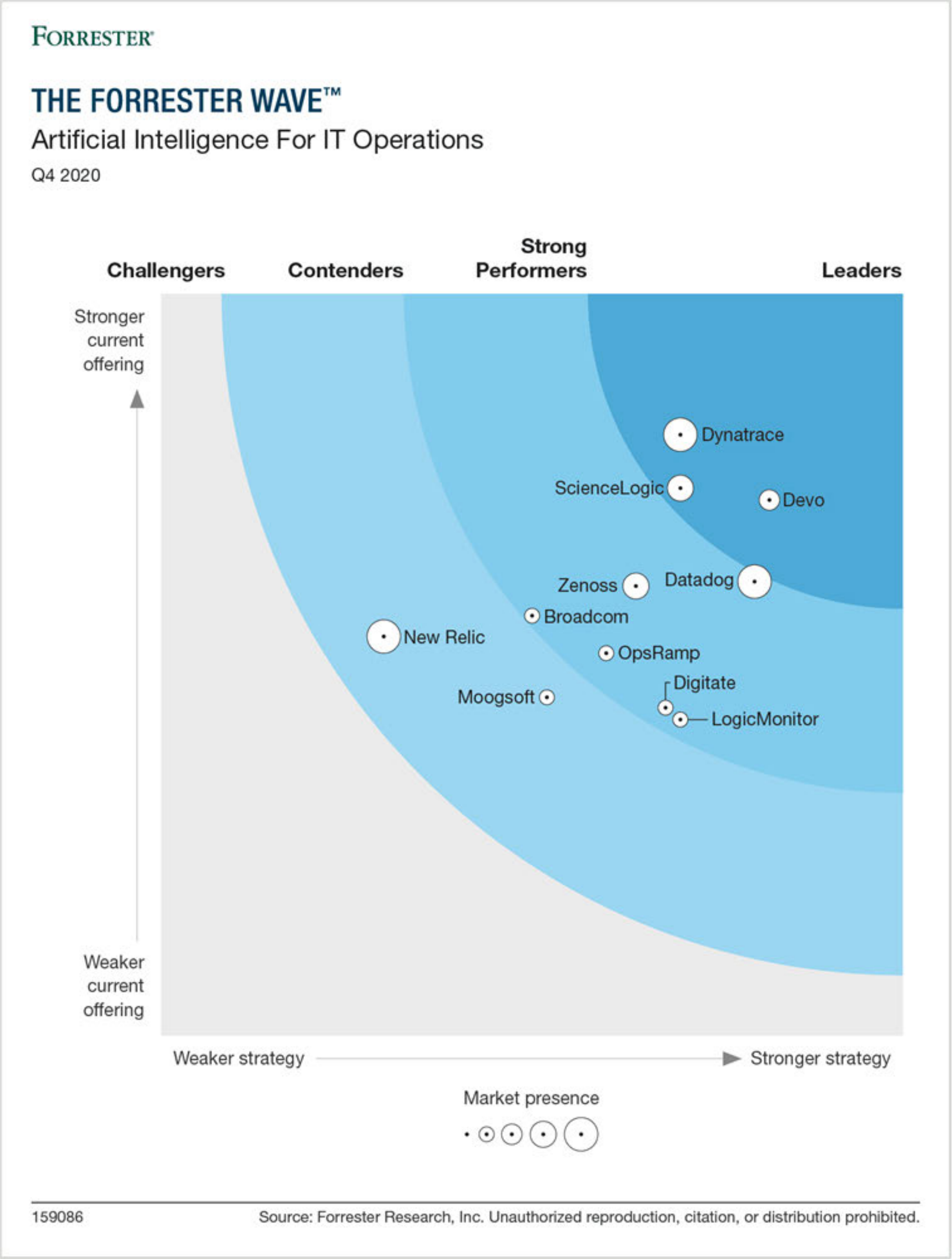
Baseline performance · Performance optimization · Service levels · Proactive management · Provide 100% coverage · Handle complex applications & environments · Session capture · UX improvement · Connect users & performance · Streamlined troubleshooting · Managed engagement · Best practices · Actionable user insights

The Business Value of Dynatrace

These key differences lead to the following results for our customers:

- **Improved Customer Satisfaction**: Seeing user behavior, along with application performance is the key to delivering perfect digital experiences every single time.
- **Faster Time to Implement & Wider-Scale Visibility**: Organizations are monitoring 100s or 1,000s of applications both on-prem & in the cloud, instead of focusing on only Tier 1 applications alone.
- **Larger-Scale Adoption:** The automation and AI analysis built into Dynatrace provides actionable answers to development, operations, product owners, and executives alike. We're seeing hundreds of users of Dynatrace within accounts vs. a traditional smaller set of performance experts.
- **DevOps and CI/CD Pipeline:** Automate monitoring as a feature of your pipeline - shift left with quality gates, shift right to enhance quality and deployment speed, and automate operations and self-healing to mitigate bad deployments in production.
- **Faster ROI:** Forrester estimates Dynatrace customers see ROI in a little more than 3 months on average. It is important to note these results are with customers who are upgrading from 2nd generation (or "Gen 2") traditional monitor-

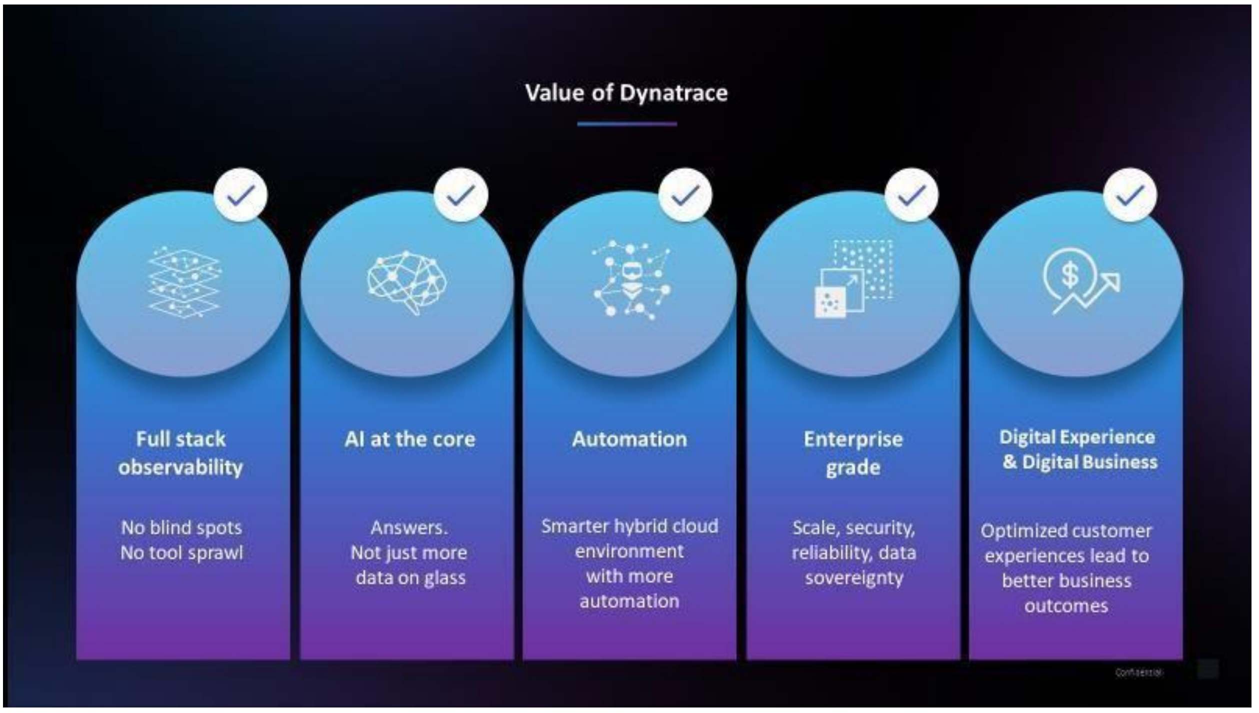
ing strategies to the new Dynatrace 3rd generation ("Gen 3") platform. If no existing monitoring strategy exists, the results can be even greater. The complete Forrester Total Economic Impact report on Dynatrace is available at https://www.dynatrace.com/forrester-total-economic-impact-report/.



Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

With Dynatrace, you will have the leading expert partner, along with an advanced open technology platform designed to help you succeed in establishing a proactive performance monitoring practice. Dynatrace has over 2,700 customers, including 386 of the Fortune 500, and is recognized the leader in performance monitoring. Gartner's 2021 APM Magic Quadrant study highlights Dynatrace as the leader in both vision and execution with a unique ability to go beyond just APM. Click here to download the Garter 2021 Magic Quadrant for APM Report.

Our ability to automate ‘lighting up” our customer’s digital ecosystems allow for faster innovation while reducing cost. Dynatrace is the only monitoring solution that is automatic in nature and **truly full-stack,** encompassing the **user, the app, process, services, infrastructure, logs, network** and **more**. We’ve completely redefined what monitoring means by producing the first and only 3rd generation APM solution on the market that is suitable for both large-scale on-prem and cloud initiatives.



Value of Dynatrace

Full stack observability

No blind spots
No tool sprawl

AI at the core

Answers.
Not just more data on glass

Automation

Smarter hybrid cloud environment with more automation

Enterprise grade

Scale, security, reliability, data sovereignty

Digital Experience & Digital Business

Optimized customer experiences lead to better business outcomes

Confidential

With Dynatrace, you and your teams will be able to spend much more time and resources innovating. For a detailed visual walkthrough on why Dynatrace provides more time to innovate, please see: https://www.dynatrace.com/solutions/.

Dynatrace deployment models

Dynatrace can be deployed either as a SaaS solution, with the option of retaining data in the cloud, or within an on-premises deployment. The on-premises version is called Dynatrace Managed. This allows customers to maintain control of where their data resides, whether in the cloud or on-premises, combining the simplicity of SaaS with the control of an on-premises deployment. With either SaaS or a Managed service, Dynatrace is automatically and effortlessly upgraded, so you always have our latest innovations.
*Dynatrace SaaS customers only need to install OneAgent. *Dynatrace Managed customers, prior to installing OneAgent, need to set up their Dynatrace cluster.

For both deployment models, it's highly recommended that you install the appropriate type of
ActiveGate. ActiveGate offers a number of proxy-specific capabilities.

Experience and Qualifications

As an eleven-time Gartner Magic Quadrant leader for Application Performance Monitoring, Dynatrace is uniquely equipped to help organizations optimize and monitor the performance of those critical Tier1/Tier-2 and other applications located both on-premises and in the cloud. As of March 31, 2020, Dynatrace Had over 2,200 talented and experienced employees. We are the leading global platform with over 2,400 enterprise customers. Our professional services team is skilled at conducting implementations in the largest and most challenging environments across the globe.

We will provide the same for Workplace Safety and Insurance Board. Dynatrace allows organizations to
not only get several steps closer to innovating for, executing on, and exceeding their digital transformation visions - The enablement and empowerment for technology teams and business executives alike, will be realized and delivered on significantly sooner and at lower overall total economic investment (TEI) with Dynatrace.

Your users deserve to benefit from the Dynatrace solutions' automation, scalability, flexibility, stability, and satisfaction – allowing YOUR ORGANIZATION to deliver perfect software experiences every time.

Realization of additional ROI, through both hard and soft dollar savings by driving efficiencies, as well as ensuring smooth future cloud-migration efforts and AIOps are well within the purview of your APM team's destiny - with a strategic partnership alongside Dynatrace. That's what this project should be all about - the benefit from Dynatrace's unique approach to software intelligence.

We know that a first-class student experience is critical to YOUR ORGANIZATION as well. Dynatrace provides full-stack observability and root cause analysis, which will positively impact those experiences from mobile to mainframe and back.

Finally, the legacy monitoring solutions used today have seemingly fallen short to support the new application platform and have put some strategies at risk. If cost takeout is a key strategic driver for YOUR ORGANIZATION, this project should save a significant amount of hard dollars by enabling you to sunset many legacy tools.

The new applications/software intelligence platform must work perfectly. YOUR ORGANIZATION's innovation, growth, and cost-cutting plans are dependent upon the success and speed of this transformation. Simply put, this is the business justification for Dynatrace.

Qualifications

	Award	Details	Link
	Gartner 2021 APM MQ	Dynatrace a leader for the 11th consecutive time, furthest overall position for Completeness of Vision.	Click here
	2021 Gartner Critical Capabilities of APM	In field of 15 vendors, Dynatrace is #1 in 4 of 5 use cases.	Click here

Gartner Magic Quadrant Leader SPRING 2020 AI BREAKTHROUGH AWARDS constellation ShortList ISG Provider Lens built in 2020 BEST PLACES TO WORK BOSTON Gartner peerinsights customers' choice FORRESTER	G2 Grid Reports	Dynatrace is #1 in the 6 observability categories: AIOps, Cloud Infrastructure Monitoring, Container Monitoring, DEM, Session Replay, and APM.	Click here
	AI Breakthrough Award, Best Overall AI-based Analytics Company	Dynatrace named the “Best Overall AI-based Analytics Company.”	Click here
	Constellation ShortList™ for Digital Performance Management	In a field of 25 vendors, Dynatrace one of few to make the Digital Performance Management ShortList.	Click here
	Built in Boston, “2020 Best Places to Work in Boston”	Built in Boston named Dynatrace a “Best Place to Work in Boston.”	Click here
	ISG Provider Lens, Cloud-Native Observability Solutions Quadrant	Dynatrace named the leader in cloud-native observability, scoring highest for portfolio attractiveness and competitive strength.	Click here
	Gartner 2020 Peer Insights Customers’ Choice for APM	Dynatrace earned the most 5-star user reviews of any vendor.	Click here
	Forrester Leader, Current Offering in AIOps	Dynatrace earned the top score in the current offering in AIOps category, with an analysis stating, “modern technology operations needs intelligence and automation.”	Click here

Embedded links will take you to additional content.

Solution/Services Description

With Dynatrace, Workplace Safety and Insurance Board will be able to accelerate the application platform transformation. Your teams will be able to focus 100% their efforts on innovating and empowering institutional growth versus wasting massive amounts of time chasing problems. The students and families you serve will see perfect solutions and software that create a competitive advantage for YOUR ORGANIZATION.

Over the last few years, Dynatrace has been evaluated and proven to be the only solution that meets customers current and future requirements. Dynatrace does so much more than just playbacks of user experience and troubleshooting issues. We will provide Workplace Safety and Insurance Board with:

- **Full-stack observability** – No more blind spots with digital experience data tied to business metrics in order to support business goals
- **AI at the core** – Real-time answers to business questions to support a positive customer experience
- **All-in-one platform** – Unified data model for Business, Development and Operations
- **Fully automated** – Simple implementation, integration, and automation into your ecosystem
- **Broadest multi-cloud & technology support** – Harness and unify even the most complex dynamic multi-clouds, with out-of-the box support for all major cloud platforms
- **Enterprise scale** - Scales and monitors your entire enterprise of critical applications located onpremises cloud, container, microservices and mainframe
- Dynatrace is the only vendor that can **manage all of these critical environments**, including native support for IBM mainframe
- **Advanced observability** – Get a broader view of your environment. One that includes metrics, logs, and traces, as well as a full topological model with distributed tracing, code-level detail, entity relationships, and even user experience and behavioral data – all in context with AI at the core.
- **Ecosystem innovation** – ServiceNow, Jira, Ansible, etc.
- **Cloud agnostic capabilities** – and timing based on YOUR ORGANIZATION's ability to accelerate delivery in a SaaS environment
- **Availability** – and access for additional business users, stakeholders, and executives
- **Scalability** – and growth at a budgetary consideration that allows for planned spend
- **Mobile to mainframe and back** – all in one place – extensible and flexible

Advanced observability

Yes, metrics, logs and traces. But you need much more...

Continuous automation

Save time, money and resources

AI-assistance

Shift team focus to value-added tasks

- Proactive action
- Innovation
- Outcomes

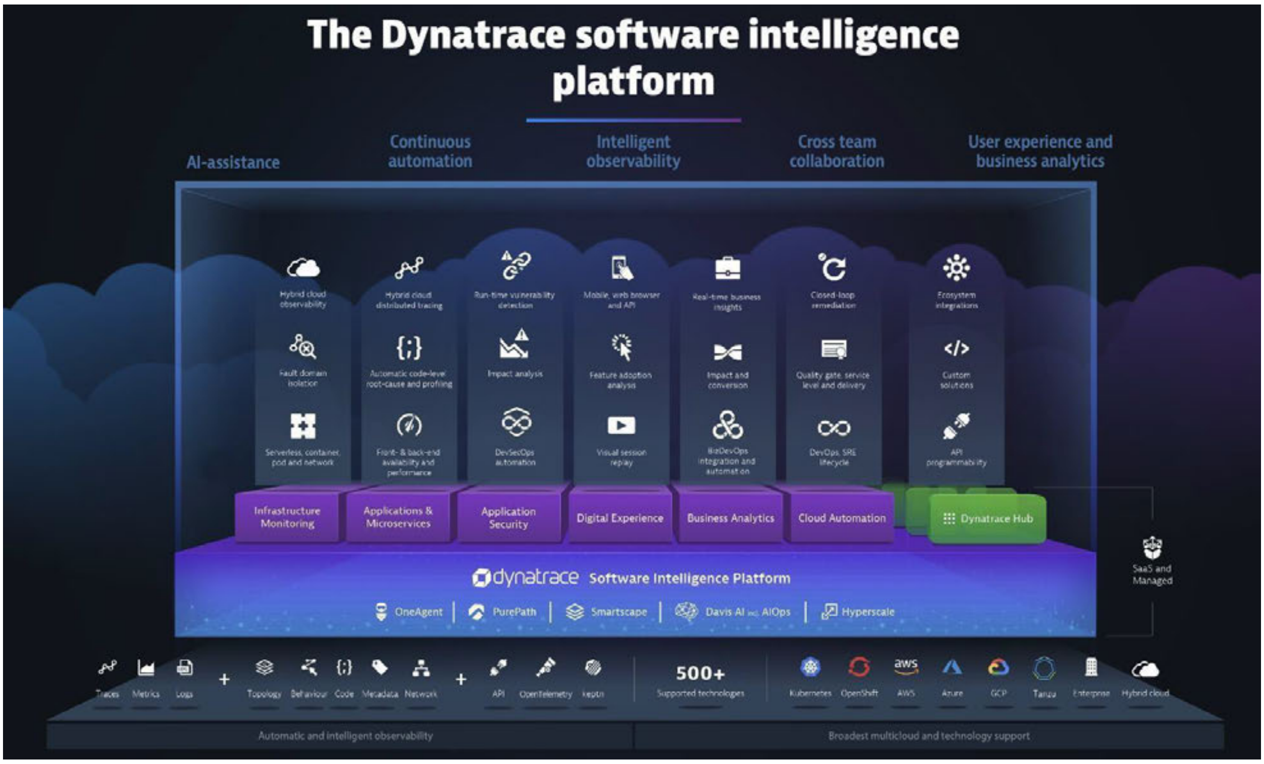
Cross-team collaboration

Eliminate silos and accelerate teamwork

User experience & business analytics

Assure your entire delivery chain is providing the results you expect

1.1 The Dynatrace Software Intelligence Platform



The Dynatrace software intelligence platform

AI-assistance
Continuous automation
Intelligent observability
Cross team collaboration
User experience and business analytics
Hybrid cloud observability
Hybrid cloud distributed tracing
Run-time vulnerability detection
Mobile, web browser and API
Real-time business insights
Closed-loop remediation
Ecosystem integrations
Fault domain isolation
Automatic code-level root-cause and profiling
Impact analysis
Feature adoption analysis
Impact and conversion
Quality gate, service level and delivery
Custom solutions
Serverless, container, pod and network
Front- & back-end availability and performance
DevSecOps automation
Visual session replay
BizDevOps integration and automation
DevOps, SRE lifecycle
API programmability
Infrastructure Monitoring
Applications & Microservices
Application Security
Digital Experience
Business Analytics
Cloud Automation
Dynatrace Hub
SaaS and Managed
dynatrace Software Intelligence Platform
OneAgent
PurePath
Smartscape
Davis AI incl. AIOps
Hyperscale
Traces
Metrics
Logs
+
Topology
Behaviour
Code
Metadata
Network
+
API
OpenTelemetry
keptn
500+
Supported technologies
Kubernetes
OpenShift
aws
AWS
Azure
GCP
Tanzu
Enterprise
Hybrid cloud
Automatic and intelligent observability
Broadest multicloud and technology support

Infrastructure Monitoring

Advanced observability across cloud and hybrid environments with continuous auto-discovery of hosts,
VMs, containers and orchestration, network, devices, logs, events and more, all in context, with precise AI-powered answers. Consolidate tools with an all-in-one

infrastructure solution that includes AIOps for precise answers about anomalies and degradations, so you don't waste time with alert storms, data silos and war rooms.

Applications and Microservices

Best-in-class APM from the category leader. Advanced observability across cloud and hybrid environments, from microservices to mainframe. Automatic full-stack instrumentation, dependency mapping and AI-assisted answers detailing the precise root-cause of anomalies, eliminating redundant manual work, and letting you focus on what matters. Dynatrace APM includes infrastructure monitoring and AIOps, delivering instant answers across the full stack.

Application Security

Empower DevSecOps to deliver digital services faster and more confidently with Runtime Application Self-Protection (RASP), optimized for the cloud and Kubernetes.

Digital Experience

Assure consistently better business outcomes and optimize user experience by maintaining an outsidein understanding of how your entire cloud stack supports the outcomes expected – service by service, journey by journey, KPI by KPI. Real user and synthetic monitoring combined with 4k movie-like session replay, provide application optimization, enhanced customer experience, and superior customer support across all digital channels. Digital experience includes AIOps, providing intelligence to improve every user experience.

Business Analytics

Get real-time, AI-powered answers to business questions by tying business metrics with data already flowing through our application performance and digital experience modules. With answers at your fingertips, data backed decisions, and real-time visibility into business KPIs, you'll deliver better digital business outcomes across all channels more efficiently than ever before. Digital business analytics includes AIOps for instant insights into key business metrics such as conversions, orders, churn, customer segments, release validation and more.

Cloud Automation

Dynatrace Cloud Automation provides developers, DevOps and SRE teams with an integrated end to end platform across production and pre-production environments bringing together full lifecycle observability with automated delivery pipelines. This results in shorter innovation cycles, higher quality software and faster time to market. Cloud Automation comes with a fully supported version of Keptn, an open-source initiative, providing you with an enterprise grade control plane for cloud native application lifecycle orchestration. This allows for seamless integration of your DevOps toolchain with Dynatrace's automatic and intelligent platform extending our openness and support for the broader DevOps ecosystem.

AIOps

With AI-assistance provided by Davis, Dynatrace auto-baselines your full stack, continuously monitors for anomalies and delivers precise answers prioritized by business impact. When a problem arises that affects users, Davis will be the first to know and provide precise root cause determination so you can focus your resources on proactive actions that matter most to drive better business outcomes. AIOps is included with every module in the platform.

Dynatrace ONE (support)

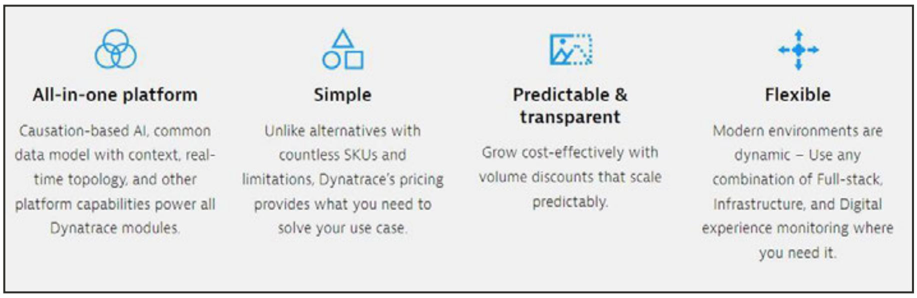
Dynatrace experts are available to every customer and will answer any question you have, when you have it, from the context of your Dynatrace environment. Technical Product Specialists, Support Engineers, and Customer Success Managers are co-located with our R&D organization to provide the assistance you need, faster.

Licensing Model

This section will further describe Dynatrace's products and services. Licensing model is the same regardless of the environment product covers (Dev, UAT, Prod).

Business Model and Licensing Overview

Dynatrace AI is a complete built-in software intelligence platform which enables customers to license in a concurrent and flexible way the necessary capabilities from infrastructure, applications and users with the combination of two license models (Host Units and sessions) in one license management. **Host Units** can be switched in nearly real-time for specific use-cases to gain optimal transparency / observability into the instrumented IT service. Host Units as well as session licenses can be consumed for on-premises as well as for cloud workloads in a seamless license model.



All-in-one platform

Causation-based AI, common data model with context, real-time topology, and other platform capabilities power all Dynatrace modules.

Simple

Unlike alternatives with countless SKUs and limitations, Dynatrace's pricing provides what you need to solve your use case.

Predictable & transparent

Grow cost-effectively with volume discounts that scale predictably.

Flexible

Modern environments are dynamic – Use any combination of Full-stack, Infrastructure, and Digital experience monitoring where you need it.

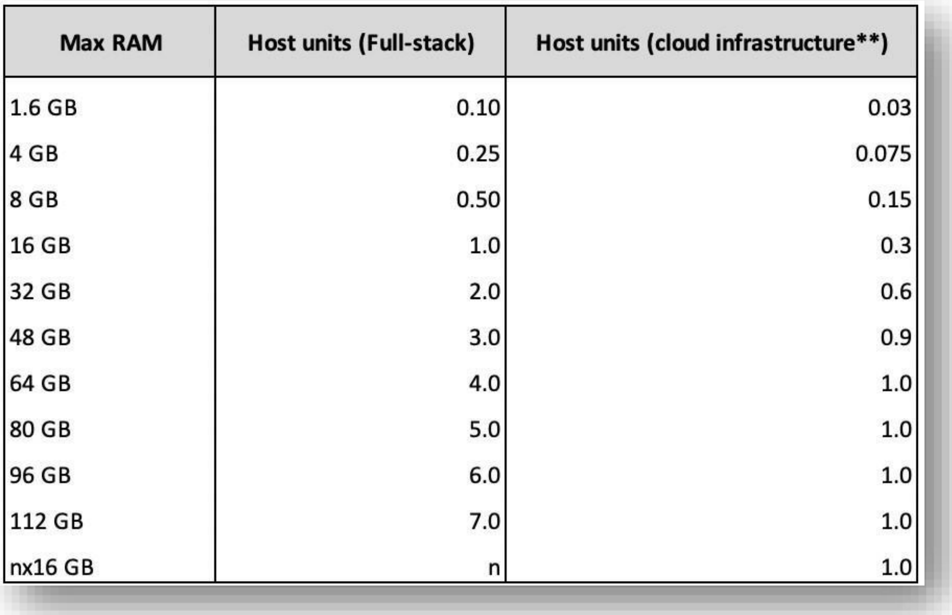
Host Units for Application and Infrastructure Monitoring

Dynatrace application and infrastructure monitoring is provided via a single Dynatrace OneAgent on each monitored host in your environment. OneAgent can operate in two different modes; both modes include automatic visibility, problem detection, and smart alerting.

Full-stack mode: Full-stack Monitoring mode provides complete application performance monitoring, code-level visibility, deep process monitoring, and infrastructure monitoring. Understand all relationships and dependencies across your applications, top-to-bottom for precise answers.

Infrastructure mode: Provides a complete solution for the monitoring of your infrastructure, including host, container, network, cloud services, log monitoring and AIOps.

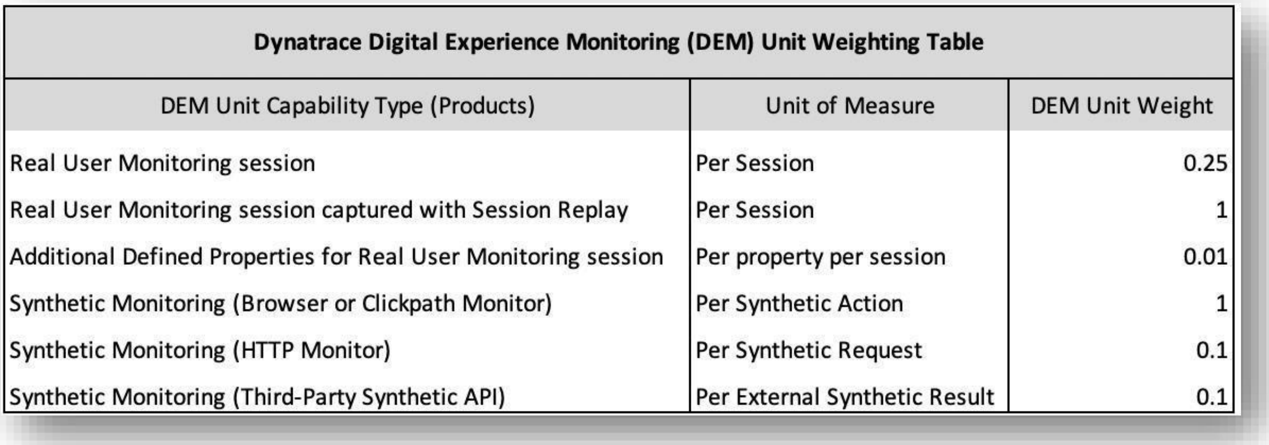
Dynatrace OneAgent is licensed per host (host units), with larger hosts (based on RAM GB) consuming more host units. Infrastructure mode consumes fewer host units than Full-stack mode as shown in the host weighting table below.



Max RAM	Host units (Full-stack)	Host units (cloud infrastructure**)
1.6 GB	0.10	0.03
4 GB	0.25	0.075
8 GB	0.50	0.15
16 GB	1.0	0.3
32 GB	2.0	0.6
48 GB	3.0	0.9
64 GB	4.0	1.0
80 GB	5.0	1.0
96 GB	6.0	1.0
112 GB	7.0	1.0
nx16 GB	n	1.0

Digital Experience Management (DEM) Units

Digital Experience Monitoring (DEM) units are used to consume Real User Monitoring, Synthetic Monitoring, and Session Replay. DEM units allow you to proactively fix web and mobile application problems before they impact users. A DEM Unit enables a customer to use any of the eligible products shown under DEM Unit Capability Type.



Dynatrace Digital Experience Monitoring (DEM) Unit Weighting Table		
DEM Unit Capability Type (Products)	Unit of Measure	DEM Unit Weight
Real User Monitoring session	Per Session	0.25
Real User Monitoring session captured with Session Replay	Per Session	1
Additional Defined Properties for Real User Monitoring session	Per property per session	0.01
Synthetic Monitoring (Browser or Clickpath Monitor)	Per Synthetic Action	1
Synthetic Monitoring (HTTP Monitor)	Per Synthetic Request	0.1
Synthetic Monitoring (Third-Party Synthetic API)	Per External Synthetic Result	0.1

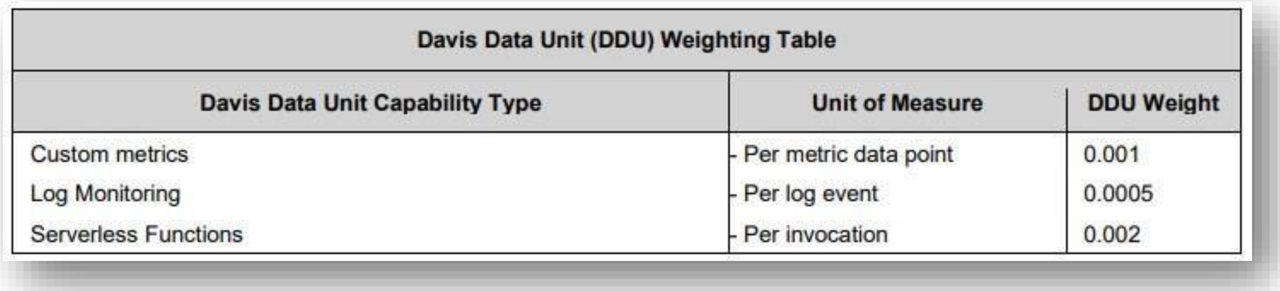
Synthetic Monitoring: Find problems across production and lower environments to prevent problems before users even see them. Automated availability and synthetic monitoring help you ensure availability and performance SLAs are achieved, across any region, 24/7.

Real User Monitoring (RUM): Understand and improve mobile and web user experiences across user segments and eliminate blind spots with advanced observability into the functionality and performance of applications from the end-user perspective.

Session Replay: Capture and visually replay actual user sessions across devices and browsers, to deeply understand the user experience, in terms anyone in the organization can understand.

Davis Data Units

DDUs provide a seamless, shared consumption model across custom metrics, log monitoring, serverless function tracing, and (soon) Open Telemetry ingest. As you monitor custom metrics, logs, and serverless functions, they will consume DDUs as described in the table below:



Davis Data Unit (DDU) Weighting Table		
Davis Data Unit Capability Type	**Unit of Measure**	**DDU Weight**
Custom metrics	Per metric data point	0.001
Log Monitoring	Per log event	0.0005
Serverless Functions	Per invocation	0.002

* Note: not all custom metrics will consume DDUs. Each OneAgent comes preloaded with a quantity of custom metrics for free as documented here.

Annex 3 – DPS Pricing £2m Commitment

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

[redacted]

REDACTED

[redacted]

Annex 4 – Velocity Gold Consultant Charges

REDACTED

REDACTED

[redacted]

REDACTED

REDACTED

REDACTED

[redacted]

REDACTED

[redacted]

Annex 5 – Dynatrace Subscription Agreement

SUBSCRIPTION AGREEMENT

THE AGREEMENT GOVERNS THE ACQUISITION, ACCESS AND USE OF DYNATRACE OFFERINGS, INCLUDING TRIAL ACCESS OR FREE USE, AND ACCESS OR USE OBTAINED THROUGH A DYNATRACEAUTHORIZED PARTNER.

CUSTOMER ACCEPTS AND AGREES TO THE TERMS BELOW BY (1) CLICKING AN “I ACCEPT” OR “I
AGREE” OR SIMILAR BUTTON OR CHECKBOX TO INDICATE ACCEPTANCE, (2) EXECUTING OR
OTHERWISE ACCEPTING AN ORDER FORM OR OTHER DOCUMENT THAT REFERENCES THIS
SUBSCRIPTION AGREEMENT, (3) ACCESSING OR USING THE DYNATRACE OFFERINGS ON AN UNPAID
BASIS, INCLUDING BUT NOT LIMITED TO TRIAL ACCESS, FREE USE, SPECIAL OFFERS, OR OTHER PROOF OF CONCEPT USE, OR (4) ACCESSING OR USING DYNATRACE OFFERINGS OBTAINED THROUGH A PARTNER.

The Agreement is effective between Customer and Dynatrace as of the date of the last signature on an Order Form incorporating this Subscription Agreement, or if not signed, on Customer’s acceptance of the Agreement.

1. **DEFINITIONS**. The following definitions shall apply unless otherwise stated:

1.1 “Account Data” means data about Customer provided to Dynatrace in connection with the administration of the Customer’s Dynatrace account, or as necessary for Customer to use the Dynatrace Offerings. For example, first and last name, username, and email address of a User, or other customer-provided contact, license consumption data, and billing information.

1.2 “Affiliate” means an entity that controls, is controlled by or is under common control with another entity, where “control” refers to ownership of more than 50% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.

1.3 “Agreement” means each Order Form that incorporates this Subscription Agreement, including all attachments and referenced terms and conditions.

1.4 “Customer” means (a) in the case of an individual accepting the Agreement in such individual’s capacity, such individual; (b) the entity or organization listed on an Order Form or on whose behalf the Agreement is otherwise accepted; and (c) any other entity or organization deemed to be a Customer by the terms of this Subscription Agreement.

1.5 “Customer Data” means data that is ingested into, and processed by, the Dynatrace Platform from Customer’s data sources, and the data insights generated by the Dynatrace Platform for the benefit of Customer, excluding Dynatrace Materials. For example, the Customer’s monitoring data and the underlying root cause of a Customer system performance problem.

1.6 “Data Protection Law” means all data protection laws and regulations applicable to the processing of Customer Personal Data under the Agreement.

1.7 “Documentation” means the then-current technical and non-technical specifications applicable to the Dynatrace Platform contained in the user, system, specification, support and configuration documentation made generally available to Dynatrace customers.

1.8 "Dynatrace" means the Dynatrace entity specified in the Order Form. If no Order Form applies, Dynatrace means the Dynatrace entity, if any, organized in the country where the Customer is headquartered, or if no such entity exists, Dynatrace LLC, a Delaware limited liability company.

1.9 "Dynatrace Materials" means all trainings, dashboards, presentations, report templates or other templates, documentation, materials, methodologies, processes, techniques, ideas, concepts, trade secrets, know-how, works of authorship, formulas, algorithms, databases, scripts, configurations, logos, symbols, designs, and other inventions embodied in the Dynatrace Platform and/or that Dynatrace develops or supplies in connection with the Dynatrace Offerings, including all copies, portions, modifications and improvements thereof, and all derivative works of any of the foregoing. Dynatrace Materials do not include Customer Data.

1.10 "Dynatrace Offerings" means the Dynatrace Platform, Support, Professional Services, and Dynatrace Materials.

1.11 "Dynatrace Platform" (may be referred to as "Product/s") means the Dynatrace software intelligence platform products, capabilities and services as identified in an Order Form, the Documentation, and any updates to

the platform provided as part of Support or during the Term. The Dynatrace Platform may be provided in the form of software in object-code, and/or cloud and hosted services provided by or on behalf of Dynatrace and in the form of electronic reports, analyses, and statistical and performance-related information.

1.12 "Intellectual Property Rights" means patents and patent rights, rights of priority, mask work rights, copyrights, moral rights, trade secrets, know-how, trademarks, trade names, logos, service marks, designs and other designations of source, any other form of intellectual, industrial property, proprietary or other protected rights in connection therewith, recognized in the world, whether or not registered, for the full period thereof, and all extensions and renewals thereof, and all applications for registration in connection with the foregoing.

1.13 "Malicious Code" means viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs.

1.14 "Order Form" means each Dynatrace order form, product schedule, quote or other order document which incorporates this Subscription Agreement and identifies the Dynatrace Offerings ordered by Customer and agreed to between Dynatrace and Customer. An Order Form may include an SOW.

1.15 "Personal Data" means any information that by itself or in combination does or can identify a specific individual or as defined in the Data Protection Law.

1.16 "Professional Services" means any implementation, training, consulting, performance analysis or other professional services provided by Dynatrace as set forth in an Order Form or SOW.

1.17 "Restricted Information" means any confidential or Personal Data that is protected by law and that requires the highest level of access control and security protection, whether in storage or in transit. Restricted Information includes, but is not limited to: (a) government-issued identification numbers, including social security numbers or other tax identification numbers, driver's license numbers, passport numbers or other state-issued identification numbers; (b) unencrypted passwords or other authentication credentials or the combination of a username or email address along with a password or security question that would permit access to an online account, (c) protected health information, or any electronic protected health

information (or other information subject to the HIPAA and HITECH Acts); (d) credit, debit or payment card information, financial or bank account information, or other information subject to PCI security standards; (e) data relating to a person under the age of 13 years old or subject to the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501-6505; (f) data that is subject to regulatory or contractual handling requirements under the
Gramm-Leach-Bliley Act; and (g) data classified as "special category data" (or similar term) under Data Protection Law, including racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual orientation, genetic data, biometric data, or the commission or alleged commission any crime or offense about residents of Switzerland or any member country of the European Union.

1.18 "Service Period" means the stated period of time that Professional Services are to be provided to Customer as set forth in an Order Form.

1.19 "Subsidiary" means a subsidiary which is greater than fifty (50%) percent owned by a party.

1.20 "Support" means the updates for supported versions of the Dynatrace Platform generally made available from time to time, and technical support services other than Professional Services, provided by Dynatrace in connection with the Dynatrace Platform.

1.21 "Term" means the initial subscription period to the Dynatrace Platform and Support as set forth in an Order Form together with any renewal of that subscription period (each a "Renewal Term").

1.22 "Third-Party User" is a third-party contractor or vendor designated by Customer as a User in accordance with Section 3.

1.23 "Usage Data" means data and related analysis about deployment, configuration, operation, use, maintenance, and support of the Dynatrace Offerings, and the technology the Customer monitors using the Dynatrace Platform. For example, features or capabilities of the Dynatrace Offering being utilized or consumed, configuration of the Dynatrace Offering, and performance and diagnostic state of the Dynatrace Offering.

1.24 "Users" means Customer or its Subsidiary's employees and Third-Party Users authorized by Customer to use the Dynatrace Offerings.

2. **AGREEMENT AND ORDER OF PRECEDENCE.** The Agreement governs Customer's and its Users' use of the applicable Dynatrace Offerings. Each Order Form that incorporates this Subscription Agreement constitutes a separate Agreement and governs its own subject-matter and not any other Agreement. In the event of a conflict between an Order Form and this Subscription Agreement, this Subscription Agreement will take precedence, except as otherwise stated.

3. THIRD PARTIES AND PARTNERS.

3.1 **Third-Party Users**. Customer may designate one or more Third-Party Users as required to facilitate Customer's permitted use of the Dynatrace Platform solely for Customer's or its Subsidiary's internal business operations and benefit, subject to the following. Each Third-Party User must be subject to non-disclosure obligations consistent with Section 9 (Confidentiality) and shall otherwise comply with the terms of the Agreement. Customer accepts responsibility for the acts and omissions of such Third-Party Users and agrees to enforce (and assist Dynatrace in enforcing) the terms of the Agreement against Third-Party Users. Dynatrace shall have no direct or indirect obligation or liability to any Third-Party User.

3.2 **Partners**. “End User” means a User for whom use of or access to the Dynatrace Offerings has been obtained through a third party (“Partner”) who has a limited right to resell the Dynatrace Offerings (directly or through a second-tier partner or marketplace). The terms of this Subscription Agreement (excluding terms relating to delivery of and payment for the Dynatrace Offering) and as applicable, the Platform Usage Supplement available at https://www.dynatrace.com/company/trust-center/customers/ (together, the “Resale End User Terms”) govern the use of any Dynatrace Offering by or for the benefit of an End User. By its use of the Dynatrace Offering, such End User agrees to and is bound by the Resale End User Terms, which are incorporated by reference into the contract for such resale transaction as if such End User was a Customer hereunder. Dynatrace is, and both End User and Partner hereby acknowledge and appoint Dynatrace as, a third-party beneficiary of the Resale End User Terms. Dynatrace is providing the Dynatrace Offerings in reliance on its status as a third-party beneficiary to the Resale End User Terms, and Dynatrace shall be entitled to enforce the Resale End User Terms directly against the End User. Dynatrace is not responsible for any acts, omissions, products or services provided by Partner. Partner is not authorized to modify the Resale End User Terms or make any commitment for Dynatrace, and Dynatrace is not bound by any obligations to End User other than as set forth in the Resale End User Terms. End User’s access to and use of Dynatrace Offerings is determined by the Order Form between Partner and Dynatrace identifying the End User. The amount paid or payable by the Partner for End User’s use of the Dynatrace Offerings will be deemed the amount paid or payable by Customer under the Agreement for the purpose of Section 16 (Limitation of Liability). For purposes of this Section, Dynatrace means Dynatrace LLC or its designated Affiliate.

4. SOFTWARE LICENSE AND SUPPORT.

4.1 **Dynatrace Platform**. During the Term, and subject to Customer’s compliance with the Agreement, Dynatrace grants Customer a limited, non-exclusive, non-transferable, non-sublicensable right and license solely for Customer and its Users to, as applicable, install, access and use the Dynatrace Platform for Customer’s internal business purposes, in accordance with the Documentation, subject to the territory, scope, type of use, and limitations on deployment and as otherwise stated in the applicable Order Form. Customer may reproduce software provided in object code and the Documentation as reasonably necessary to support its authorized use of the Dynatrace Platform, and for backup and archival purposes, provided Customer does not remove any Dynatrace proprietary markings and notices.

4.2 **Support.** Dynatrace will provide Support for the Dynatrace Platform in accordance with the support levels and fees identified in the applicable Order Form and the Dynatrace online support and service level policies.

5. PROFESSIONAL SERVICES.

5.1 **Statements of Work**. During the Service Period, Dynatrace will provide the Professional Services identified in an Order Form, which may be further described in SOWs attached to the Order Form. Each SOW may include, without limitation: (a) a description of the scope and type of Professional Services; (b) the location where the Professional Services will be performed; (c) the schedule for performance; and (d) any applicable additional fees, out of pocket expenses, and payment terms.

5.2 **Use of Dynatrace Materials.** During the Term and/or Service Period, and subject to Customer's compliance with the Agreement, Dynatrace grants Customer a limited, non-exclusive, non-transferable, nonsublicensable license to use the Dynatrace Materials that Dynatrace may provide to Customer in connection with the Professional Services or otherwise to be used solely for Customer's internal business purposes by Customer and its Users in connection with its subscription to the Dynatrace Platform. Training sessions may not be recorded without Dynatrace's prior written consent.

6. OWNERSHIP AND OTHER RIGHTS.

6.1 **Dynatrace Offerings**. This is not an agreement for custom development or "work for hire." Dynatrace Offerings are licensed, not assigned, to Customer. Except for the limited licenses set forth herein, Customer shall not acquire any rights, title or interest in the Dynatrace Offerings, and Dynatrace or its licensors, as applicable, shall retain all ownership, including without limitation, Intellectual Property Rights, in the Dynatrace Offerings.

6.2 **Customer Data**. As between the parties, Customer shall retain all ownership, including without limitation, Intellectual Property Rights, in the Customer Data. Customer grants to Dynatrace a limited, non-exclusive, royalty-free, worldwide license to use the Customer Data and perform all acts with respect to the Customer Data as may be necessary for Dynatrace to provide the Dynatrace Offerings to Customer or as otherwise agreed by Customer in writing.

6.3 **Feedback and Usage Data**. At its option, Customer may provide feedback or suggestions about the Dynatrace Offerings to Dynatrace ("Feedback"). Customer grants to Dynatrace and its Affiliates a nonexclusive, worldwide, royalty-free, fully paid, sublicensable, perpetual, and irrevocable right and license to use, modify, distribute, and commercialize the Feedback without restriction or obligation. Dynatrace may monitor and collect Usage Data to improve Dynatrace's current and future offerings, and if aggregated and not identifying Customer or any individual, for industry analysis, benchmarking, and analytics.

7. PAYMENT.

7.1 **Pricing**. Prices for the Dynatrace Offerings are set forth in the applicable Order Form.

7.2 **Invoicing and Payments.** Unless otherwise stated in an Order Form, fees are invoiced in advance and Customer shall pay Dynatrace the amounts invoiced in the specified currency within thirty (30) days of the invoice date. If Customer fails to pay any fee when due, without limiting any of its other rights or remedies, Dynatrace may impose a late payment charge not to exceed the maximum rate allowed by law, and/or Dynatrace may suspend performance until Dynatrace receives all past due amounts from Customer. Should Dynatrace be forced to commence legal action to collect fees owed, Dynatrace is entitled to recover its reasonable attorneys' fees and direct costs of collection. Multiple Order Forms may be executed under this Subscription Agreement and multiple invoices may be issued under each Order Form. Customer shall have no right to set-off or reduce payments owed under any Order Form without Dynatrace's prior written consent. Customer's obligation to pay for Dynatrace Offerings ordered under one Order Form is separate from, and not contingent on delivery or performance of Dynatrace Offerings ordered under any other Order Form. In the event of a good faith dispute of payment on an invoice, within fifteen (15) days of receipt of the invoice, Customer will notify Dynatrace in writing of the dispute and the parties will use commercially reasonable efforts to resolve such dispute. Undisputed amounts remain payable by Customer. The existence of a dispute shall not restrict Dynatrace's rights to collect such amounts or enforce its right to payment.

7.3 **Purchase Orders.** Upon request for Customer's administrative convenience, Dynatrace will reference

Customer's purchase order/reference number ("PO") on its invoices, provided the PO references the Order Form, is received reasonably prior to the date of the invoice, and is not conditioned on the PO being signed by Customer. The terms stated in any Customer PO shall have no force or effect. Dynatrace has the right to issue an invoice and collect payment without a corresponding PO.

7.4 **Delivery**. Dynatrace shall make the Dynatrace Platform available by electronic delivery, and acceptance is deemed to occur upon issuance of the license key or when electronic notice is sent that the purchased items are available.

7.5 **Renewal Term Pricing**. Fees for each Renewal Term are subject to a price increase which will be effective upon the commencement of the applicable Renewal Term, and unless otherwise agreed, shall not exceed the "Uplift Cap". The Uplift Cap is applied to the highest annualized fee level, unit prices, and minimum annual commitment (if any) in the immediately preceding subscription term. The applicable Uplift Cap is determined as follows: (a) 1-year Renewal Term, eight percent (8%); (b) 2-year Renewal Term, nine percent (9%); or (c) 3-year Renewal Term, ten percent (10%). Notwithstanding the foregoing, any renewal that has decreased in

units, volume, term, minimum annual commitment, or otherwise from its immediately preceding subscription term will result in re-pricing at renewal and the Uplift Cap will not apply.

7.6 **Taxes and Duties.** Customer will pay all sales, seller's use, VAT, GST, or similar taxes ("Transaction Taxes") due under the Agreement, except for taxes based on Dynatrace net income, unless Customer provides Dynatrace with a properly completed exemption certificate. Transaction Taxes will be separately stated on a Dynatrace invoice. Except as specifically identified in an Order Form, all prices are exclusive of all taxes, duties, withholdings and other governmental assessments.

If Customer is required to pay any Transaction Taxes to taxing authorities, directly or through withholding obligations, Customer will deduct the amount of such taxes from any amounts due to Dynatrace hereunder and promptly pay that amount to the relevant taxing authority. Customer will provide Dynatrace with documentation evidencing the payment or withholding of any such taxes to the proper taxing authorities.

8. CUSTOMER RESPONSIBILITIES.

8.1 Customer is responsible for: (a) the accuracy, quality and legality of Customer Data; (b) the means by which Customer acquired Customer Data; and (c) obtaining all necessary rights to use the Customer Data in connection with the Dynatrace Offerings, including without limitation, any required notices and consents in connection with any Personal Data included in Customer Data.

8.2 Customer will ensure that all Account Data is current and accurate.

8.3 Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls. Customer is responsible for: (a) its configuration of data privacy settings as described in the Documentation; (b) its secure use of the Dynatrace Offerings, including securing its account authentication credentials; (c) protecting the security of Customer Data when in transit to and from the Dynatrace Platform or Dynatrace; and

(d) taking any appropriate steps to securely encrypt or backup any Customer Data.

8.4 Customer assumes sole responsibility for determining whether the Dynatrace Offerings are appropriate for storage and processing of any Customer Data subject to any specific law or regulation, and for results obtained from the Dynatrace Platform. Notwithstanding the foregoing: (a) Customer acknowledges that the Dynatrace Offerings do not require and are not intended for the collection, storage, or other processing of Restricted Information; (b) Customer agrees not to provide Restricted Information to Dynatrace; and (c) Customer will use reasonable efforts to provide other Personal Data to Dynatrace only as necessary.

8.5 Customer will use commercially reasonable efforts to prevent unauthorized access to or use of the Dynatrace Offerings, and promptly notify Dynatrace of any such unauthorized use or access. Customer must notify Dynatrace without undue delay about any possible misuse of its accounts or authentication credentials or any security incident related to the Dynatrace Offerings.

8.6 Customer will not make any Dynatrace Offering available to anyone other than Customer or Users, or use any Dynatrace Offering for the benefit of anyone other than Customer. Customer will not sell, resell, sublicense, distribute, transfer, or otherwise commercially exploit its rights to use any Dynatrace Offering to or for any third party, including as part of a managed services offering, service bureau, outsourcing offering, software as a service, cloud or other technology or service (unless such managed services are expressly authorized by a separate executed agreement between the parties). Customer will not provide access to the Dynatrace Offerings to Dynatrace's direct competitors except with Dynatrace's prior written consent.

8.7 Customer will not (a) reverse engineer, decompile, disassemble or otherwise attempt to derive or gain access to the object code, source code or other operational mechanisms or the underlying ideas, methodologies or algorithms of the Dynatrace Offerings (except and to the extent such restriction is specifically prohibited by applicable law without the possibility of waiver, and then on prior written notice to Dynatrace); (b) modify, adapt, translate, copy or create derivative works based on any element of the Dynatrace Offerings; (c) use the Dynatrace Platform to store or transmit Malicious Code; (d) attempt to gain unauthorized access to the Dynatrace Platform or its related systems or networks, including through direct or indirect penetration testing; or (e) access or use any Dynatrace Offerings in order to (i) copy or re-use ideas, features, functions or graphics, (ii) create or distribute a product or service that competes with any Dynatrace Offering, (iii) perform or publish benchmarks or competitive analyses, or (iv) determine whether Dynatrace Offerings are within the scope of any patent.

9. CONFIDENTIALITY.

9.1 **Definition of Confidential Information**. "Confidential Information" means any and all non-public information disclosed by one party (the "Disclosing Party") to the other party (the "Receiving Party") pursuant to the Agreement, in any form or medium, whether oral or written, that is designated confidential or proprietary, or that a reasonable person should understand is confidential or proprietary. Confidential Information includes without limitation: the terms of the Agreement, information related to either party's technology, products, know-how, trade secrets, whether or not patentable or copyrightable, security reports, specifications, customers, business plans, pricing information, promotional and marketing activities, finances and other business affairs, and the Dynatrace Offerings. Customer will not remove or destroy any proprietary markings or restrictive legends contained in the Dynatrace Offerings.

9.2 **Nondisclosure Obligations**. The Receiving Party will not use the Confidential Information of the Disclosing Party for any purpose other than as necessary to fulfill its obligations or to exercise its rights under the Agreement (the "Purpose"). The Receiving Party will not disclose Confidential Information of the Disclosing Party to any third party; provided that the Receiving Party may disclose Confidential Information to its partners, officers, directors, employees, contractors, Affiliates, agents, advisors, or representatives ("Representatives") who need access to such Confidential Information for the Purpose and who are subject to written confidentiality obligations at least as stringent as the obligations set forth in this Section. Each party accepts responsibility for the actions of its Representatives and will protect the other party's Confidential Information in the same manner as it protects its own valuable confidential information, but with no less than reasonable care. The Receiving Party will promptly notify the Disclosing Party upon becoming aware of a breach or threatened breach hereunder and will cooperate with any reasonable request of the Disclosing Party in enforcing its rights.

9.3 **Exceptions to Confidential Information**. Confidential Information does not include information which: (a) is known by the Receiving Party prior to receipt from the Disclosing Party without any obligation of confidentiality; (b) becomes known to the Receiving Party directly or indirectly from a source other than one having an obligation of confidentiality to the Disclosing Party; (c) lawfully becomes publicly known or otherwise publicly available, except through a breach of the Agreement; or (d) is independently developed by the Receiving Party without use of or access to the Disclosing Party's Confidential Information. The Receiving Party may disclose Confidential Information pursuant to the requirements of applicable law or legal process but only after it notifies the Disclosing party (if legally permissible) to enable the Disclosing party to seek a protective order or otherwise contest required disclosure, at the Disclosing Party's expense.

9.4 **Injunctive Relief**. The parties agree that any unauthorized disclosure of Confidential Information may cause immediate and irreparable injury to the Disclosing Party and that, in the event of such breach, the Disclosing Party will be entitled, in addition to any other available remedies, to seek immediate injunctive and other equitable relief, without bond and without the necessity of showing actual monetary damages.

10. DATA PRIVACY AND SECURITY.

10.1 Dynatrace has implemented and will follow appropriate technical and organizational measures intended to protect Personal Data against accidental, unauthorized, or unlawful access, disclosure, damage, alteration, loss, or destruction.

10.2 If Dynatrace becomes aware of any unlawful access to any Customer Personal Data stored on Dynatrace equipment or in a Dynatrace facility, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Personal Data (each a "Security Incident"), Dynatrace will notify Customer of the Security Incident without undue delay (provided that such notification may be delayed as required by a law enforcement agency) and take commercially reasonable steps to comply with its obligations under applicable Data Protection Law pertaining to responding to a Security Incident. Dynatrace's obligation to report or respond to a Security Incident under this Section is not an acknowledgement by Dynatrace of any fault or liability with respect to the Security Incident.

10.3 **Data Processing Agreement.** To the extent Dynatrace processes any Personal Data on Customer's behalf that is subject to the Data Protection Law, and the parties have not executed a separate data processing agreement that complies with such Data Protection Law, the Data Processing Agreement located at https://www.dynatrace.com/company/trust-center/customers/ is incorporated by reference and shall apply.

11. WARRANTIES.

11.1 **Mutual Warranty.** Each party represents, warrants and covenants that: (a) it has the full power and authority to enter into the Agreement and to perform its obligations hereunder, without the need for any consents, approvals or immunities not yet obtained; and (b) its acceptance of and performance under the Agreement will not breach any agreement with any third party or any obligation owed by it to any third party.

11.2 **Limited Warranties and Remedies**. The following limited warranties apply only to the extent that Customer has purchased the applicable Dynatrace Offering:

11.2.1 **Dynatrace Platform**. Dynatrace warrants that the Dynatrace Platform will operate substantially in compliance with the applicable Documentation during the Term, provided that the purchased items have been properly installed and/or configured, used as described in the Documentation, and have not been modified or added to other than by Dynatrace. If the Dynatrace Platform does not perform as warranted and Customer notifies Dynatrace within thirty (30) days, Dynatrace will undertake at its sole option and as Customer's exclusive remedy, to (a) correct the non-conformance; or (b) replace the non-conforming item, provided that if Dynatrace determines that it is not commercially reasonable or possible to correct or replace a material non-conformity within a reasonable time from receipt of written notice from Customer detailing the warranty claim, the affected subscription will be cancelled and Dynatrace will refund any unused prepaid fees for the affected subscription.

11.2.2 **Professional Services**. Dynatrace will use commercially reasonable efforts to perform the Professional Services and provide the accompanying Dynatrace Materials according to the specifications, if any, set forth in the relevant Order Form and SOW. If Dynatrace fails to do so and Customer notifies Dynatrace within thirty (30) days of the date the Professional Services were performed, Dynatrace will undertake at its sole option and as Customer's exclusive remedy to (a) re-perform the non-conforming Professional Services; or (b) if Dynatrace determines that reperformance is not commercially reasonable, the affected Professional Services will be cancelled and Dynatrace will refund to Customer any pre-paid fees corresponding to the affected Professional Services.

11.3 **WARRANTY DISCLAIMER.** TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR THE EXPRESS WARRANTIES SPECIFIED ABOVE, DYNATRACE DISCLAIMS ALL OTHER WARRANTIES, WHETHER WRITTEN, ORAL, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, AND NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, DYNATRACE DOES NOT WARRANT

THAT THE DYNATRACE OFFERINGS OR RESULTS OF THE USE THEREOF WILL: (A) OPERATE IN COMBINATION WITH ANY OTHER HARDWARE, SOFTWARE,
SYSTEM OR DATA; (B) MEET CUSTOMER'S REQUIREMENTS OR EXPECTATIONS; (C) BE
UNINTERRUPTED, ERROR-FREE OR VIRUS-FREE; (D) IDENTIFY, BLOCK, OR REMEDIATE ALL SECURITY VULNERABILTIES, THREATS, OR ATTACKS; OR (E) RENDER THE CUSTOMER ENVIRONMENT INVULNERABLE TO UNAUTHORISED ACCESS AND/OR THIRD-PARTY INTERFERENCE. IN ADDITION, DYNATRACE MAKES NO WARRANTY ABOUT ANY THIRD-PARTY PRODUCTS OR CONTENT.

12. TERM AND TERMINATION.

12.1 **Subscription Agreement**. This Subscription Agreement may be updated from time to time by Dynatrace provided that no update or modification will apply to any Order Form previously executed or agreed to by the parties.

12.2 **Order Form and SOW**. Each Order Form or SOW begins on its effective date and continues in effect through the end date of the Term or the Service Period thereof. Except as expressly provided under the Agreement, Order Forms and SOWs may not be terminated, cancelled or reduced during the Term or Service Period, payment obligations are non-cancelable, and fees are non-refundable. Each Dynatrace Platform and Support subscription will automatically renew for additional periods equal to the greater of the expiring subscription term or one (1) year unless either party gives the other written notice at least sixty (60) days before the expiration thereof. Notice to Dynatrace should be provided via email to WW-RenewalsTeam@dynatrace.com with a copy to: legalnotices@dynatrace.com.

12.3 **Termination for Cause**. Either party may terminate any Order Form or SOW incorporating this Subscription Agreement, in whole or in part, for cause: (a) on thirty (30) days' written notice to the other party of a material breach thereof if such breach remains uncured at the expiration of such period (or immediately if the material breach is not capable of being remedied); or (b) immediately upon written notice if the other party becomes the subject of a petition in bankruptcy or any other proceeding relating to insolvency, receivership, liquidation, or an assignment for the benefit of creditors**.** In addition, Dynatrace may terminate any Order Form or SOW incorporating this Subscription Agreement immediately on written notice in the event: (a) Customer fails to pay any amounts due thereunder, and such failure continues more than ten (10) days after written notice by Dynatrace; or (b) Customer or its Users infringe or misappropriate Dynatrace's Intellectual Property Rights, including without limitation, use of a Dynatrace Offering other than as authorized under the Agreement.

12.4 **Effect of Termination or Expiration.**

12.4.1 Termination of one Order Form will not terminate any other Order Form or other Agreement.

12.4.2 On termination or expiration of an Order Form, Customer and Users shall immediately cease to use the applicable Dynatrace Offerings. Customer shall either uninstall or destroy all copies of software provided by Dynatrace and certify such in writing to Dynatrace upon request. With respect to any SaaS subscription, Dynatrace will make any remaining Customer Data stored in connection with the SaaS subscription available to Customer in the format in which it is stored for up to thirty (30) days following the effective date of termination or expiration. After such period, unless otherwise stated or legally prohibited, Dynatrace will have no obligation to maintain or provide any Customer Data and may delete all Customer Data in its possession or under its control.

12.4.3 If an Order Form or SOW is terminated by Customer for cause in accordance with Section 12.3, Dynatrace will refund Customer any unused prepaid fees for the Dynatrace Offering terminated. If an Order Form or SOW is terminated by Dynatrace for cause in accordance with Section 12.3, Customer will immediately pay Dynatrace any unpaid fees and reasonably incurred expenses covering the remainder of the Term/Service Period of such terminated Dynatrace Offering.

13. DYNATRACE INDEMNITY.

13.1 **IP Claims**. Dynatrace, at its expense, will defend Customer and its Affiliates and their respective officers, directors and employees (the "Customer Indemnified Parties") from and against all actions, proceedings, claims and demands by a third party (a "Third-Party Claim") alleging that the Dynatrace Offerings received by Customer under the applicable Order Form, as of the delivery date, infringes any copyright or misappropriates any trade secret, and Dynatrace will pay all damages, costs and expenses, including attorneys' fees and costs (whether by settlement or final award) incurred by the Customer Indemnified Parties directly from any such Third-Party Claim. Together with the mitigation obligations set forth below, this represents Dynatrace's entire liability, and Customer's sole and exclusive remedy, for infringement of any intellectual property or proprietary rights by any Dynatrace Offering. Notwithstanding anything to the contrary in the Agreement, the foregoing obligations will not apply with respect to a claim of infringement that arises out of (a) infringing or illegal Customer Data; (b) use of the Dynatrace Offering in combination with any software, hardware, network, technology or system not supplied by Dynatrace where the alleged infringement relates to such combination; (c) any modification or alteration of the Dynatrace Offering other than by Dynatrace; (d) Customer's continued use of the Dynatrace Offering after Dynatrace notifies Customer to discontinue use because of an infringement claim; (e) use of the Dynatrace Offering other than as authorized under the Agreement or Documentation; or (f) failure to implement an update, upgrade or bug fix that Dynatrace has provided at no charge where such implementation may avoid infringement.

13.2 **Mitigation.** If any Third-Party Claim which Dynatrace is obligated to defend has occurred, or in Dynatrace's determination, is likely to occur, Dynatrace may, at its option: (a) obtain for Customer the right to continue using the Dynatrace Offering; (b) replace or modify the Dynatrace Offering so that it avoids such claim; or (c) if such remedies are not reasonably available, terminate Customer's license for the infringing Dynatrace Offering and provide Customer with a refund of any unused fees Customer prepaid to Dynatrace for the infringing Dynatrace Offering. If such termination materially affects Dynatrace's ability to meet its remaining obligations under the relevant Order Form then Dynatrace may, at its option and upon written notice, terminate the Order Form, in whole or in part, and refund such other unused fees prepaid to Dynatrace for the terminated Dynatrace Offering.

14. **CUSTOMER INDEMNITY**. Customer will, at its expense, defend Dynatrace, its Affiliates, licensors and their respective officers, directors and employees (the "Dynatrace Indemnified Parties") from and against any and all Third-Party Claims which arise out of or

relate to: (a) a claim or threat that the Customer Data infringes, misappropriates or violates any third party's privacy or Intellectual Property Rights; (b) Customer's breach of Section 8 (Customer's Responsibilities); and (c) the occurrence of any of the exclusions (a) through (f) set forth above in Section 13.1 (IP Claims). Customer will pay all damages, fines, costs and expenses, including attorneys' fees and costs (whether by settlement or award of by a final judicial judgment) incurred by the Dynatrace Indemnified Parties from any such Third-Party Claim.

15. **INDEMNIFICATION PROCEDURES**. Either Party's respective indemnification obligations (each an "Indemnifying Party") are conditioned upon: (a) being promptly notified in writing of any Third-Party Claim; (b) having the sole and exclusive right to control the defense and settlement of the Third-Party Claim; and (c) the Dynatrace or Customer Indemnified Parties (as applicable the "Indemnified Party") providing all reasonable assistance (at the Indemnifying Party's expense and reasonable request) in the defense of such Third-Party Claim. In no event will an Indemnified Party settle any claim without the Indemnifying Party's prior written approval. The Indemnified Party may, at its own expense, engage separate counsel to advise it regarding a Third-Party Claim and to participate in the defense of the Third-Party Claim, subject to the Indemnifying Party's right to control the defense and settlement.

16. **LIMITATION OF LIABILITY.**

16.1 EXCEPT FOR CUSTOMER'S PAYMENT OBLIGATIONS, CUSTOMER'S BREACH OF SECTION 8 (CUSTOMER RESPONSIBILITIES), OR EITHER PARTY'S INDEMNITY OBLIGATIONS, THE CUMULATIVE LIABILITY OF EACH PARTY AND ITS AFFILIATES WILL NOT EXCEED THE ANNUAL FEES PAID OR PAYABLE BY CUSTOMER FOR THE APPLICABLE DYNATRACE OFFERING AT THE TIME THE CLAIM ARISES.

16.2 EXCEPT FOR CUSTOMER'S BREACH OF SECTION 8 (CUSTOMER RESPONSIBILITIES) OR EITHER PARTY'S BREACH OF SECTION 9 (CONFIDENTIALITY), NEITHER PARTY WILL BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO BUSINESS INTERRUPTION, LOST PROFITS, LOSS OF DATA OR COST OF COVER, EVEN IF SUCH PARTY KNEW OR SHOULD HAVE KNOWN OF THE POSSIBILITY OF SUCH DAMAGES.

16.3 THE WAIVERS AND LIMITATIONS IN THIS SECTION 16 APPLY REGARDLESS OF THE FORM OF ACTION OR THEORY OF LIABILITY ASSERTED, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, PRODUCT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY, AND WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY IN THE AGREEMENT FAILS OF ITS ESSENTIAL PURPOSE.

16.4 NEITHER PARTY LIMITS OR EXCLUDES ITS LIABILITY FOR: (A) DEATH OR PERSONAL INJURY CAUSED BY NEGLIGENCE; (B) FRAUDULENT MISREPRESENTATION OR WILLFUL MISCONDUCT; OR (C) ANY OTHER LIABILITY TO THE EXTENT THAT SUCH LIABILITY CANNOT BE EXCLUDED OR LIMITED BY APPLICABLE LAW.

17. **TRIAL USE.** Dynatrace may offer free or trial use of Dynatrace Offerings ("Trial Use") in its sole discretion, Trial Use is governed by this Subscription Agreement. Trial Use is for the sole and exclusive purpose of enabling Customer to evaluate a prospective purchase and shall not be deployed as part of Customer's business processes. At any time, in its sole discretion, Dynatrace may terminate or suspend all or a portion of the Trial Use without prior notice. Certain features, technical support and other support in connection with Trial Use may not be available. If applicable, Customer is solely responsible for exporting Customer Data from the Dynatrace Platform prior to termination or expiration of the Trial Use. All Trial Use is provided "AS IS" and no express or implied warranties shall apply. Dynatrace shall have no liability of any kind with respect to Trial Use unless otherwise required by applicable law, in which case Dynatrace's liability shall not exceed $1,000.00.

18. **INDEPENDENT CONTRACTORS.** The parties are independent contractors and will represent themselves accordingly in all regards.

19. **FORCE MAJEURE.** Neither party will be liable for delay or default in the performance of their respective obligations, excluding payment obligations, if the delay or default is caused by conditions beyond its reasonable control, including but not limited to, acts of God, war, acts of terrorism (whether actual or threatened), riot or civil unrest, failure of electrical, Internet, co-location or telecommunications service, nonDynatrace applications, denial of service or similar attacks, acts of civil or military authorities, fire, floods, weather disturbances, volcanic eruption, earthquakes, accidents, strikes or labor actions, epidemics, pandemics, quarantines, or energy crises.

20. **COMPLIANCE WITH LAWS**. Customer shall comply with all laws and regulations applicable to its use of the Dynatrace Offerings. Dynatrace shall comply with all laws and regulations applicable to its provision of the Dynatrace Offerings. Dynatrace is not responsible for compliance with any laws or regulations that apply to Customer or Customer's industry that are not otherwise applicable to Dynatrace (e.g., Dynatrace does not determine whether Customer Data includes information subject to any specific law or regulation).

21. **ASSIGNMENT.** Neither party may transfer or assign the Agreement or any Order Form, in whole or in part, without the other's prior written consent. A transfer or assignment upon a change of control, through a merger, consolidation, reorganization, operation of law or otherwise, will be deemed a transfer or assignment that requires the other party's prior written consent. Notwithstanding the foregoing, Dynatrace may, without Customer's consent assign any Agreement or any Order Form to any of its Affiliates, or to an entity who acquires all or substantially all of its business or assets, or in connection with a change in control of Dynatrace (through merger, consolidation, reorganization, operation of law or otherwise). Any assignment in violation of this Section will be void *ab initio* and of no effect. Subject to the foregoing, the Agreement is binding upon, inures to the benefit of and is enforceable by the parties and their respective successors and assigns.

22. **ELECTRONIC COMMUNICATION; NOTICES.** Dynatrace may use electronic means to communicate with Customer related to its performance of obligations under the Agreement, including but not limited to, email, notices posted in portals, online Documentation, in-product chat, and RSS subscriptions to be notified of updates. Customer consents to receive communications in an electronic form and agrees that all communications that Dynatrace provides to Customer electronically constitute a written communication.

Either party may give notice by written communication, sent by first class postage prepaid mail or nationally recognized overnight delivery service, to the other party's address as specified in the Agreement. Customer may send notices to Dynatrace at 1601 Trapelo Road, Suite 116, Waltham, MA 02451, Attention: General Counsel, with a copy to legalnotices@dynatrace.com. Dynatrace may send notices to Customer at the address set forth at the top of the Order Form. If Dynatrace requires an email address from Customer, Customer is responsible for providing and updating its most current email address for the purpose requested. Either party may change its address for notices under this Section by giving the other party notice of the change in accordance with this Section.

23. **CUSTOMER REFERENCE.** Customer agrees that Dynatrace may reference Customer as a Dynatrace customer, subject to Customer's trademark and logo usage guidelines provided by Customer, and that occasionally, after Customer review, Dynatrace may issue a press release and case study.

24. **GOVERNING LAW.** The Agreement will be governed by the laws of the State of Delaware without regard to its conflicts of law principles. The parties hereby consent to the personal and exclusive jurisdiction of the federal and state courts of the State of Delaware. If the entity selling the Dynatrace Offerings is an Affiliate of Dynatrace LLC, the Agreement will be governed by the laws of the country in which such Dynatrace Affiliate is situated, and the parties consent to the exclusive jurisdiction of the courts where such Dynatrace Affiliate is located, or in the event of multiple offices, where the head office of such Affiliate is located. The 1980 United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to the Agreement. If any provision of the Agreement is contrary to an applicable law, such provision will be considered null and void to the extent that it is contrary to such law, but all other provisions of the Agreement will remain in effect.

25. **EXPORT CONTROLS.** Customer shall comply with applicable United States, EU and UN export and reexport laws, regulations and requirements ("Trade Laws"). Customer shall not export, re-export, use, or make available any software or service that may be subject to the Trade Laws, to any location, or to or on behalf of any end user, or for any end use, without first obtaining any export license, permit or other approval that may be required and providing notice of such actions to Dynatrace at legalnotices@dynatrace.com. Without limiting the foregoing, Customer shall not export or re-export any software, or use or make available any software or service, subject to the Agreement (a) to any Group E country listed in Supplement No. 1 to Part 740, Title 15, or the Crimea, Donetsk, or Luhansk region of Ukraine; (b) to any party of concern listed at www.trade.gov/consolidated-screening-list, www.trade.gov/consolidated-screening-list,or to any party owned or controlled by any such party of concern; or (c) for any end use related to the development, production or use of nuclear, chemical or biological weapons or missiles. If, at any time during the Term or Service Period, Dynatrace is not permitted, as a result of applicable Trade Laws, sanctions or similar government restrictions, to supply the Dynatrace Offerings to Customer or receive payment from Customer's financial institution or payment processor, Dynatrace may terminate or suspend its performance under the Agreement upon written notice without penalty.

26. **ANTI-CORRUPTION.** Each party shall maintain its own policies and procedures relating to anti-bribery and anti-corruption to ensure compliance with applicable law, and will enforce them where appropriate; and will promptly report to the other party any request or demand for any undue financial or other advantage of any kind in connection with the performance of the Agreement.

27. **GOVERNMENT USE**. U.S federal government end users acknowledge and agree that: (a) Dynatrace Offerings are "commercial items" as defined in Federal Acquisition Regulation (FAR) 2.101; (b) any agreement between Dynatrace and Partner or its end user as Customer is a commercial-item subcontract governed by FAR 52.244-6 or 52.212-5(e) as applicable; and (c) only the mandatory flow-down clauses of FAR 52.244-6 or 52.212-5(e) apply to Dynatrace unless other FAR and FAR Supplement clauses are specifically identified and accepted by Dynatrace in writing. For all U.S. federal government Customers and end users, the terms of this standard commercial software license customarily provided to the public govern, as provided by FAR 12.212, Defense FAR Supplement (DFARS) 227.7202-1 and 227.7202-3, or other applicable laws and regulations. No other license to the Dynatrace Platform is valid or enforceable unless (and solely to the extent) specifically agreed to in writing by Dynatrace. For all other government entities, license

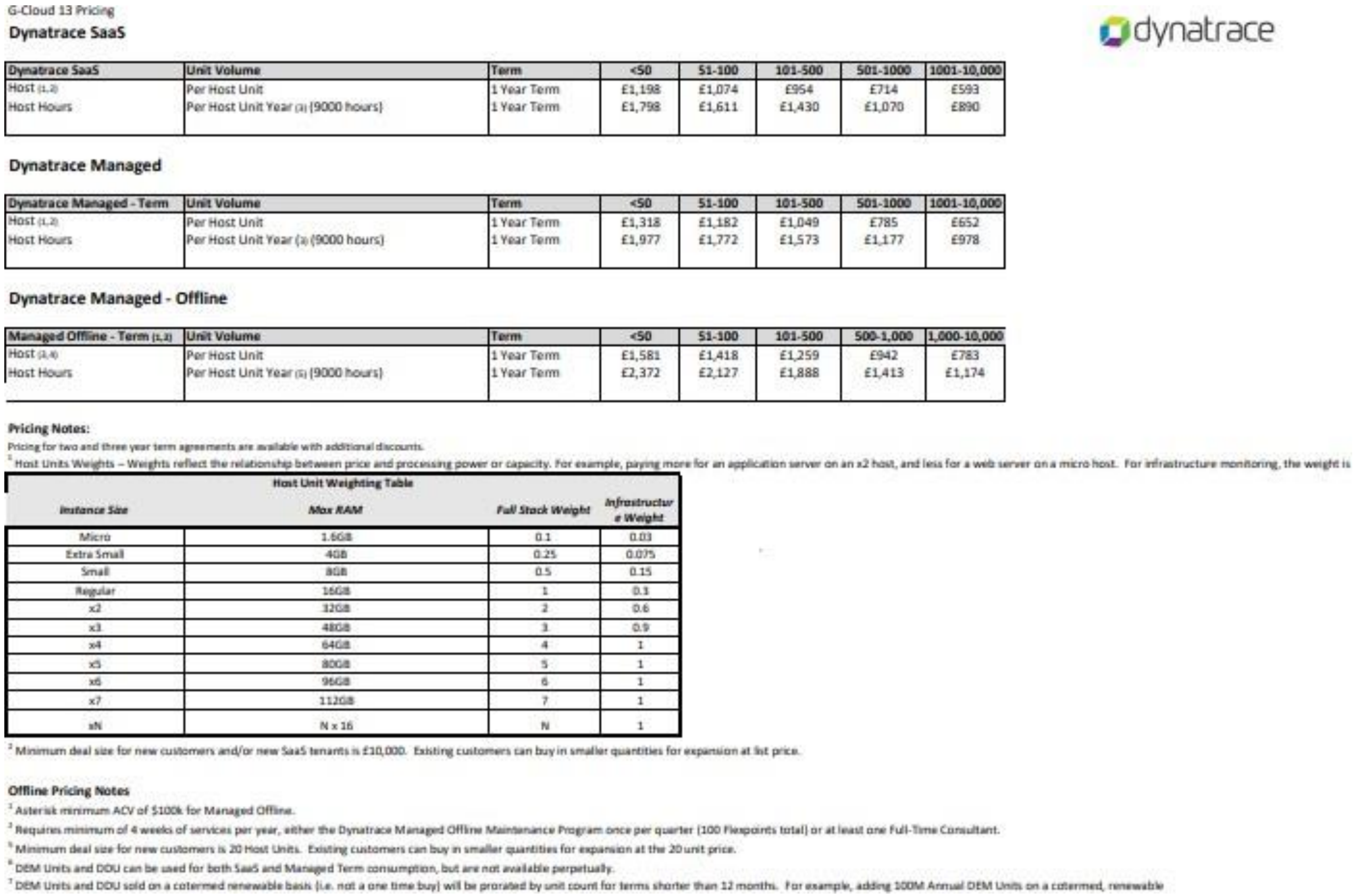
to the Dynatrace Platform is offered only under this license; no other license to the Dynatrace Platform is valid or enforceable unless (and solely to the extent) specifically agreed to in writing by Dynatrace.

28. **OPEN SOURCE**. "Open Source Software" means any open source, community, or other free code or libraries of any type, including, without limitation, any code which is generally made available on the Internet without charge, such as, for illustrative purposes only, any code licensed under the GNU Affero General Public License (AGPL), GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL), Apache License, BSD licenses, or other licenses approved by the Open Source Initiative. Dynatrace maintains an updated list of applicable Open Source Software online. Notwithstanding the foregoing license grants, the Agreement is not meant to modify the terms of any Open Source Software license applicable to the Dynatrace Platform, and in the event of a conflict, the terms of such Open Source Software license will prevail.

29. **SURVIVAL.** The following provisions will survive expiration or termination of the Agreement: (a) any payment obligations of Customer hereunder; (b) Section 3.2 (Partners), Section 6 (Ownership and Other Rights), Section 7 (Payment), Section 8 (Customer Responsibilities), Section 9 (Confidentiality), Section 12 (Term and Termination), Sections 13-15 (Indemnity), Section 16 (Limitation of Liability), Section 22 (Electronic Communication; Notices), Section 24 (Governing Law); and (c) any rights or obligations which are stated to, or by their nature will, survive. The expiration or termination of the Agreement does not affect any rights which accrued before the date of expiration or termination.

30. **MISCELLANEOUS.** The Agreement sets forth the entire agreement and understanding between the parties, and supersedes any other agreements, discussions, proposals, representations or warranties, written or oral, with respect to the subject matter hereof. Any other terms stated in any PO delivered to Dynatrace in connection with an Order Form or invoice thereunder shall have no effect. Each party acknowledges that it has reviewed and accepted the terms of the Agreement and agrees that contractual ambiguities are not to be construed in favor of or against any party based on its role in drafting the Agreement. Performance of any obligation required by a party under the Agreement may be waived only by a written waiver signed by an authorized representative of the other party. Failure or delay by either party in exercising any right or remedy will not constitute a waiver. If any provision of the Agreement is declared invalid, the entire Agreement will not fail on its account, and that provision will be severed, with the balance of the Agreement continuing in full force and effect. The Agreement may only be amended in writing signed by both parties.

Annex 6 – G-Cloud 13 Pricing Document



G-Cloud 13 Pricing

Dynatrace SaaS

Dynatrace SaaS	Unit Volume	Term	<50	51-100	101-500	501-1000	1001-10,000
Host (1,2)	Per Host Unit	1 Year Term	£1,198	£1,074	£954	£714	£593
Host Hours	Per Host Unit Year (3) (9000 hours)	1 Year Term	£1,798	£1,611	£1,430	£1,070	£890

Dynatrace Managed

Dynatrace Managed - Term	Unit Volume	Term	<50	51-100	101-500	501-1000	1001-10,000
Host (1,2)	Per Host Unit	1 Year Term	£1,318	£1,182	£1,049	£785	£652
Host Hours	Per Host Unit Year (3) (9000 hours)	1 Year Term	£1,977	£1,772	£1,573	£1,177	£978

Dynatrace Managed - Offline

Managed Offline - Term (1,2)	Unit Volume	Term	<50	51-100	101-500	500-1,000	1,000-10,000
Host (3,4)	Per Host Unit	1 Year Term	£1,581	£1,418	£1,259	£942	£783
Host Hours	Per Host Unit Year (5) (9000 hours)	1 Year Term	£2,372	£2,127	£1,888	£1,413	£1,174

Pricing Notes:

Pricing for two and three year term agreements are available with additional discounts.

[1] Host Units Weights – Weights reflect the relationship between price and processing power or capacity. For example, paying more for an application server on an x2 host, and less for a web server on a micro host. For infrastructure monitoring, the weight is

Host Unit Weighting Table			
Instance Size	*Max RAM*	*Full Stack Weight*	*Infrastructure Weight*
Micro	1.6GB	0.1	0.03
Extra Small	4GB	0.25	0.075
Small	8GB	0.5	0.15
Regular	16GB	1	0.3
x2	32GB	2	0.6
x3	48GB	3	0.9
x4	64GB	4	1
x5	80GB	5	1
x6	96GB	6	1
x7	112GB	7	1
xN	N x 16	N	1

[2] Minimum deal size for new customers and/or new SaaS tenants is £10,000. Existing customers can buy in smaller quantities for expansion at list price.

Offline Pricing Notes

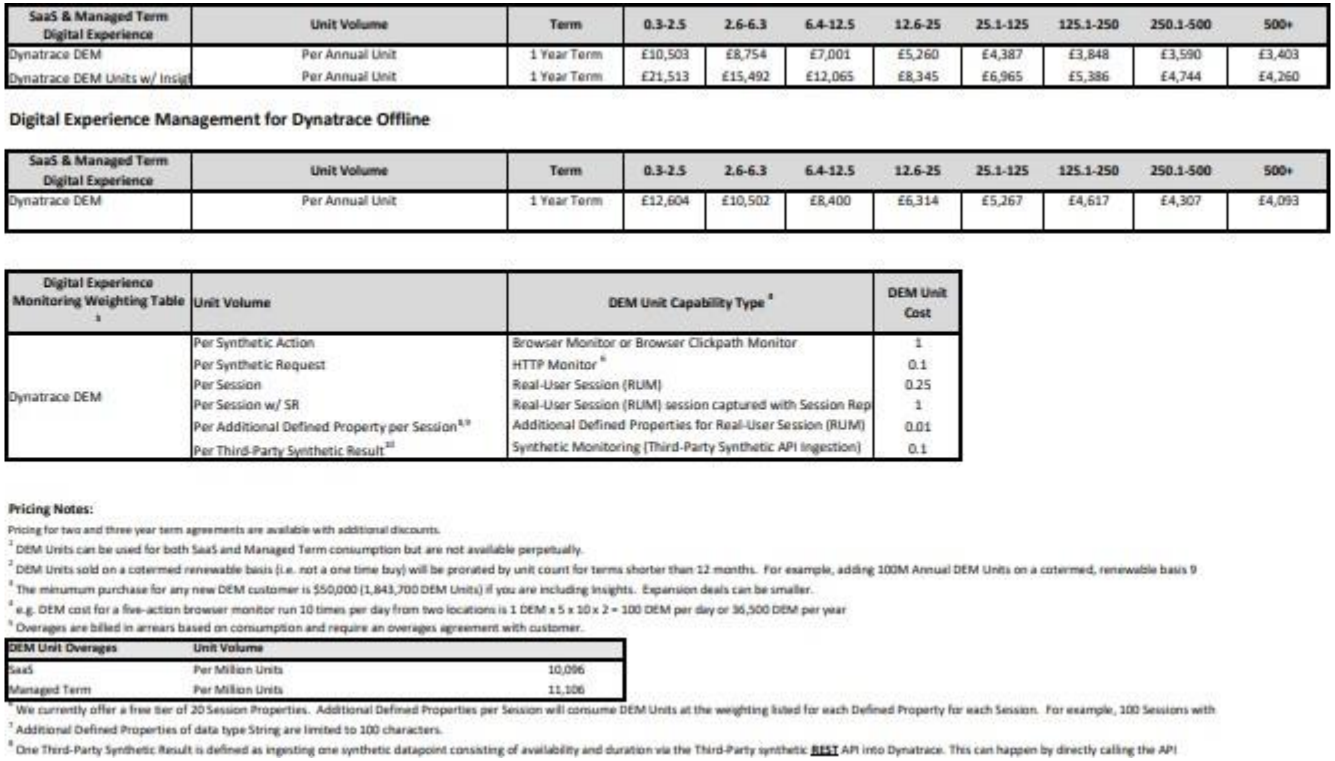
[1] Asterisk minimum ACV of $100k for Managed Offline.

[2] Requires minimum of 4 weeks of services per year, either the Dynatrace Managed Offline Maintenance Program once per quarter (100 Flexpoints total) or at least one Full-Time Consultant.

[5] Minimum deal size for new customers is 20 Host Units. Existing customers can buy in smaller quantities for expansion at the 20 unit price.

[6] DEM Units and DDU can be used for both SaaS and Managed Term consumption, but are not available perpetually.

[7] DEM Units and DDU sold on a cotermed renewable basis (i.e. not a one time buy) will be prorated by unit count for terms shorter than 12 months. For example, adding 100M Annual DEM Units on a cotermed, renewable



SaaS & Managed Term Digital Experience	Unit Volume	Term	0.3-2.5	2.6-6.3	6.4-12.5	12.6-25	25.1-125	125.1-250	250.1-500	500+
Dynatrace DEM	Per Annual Unit	1 Year Term	£10,503	£8,754	£7,001	£5,260	£4,387	£3,848	£3,590	£3,403
Dynatrace DEM Units w/ Insig	Per Annual Unit	1 Year Term	£21,513	£15,492	£12,065	£8,345	£6,965	£5,386	£4,744	£4,260

Digital Experience Management for Dynatrace Offline

SaaS & Managed Term Digital Experience	Unit Volume	Term	0.3-2.5	2.6-6.3	6.4-12.5	12.6-25	25.1-125	125.1-250	250.1-500	500+
Dynatrace DEM	Per Annual Unit	1 Year Term	£12,604	£10,502	£8,400	£6,314	£5,267	£4,617	£4,307	£4,093

Digital Experience Monitoring Weighting Table [1]	Unit Volume	DEM Unit Capability Type [4]	DEM Unit Cost
Dynatrace DEM	Per Synthetic Action	Browser Monitor or Browser Clickpath Monitor	1
	Per Synthetic Request	HTTP Monitor [6]	0.1
	Per Session	Real-User Session (RUM)	0.25
	Per Session w/ SR	Real-User Session (RUM) session captured with Session Rep	1
	Per Additional Defined Property per Session[8,9]	Additional Defined Properties for Real-User Session (RUM)	0.01
	Per Third-Party Synthetic Result[10]	Synthetic Monitoring (Third-Party Synthetic API ingestion)	0.1

Pricing Notes:

Pricing for two and three year term agreements are available with additional discounts.

[1] DEM Units can be used for both SaaS and Managed Term consumption but are not available perpetually.

[2] DEM Units sold on a cotermed renewable basis (i.e. not a one time buy) will be prorated by unit count for terms shorter than 12 months. For example, adding 100M Annual DEM Units on a cotermed, renewable basis 9

[3] The minumum purchase for any new DEM customer is $50,000 (1,843,700 DEM Units) if you are including Insights. Expansion deals can be smaller.

[4] e.g. DEM cost for a five-action browser monitor run 10 times per day from two locations is 1 DEM x 5 x 10 x 2 = 100 DEM per day or 36,500 DEM per year

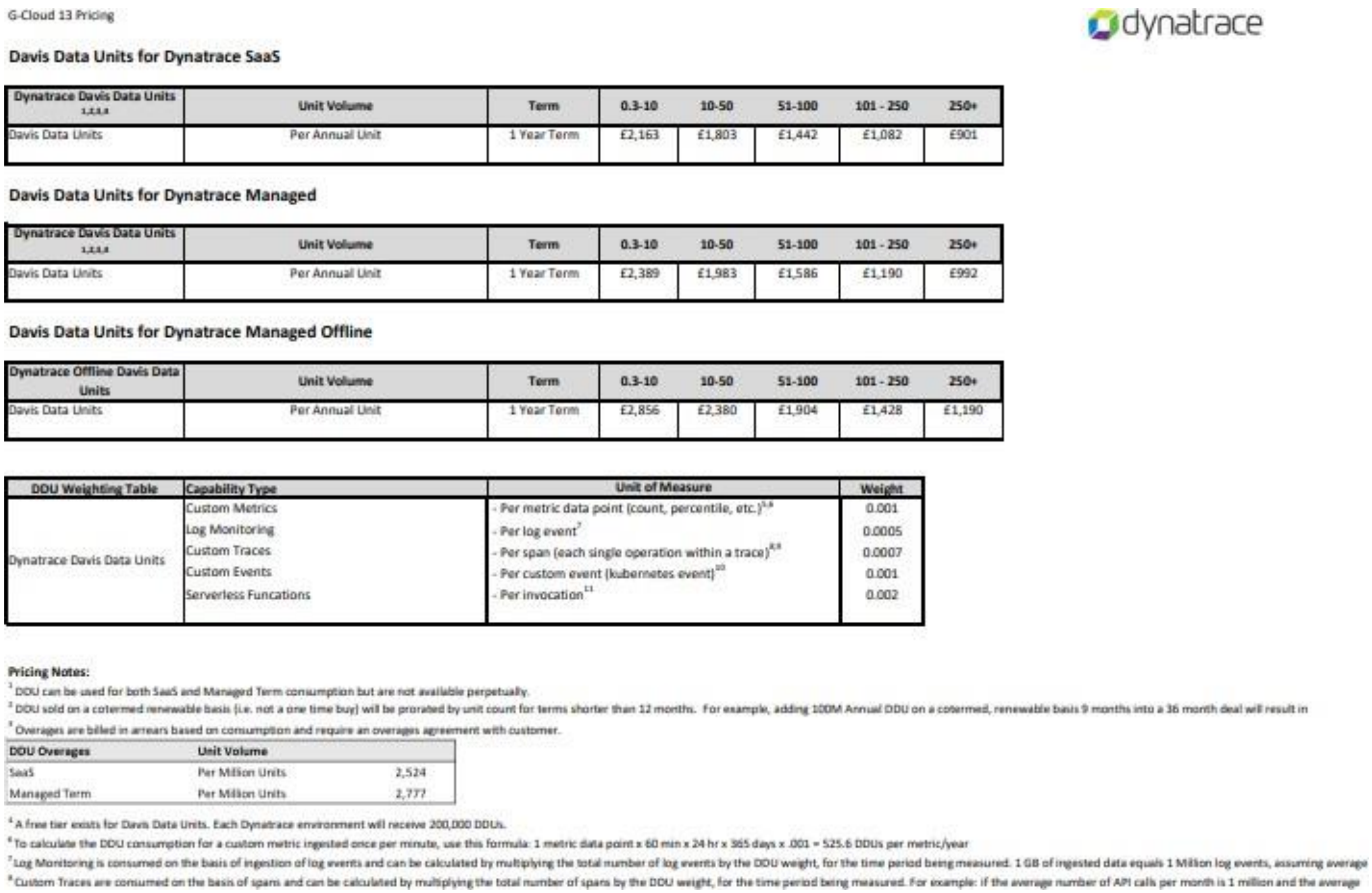
[5] Overages are billed in arrears based on consumption and require an overages agreement with customer.

DEM Unit Overages	Unit Volume	
SaaS	Per Million Units	10,096
Managed Term	Per Million Units	11,106

[6] We currently offer a free tier of 20 Session Properties. Additional Defined Properties per Session will consume DEM Units at the weighting listed for each Defined Property for each Session. For example, 100 Sessions with

[7] Additional Defined Properties of data type String are limited to 100 characters.

[8] One Third-Party Synthetic Result is defined as ingesting one synthetic datapoint consisting of availability and duration via the Third-Party synthetic REST API into Dynatrace. This can happen by directly calling the API



G-Cloud 13 Pricing

dynatrace

Davis Data Units for Dynatrace SaaS

Dynatrace Davis Data Units [1,2,3,4]	Unit Volume	Term	0.3-10	10-50	51-100	101 - 250	250+
Davis Data Units	Per Annual Unit	1 Year Term	£2,163	£1,803	£1,442	£1,082	£901

Davis Data Units for Dynatrace Managed

Dynatrace Davis Data Units [1,2,3,4]	Unit Volume	Term	0.3-10	10-50	51-100	101 - 250	250+
Davis Data Units	Per Annual Unit	1 Year Term	£2,389	£1,983	£1,586	£1,190	£992

Davis Data Units for Dynatrace Managed Offline

Dynatrace Offline Davis Data Units	Unit Volume	Term	0.3-10	10-50	51-100	101 - 250	250+
Davis Data Units	Per Annual Unit	1 Year Term	£2,856	£2,380	£1,904	£1,428	£1,190

DDU Weighting Table	Capability Type	Unit of Measure	Weight
Dynatrace Davis Data Units	Custom Metrics Log Monitoring Custom Traces Custom Events Serverless Funcations	- Per metric data point (count, percentile, etc.)[5,6] - Per log event[7] - Per span (each single operation within a trace)[8,9] - Per custom event (kubernetes event)[10] - Per invocation[11]	0.001 0.0005 0.0007 0.001 0.002

Pricing Notes:

[1] DDU can be used for both SaaS and Managed Term consumption but are not available perpetually.

[2] DDU sold on a cotermed renewable basis (i.e. not a one time buy) will be prorated by unit count for terms shorter than 12 months. For example, adding 100M Annual DDU on a cotermed, renewable basis 9 months into a 36 month deal will result in

[3] Overages are billed in arrears based on consumption and require an overages agreement with customer.

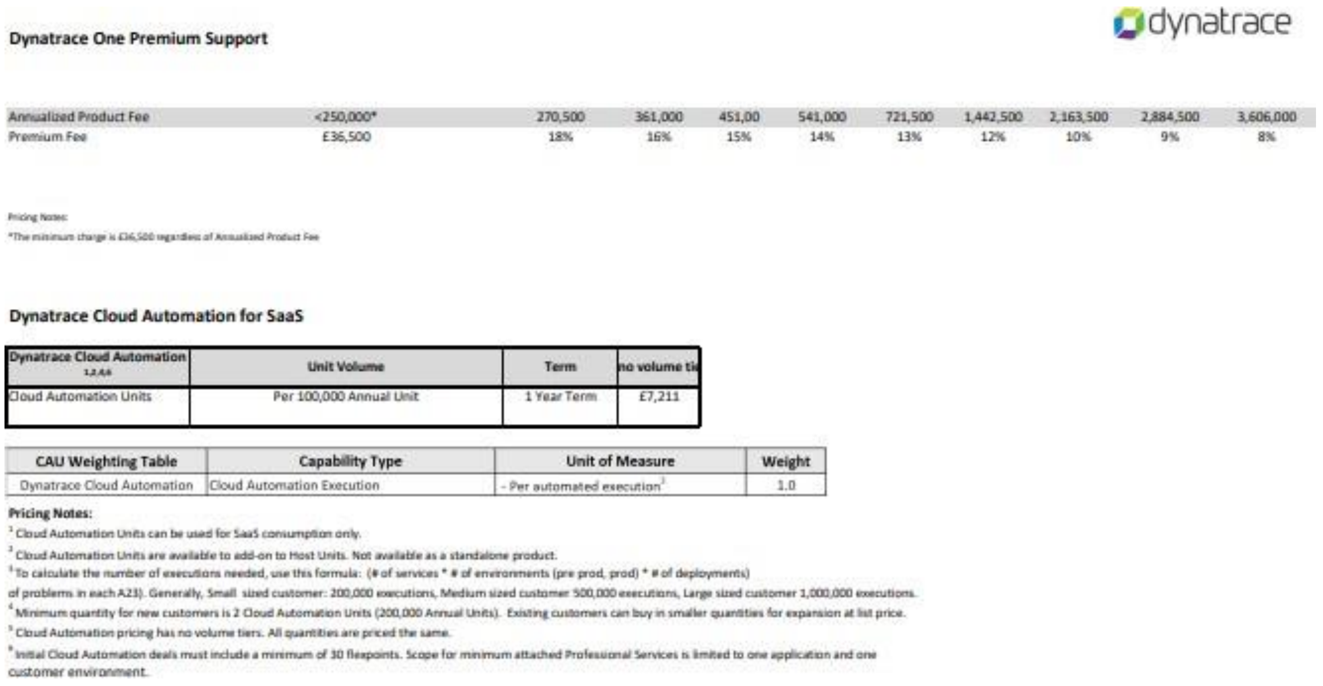
DDU Overages	Unit Volume	
SaaS	Per Million Units	2,524
Managed Term	Per Million Units	2,777

[4] A free tier exists for Davis Data Units. Each Dynatrace environment will receive 200,000 DDUs.

[6] To calculate the DDU consumption for a custom metric ingested once per minute, use this formula: 1 metric data point x 60 min x 24 hr x 365 days x .001 = 525.6 DDUs per metric/year

[7] Log Monitoring is consumed on the basis of ingestion of log events and can be calculated by multiplying the total number of log events by the DDU weight, for the time period being measured. 1 GB of ingested data equals 1 Million log events, assuming average

[8] Custom Traces are consumed on the basis of spans and can be calculated by multiplying the total number of spans by the DDU weight, for the time period being measured. For example: if the average number of API calls per month is 1 million and the average



Dynatrace One Premium Support

Annualized Product Fee	<250,000*	270,500	361,000	451,00	541,000	721,500	1,442,500	2,163,500	2,884,500	3,606,000
Premium Fee	£36,500	18%	16%	15%	14%	13%	12%	10%	9%	8%

Pricing Notes:

*The minimum charge is £36,500 regardless of Annualized Product Fee

Dynatrace Cloud Automation for SaaS

Dynatrace Cloud Automation [1,2,4,6]	Unit Volume	Term	no volume ti
Cloud Automation Units	Per 100,000 Annual Unit	1 Year Term	£7,211

CAU Weighting Table	Capability Type	Unit of Measure	Weight
Dynatrace Cloud Automation	Cloud Automation Execution	- Per automated execution[3]	1.0

Pricing Notes:

[1] Cloud Automation Units can be used for SaaS consumption only.

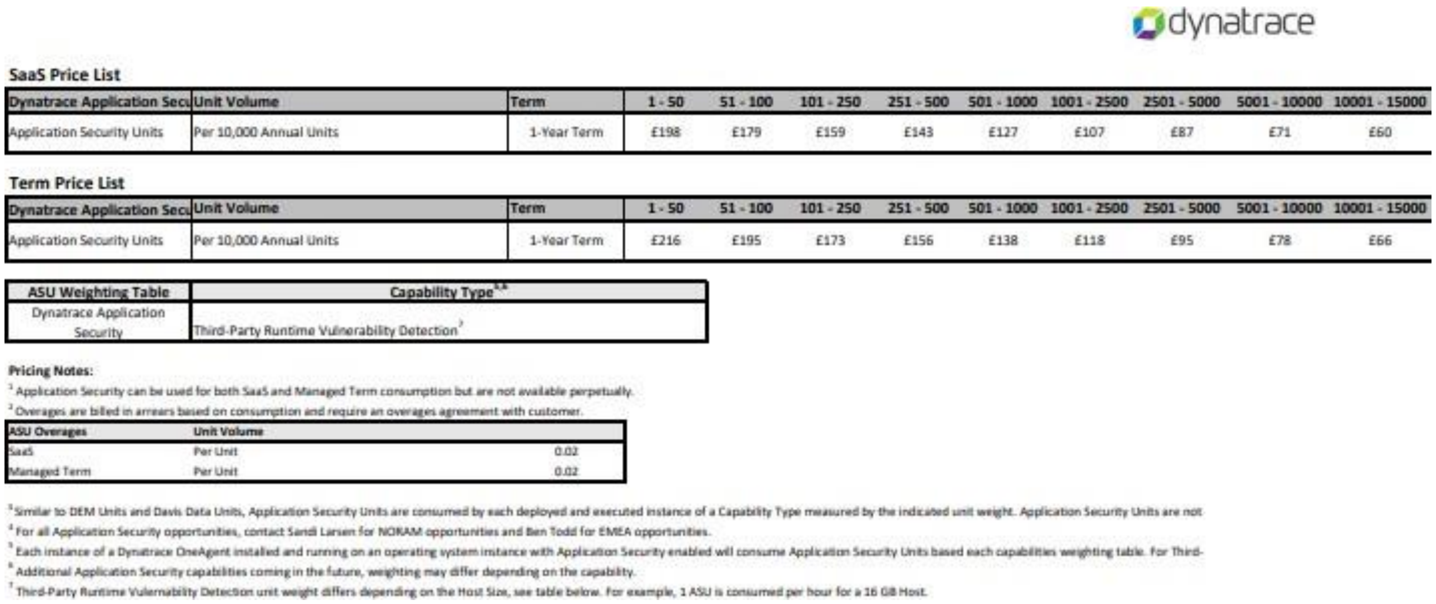
[2] Cloud Automation Units are available to add-on to Host Units. Not available as a standalone product.

[3] To calculate the number of executions needed, use this formula: (# of services * # of environments (pre prod, prod) * # of deployments) of problems in each A23). Generally, Small sized customer: 200,000 executions, Medium sized customer 500,000 executions, Large sized customer 1,000,000 executions.

[4] Minimum quantity for new customers is 2 Cloud Automation Units (200,000 Annual Units). Existing customers can buy in smaller quantities for expansion at list price.

[5] Cloud Automation pricing has no volume tiers. All quantities are priced the same.

[6] Initial Cloud Automation deals must include a minimum of 30 flexpoints. Scope for minimum attached Professional Services is limited to one application and one customer environment.



dynatrace

SaaS Price List

Dynatrace Application Secu	Unit Volume	Term	1 - 50	51 - 100	101 - 250	251 - 500	501 - 1000	1001 - 2500	2501 - 5000	5001 - 10000	10001 - 15000
Application Security Units	Per 10,000 Annual Units	1-Year Term	£198	£179	£159	£143	£127	£107	£87	£71	£60

Term Price List

Dynatrace Application Secu	Unit Volume	Term	1 - 50	51 - 100	101 - 250	251 - 500	501 - 1000	1001 - 2500	2501 - 5000	5001 - 10000	10001 - 15000
Application Security Units	Per 10,000 Annual Units	1-Year Term	£216	£195	£173	£156	£138	£118	£95	£78	£66

ASU Weighting Table	Capability Type[5,6]
Dynatrace Application Security	Third-Party Runtime Vulnerability Detection[7]

Pricing Notes:

[1] Application Security can be used for both SaaS and Managed Term consumption but are not available perpetually.

[2] Overages are billed in arrears based on consumption and require an overages agreement with customer.

ASU Overages	Unit Volume	
SaaS	Per Unit	0.02
Managed Term	Per Unit	0.02

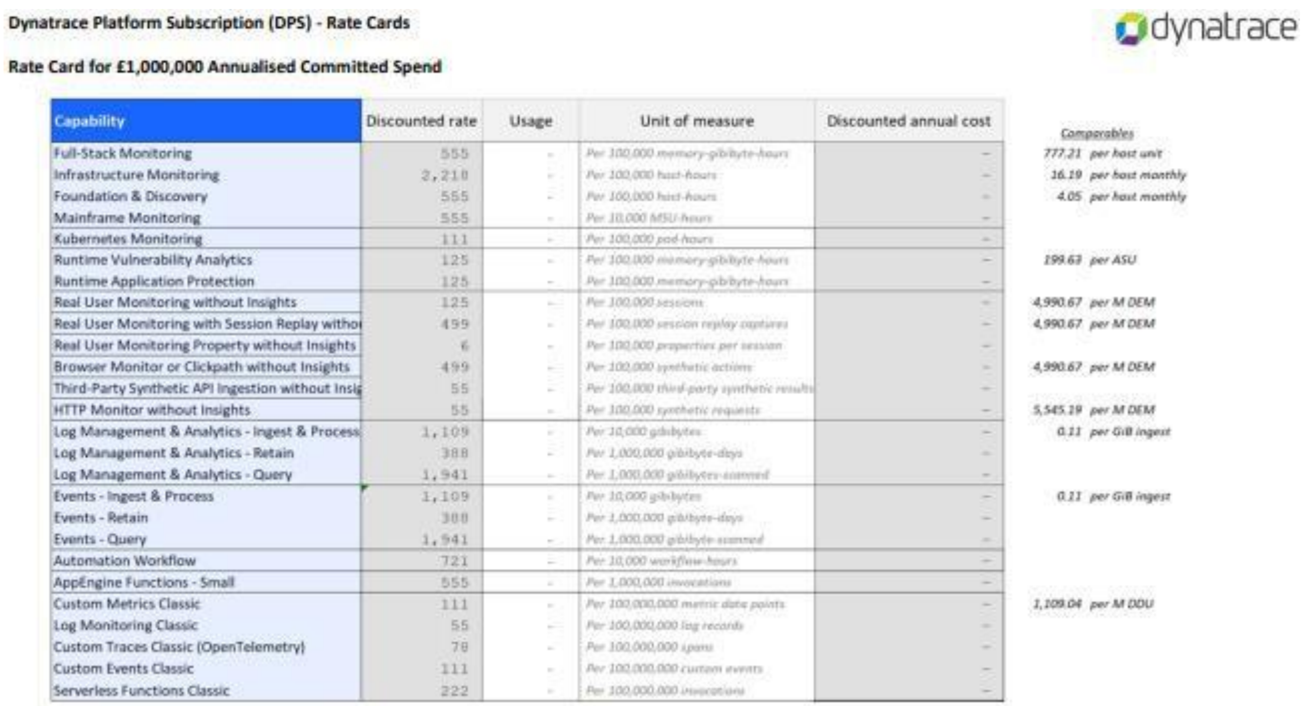
[3] Similar to DEM Units and Davis Data Units, Application Security Units are consumed by each deployed and executed instance of a Capability Type measured by the indicated unit weight. Application Security Units are not

[4] For all Application Security opportunities, contact Sandi Larsen for NORAM opportunities and Ben Todd for EMEA opportunities.

[5] Each instance of a Dynatrace OneAgent installed and running on an operating system instance with Application Security enabled will consume Application Security Units based each capabilities weighting table. For Third-

[6] Additional Application Security capabilities coming in the future, weighting may differ depending on the capability.

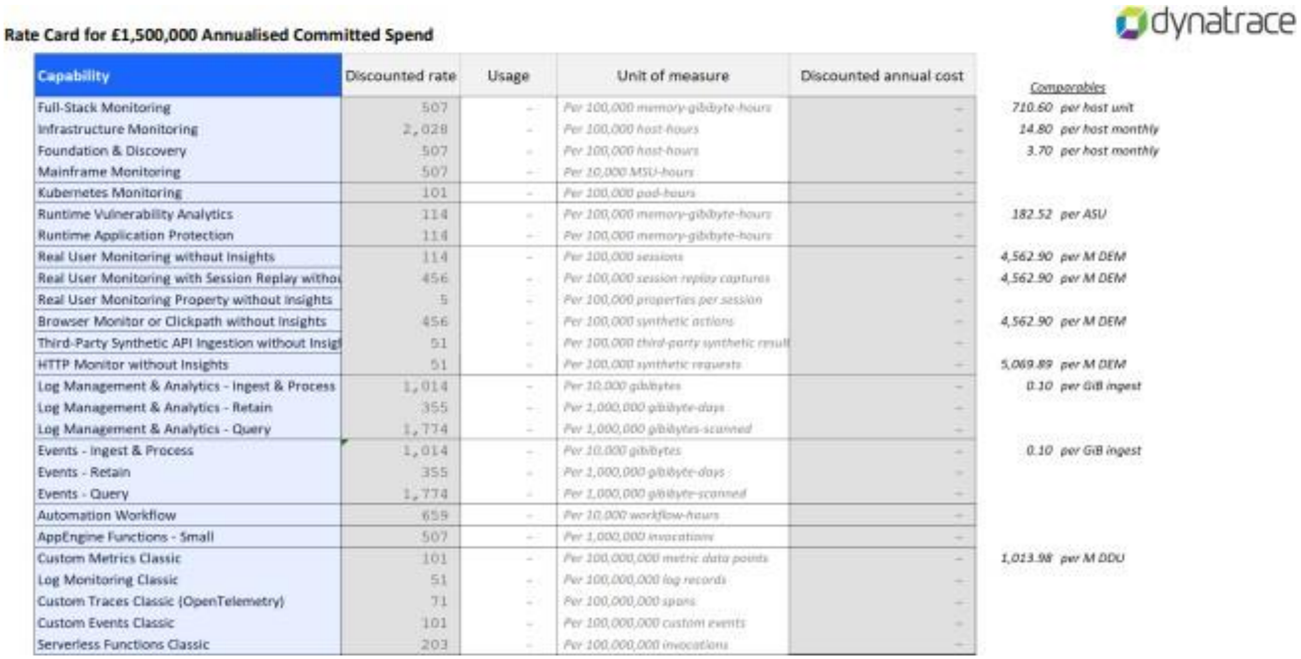
[7] Third-Party Runtime Vulnerability Detection unit weight differs depending on the Host Size, see table below. For example, 1 ASU is consumed per hour for a 16 GB Host.



Dynatrace Platform Subscription (DPS) - Rate Cards

Rate Card for £1,000,000 Annualised Committed Spend

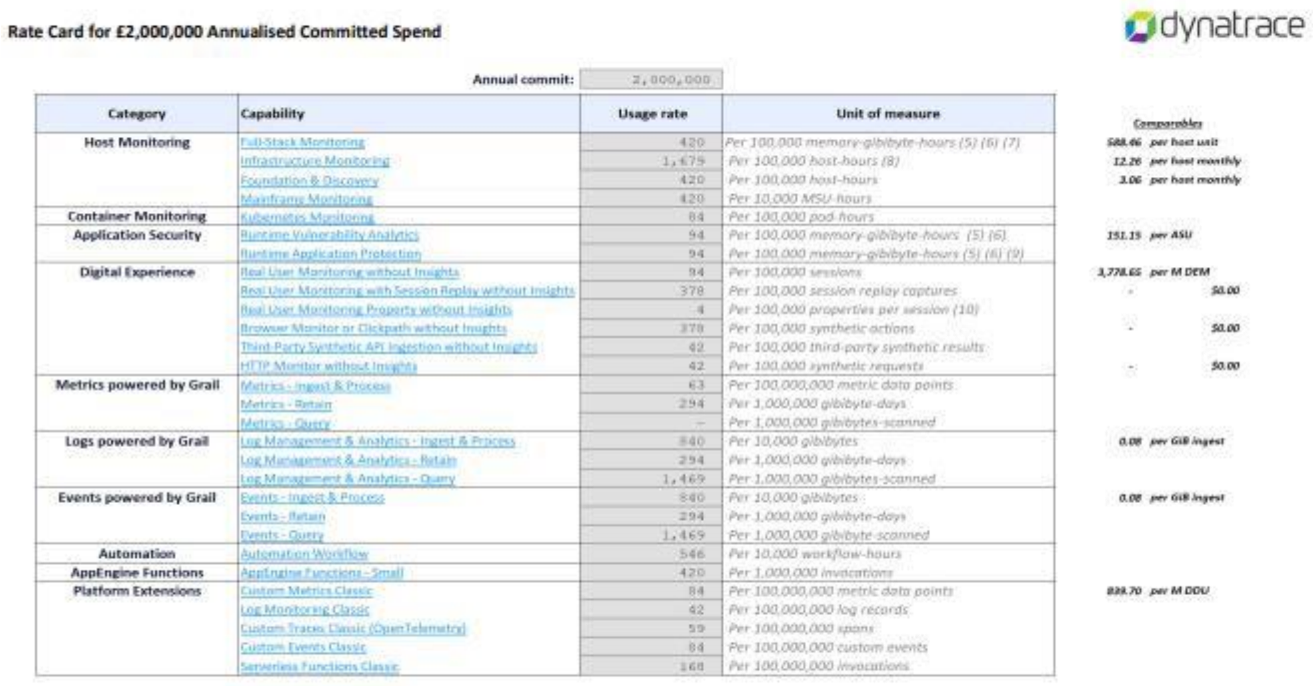
Capability	Discounted rate	Usage	Unit of measure	Discounted annual cost	Comparables	
Full-Stack Monitoring	555	-	Per 100,000 memory-gibibyte-hours	–	777.21	per host unit
Infrastructure Monitoring	2,218	-	Per 100,000 host-hours	–	16.19	per host monthly
Foundation & Discovery	555	-	Per 100,000 host-hours	–	4.05	per host monthly
Mainframe Monitoring	555	-	Per 10,000 MSU-hours	–		
Kubernetes Monitoring	111	-	Per 100,000 pod-hours	–		
Runtime Vulnerability Analytics	125	-	Per 100,000 memory-gibibyte-hours	–	199.63	per ASU
Runtime Application Protection	125	-	Per 100,000 memory-gibibyte-hours	–		
Real User Monitoring without Insights	125	-	Per 100,000 sessions	–	4,990.67	per M DEM
Real User Monitoring with Session Replay withou	499	-	Per 100,000 session replay captures	–	4,990.67	per M DEM
Real User Monitoring Property without Insights	6	-	Per 100,000 properties per session	–		
Browser Monitor or Clickpath without Insights	499	-	Per 100,000 synthetic actions	–	4,990.67	per M DEM
Third-Party Synthetic API Ingestion without Insig	55	-	Per 100,000 third-party synthetic results	–		
HTTP Monitor without Insights	55	-	Per 100,000 synthetic requests	–	5,545.19	per M DEM
Log Management & Analytics - Ingest & Process	1,109	-	Per 10,000 gibibytes	–	0.11	per GiB ingest
Log Management & Analytics - Retain	388	-	Per 1,000,000 gibibyte-days	–		
Log Management & Analytics - Query	1,941	-	Per 1,000,000 gibibytes scanned	–		
Events - Ingest & Process	1,109	-	Per 10,000 gibibytes	–	0.11	per GiB ingest
Events - Retain	388	-	Per 1,000,000 gibibyte-days	–		
Events - Query	1,941	-	Per 1,000,000 gibibyte scanned	–		
Automation Workflow	721	-	Per 10,000 workflow-hours	–		
AppEngine Functions - Small	555	-	Per 1,000,000 invocations	–		
Custom Metrics Classic	111	-	Per 100,000,000 metric data points	–	1,109.04	per M DDU
Log Monitoring Classic	55	-	Per 100,000,000 log records	–		
Custom Traces Classic (OpenTelemetry)	78	-	Per 100,000,000 spans	–		
Custom Events Classic	111	-	Per 100,000,000 custom events	–		
Serverless Functions Classic	222	-	Per 100,000,000 invocations	–		



Rate Card for £1,500,000 Annualised Committed Spend

dynatrace

Capability	Discounted rate	Usage	Unit of measure	Discounted annual cost	Comparables	
Full-Stack Monitoring	507	-	*Per 100,000 memory-gibibyte-hours*	-	*710.60*	*per host unit*
Infrastructure Monitoring	2,028	-	*Per 100,000 host-hours*	-	*14.80*	*per host monthly*
Foundation & Discovery	507	-	*Per 100,000 host-hours*	-	*3.70*	*per host monthly*
Mainframe Monitoring	507	-	*Per 10,000 MSU-hours*	-		
Kubernetes Monitoring	101	-	*Per 100,000 pod-hours*	-		
Runtime Vulnerability Analytics	114	-	*Per 100,000 memory-gibibyte-hours*	-	*182.52*	*per ASU*
Runtime Application Protection	114	-	*Per 100,000 memory-gibibyte-hours*	-		
Real User Monitoring without Insights	114	-	*Per 100,000 sessions*	-	*4,562.90*	*per M DEM*
Real User Monitoring with Session Replay withou	456	-	*Per 100,000 session replay captures*	-	*4,562.90*	*per M DEM*
Real User Monitoring Property without Insights	5	-	*Per 100,000 properties per session*	-		
Browser Monitor or Clickpath without Insights	456	-	*Per 100,000 synthetic actions*	-	*4,562.90*	*per M DEM*
Third-Party Synthetic API Ingestion without Insig	51	-	*Per 100,000 third-party synthetic result*	-		
HTTP Monitor without Insights	51	-	*Per 100,000 synthetic requests*	-	*5,069.89*	*per M DEM*
Log Management & Analytics - Ingest & Process	1,014	-	*Per 10,000 gibibytes*	-	*0.10*	*per GiB ingest*
Log Management & Analytics - Retain	355	-	*Per 1,000,000 gibibyte-days*	-		
Log Management & Analytics - Query	1,774	-	*Per 1,000,000 gibibytes-scanned*	-		
Events - Ingest & Process	1,014	-	*Per 10,000 gibibytes*	-	*0.10*	*per GiB ingest*
Events - Retain	355	-	*Per 1,000,000 gibibyte-days*	-		
Events - Query	1,774	-	*Per 1,000,000 gibibyte-scanned*	-		
Automation Workflow	659	-	*Per 10,000 workflow-hours*	-		
AppEngine Functions - Small	507	-	*Per 1,000,000 invocations*	-		
Custom Metrics Classic	101	-	*Per 100,000,000 metric data points*	-	*1,013.98*	*per M DDU*
Log Monitoring Classic	51	-	*Per 100,000,000 log records*	-		
Custom Traces Classic (OpenTelemetry)	71	-	*Per 100,000,000 spans*	-		
Custom Events Classic	101	-	*Per 100,000,000 custom events*	-		
Serverless Functions Classic	203	-	*Per 100,000,000 invocations*	-		

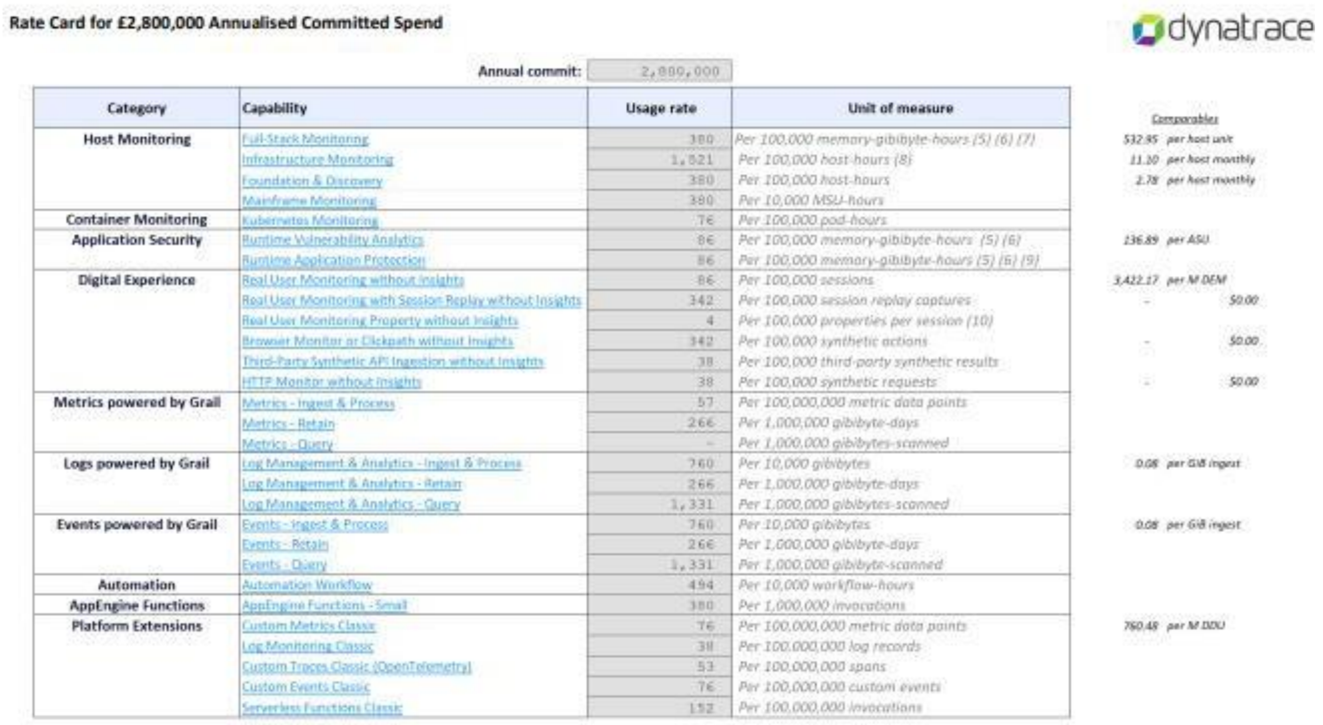


Rate Card for £2,000,000 Annualised Committed Spend

dynatrace

Annual commit: 2,000,000

Category	Capability	Usage rate	Unit of measure	Comparables
Host Monitoring	Full-Stack Monitoring	420	Per 100,000 memory-gibibyte-hours (5) (6) (7)	588.46 per host unit
	Infrastructure Monitoring	1,679	Per 100,000 host-hours (8)	12.26 per host monthly
	Foundation & Discovery	420	Per 100,000 host-hours	3.06 per host monthly
	Mainframe Monitoring	420	Per 10,000 MSU-hours	
Container Monitoring	Kubernetes Monitoring	84	Per 100,000 pod-hours	
Application Security	Runtime Vulnerability Analytics	94	Per 100,000 memory-gibibyte-hours (5) (6)	151.15 per ASU
	Runtime Application Protection	94	Per 100,000 memory-gibibyte-hours (5) (6) (9)	
Digital Experience	Real User Monitoring without Insights	94	Per 100,000 sessions	3,778.65 per M DEM
	Real User Monitoring with Session Replay without Insights	378	Per 100,000 session replay captures	- $0.00
	Real User Monitoring Property without Insights	4	Per 100,000 properties per session (10)	
	Browser Monitor or Clickpath without Insights	378	Per 100,000 synthetic actions	- $0.00
	Third-Party Synthetic API Ingestion without Insights	42	Per 100,000 third-party synthetic results	
	HTTP Monitor without Insights	42	Per 100,000 synthetic requests	- $0.00
Metrics powered by Grail	Metrics - Ingest & Process	63	Per 100,000,000 metric data points	
	Metrics - Retain	294	Per 1,000,000 gibibyte-days	
	Metrics - Query	–	Per 1,000,000 gibibytes-scanned	
Logs powered by Grail	Log Management & Analytics - Ingest & Process	840	Per 10,000 gibibytes	0.08 per GiB ingest
	Log Management & Analytics - Retain	294	Per 1,000,000 gibibyte-days	
	Log Management & Analytics - Query	1,469	Per 1,000,000 gibibytes-scanned	
Events powered by Grail	Events - Ingest & Process	840	Per 10,000 gibibytes	0.08 per GiB ingest
	Events - Retain	294	Per 1,000,000 gibibyte-days	
	Events - Query	1,469	Per 1,000,000 gibibyte-scanned	
Automation	Automation Workflow	546	Per 10,000 workflow-hours	
AppEngine Functions	AppEngine Functions - Small	420	Per 1,000,000 invocations	
Platform Extensions	Custom Metrics Classic	84	Per 100,000,000 metric data points	839.70 per M DDU
	Log Monitoring Classic	42	Per 100,000,000 log records	
	Custom Traces Classic (OpenTelemetry)	59	Per 100,000,000 spans	
	Custom Events Classic	84	Per 100,000,000 custom events	
	Serverless Functions Classic	168	Per 100,000,000 invocations	



Rate Card for £2,800,000 Annualised Committed Spend

Annual commit: 2,800,000

Category	Capability	Usage rate	Unit of measure	Comparables	
Host Monitoring	Full-Stack Monitoring	380	Per 100,000 memory-gibibyte-hours (5) (6) (7)	532.95	per host unit
	Infrastructure Monitoring	1,521	Per 100,000 host-hours (8)	11.10	per host monthly
	Foundation & Discovery	380	Per 100,000 host-hours	2.78	per host monthly
	Mainframe Monitoring	380	Per 10,000 MSU-hours		
Container Monitoring	Kubernetes Monitoring	76	Per 100,000 pod-hours		
Application Security	Runtime Vulnerability Analytics	86	Per 100,000 memory-gibibyte-hours (5) (6)	136.89	per ASU
	Runtime Application Protection	86	Per 100,000 memory-gibibyte-hours (5) (6) (9)		
Digital Experience	Real User Monitoring without Insights	86	Per 100,000 sessions	3,422.17	per M DEM
	Real User Monitoring with Session Replay without Insights	342	Per 100,000 session replay captures	-	$0.00
	Real User Monitoring Property without Insights	4	Per 100,000 properties per session (10)		
	Browser Monitor or Clickpath without Insights	342	Per 100,000 synthetic actions	-	$0.00
	Third-Party Synthetic API Ingestion without Insights	38	Per 100,000 third-party synthetic results		
	HTTP Monitor without Insights	38	Per 100,000 synthetic requests	-	$0.00
Metrics powered by Grail	Metrics - Ingest & Process	57	Per 100,000,000 metric data points		
	Metrics - Retain	266	Per 1,000,000 gibibyte-days		
	Metrics - Query	-	Per 1,000,000 gibibytes-scanned		
Logs powered by Grail	Log Management & Analytics - Ingest & Process	760	Per 10,000 gibibytes	0.08	per GiB ingest
	Log Management & Analytics - Retain	266	Per 1,000,000 gibibyte-days		
	Log Management & Analytics - Query	1,331	Per 1,000,000 gibibytes-scanned		
Events powered by Grail	Events - Ingest & Process	760	Per 10,000 gibibytes	0.08	per GiB ingest
	Events - Retain	266	Per 1,000,000 gibibyte-days		
	Events - Query	1,331	Per 1,000,000 gibibyte-scanned		
Automation	Automation Workflow	494	Per 10,000 workflow-hours		
AppEngine Functions	AppEngine Functions - Small	380	Per 1,000,000 invocations		
Platform Extensions	Custom Metrics Classic	76	Per 100,000,000 metric data points	760.48	per M DDU
	Log Monitoring Classic	38	Per 100,000,000 log records		
	Custom Traces Classic (OpenTelemetry)	53	Per 100,000,000 spans		
	Custom Events Classic	76	Per 100,000,000 custom events		
	Serverless Functions Classic	152	Per 100,000,000 invocations		