

AMENDMENT SIX
STATE TERM CONTRACT 204X
(IFB ITS-400277)

THIS AMENDMENT 6 is entered into by and between North Carolina Department of Information Technology (“DIT”), 3700 Wake Forest Road, Raleigh, NC 27609, and Cisco Systems, Inc. (“Cisco”), 170 W. Tasman Drive, San Jose, CA 95134 (“Vendor”).

The parties acknowledge they entered into a contract, IFB ITS-400277, in April 2019 to provide Cisco server, storage, and networking equipment, maintenance, and related professional services to the State of North Carolina. The contract was amended in May 2019 (Amendment 1) to correct a pricing error with the Minimum Percentage off List Discounts in Cisco Best and Final Offer Response to IFB ITS-400277. The contract was further amended in September 2020 (Amendment 2) to add the Cisco Universal Cloud Agreement and specific Cisco Cloud and SaaS product offerings, in December 2020 (Amendment 3) to add the Cisco Enterprise Agreement Program Terms and Conditions (“Cisco EA 2.0”), in April 2021 (Amendment 4) to add Cisco Duo and WebEx Cloud and SaaS product offerings, and again in June 2022 to add the Cisco Enterprise Agreement 3.0 Program Terms and Conditions (“Cisco EA 3.0”) (“Agreement”).

The parties now wish to amend the Agreement as follows:

- 1) Add the following Cisco Cloud and SaaS product offering (Licensor’s Agreement) to the 204X Agreement (Exhibit A):
 - Product Description for ThousandEyes Cloud Service (as modified herein)
 - Cisco Trust Documents consisting of Cisco Systems Information Data brief, Personal Data brief, Customer Content Data brief, and Information Security Exhibit Data Brief (as modified herein).
 - ThousandEyes-Cisco Catalyst 9000 Switches-Entitlements
 - ThousandEyes Privacy Data Sheet
 - ThousandEyes Support Services Policy (as modified herein)
 - ThousandEyes Service Level Agreement

- 2) The Licensor’s Agreement is modified by this Amendment, and therefore, conflicts arising among the terms of the Licensor’s Agreement and the terms of this Amendment shall be resolved by the following order of precedence:
 - a) This Amendment
 - b) Amendment Two (2) – Cisco Universal Cloud Agreement
 - c) BAFO ITS-400277
 - d) IFB ITS-400277 not superseded by the BAFO
 - e) The Licensor’s Agreement
 - f) Terms and other documents incorporated by reference in the Licensor’s Agreement

- 3) General modifications to the Cisco Licensor’s Agreement:
 - a) Applicable law, for the purpose of this Agreement and all services shall exclude laws of non-US jurisdictions, including but not limited to the European Union General Data Protection Regulation (“GDPR”) and its implementation in European Countries and the Asia-Pacific Economic Cooperation (“APEC”).
 - b) In the event of any conflict between Cisco Trust Documents, consisting of Cisco Systems

Information Data brief, Personal Data brief, Customer Content Data brief, and Information Security Exhibit Data brief, and the terms and conditions in Section 3(e) "SECURITY OF STATE DATA" of Amendment Two, those terms and conditions in Amendment Two shall take precedence.

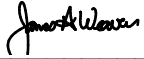
- 4) The following modification is made to the Product Description for ThousandEyes Cloud Service
 - a) Any reference to the "End User License Agreement or General Terms" shall be replaced with the "*Cisco Universal Cloud Agreement negotiated under Amendment Two to NC State Contract 204X (the "Agreement")*".
 - b) The hyperlink in Paragraph 6 Special Terms for the "Cisco DNA Software SD-WAN and Routing Matrices" shall have no force or effect as these Cisco product(s) are not offered pursuant to the NC State Contract 204X.
- 5) The following modification is made to the ThousandEyes Support Services Policy:
 - a) The first paragraph is modified as follows:

This ThousandEyes Support Services Policy (this "**Policy**") describes the policies and procedures under which Thousand Eyes, Inc. ("**ThousandEyes**", or "**we/us/our**") provides support services ("Support Services") to its customers (each, a "**Customer**" or "**you/your**"). Support Services are provided for the Service pursuant to the ~~separate subscription or license agreement~~ *Cisco Universal Cloud Agreement negotiated under Amendment Two to NC State Contract 204X between ThousandEyes Cisco and Customer* ("Subscription Agreement") and are subject to such Subscription Agreement and this policy. Support Services are provided for the Subscription Term. Capitalized terms not otherwise defined in this policy have the meanings given in the Subscription Agreement.
 - b) Notwithstanding any language to the contrary in the ThousandEyes Support Services Policy, in the event that the Vendor may be eligible to be reimbursed for travel expenses arising under the performance of this Agreement, reimbursement will be at the out-of-state rates set forth in GS §138-6; as amended from time to time.

Except as modified herein, the Agreement continues in effect as written and agreed.

Executed by authorized officials as of the day and date indicated below.

**State of North Carolina
Department of Information Technology**



Signature

Jim Weaver Secretary and State CIO

Printed Name of Signatory & Title

06/01/2023

Date

Cisco Systems, Inc.



Signature

Jenn Pate, Authorized Signatory

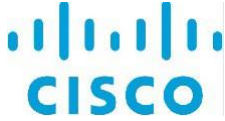
Printed Name of Signatory & Title

May 30, 2023

Date

APPROVED BY LEGAL

EXHIBIT A



Offer Description: ThousandEyes

This Offer Description (the “**Offer Description**”) describes the ThousandEyes cloud service (“**ThousandEyes**” or the “**Cisco Technology**”). Your use of the Cisco Technology is governed by this Offer Description and the Cisco End User License Agreement located at www.cisco.com/go/eula (or similar terms existing between you and Cisco) (the “**Agreement**”). If capitalized terms are not defined in this Offer Description, then they have the meaning given to them in the Agreement or order(s).

1. Description

The Cisco Technology is a suite of Cloud Services designed to help You measure and monitor the availability and performance of web applications, hosted services and networks. The Documentation describing the Cisco Technology in greater detail is located at: <https://docs.thousandeyes.com/>.

2. Data Protection and Use

Cisco processes, uses and protects all categories of data in connection with Your use of the Cisco Technology in accordance with applicable privacy and data protection laws, and as described in more detail at [Cisco’s Security and Trust Center](#). The [ThousandEyes Privacy Data Sheet](#) describes the specific Personal Data that Cisco collects and processes as part of the delivery of the Cisco Technology.

3. Support & Maintenance

During the Usage Term, ThousandEyes will provide support services as described in the Support Services Policy located at: <https://www.thousandeyes.com/legal/support>.

4. Embedded License Restrictions

If You receive license entitlements (“Capacity”) to the Cisco Technology under the Product ID “TE-EMBEDDED” (typically included as part of another Cisco offering, e.g., Cisco DNA Advantage or Cisco DNA Premier), You may only use such Capacity for tests generated from Enterprise Agent vantage points. You may not use such Capacity with Cloud Agents or any other vantage points. Enterprise Agents and Cloud Agents are both described in detail in the Documentation referenced above.

EXHIBIT A



Product Description for ThousandEyes Cloud Service

This Product Description is for the ThousandEyes Cloud Service platform (the “**Product**”) and is a part of the End User License Agreement or General Terms (as applicable) located at www.cisco.com/go/eula. Capitalized terms, unless defined in this document, have the meaning in the applicable agreement above. For clarity, this Product Description has historically been referred to as an Offer Description or Supplemental End User License Agreement. References to those documents should be interpreted as a reference to this Product Description.

1. Summary

The Product is a network intelligence platform, which is provided to You as a Cloud Service with optional cloud and on-premises agents (collectively, “Cloud Agents,” “Endpoint Agents”, and “Enterprise Agents” are referred to as “**Vantage Points**”). The Product is designed to help You measure and monitor the availability and performance of web applications, hosted services and networks as described in the Documentation at <https://docs.thousandeyes.com/>, which may be amended from time to time. The Product comprises several different visibility features (“**Paid Features**”), such as Network & App Synthetics, End User Monitoring, Internet Insights, etc., which enable You to customize the platform based on Your visibility needs. The Documentation provides further information on technical specifications, configuration requirements, features and functionalities related to the Product.

2. Usage Rights

2.1 Usage Rights. Your Usage Rights in the Product are based on one of the following metrics as more specifically described below:

Product	Metric	Duration
Enterprise Agents	Unit	Subscription
Cloud Agents	Unit	Subscription
Internet Insights	Package	Subscription
Endpoint Agents	User	Subscription

If You received Your Usage Rights as part of another Cisco offering, please see Section 6 below.

2.2 Limited Preview Features

From time to time, Cisco may add beta, limited preview, trial or other evaluation features to the Product for You to evaluate the new feature(s) (“**Limited Preview Features**”). Collectively, any Limited Preview Feature(s) will be considered “**Evaluation Software and Services**” and will be subject to the terms and conditions applicable to Evaluation Software and Services set forth in the End User License Agreement or General Terms (as applicable). In the context of this Product, Cisco may end the duration of the Limited Preview Features in its discretion.

3. Support and Other Services

EXHIBIT A

During the Usage Term, Cisco will provide support services as described in the Support Services Policy located at: <https://www.thousandeyes.com/legal/support>.

4. Performance Standards

This Product is subject to the Service Level Agreement (“SLA”) described in the Support Services Policy located at: https://www.thousandeyes.com/pdf/ThousandEyes_SLA.pdf. The SLA is subject to Your compliance with the terms and conditions of this Product Description and the End User License Agreement or General Terms (as applicable) and includes the sole and exclusive remedies stated in the SLA.

5. Data Protection

The Privacy Data Sheet (<https://trustportal.cisco.com/c/r/ctp/trust-portal.html#/1610384661419206>) describes the Personal Data that Cisco collects and processes as part of delivering the Product. For further details on how Cisco processes, uses and protects all categories of data, please visit Cisco’s [Security and Trust Center](#).

6. Special Terms

Additional License Restrictions - Receiving the Product as part of other Cisco Technology

Depending on Your purchase, You may receive Usage Rights to this Product as part of another purchase you have made with Cisco. The table below describes additional license restrictions that may apply to You.

Cisco Product ID	Additional License Restrictions
TE-EMBEDDED (Solely included as part of Cisco DNA Advantage for Catalyst 9300 and 9400.)	You may only use the Product for tests generated from Enterprise Agents and no other Vantage Point. The number of entitlements is further described here: ThousandEyes-Cisco-Catalyst-9000-Entitlements-Summary.pdf
TE-EMBED-WANI ThousandEyes WAN Insights (available as SD-WAN Predictive Path Recommendations) (Solely included as part of Cisco DNA Advantage or DNA Premier for SD-WAN .)	Your Usage Rights only entitle You to use and access the Product to generate a default ThousandEyes’ quality score using the measurement data from Your SD-WAN probes and the path recommendation that leverages the quality of the last seven days to recommend the best path (the "WAN Insights Functionality"). The number of supported applications or application categories included as part of Your entitlement is further described in the Cisco DNA Software SD-WAN and Routing Matrices . You will not have the right to use and access the Product’s other features – for example, You may not use the Product to run any tests from any Vantage Point as part of this Usage Right. The WAN Insights Functionality is not currently available in all geographies/regions including China, Hong Kong, and Macau; thus, even if the Product ID “TE-EMBED-WANI” has been enabled in Your Cisco Smart Software Manager Smart or Virtual account as part of Cisco SD-WAN entitlement, You will only have the right to use the WAN Insights Functionality in the geographies/regions where it is commercially available.

7. Additional Definitions

“Cloud Agents” means ThousandEyes’ cloud agent software maintained by ThousandEyes, distributed throughout the internet, and shared by our customers. Cloud Agents are described in more detail here: <https://docs.thousandeyes.com/product-documentation/global-vantage-points/cloud-agents>.

“Endpoint Agents” means ThousandEyes’ endpoint agent software that is installed on end user Windows or macOS machines to collect network and application layer performance data when Your users access specific websites from

EXHIBIT A

within Your monitored networks. Endpoint Agents are described in more detail here: <https://docs.thousandeyes.com/product-documentation/global-vantage-points/endpoint-agents>.

“Enterprise Agents” means ThousandEyes’ enterprise agent software deployed and managed by a You for Your exclusive use (in contrast to Cloud Agents, which are managed by ThousandEyes and shared by our customers), to test targets from inside Your network, or from within infrastructure within Your control. Enterprise Agents are described in more detail here: <https://docs.thousandeyes.com/product-documentation/global-vantage-points/enterprise-agents>.

“Package” means the collection of Internet Insights catalog entries with the same provider type and region as described in more detail here: [Terminology - ThousandEyes Documentation](#).

“Unit” means the unit of measurement required for tests from Cloud Agents or Enterprise Agents. Each test consumes a specific number of test units, based upon the test type and test configuration as described in more detail here: [How Unit Consumption Works - ThousandEyes Documentation](#).

“User” means, in the context of an Endpoint Agent, an internet-connected user of Endpoint Agents.

Systems Information

In order to give you, our customers, the full value of your Cisco products and services, we receive and use certain technical data and information about the operation and performance of your Cisco solutions, which we refer to as Systems Information. **Systems Information** means data generated or collected in connection with your use and operation of Cisco solutions, and data provided by you in connection with our delivery of products and services to you (including, for example, when you submit a request related to support services). Systems Information is composed of Telemetry Data, Support Data, Install Base Information, Entitlement Information, Customer Feedback and Security Threat Data, as defined further below.

Guiding Principles

- **Transparency** – We only use Systems Information for the purposes set out in the objectives noted below.
- **Trusted Ecosystem** – Systems Information that can be attributable to you is only shared within our trusted ecosystem, meaning the partners, distributors and contractors who help provide our solutions to you and who are also committed to protecting that data.
- **Customer Control** – There are certain products and services that require Systems Information in order to function and provide the solution to you. We will be transparent about these requirements so you may then choose whether or not to install or use the product, service or specific feature that requires that access. For other products and services, you may have the option to configure whether Systems Information is shared with us or the ability to decline our requests to provide Systems Information to us.
- **Restricted Data Types** – We recognize and respect that your Personal Data (also referred to as Personally Identifiable Information) and Customer Content are especially sensitive and require separate treatment specific to those data types. If any such Personal Data or Customer Content is incidentally received, we will treat that data as you would expect – as Personal Data or Customer Content, not as Systems Information – and always consistent with applicable law and your contracts or agreements with us. For more information on Personal Data, please see [here](#). For more information about Customer Content, please see [here](#).

How we use Systems Information

The following key objectives form the basis of how and when we use Systems Information:

Objective	Examples
1. Solution Delivery	Systems Information is used to operate our products and deliver services to you with critical and timely system insights, as well as to provide you with warranty coverage, technical support and similar services.
2. Accelerate Adoption	Systems Information is used to derive insights and analytics to help you achieve greater value from our solutions to enable your business objectives. These insights and analytics are critical to provide you with network consultation, recommendations, expert insights, analysis and training so you can utilize our products and services in a way that best meets your needs, improves your user experiences and applies a customer-focused quality of service.
3. Trusted Relationship	Systems Information is used to help us ensure that you receive what you purchased or are entitled to, including managing subscription renewals, validating and managing entitlement, trial use and similar activities. We also rely on Systems information to help enhance our relationships with you.
4. Solution Improvements	Our solutions must evolve and improve to meet our customers' changing needs. Systems Information is used to gain insights that show us how our solutions are working and being used. Based on these insights, we use Systems Information to modify and improve our solutions, as well as to develop new solutions.

For examples of how we use Systems Information to meet these key objectives, see [Table 2](#) below.

How we collect and generate Systems Information

We collect and generate Systems Information in a variety of ways, and we use this Systems Information solely to meet the objectives stated above. There are some products and services that require Systems Information to properly or fully function. There are other purchase arrangements, such as utility billing arrangements, that require us to collect Systems Information to determine usage. If you choose not to provide us with Systems Information, it may limit or prevent our ability to deliver the solutions you purchased and related advanced feature functions, security capabilities, services and other insights and analytics.

Systems Information Generated by our Products and Services

We may receive Systems Information from some of our products and services that generate Systems Information in the ordinary course of use (including, for example, by our instrumentation and logging systems).

Systems Information Collected by our Data Collection Tools

When you purchase and use certain Cisco products and services, we collect Systems Information through the use of data collection tools and related tools, such as Cisco's Common Services Platform Collector software, Cisco Software Subscription Manager, onsite hardware appliances, cloud-based software, or third party network collectors. When you install a data collection tool in your network, it securely communicates with network devices and directly transmits Systems Information back to us. While it is ultimately your choice whether or not to install and activate these data collection tools in your environment, these tools may be necessary and critical to providing services to you and operating products in your network.

Systems Information Provided by You

We sometimes receive Systems Information directly from you as part of our delivery of products and services. For instance, we may receive Support Data (as described in Table 1 below) and other Systems Information from you about the Cisco or third party products and solutions deployed in your network so we can provide support services, or help you plan, design, implement and optimize your network, etc.

How we share Systems Information

We sometimes need to share Systems Information with our trusted ecosystem of partners, distributors and contractors. If you purchase a solution through a Cisco partner, we may provide your partner or its distributor with the System Information needed to deliver and perform that solution, manage your subscription, and fulfill subscription billing and administrative activities, consistent with the objectives described above. We may also contract with service providers and share Systems Information necessary to operate and service our solutions. In each instance, each participant in our trusted ecosystem has agreed to confidentiality, applicable law and other requirements with us that are consistent with our commitments to you.

If the Systems Information does not identify a specific customer, such as when the Systems Information is effectively de-identified, then we may freely use and share Systems Information and related insights and analytics.

Data Protection and Information Security

We use information security best practices and controls to protect data in our possession. For further information about how Cisco protects, uses and shares data responsibly, including compliance with applicable laws, data breach notification, data storage, and our data protection requirements, please see [here](#). For information about how we respond to requests for information from governments and courts, please see [here](#).

Definitions and Examples

Table 1. Systems Information

Systems Information Sub-Categories	Definitions and Examples
<p>Telemetry Data</p>	<p>Data generated by instrumentation and logging systems created through the use and operation of the product or service.</p> <p>Examples:</p> <ul style="list-style-type: none"> • <i>Product Identification</i>. Cisco product serial numbers and other identification information. Information characterizing devices connected to a network. • <i>Sensor Data</i>. Data generated by sensors, devices and machinery, product or service features or functionality activated, accessed or utilized. • <i>Configuration Data</i>. Network policy, hardware module and software components installed, connections and topology relationships between products. • <i>Cookies and Beacons</i>. Data relating to the existence of cookies, web beacons, and other similar applications. • <i>Application Information</i>. The types of Cisco software or applications installed on a network or device. • <i>Network, Software and Cloud Traffic</i>. Data related to the usage, origin of use, traffic density and patterns. Behavior of workloads, and applications across a network or cloud service.

Support Data	Data we collect when you submit a request for support services or other troubleshooting, including information about hardware, software and other details related to the support incident.
Install Base Information	Types, quantities and location of installed Cisco devices, products, or software releases.
Entitlement Information	Software license, warranty, cloud and service subscription information.
Customer Feedback	Technical data or suggestions contained in oral or written communications you provide us regarding modifications or improvements to a product or service.
Security Threat data	Threat intelligence data, URLs, metadata, net flow data, origin and nature of malware and other information necessary to enable security features of a product or service.

Table 2. Objectives

The following is a representative, but not exhaustive, list of the objectives for which we use Systems Information:

Objective	Examples
Solution Delivery	<ul style="list-style-type: none"> • Critical support actions, recommendations. Reactive, Proactive and Predictive problem detection and remediation, insights and analytics. • Automation and orchestration of lifecycle services: migration, development, test, release, operations. • Solution integration to customer business and IT processes.
Accelerate Adoption	<ul style="list-style-type: none"> • Product usage, feature usage, application interaction, • Selecting relevant learning and training content. • Planning and readiness for new technology evaluation and deployment • Recommendations to maximize solution value and return on investment.
Trusted Relationship	<ul style="list-style-type: none"> • Support coverage, and entitlement assurance and renewal eligibility. • Notification of known product security vulnerabilities, field notices and bugs • Verification of system integrity, authentic system hardware signature and signed/ encrypted software signatures. • Recommendations regarding changes to or new products and services.
Solution Improvements	<ul style="list-style-type: none"> • Product innovation, software updates, development of new features and offers, threat intelligence detection improvements. • Serviceability and product quality improvements aligned to customer satisfaction.

Personal Data

Cisco is committed to protecting and respecting Personal Data, no matter where it comes from or where it flows. When we refer to Personal Data (also referred to as Personally Identifiable Information) we mean any information relating to an identified or identifiable natural person (for more information click [here](#)).

Our [Global Personal Data Protection and Privacy Policy](#) demonstrates our commitment to protecting Personal Data and complying with applicable laws regarding Personal Data. In that Policy, we commit to the following principles regarding Personal Data:

- **Fairness.** We will process Personal Data in a lawful, legitimate, and transparent manner.
- **Purpose Limitation.** We will only collect Personal Data for specific, explicit, and legitimate purposes. Any subsequent processing should be compatible with those purposes, unless we have obtained the individual's consent, or the processing is otherwise permitted by law.
- **Proportionality.** We will only process Personal Data that is adequate, relevant, and not excessive for the purposes for which it is processed.
- **Data Integrity.** We will keep Personal Data accurate, complete, and up-to-date as is reasonably necessary for the purposes for which it is processed.
- **Data Retention.** We will keep Personal Data in a form that is personally identifiable for no longer than necessary to accomplish the purposes, or other permitted purpose(s), for which the Personal Data was obtained.
- **Data Security.** We will implement appropriate and reasonable technical and organizational measures to safeguard Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, use, or access. We will instruct and contractually require third parties processing Personal Data on behalf of Cisco, if any, to: (a) process it only for purposes consistent with Cisco's purposes for processing; and (b) implement appropriate technical and organizational measures to safeguard the Personal Data.
- **Individual Rights.** We will process Personal Data in a manner that respects individuals' rights under applicable data protection laws.
- **Accountability.** We will implement appropriate governance, policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of Personal Data is in accordance with our Global Personal Data Protection and Privacy Policy and applicable data protection laws.

Why we process Personal Data

The following key objectives form the basis of how and when we use Personal Data:

Objective	Summary
Solution Delivery	Personal Data may be used to operate our products and deliver services to you with critical and timely system insights. For example, our Cloud offers depend on proper user authentication. Personal Data is also needed for us and our partners to provide you with warranty support, technical support and other services.
Accelerate Adoption	Our products and services contain various features that you can employ to best address your business objectives. We work closely with your organization to accelerate your time to realize the value of our products and services, provide consultation, recommendations, expert insights, analysis and training so you can best utilize the many features of our products and services in a way that best meets your needs.
Trusted Relationship	We view ourselves as a trusted advisor to you and maintain a number of relationships within your organization. We need these contacts for a number of purposes, such as to advise and guide you in your buying decisions, to keep you up to date on renewals, and to ultimately help you transact business with us and your partners or distributors (if any).
Solution Improvements	Our solutions must evolve and improve to meet our customers' changing needs. These improvements are guided by the insights gained from Systems Information that show us how our solutions are working and being used. If Personal Data is received in connection with Systems Information, we will treat that data as you would expect - as Personal Data, not as Systems Information - and always consistent with applicable law and your contracts or agreements with us.

Our Privacy Data Sheets and Privacy Data Maps

We maintain Privacy Data Sheets and Privacy Data Maps on the [Cisco Trust Portal](#) for specific products and services that provide you with additional information such as what Personal Data we process, where and for how long we store the information, and what sub-processors we may use.

Our Master Data Protection Agreement

When Cisco is acting as data processor (i.e. managing Personal Data on behalf of our customers), our Master Data Protection Agreement (MDPA), applicable Privacy Data Sheets and our Online Privacy Statement provide details about our commitments regarding our processing of Personal Data when you use our products and services. Our MDPA is publicly available on the Cisco Trust Center ([here](#)). Key elements in the MDPA include:

- terms and conditions consistent with the principles in this document that will govern the processing of Personal Data;
- technical and organizational security measures that will be implemented to minimize the risk of accidental loss, destruction, alteration, unauthorized disclosure, unauthorized access, or unlawful destruction of Personal Data; and
- incorporation of the European Union Standard Contractual Clauses, and APEC Cross Border Privacy Rules system requirements for international data transfers.

Our Online Privacy Statement

When you access our websites or use one of our solutions, our [Online Privacy Statement](#) describes how we handle Personal Data and provides the choices available to you regarding our collection, use, and access to that information.

Sharing Personal Data

We require our suppliers and contractors to adhere to applicable data protection laws and terms and conditions consistent with the principles in this document when handling Personal Data on our behalf by signing our Supplier MDPA, which is publicly available [here](#).

Similarly, we require all of our partners and distributors to comply with applicable laws, including privacy and data protection laws, and the confidentiality provisions in our agreement with them.

How Individuals can control their Personal Data

We respect the rights of individuals regarding their Personal Data. We provide a [Cisco Profile Management Tool](#) that allows you to view, edit and set the preferences related to the Personal Data in for your Cisco profile. We also provide a [Privacy Request Form](#) to assist you and your end users with any inquiries about your Personal Data and process requests, such as to opt-out from communications etc.

Our Information Security Program

We maintain a robust Information Security Program. For detailed information, please click [here](#).

Data Transfer Mechanisms

We have invested in the following transfer mechanisms when transferring Personal Data across jurisdictions:

- [EU Standard Contractual Clauses](#)
- [Binding Corporate Rules](#) for Controllers
- Binding Corporate Rules for Processors (pending approval)
- [APEC Cross Border Privacy Rules](#)
- [APEC Privacy Recognition for Processors](#)

Breach Notification Processes

The Data Protection & Privacy team within Cisco's Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. Our Incident Commander directs and coordinates our response, using diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG). For additional information regarding our breach notification process, please see Cisco's MDPA [here](#).

Customer Content

As part of your use of Cisco solutions, we understand there are times when you will share Customer Content with us. Customer Content means data such as text, audio, video or image files, provided by you to Cisco in connection with your use of Cisco solutions, and data developed at your specific request related to a statement of work or contract. For more examples of Customer Content, see the Examples table below.

Guiding Principles

- **Transparency** – We recognize that your Customer Content shall be treated confidentially and requires separate treatment from Systems Information and other data types.
- **Trusted Ecosystem** – If we are required to share Customer Content to accomplish the purposes for which it was provided to us, then it will only be shared within our trusted ecosystem, meaning the distributors, partners and contractors, as necessary to accomplish those purposes.
- **Customer Control** – Customer Content will be used solely for the purposes you provided it to us for. We will work with you to identify, limit and manage what Customer Content is provided to us.
- **Restricted Data Types** – To the extent that any Customer Content is also considered Personal Data under applicable law or otherwise cannot be separated from Personal Data, we will treat Personal Data according to applicable law and your contracts or agreements with us. For more information on Personal Data, [here](#).

Why we use Customer Content

The following key objectives form a basis on how and when we use and share any Customer Content:

Objective	Summary
1. Solution Delivery	You may provide us with Customer Content so we can provide security threat protection and other solutions. You may also provide Customer Content, such as log, configuration or firmware files, or core dumps, taken from a product and provided to us so we can deliver services such as TAC support, product implementation, business process automation and other services.

2. Accelerate Adoption	You may provide us with Customer Content so we may provide you with insights, analytics and recommendations to help you achieve greater value from our solutions to enable your business objectives.
3. Trusted Relationship	You may provide us with Customer Content so that we may assist you with system design, context for troubleshooting, and purchase decisions.
4. Solution Improvements	We do not use Customer Content for solution improvement or development. We use it solely as outlined herein.

Sharing Customer Content

There may be limited reasons for sharing Customer Content. For example, if a product or service you are using includes a hosting or other third party service element, your Customer Content may be hosted or shared with that third party for that reason. These third party contractors will be required to meet our information security requirements before receiving this data. Otherwise, we will not share Customer Content without your prior consent.

Our Information Security Program

We use information security best practices and controls. For further information about how Cisco protects, uses and shares data responsibly, including compliance with applicable laws, data breach notification, data storage, and our data protection requirements, please click [here](#). For information about how we respond to requests for information from governments and courts, please see [here](#).

Examples of Customer Content

The following is a representative, but not exhaustive, list of Customer Content examples:

Examples
Webex Meetings recordings
Cisco and Meraki Smart Camera video recordings
Webex Teams rooms content

Data Brief:

Information Security Exhibit

1. Scope

This document describes the technical and organizational security measures that shall be implemented by Cisco to secure Personal Data, Customer Content and Systems Information (collectively, “Data”) prior to any processing under the Agreement.

2. General Security Practices

Cisco has implemented and shall maintain appropriate technical and organizational measures designed to protect Data against accidental loss, destruction or alteration, unauthorized disclosure or access, or unlawful destruction, including the policies, procedures, and internal controls set forth in this document for its Representatives, facilities, and equipment at Cisco’s locations involved in Cisco’s performance of its obligations under the Agreement.

3. General Compliance

- 3.1. Compliance.** Cisco shall document and implement processes to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security or other security requirements. Such processes shall be designed to provide appropriate security to protect Data given the risk posed by the nature of the Data processed by Cisco. Cisco shall implement and operate information security in accordance with Cisco’s own policies, which shall be no less strict than the information security requirements set forth in this document.
- 3.2. Protection of logs and records.** Cisco shall implement appropriate procedures designed to protect logs and records from loss, destruction, falsification, unauthorized access, and unauthorized release, in accordance with legislative, regulatory, and contractual requirements.
- 3.3. Review of information security.** Cisco’s approach to managing information security and its implementation shall be reviewed at planned intervals or when significant changes occur by appropriate internal or external assessors.
- 3.4. Compliance with security policies and standards.** Cisco’s management shall regularly review the compliance of information processing and procedures with the appropriate applicable security policies and standards.
- 3.5. Technical compliance review.** Cisco shall regularly review information systems for compliance with Cisco’s information security policies and standards.

- 3.6. Information Risk Management (“IRM”).** Cisco shall implement and utilize an appropriate information risk management process to frame, assess, respond and monitor risk, consistent with applicable contractual and legal obligations. Threat and vulnerability assessments must be reviewed periodically and prompt remediation actions taken where material weaknesses are found.
- 3.7. Processing of Sensitive Personal Data.** To the extent that Cisco processes Sensitive Personal Data and the security measures referred to in this document are deemed to provide insufficient protection, Customer may request that Cisco implement additional security measures.

4. Technical and Organizational Measures for Security

4.1. Organization of Information Security

- a. Security Ownership.** Cisco shall appoint one or more security officers responsible for coordinating and monitoring the security requirements and procedures. Such officers shall have the knowledge, experience, and authority to serve as the owner(s) of, with responsibility and accountability for, information security within the organization.
- b. Security Roles and Responsibilities.** Cisco shall define and allocate information security responsibilities in accordance with Cisco’s approved policies for information security. Such policies (or summaries thereof) shall be published and communicated to employees and relevant external parties required to comply with such policies.
- c. Project Management.** Cisco shall address information security in project management to identify and appropriately address information security risks.

4.2. Human Resources Security

- a. General.** Cisco shall ensure that its personnel are subject to confidentiality obligations and shall provide adequate training about relevant privacy and security policies and procedures. Cisco shall further inform its personnel of possible consequences of breaching Cisco’s security policies and procedures, which must include disciplinary action, including possible termination of employment for Cisco’s employees and termination of contract or assignment for relevant external Representatives (e.g., contractors, agents, consultants etc.).
- b. Training.** Representatives with access to Data shall receive appropriate, periodic (i.e., at least annual) education and training regarding privacy and security procedures to aid in the prevention of unauthorized use (or inadvertent disclosure) of Data and training regarding how to effectively respond to security incidents. Training shall be provided before Representatives are granted access to Data or begin providing Services. Training shall be regularly reinforced through refresher training courses, emails, posters, notice boards, and other training and awareness materials.
- c. Background Checks.** Cisco shall require criminal and other relevant background checks for Representatives in compliance with mandatory applicable law and Cisco’s policies.

4.3. Access Controls

- a. Access.**
- i. Limited Use. Cisco will not (i) access the Customer’s computer systems for any purpose other than as necessary to perform its obligations under the Agreement or as otherwise agreed to by the parties; or (ii) use any system access information or log-in credentials to gain unauthorized access to Data or Customer’s systems, or to exceed the scope of any authorized access.

- ii. Authorization. Cisco shall restrict access to Data and systems at all times solely to those Representatives whose access is necessary.
 - iii. Suspension or Termination of Access Rights. At Customer's reasonable request, Cisco shall promptly and without undue delay suspend or terminate the access rights to Data and systems for any Representatives reasonably suspected of breaching any of the provisions of this document; and Cisco shall remove access rights of all Cisco employees and relevant external parties upon suspension or termination of their employment or engagement.
 - iv. Information Classification. Cisco shall classify, categorize, and/or tag Data to help identify it and to allow for access and use to be appropriately restricted.
- b. Access Policy.** Cisco shall determine appropriate access control rules, rights, and restrictions for each specific user's roles towards their assets. Cisco shall maintain a record of security privileges of Representatives that have access to Data, networks, and network services. Cisco shall restrict the use of utility programs that might be capable of overriding system and application controls.
- c. Access Authorization**
- i. Cisco shall have user account creation and deletion procedures, with appropriate approvals, for granting and revoking access to its systems and networks. Cisco shall use an enterprise access control system that requires revalidation of Representatives by managers at regular intervals based on the principle of "least privilege" and need-to-know criteria based on job role.
 - ii. Cisco shall maintain and update a record of its users authorized to access systems that contain Data and Cisco shall review such users' access rights at regular intervals.
 - iii. For systems that process Data, Cisco shall revalidate (or where appropriate, deactivate) access of Representatives who change Cisco reporting structure and deactivate authentication credentials that have not been used for a period of time not to exceed six (6) months.
 - iv. Cisco shall restrict access to program source code and associated items such as software object code, designs, specifications, verification plans, and validation plans, to prevent the introduction of unauthorized functionality and to avoid unintentional changes.
- d. Network Design.** For systems that process Data, Cisco shall have controls to avoid Representatives assuming access rights that could be used to gain unauthorized access to Data.
- e. Least Privilege.** Cisco shall limit Representatives' access to Data to those Representatives who have an actual need to access such Data to perform their assigned duties.
- f. Authentication**
- i. Cisco shall use industry standard practices including ISO/IEC 27002:2013 and NIST SP 800-63B (Digital Identity Guidelines) to identify and authenticate users who attempt to access information systems.
 - ii. Where authentication mechanisms are based on passwords, Cisco shall require the password to conform to strong password control parameters (e.g., length, character complexity, and/or non-repeatability) with at least 8 characters and containing the following four classes: upper case, lower case, numeral, special character.

- iii. Cisco shall maintain industry standard procedures to prevent de-activated or expired identifiers and log-in credentials from being granted to other individuals.
- iv. Cisco shall monitor repeated failed attempts to gain access to its information systems.
- v. Cisco shall maintain industry standard procedures to deactivate log-in credentials that have been corrupted or inadvertently disclosed.
- vi. Cisco shall use industry standard log-in credential protection practices, including practices designed to maintain the confidentiality and integrity of log-in credentials when they are assigned and distributed, and during storage (e.g., log-in credentials shall not be stored or shared in plain text). Such practices shall be designed to ensure strong, confidential log-in credentials.
- vii. Cisco shall implement a multi-factor authentication solution to authenticate Representatives accessing its information systems.

4.4. Physical and Environmental Security

a. Physical Access to Facilities

- i. Cisco shall limit access to facilities where systems that process Data are located to authorized individuals.
- ii. Security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.
- iii. Facilities shall be monitored and access-controlled at all times (24x7).
- iv. Access shall be controlled through key card and/or appropriate sign-in procedures for facilities with systems processing Data. Cisco must register authorized individuals and require them to carry appropriate identification badges.

b. Physical Access to Equipment. Cisco equipment used to process Data shall be protected using industry standard processes to limit access to authorized Representatives.

c. Protection from Disruptions. Cisco shall implement appropriate measures designed to protect against loss of data due to power supply failure or line interference.

d. Clear Desk. Cisco shall have policies requiring a “clean desk/clear screen” designed to prevent inadvertent disclosure of Data.

4.5. Operations Security

a. Operational Policy. Cisco shall maintain written policies describing its security measures and the relevant procedures and responsibilities of Representatives who have access to Data and to its systems and networks. Cisco shall communicate its policies and requirements to all Representatives involved in the processing of Data. Cisco shall implement the appropriate management structure and control designed to maintain compliance with such policies and with mandatory applicable law concerning the protection and processing of Data.

b. Security and Processing Controls.

- i. **Areas.** Cisco shall maintain, document, and implement standards and procedures to address the configuration, operation, and management of systems and networks that process Data.

- ii. **Standards and Procedures.** Such standards and procedures shall include security controls, identification and patching of security vulnerabilities, change control process and procedures, and incident prevention, detection, remediation, and management.
- c. **Logging and Monitoring.** Cisco shall maintain logs of administrator and operator activity and data recovery events related to Data.

4.6. **Communications Security and Data Transfer**

- a. **Networks.** Cisco shall, at a minimum, use the following controls to secure its corporate networks that process Data:
 - i. Network traffic shall pass through firewalls, which are monitored at all times. Cisco must implement intrusion detection systems and/or intrusion prevention systems.
 - ii. Anti-spoofing filters and controls must be enabled on routers.
 - iii. Network, application, and server authentication passwords are required to meet the same industry standard practices used for the authentication of users set forth in Section 4.34.3.f above (Authentication). System-level passwords (privileged administration accounts or user-level accounts with privileged administration access) must be changed at minimum every 90 days.
 - iv. Initial user passwords are required to be changed at first log-on. Cisco shall have a policy prohibiting the sharing of user IDs, passwords, or other log-in credentials.
 - v. Firewalls must be deployed to protect the perimeter of Cisco's networks.
- b. **Virtual Private Networks ("VPN").** When using VPN to remotely connect to the Customer's or Cisco's network for processing of Data:
 - i. Connections must be encrypted using industry standard cryptography.
 - ii. Connections shall only be established using VPN servers.
 - iii. The use of multi-factor authentication is required.
- c. **Data Transfer.** Cisco shall have formal transfer policies in place to protect the transfer of Data through the use of all types of communication facilities that adhere to the requirements of this document. Such policies shall be designed to protect transferred Data from unauthorized interception, copying, modification, corruption, routing and destruction.

4.7. **System Acquisition, Development, and Maintenance**

- a. **Security Requirements.** Cisco shall adopt security requirements for the purchase, use, or development of information systems, including for application services delivered through public networks.
- b. **Development Requirements.** Cisco shall have policies for secure development, system engineering, and support. Cisco shall conduct appropriate tests for system security as part of acceptance testing processes. Cisco shall supervise and monitor the activity of outsourced system development.

4.8. **Penetration Testing and Vulnerability Scanning & Audit Reports**

- a. **Testing.** Cisco will perform periodic vulnerability scans and penetration tests on its internet perimeter network. These scans and tests will be conducted by qualified professionals, including

among other entities, Cisco's independent internal compliance team, using industry standard tools and methodologies.

- b. Audits and Certifications.** Cisco shall cooperate with reasonable requests by Customer for legally required security audits (subject to mutual agreement on the time, duration, place, scope and manner of the audit), and respond to reasonable requests for testing reports. Cisco shall make available to Customer, upon written request and without undue delay, copies of any third party audit reports or certifications it maintains (such as SSAE 16 – SOC1, SOC2, SOC3 attestations or ISO 27001:2013 certifications (or their equivalent under any successor standards)) that apply to the Service, to the extent that Cisco maintains such certifications in its normal course of business. Customer shall treat the contents of reports related to Cisco's security and certifications as confidential information.
- c. Remedial Action.** If any penetration test or vulnerability scan referred to in Section 4.8.a above reveals any deficiencies, weaknesses, or areas of non-compliance, Cisco shall promptly take such steps as may be required, in Cisco's reasonable discretion, to address material deficiencies, weaknesses, and areas of non-compliance as soon as may be practicable considering Cisco's prioritization of such, based upon their criticality (e.g. nature, severity, likelihood).
- d. Status of Remedial Action.** Upon request, Cisco shall keep Customer reasonably informed of the status of any remedial action that is required to be carried out, including the estimated timetable for completing the same.

4.9. Contractor Relationships

- a. Policies.** Cisco shall have information security policies or procedures for its use of external Representatives that impose requirements consistent with this document.
- b. Monitoring.** Cisco shall monitor and audit service delivery by its external Representatives and review its external Representatives' security practices against the security requirements set forth in Cisco's agreements with such Representatives.

4.10. Management of Data Breaches and Improvements

- a. Responsibilities and Procedures.** Cisco shall establish procedures to ensure a quick, effective, and orderly response to Data Breaches.
- b. Reporting Data Breaches.** Cisco shall implement procedures for Data Breaches to be reported as appropriate. Representatives should be made aware of their responsibility to report Data Breaches as quickly as reasonably possible.
- c. Reporting Information Security Weaknesses.** Cisco's Representatives are required to note and report any observed or suspected information security weaknesses in systems or services.
- d. Assessment of Information Security Events.** Cisco shall have classification scale in place in order to decide whether an information security event should be classified as a Data Breach.
- e. Response Process.** Cisco shall maintain a record of Data Breaches with a description of the incident, the effect of the incident, the name of the reporter and to whom the incident was reported, the procedure for rectifying the incident, and the remedial action taken to prevent future security incidents.

4.11. Information Security Aspects of Business Continuity Management

- a. **Planning.** Cisco shall maintain emergency and contingency plans for the facilities where Cisco information systems that process Data are located. Cisco shall verify the established and implemented information security continuity controls at regular intervals.
- b. **Data Recovery.** Where and as applicable, Cisco shall design redundant storage and procedures for recovering Data in its possession or control in a manner sufficient to reconstruct Data in its original state as found on the last recorded backup provided by the Customer or in a manner sufficient to resume the Service.

5. Definitions

- 5.1. **“Affiliates”** means companies within the Cisco group that may process Data in order to provide the Products and/or Services. Such Affiliates include Cisco Systems, Inc., Cisco Commerce India Private Limited, Cisco Systems G.K., Cisco Systems Australia Pty Limited, Cisco Systems Canada Co., Cisco International Limited, Cisco Systems (Italy) S.R.L., Cisco Systems International B.V., ThousandEyes LLC, Broadsoft, Inc., AppDynamics LLC, AppDynamics International Ltd. and Meraki LLC. Unless otherwise explicitly agreed by the Parties, any legal entities which become part of the Cisco group of companies through an acquisition or merger are not considered Affiliates for the purposes of this document.
- 5.2. **“Agreement”** means the written or electronic agreement between Customer and Cisco or the relevant Cisco Affiliate for the provision of the Services and/or Products to Customer.
- 5.3. **“Customer Content”** means data such as text, audio, video or image files, provided by you to Cisco in connection with your use of Cisco solutions, and data developed at your specific request related to a statement of work or contract.
- 5.4. **“Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Data relating to you.
- 5.5. **“Personal Data”** means any information about, or relating to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual, natural person.
- 5.6. **“Product”** means Cisco or its Affiliates’ branded hardware and software that is purchased under the Agreement.
- 5.7. **“Representatives”** means Cisco’s or its Affiliates’ officers, directors, employees, agents, contractors, temporary personnel, subcontractors and consultants.
- 5.8. **“Service”** means Cisco or its Affiliates’ branded service offering that is purchased by Customer under the Agreement.
- 5.9. **“Sensitive Personal Data”** refers to sensitive personal information (as defined under the California Consumer Protection Act), special categories of personal data (as described in Article 9 of the General Data Protection Regulation), and other similar categories of Personal Data that are afforded a higher level of protection under applicable law.
- 5.10. **“Systems Information”** means data generated or collected in connection with your use and operation of Cisco solutions, and data provided by you in connection with our delivery of products and services to you (including, for example, when you submit a request related to support services). Systems Information is composed of Telemetry Data, Support Data, Install Base Information, Entitlement Information, Customer Feedback and Security Threat Data as defined further [here](#).



ThousandEyes is
now part of Cisco.



ThousandEyes with Cisco Catalyst 9000 Switches

Each Catalyst 9300 or 9400 Cisco DNA Advantage subscription entitles each Customer Organization (as defined below) to run the equivalent of 22 units per month of network or web test capacity, not to exceed the maximum of 110,000 units per month of ThousandEyes test capacity per Customer Organization, regardless of the number of purchased Cisco DNA Advantage licenses. A ThousandEyes network or web test every can run every 5 minutes subject to the foregoing. For example only, if customer has 10 DNA Advantage licenses, then customer may run up to 220 units of network or web test capacity. ThousandEyes Cloud Agent access is not included in the Cisco DNA license entitlement. Test capacity can be increased and Cloud Agents accessed with purchase of additional ThousandEyes Network and Application Synthetics. The Cisco DNA license entitlements will ONLY be provisioned in Customer Organizations on the usage billing model. Customer Organizations on the legacy metered billing model are ineligible. "Customer Organization" means Customer and its Affiliates (as defined in the Cisco End User License Agreement) collectively who are Cisco DNA Advantage license holders.



ThousandEyes is
now part of Cisco.



ThousandEyes

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) in the ThousandEyes service (“ThousandEyes Service”) by ThousandEyes and its affiliates (“ThousandEyes”).

ThousandEyes is a cloud-based internet and cloud intelligence platform that enables infrastructure and operations teams to proactively monitor internet-enabled networks and applications. The platform is made available by Cisco to companies or persons who acquire it for use by their authorized users.

Cisco will process personal data from ThousandEyes Service in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Cisco is the Data Controller for the personal data processed to administer and manage the customer relationship. Cisco is the Data Processor for the personal data processed by ThousandEyes in order to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the [Cisco Online Privacy Statement](#).

1. Overview

The ThousandEyes Service combines a variety of active and passive monitoring techniques to give organizations deep insight into user experience across the applications and services the organization provides and consumes. The ThousandEyes Service leverages its expansive Internet monitoring data set to help provide real-time Internet outage detection, powered by collective intelligence.

The ThousandEyes Service may collect personal data using the following products:

Web Platform: The ThousandEyes Service web platform is the primary user interface for the ThousandEyes Service, and as such, it stores the login credentials for any users authorized by the customer administrator, including usernames, email addresses, and passwords for the purpose of authentication and email delivery. For security audit purposes, user email addresses and their IP addresses are captured in the system and application logs.

Cloud Agents: Cloud Agents are testing nodes situated in the cloud around the world, operating in over 175 cities and 54 countries. Customer-configured tests running from each node provide performance data which simulates end-user experience, gathered from local transit providers and last-mile ISPs. Cloud Agents are generally used to monitor the public internet but may process personal information if tests configured by the customer include personal information.

Enterprise Agents: Enterprise Agents are equivalent to Cloud Agents but are hosted in customer-controlled environments. Customers are able to configure tests to monitor the health of their network infrastructure and the performance of key applications from their networks across the public internet. Enterprise Agents are most commonly installed in branch sites and within data centers to provide a detailed understanding of wide area networks, internet connectivity, and latency. As with Cloud Agents, Enterprise Agent may process personal information if tests configured by the customer includes such information.

Endpoint Agents: Endpoint Agents are software testing agents deployed by customers on computers within their organization to help troubleshoot network and application performance. Customer's administrators configure the tests, which specify the types and sources of information collected by the Endpoint Agents. The test results (e.g., page load time) are uploaded to the customer's account on the ThousandEyes platform. If so configured by a customer, Endpoint users may also manually record data performance metrics by targeting a specified domain. Endpoint Agent may process the following personal information: end-user computer name, name of logged-in user, IP address, metro area location information derived from the IP address, and any personal information included or resulting from customer-configured tests.

The Customer can configure the Endpoint Agent to collect data in four ways:

1. Automatic data collection: The Endpoint Agent will gather performance data associated with the end-user's browsing session when the computer is operating within networks selected by customer administrators, and the end-user visits a website which is selected for monitoring by customer administrators.
2. Manual data collection: The end-user can initiate data collection from within Google Chrome by clicking the ThousandEyes logo in the extension toolbar. While the Endpoint Agent is recording the browsing session, the top of the page will show a banner indicating that the ThousandEyes Service Endpoint Agent is debugging the tab. To stop recording, simply click the ThousandEyes logo in the toolbar, or click the Cancel button on the banner.
3. Scheduled data collection: The Endpoint Agent may be configured to collect data about network and application performance to specified destinations at regular intervals, as defined by the customer's administrator.
4. Instant test data collection: To provide rapid assistance when troubleshooting, a customer administrator can initiate a test immediately. This test will run straight away without waiting for a scheduled event. The data collected is identical to a scheduled test.

Endpoint Agent Pulse: Endpoint Agent Pulse is typically used by customers to troubleshoot connectivity into unmanaged networks, such as their client sites or employee-owned devices. Customer's administrators configure the tests, which specify the types and sources of information collected by the Endpoint Agent Pulse. The test results (e.g. availability, response time) are uploaded to the customer's account on the ThousandEyes platform. Endpoint Agent Pulse may process the following personal information: end-user computer name, IP address, metro area location information derived from the IP address, and any personal information included or resulting from customer-configured tests.

The customer can configure Endpoint Agent Pulse to collect data in two ways:

1. Scheduled data collection: The Endpoint Agent may be configured to collect data about network and application performance to specified destinations at regular intervals, as defined by the customer's administrator.
2. Instant test data collection: To provide rapid assistance when troubleshooting, a customer administrator can initiate a test immediately. This test will run straight away without waiting for a scheduled event. The data collected is identical to a scheduled test.

WAN Insights: WAN Insights is a SaaS-based solution that enables customers to improve quality of experience of applications in their Cisco SD-WAN network. The solution uses data from compatible Cisco routers enabled by [vAnalytics](#) to make predictions on potential connectivity issues and recommends an alternate path for the supported applications. With WAN Insights, customers have visibility to supported applications on a dashboard, including:

1. potential violations of application experience thresholds; and
2. alternate path recommendations.

WAN Insights processes the vAnalytics data to the extent enabled by the Customer administrators.

ThousandEyes integrates with various Cisco products. Please see the SD-WAN Cloud [Privacy Data Sheet](#) for details regarding processing of personal data by the Cisco vAnalytics feature.

2. Personal Data Processing

The table below lists the personal data used by the ThousandEyes Service to carry out the services and describes why the ThousandEyes Service processes the data.

Personal Data Category	Types of Personal Data	Purpose of Processing
Registration Data	<ul style="list-style-type: none"> User email address User first and last name User Password User IP address Billing contact name 	<ul style="list-style-type: none"> Activation of service Billing/invoicing Product notifications Technical support Authentication/Authorization Activity logs
Support Information	<ul style="list-style-type: none"> First name, Last name, Email, Phone number of the individual opening the service request Customer account information 	<ul style="list-style-type: none"> Technical support Review of the support service quality Troubleshooting Analysis of service
Application credentials	<ul style="list-style-type: none"> Credentials used by Cloud and Enterprise agents to execute web transaction tests 	<ul style="list-style-type: none"> Authentication by the application being tested
Usage Information Collected by Endpoint Agent	<ul style="list-style-type: none"> IP address and logged-in username for the end-user computer where endpoint agent is installed Computer hostname Geolocation data for Endpoints 	<ul style="list-style-type: none"> Measure network performance against either internal or public internet-based network assets
Additional Usage Information Customer Can Configure Endpoint Agent to Process	<ul style="list-style-type: none"> Administrator-selected website page names, object names on target pages (for load time monitoring) 	<ul style="list-style-type: none"> Measure network performance against either internal or public internet-based network assets
Any category of information displayed on a web page being tested during a screenshot capture (if any)	<ul style="list-style-type: none"> Information displayed on a captured image when a transaction test encounters a script error Information displayed on a web page during a transaction test when the user instructs the service to capture a screenshot 	<ul style="list-style-type: none"> Troubleshooting and monitoring script execution
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)	<ul style="list-style-type: none"> IP address of end-user devices 	<ul style="list-style-type: none"> To count the number of sessions impacted by quality of experience degradation IP addresses of end-user devices are hashed and anonymized.

3. Data Center Locations

ThousandEyes leverages third party cloud hosting providers to provide services.

Infrastructure Provider	Description	Location
Amazon Web Services	AWS US-WEST1	Northern California, U.S.A.
Amazon Web Services	AWS US-WEST2	Oregon, U.S.A.
Amazon Web Services	AWS US-EAST	Northern Virginia, U.S.A.
Amazon Web Services	AWS EU-CENTRAL	Frankfurt, Germany
Amazon Web Services	AWS EU-WEST	Dublin, Ireland

4. Cross-Border Data Transfer Mechanisms

Except as it relates to the provision of technical support, as set forth below, the ThousandEyes Service only processes personal data in the United States. ThousandEyes utilizes a 24/7 “follow the sun” technical support model, leveraging support engineers in Australia, Bosnia-Herzegovina, Bulgaria, France, Germany, Japan, India, Ireland, Mexico, the Netherlands, Poland, Portugal, Singapore, Slovenia, Switzerland, the United States, and the United Kingdom. ThousandEyes may update this list of countries from time to time in its sole discretion.

ThousandEyes has invested in a number of transfer mechanisms to enable the lawful use of data across jurisdictions. In particular:

- [Binding Corporate Rules \(Controller\)](#)
- [APEC Cross-Border Privacy Rules](#)
- [APEC Privacy Recognition for Processors](#)
- [EU Standard Contractual Clauses](#)

5. Access Control

The table below lists the personal data used by ThousandEyes to carry out the service, who can access that data, and why.

Personal Data Category	Who Has Access	Purpose of the Access
Registration Data/Support Information	<ul style="list-style-type: none"> ● Customer Administrator ● ThousandEyes 	<ul style="list-style-type: none"> ● Modify and control certain administrative information ● Provision customer’s account; billing/invoicing; supporting the service in accordance with ThousandEyes’s data access and security controls process
Usage Information	<ul style="list-style-type: none"> ● Customer Administrator ● ThousandEyes 	<ul style="list-style-type: none"> ● Measure network performance against either internal or public internet-based network assets

6. Data Portability

A customer has capability to export all personal information stored in the ThousandEyes Service system utilizing an Application Program Interface.

7. Data Deletion & Retention

A customer may request deletion of Personal Data by emailing privacy@thousandeyes.com. When customer makes a request for deletion, the ThousandEyes Service will purge the Personal Data from its systems, except for administrative data required for legitimate business purposes (e.g. billing records, audit logs, taxes). The table below describes the retention period and the business reasons that the ThousandEyes Service retains the personal data.

Type of Data	Retention Period	Reason for Retention
Registration Data/Support Information	Data is deleted upon request	To allow customer to authenticate and use the service, as well as, to address any billing related issues
Usage Information	Automatically deleted after 90 days; Cloud Agent and Enterprise Agent screenshots from web transaction tests are deleted after 45 days	To allow customer to authenticate and use the service, as well as, to address any billing related issues

8. Personal Data Security

ThousandEyes has implemented technical and organizational security measures to protect Customer’s personal data from unauthorized access, use, or disclosure as required by law. Enterprise Agents and Endpoint Agents encrypt data at rest as long as they are hosted on a device with encryption capabilities and the device is configured to utilize such encryption. All backend database systems utilize encryption at rest technologies. All personal information is always encrypted in transit over untrusted networks.

Personal Data Category	Security Controls and Measures
Registration Data	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Support Information	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Application credentials	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Usage Information Collected by Endpoint Agent	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Additional Usage Information Customer Can Configure Endpoint Agent to Process	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Any category of information displayed on a web page being tested during a screenshot capture (if any)	<ul style="list-style-type: none"> ● See ISO 27001, 27701, 27018 certification ● SOC2 Type 2 ● Data Protection Addendum
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)	<ul style="list-style-type: none"> ● Data Protection Addendum

9. Sub-processors

ThousandEyes utilizes and contracts with third party service providers that can provide the same level of data protection and information security expected of ThousandEyes. ThousandEyes does not rent or sell Customer’s information. ThousandEyes follows the data minimization principle and only provides the data that is necessary to fulfill the subprocessor’s purpose. When personal data is changed the change (including deletion) is propagated through relevant systems including subcontractor systems

A current list of sub-processors for the U.S. service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Salesforce.com, Inc. 1 Market Street, San Francisco, CA 94105 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS CRM	USA
Marketo, Inc. 901 Mariners Island Blvd, San Mateo, CA 94404 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS Marketing automation	USA
Amazon Web Services 1200 12th Avenue South, Suite 1200 Seattle, WA 98144 USA	<ul style="list-style-type: none"> Registration Data; Support Information; Application Credentials; Usage Information; Collected by Endpoint Agent; Additional Usage Information Customer Can Configure Endpoint Agent to Process; Any category of information displayed on a web page being tested during a screenshot capture (if any) 	PaaS	USA
Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	PaaS	USA
Heap Inc. 460 Bryant Street, 3rd floor, San Francisco, CA 94107 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS Web analytics	USA
Drift.com, Inc. 703 Market St., Floor 15, San Francisco, CA 94103 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	WWW Website chat	USA
Looker Data Sciences, Inc. 101 Church Street, Santa Cruz, CA 95062 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS Web analytics	USA
MongoDB, Inc. 1633 Broadway, 38th Floor, New York, NY 10019 USA	<ul style="list-style-type: none"> Registration Data; Support Information; Application Credentials; Usage Information Collected by Endpoint Agent; Additional Usage Information Customer Can Configure Endpoint Agent to Process; Any category of information displayed on a web page being tested during a screenshot capture (if any) 	PaaS	USA
Bizible, Inc. 300 Deschutes Way Southwest, Suite 304, Tumwater, WA 98501 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS Marketing Attribution	USA
Snowflake, Inc. 450 Concar Dr, San Mateo, CA 94402 USA	<ul style="list-style-type: none"> Registration Data; Support Information 	SaaS Reporting analytics	USA
Fivetran, Inc. 1221 Broadway, Suite 2400, Oakland, CA 94612	<ul style="list-style-type: none"> Registration Data; Support Information; Application Credentials; Usage Information Collected by Endpoint Agent; Additional Usage Information Customer Can Configure Endpoint Agent to Process 	SaaS Data Synchronization	USA

Okta, Inc. 100 1st Street, 6th Floor, San Francisco, CA 94105 USA	<ul style="list-style-type: none"> • Application Credentials; • Support Information 	SaaS Authentication Provider	USA
OwnBackup, Ltd. 940 Sylvan Ave Englewood Cliffs, NJ 07632 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS CRM Backup	USA
Catalyst Inc. 235 West 23rd Street, Floor 8, New York, NY, 10011 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS CRM	USA

A current list of sub-processors for the E.U. service is below:

Sub-processor	Personal Data	Service Type	Location of Data Center
Salesforce.com, Inc. 1 Market Street, San Francisco, CA 94105 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS CRM	USA
Marketo, Inc. 901 Mariners Island Blvd, San Mateo, CA 94404 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS Marketing automation	USA
Amazon Web Services 1200 12th Avenue South, Suite 1200 Seattle, WA 98144 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information; • Application Credentials; • Usage Information; • Collected by Endpoint Agent; • Additional Usage Information Customer Can Configure Endpoint Agent to Process; Any category of information displayed on a web page being tested during a screenshot capture (if any) 	PaaS	Germany Ireland
Looker Data Sciences, Inc. 101 Church Street, Santa Cruz, CA 95062 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS Web analytics	USA
MongoDB, Inc. 1633 Broadway, 38th Floor, New York, NY 10019 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information; • Application Credentials; • Usage Information Collected by Endpoint Agent; • Additional Usage Information Customer Can Configure Endpoint Agent to Process; Any category of information displayed on a web page being tested during a screenshot capture (if any) 	PaaS	Germany Ireland
Bizible, Inc. 300 Deschutes Way Southwest, Suite 304, Tumwater, WA 98501 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS Marketing Attribution	USA
Snowflake, Inc. 450 Concar Dr, San Mateo, CA 94402 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS Reporting analytics	USA
Fivetran, Inc. 1221 Broadway, Suite 2400, Oakland, CA 94612	<ul style="list-style-type: none"> • Registration Data; • Support Information; • Application Credentials; • Usage Information Collected by Endpoint Agent; • Additional Usage Information Customer Can Configure Endpoint Agent to Process 	SaaS Data Synchronization	USA
Okta, Inc. 100 1st Street, 6th Floor, San Francisco, CA 94105 USA	<ul style="list-style-type: none"> • Application Credentials; • Support Information 	SaaS Authentication Provider	USA
OwnBackup, Ltd. 940 Sylvan Ave Englewood Cliffs, NJ 07632 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS CRM Backup	USA

Catalyst Inc. 235 West 23rd Street, Floor 8, New York, NY, 10011 USA	<ul style="list-style-type: none"> • Registration Data; • Support Information 	SaaS CRM	USA
---	---	----------	-----

10. Information Security Incident Management

Breach and Incident Notification Processes

The Information Security team within Cisco’s Security & Trust Organization coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident Commander directs and coordinates Cisco’s response, leveraging diverse teams including the Cisco Product Security Incident Response Team (PSIRT), the Cisco Security Incident Response Team (CSIRT), and the Advanced Security Initiatives Group (ASIG).

PSIRT manages the receipt, investigation, and public reporting of security vulnerabilities related to Cisco products and networks. The team works with Customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security issues with Cisco products and networks. The [Cisco Security Center](#) details the process for reporting security incidents.

The Cisco Notification Service allows Customers to subscribe and receive important Cisco product and technology information, including Cisco security advisories for critical and high severity security vulnerabilities. This service allows Customers to choose the timing of notifications, and the notification delivery method (email message or RSS feed). The level of access is determined by the subscriber’s relationship with Cisco. If you have questions or concerns about any product or security notifications, contact your Cisco sales representative.

11. Certifications and Compliance with Privacy Requirements

The Security & Trust Organization and Cisco Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Cisco products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

In addition to the Cross-Border Data Transfer Mechanisms/Certifications listed in Section 4, Cisco has the following:

- [EU-US Privacy Shield Framework](#)
- [Swiss-US Privacy Shield Framework](#)

Further, in addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

12. Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Cisco account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller, may be redirected to their employer for a response.

Requests can be made by submitting a request via:

- 1) the Cisco [Privacy Request form](#)
- 2) by postal mail:

<p>Chief Privacy Officer Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES</p>		
<p>Americas Privacy Officer</p> <p>Cisco Systems, Inc. 170 W. Tasman Drive San Jose, CA 95134 UNITED STATES</p>	<p>APJC Privacy Officer</p> <p>Cisco Systems, Inc. Bldg 80, Lvl 25, Mapletree Biz City, 80 Pasir Panjang Road, Singapore, 117372 SINGAPORE</p>	<p>EMEAR Privacy Officer</p> <p>Cisco Systems, Inc. Haarlerbergweg 13-19, 1101 CH Amsterdam-Zuidoost NETHERLANDS</p>

We will endeavor to timely and satisfactorily respond to inquiries and requests. If a privacy concern related to the personal data processed or transferred by Cisco remains unresolved, contact Cisco’s [US-based third-party dispute resolution provider](#). Alternatively, you can contact the data protection supervisory authority in your jurisdiction for assistance. Cisco’s main establishment in the EU is in the Netherlands. As such, our EU lead authority is the Dutch [Autoriteit Persoonsgegevens](#).

13. General Information

For more general information and FAQs related to Cisco’s Security Compliance Program, please visit [The Cisco Trust Center](#).

Cisco Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis. For the most current version, go to the [Personal Data Privacy](#) section of the Cisco Trust Center.

To receive email notifications of updates to the Privacy Data Sheet, click the “Subscribe” link in the upper right corner of the Trust Portal.

SUPPORT SERVICES POLICY

This ThousandEyes Support Services Policy (this “**Policy**”) describes the policies and procedures under which Thousand Eyes, Inc. (“**ThousandEyes**”, or “**we/us/our**”) provides support services (“**Support Services**”) to its customers (each, a “**Customer**” or “**you/your**”). Support Services are provided for the Service pursuant to the separate subscription or license agreement between ThousandEyes and Customer (“**Subscription Agreement**”) and are subject to such Subscription Agreement and this policy. Support Services are provided for the Subscription Term. Capitalized terms not otherwise defined in this policy have the meanings given in the Subscription Agreement.

ThousandEyes is committed to delivering a quality monitoring experience to our customers. As part of our commitment, it is our goal to improve the Service by effectively managing and endeavoring to quickly resolve technical inquiries. The purpose of this Policy is to communicate the support options and processes and clearly set expectations regarding Support Services.

1. SUPPORT SERVICES:

Standard Support

This level of support provides access to our support organization via our application. Access to ThousandEyes Customer Engineering resources is available at <https://app.thousandeyes.com/support>, and can also be accessed via the help and support link while logged into the Service. In addition, ThousandEyes provides access to a documentation site at <https://docs.thousandeyes.com> as well as access to ThousandEyes Customer Engineering, development, and product management personnel. This is the primary point of access for self-service technical support.

ThousandEyes’s customer engineering hours are 24 hours a day, 7 days per week. Target response times are based on the priority level of reported problems and are further set forth in the priority and target response time matrix below.

Premium Support

Premium Support services are a for-fee subscription service, typically purchased in conjunction with platform subscriptions. Technical Account Managers (“**TAM**”) are available as a premium support service offering. The TAM is a named support resource, providing business-hours support, focused on proactive and reactive support. Customers should continue to leverage Standard Support for after-hours assistance.

TAM Support Services

TAM Value	Your TAM acts as a technical advocate for you within ThousandEyes, by overseeing the technical support process and helping to prioritize open cases within the Support Services desk, provide training, managing ongoing technical projects and requests, and providing feedback on how you can optimize and maximize value from your ThousandEyes Service purchase through regular business reviews.
Purchase Options	TAM service can be purchased as a designated remote resource, a dedicated remote resource, or a dedicated onsite resident resource.
Resource Back-up	A back-up TAM resource will also be identified in the event the primary TAM is unavailable.
Support Hours	A TAM provides agreed upon business-hours support. Contact the 24x7 support team for escalations, non-business hours support, or support when the TAM is unavailable. TAM’s observe ThousandEyes holidays.
Full Time Resident TAM	The starting availability of a Resident TAM may require up to 6 months to hire and train, in most locations. Resident TAM’s will spend certain days onsite and some remote, as agreed upon with customer.

EXHIBIT A



TAM Service Start Date	The TAM service starts on the same day as the platform service date for new accounts and will not be delayed or scheduled to start at a later date for any reason. A TAM provides premium support value day one of the service subscription, acting as an available primary support contact.
Multiyear TAM Service Subscription	Simply purchase multiple TAM service one (1) year subscriptions and they will start and end, back-to-back.
TAM Services versus Professional Services	<p>A TAM service is not meant to replace Professional Services, but to complement Professional Services and Standard Support.</p> <p>TAMs will perform optimization, project management, supplemental training, continuation of standard implementation post-initial deployment, and product support.</p> <p>TAMs will not perform initial deployments or non-standard implementations or integrations, post-initial deployment, as these are all paid professional services.</p>

ThousandEyes Customer Engineering Resources

The ThousandEyes Customer Engineering organization consists of technical professionals dedicated to bringing customers optimal value from the Service. This is your primary point of contact with ThousandEyes for all technical support issues; this team manages your case from initial inquiry to case resolution.

- Customer Service Representatives (“**CSRs**”): ThousandEyes solution experts who are able to answer questions regarding product use, service problems, data analysis, and more. CSRs will manage and resolve or escalate your technical issues.
- Technical Support Engineers (“**TSEs**”): ThousandEyes technology experts who provide basic to advanced technical support, and work with the Customer Service Representatives to investigate complex issues. TSEs will manage and resolve or escalate your advanced technical issues.

ThousandEyes Additional Resources

During a support request, you may interact with ThousandEyes representatives operating in one or more of these roles:

- Technical Account Managers (“**TAM**”) – Available as a premium service offering, the TAM is a named resource within ThousandEyes, with ThousandEyes solution and customer relationship expertise. Your TAM acts as an advocate for you within ThousandEyes by overseeing the technical support process and helping to prioritize open cases within the Customer Engineering team, managing ongoing technical projects and requests, and providing feedback on how you can maximize value from your ThousandEyes Service purchase through a regular business review.
- Professional Services Consultants (“**PSC**”) – Available as a premium service offering, the PSC is a resource within ThousandEyes who specializes in delivery of training and custom engagements. Billable on either a fixed-fee or hourly basis, PSCs work with you to maximize your efficiency within the Service and to transfer knowledge and best practices in order to ensure an optimal deployment.
- Customer Success Managers (“**CSM**”) - Will engage with you on your ongoing satisfaction, new product offerings, and guidance during your solution subscription renewal. This team consists of customer relationship experts, who ensure a successful customer journey at ThousandEyes.
- Site Reliability Engineering (“**SRE**”) – For network and other service--related inquiries, if the customer engineering team is unable to resolve your issue after the initial troubleshooting phase, representatives of the SRE team may be called in to assist.

- Product Engineering (“**ENG**”) – For product related support issues, if the prior layers of technical support are unable to resolve your issue, the inquiry will be escalated to the ThousandEyes product engineering team, which includes product developers from the core technology team within ThousandEyes.

Contacting and Working with the ThousandEyes Customer Engineering Team

Reporting a Problem

You may use one of the following methods to report a support issue:

- Online (Live Chat) – click the Chat with Support link under the Help & Support menu when you are logged into the Service, or from the login page when you are not logged into the service.
- Online (Form Submission) – click the Contact Support link under the Help & Support menu when logged into the service.
- Via Email – send an email to support@thousandeyes.com, including the information requested below. Your email will be routed to our support system and your request will be assigned a case ID.
- Via Telephone – contact our support team by calling +1 (415) 237-EYES (3937)

Case Notification

Customers can expect to receive an automated notification immediately following a case creation activity. The notification will include the case ID, a summary of the inquiry and the priority level that has been assigned. Case notification will always be done via email, to the email address on record for a user.

For problems reported via email, initial contact from the representative handling your case will be made in accordance with the priority and target response time matrix below.

Information You Provide to ThousandEyes

If you are reporting a new issue, be prepared to:

- Provide your account name or the username that you use to access the Service. This information is automatically populated for Customers who are authenticated with the Service.
- Provide the results of any troubleshooting measures you may have already undertaken, and a list of steps that can be followed to reproduce the issue.
- Provide as many other details about the issue as possible, including any co-existing issues and any recent updates or changes that may have been made to the network topology or infrastructure.

For subsequent communications about existing cases, be prepared to:

- Provide your previously assigned case ID. This is provided in the format S-CS-XXXXXXX.
- Provide any additional details about your issue since you were last in contact with the ThousandEyes Customer Engineering resources.

EXHIBIT A



Priority and Response Target Matrix

During case creation, a ThousandEyes Customer Engineering representative will assign a priority level, based on the criteria described in the matrix below. ThousandEyes will use commercially reasonable efforts to respond to Customer inquiries within specified targets based on the priority of the reported issue according to the matrix.

Priority #	Priority Level	Description	Target Response Time
Priority 1	Urgent	The Service is unavailable or is so seriously impaired that it is unusable, and no alternative is available.	1 hour
Priority 2	High	The Service is impacted affecting many users, where major functionality is affected, a data integrity issue, or the service is unreachable from some locations, and no alternative is available.	4 hours
Priority 3	Medium	The Service is impacted, a system performance issue or a bug affecting some but not all users, where no workaround is available. Includes issues related to scripts developed by Customer (or third-party developers acting on behalf of Customer) which leverage the ThousandEyes-published API; and user authentication problems.	8 hours
Priority 4	Low	A feature of the Service is not functioning correctly but does not impact data quality or access.	Next day

Case Resolution

A case will be closed when a Customer's inquiry is resolved. A resolution is typically one of the following: an answer to the question, a suggestion on how to perform a particular task, an acceptable workaround to a product issue, or the deployment of a code fix. Customers will be notified of case closures, and this closure notification will always be done via email, to the email address on record. Cases may be closed if Customer fails to respond following two successive contact attempts by ThousandEyes.

A case can be reopened at any time at a Customer's request, if further investigation is required.

Case Escalations

Notification of Customer-initiated requests are created and sent via email to all concerned parties, including the reporting Customer, all ThousandEyes Customer Success resources, and account teams assigned to the Customer account. Customer may

EXHIBIT A



initiate escalation of requests at Priority levels 1, 2, or 3 by sending an email request for escalation to support@thousandeyes.com, or by contacting our team via phone.

Escalation requests must contain the case ID, Customer contact, and reason for requesting the escalation. ThousandEyes will consider all escalation requests in good faith; however, ThousandEyes' conclusion will be determinative.

Support Restrictions

Access to ThousandEyes Customer Engineering resources is restricted to Customers whose accounts are in good standing with ThousandEyes. This includes all means of accessing the Customer Engineering team.

Customer Cooperation

Customer will provide all information and access to Customer resources as reasonably required for ThousandEyes to provide Support Services, which may include access to Customer servers, participation in web meetings using online collaboration services (such as Cisco Webex), physical access to Customer facilities, and assistance from Customer personnel. ThousandEyes will be excused from any non-performance of its obligations hereunder to the extent any such non-performance is attributable to Customer's failure or delay to cooperate as set forth in this Policy.

Exclusions from Support and SLA

Support Services and the ThousandEyes SLA (see below) do not cover (and ThousandEyes is not responsible for) issues arising from: (i) Customer's equipment, software, network connections or other infrastructure; (ii) use of the Service by Customer in a manner not consistent with the Documentation, (iii) modifications to the Service by any party other than ThousandEyes, (iv) third party acts or systems or (v) general Internet problems, force majeure events (as described in the Subscription Agreement) or other factors outside of ThousandEyes' reasonable control.

ThousandEyes SLA

ThousandEyes uses its own service to monitor and report on application availability, from at least 30 global monitoring points. The Service is deemed to be available when (a) packet loss from at least 70% of reporting global monitoring points targeting the Service is measured at less than 50%, and (b) at least 70% of reporting global monitoring points targeting the Service return an expected HTTP response code (HTTP/200).

ThousandEyes reports on performance against these availability targets on a monthly and quarterly basis; copies of these reports are shared on an as-requested basis.

Target availability for the Service is measured on a property-by-property basis and is deemed to be unavailable when one or more properties violates the rules specified above. Monitored properties include app.thousandeyes.com, and api.thousandeyes.com.

1. **Target**. Target availability for the Service is ninety-nine point five percent (99.5%) per calendar month ("**Target Availability**"). For any partial months during which Customer subscribes to the Service, Target Availability will be calculated based on the entire calendar month. Target Availability excludes Scheduled Downtime.
2. **Scheduled Downtime**. From time to time, ThousandEyes will conduct planned maintenance, including to improve the quality or reliability of the Service, and make available new capabilities. During these periods, the Service will be down (and inaccessible) on a schedule posted by ThousandEyes ("**Scheduled Downtime**"). Cumulative Scheduled Downtime will not exceed four and one-half (4.5) hours in any calendar month). Where Scheduled Downtime is required, ThousandEyes will use commercially reasonable efforts to notify customers of Scheduled Downtime at least seventy-two (72) hours in advance.

EXHIBIT A



3. Service Credits. If Customer believes that the Service has failed to meet Target Availability for a particular month and wishes to receive a Service Credit (as defined below), Customer must notify ThousandEyes within twenty (20) days of the end of the month in which the failure occurred. Service level claims will be verified against ThousandEyes' system records, which will prevail in event of any conflict with Customer records. Target Availability measurements will be conducted from multiple nodes worldwide (and ThousandEyes may change the set of nodes used to calculate Target Availability from time to time in its sole discretion). Subject to the procedures in this section, in the event of a verified failure during a given month, ThousandEyes will credit Customer's account one percent (1%) of such month's fees for each one full percent (1%) of Service unavailability in such month below the Target Availability percentage ("**Service Credits**"). Service Credits in any month will not exceed one hundred percent (100%) of monthly fees and will be applied during the Term only to excess usage and/or additional Purchased Units as set forth in Section 4.2 of this Agreement ("**Excess Usage; Additional Purchased Units**"). Service Credits constitute liquidated damages and are not a penalty. Receipt of Service Credits will be Customer's sole and exclusive remedy for any failure or interruption of the Service. Scheduled Downtime and the circumstances in the "**Exclusions from Support and SLA**" section above are excluded from calculating Service unavailability.

2. PROFESSIONAL SERVICES

Professional services are paid services offered and delivered in fixed-fee professional services or custom (hourly) professional services. Fixed-fee services may also be sold in bundles and sized according to company size and needs.

Fixed-Fee Professional Services

Fixed-Fee Service Name	Service Description
Customer Onboarding	<ul style="list-style-type: none">● Service Goal = Provide new customers with training and guidance to implement, operate, and manage their solution● Initial solution set-up:<ul style="list-style-type: none">○ Account and user set-up○ General set-up● Enable customers through example implementation guidance:<ul style="list-style-type: none">○ Planning and implementation of example tests○ Planning and implementation of example reports○ Planning and implementation of example dashboards○ Planning and implementation of example alerts○ Test result data analysis sessions● Guidance and training on:<ul style="list-style-type: none">○ Operating the solution○ Maintaining the solution○ How to create tests○ How to optimize tests○ How to set-up alerts○ How to share and save test results○ How to analyze test results● Onboarding Service may be sold in packages and sized according to company size and need. See "Onboarding Deliverables by Package Size"

Health Check	<ul style="list-style-type: none"> ● Service Goal = Provide existing customers with quarterly optimization review for a one year period, consisting of four reviews ● Review optimization of: <ul style="list-style-type: none"> ○ Tests ○ Reports ○ Dashboards ○ Alerts ● Provide service optimization analysis report ● Service may be sold in bundles, and sized according to company size and need ● Optimization is not performed; additional service is required
Renewal Optimization Package	<ul style="list-style-type: none"> ● Service Goal = Provide existing customers with one-time optimization assistance, expansion assistance, or additional training ● Review and offer optimization guidance on: <ul style="list-style-type: none"> ○ Tests ○ Reports ○ Dashboards ○ Alerts ● Test result data analysis sessions ● Additional training on: <ul style="list-style-type: none"> ○ Operating the solution ○ Maintaining the solution ○ How to create tests ○ How to optimize tests ○ How to set-up alerts ○ How to share and save test results ○ How to analyze test results ● Service may be sold in bundles, and sized according to company size and need
Alerting System Configuration	<ul style="list-style-type: none"> ● Service goal = Product alert configuration using the webhook notification service ● Standard alert rule configuration into a third-party service ● The service covers the cost of either configuring an intermediate server (provided by Customer) to translate the notification between services or assisting with Customer's configuration to directly connect with a third-party service ● Does not cover configurations involving anything in the API outside of the base alert rule webhook functionality ● One-year maintenance for defect or security related problems. Professional Services will fix any defects in the Java configuration for customers for up to one year from the date of implementation. A defect is determined to be incorrect logic within the .jar file that results in erroneous behavior. A defect is not defined as a change in ThousandEyes webhook payload structure, functionality enhancements to the .jar logic, nor changes to the customer infrastructure or alerting system. Customer can contact services@thousandeyes.com if they suspect a defect is present ● Enhancements will require an additional services package

Onboarding Deliverables By Package Size

<u>Onboarding Package Deliverables</u>	<u>Small</u>	<u>Medium</u>	<u>Large</u>	<u>Extra Large</u>
<u>Org/Account Group Setup</u>	X	X	X	X
<u>Cloud/Enterprise Agent Implementation Guidance</u>		X	X	X
<u>Endpoint Agent Implementation Guidance</u>	X	X	X	X
<u>Internet Insights Implementation Guidance</u>			X	X
<u>Training - 1 group</u>	X			
<u>Training - 2 groups</u>		X		
<u>Training - 3 groups</u>			X	
<u>Training - 4 groups</u>				X
<u>Continuous Enablement - office hours</u>			X	X
<u>Continuous Enablement - solution refresher</u>				X

Custom (Hourly) Professional Services

<u>General Terms</u>	<ul style="list-style-type: none"> ● Provided on a time and material basis ● Required an agreed-to Scope of Work
<u>General Time Accounting</u>	<ul style="list-style-type: none"> ● Time is accounted for in fifteen (15) minute increments ● Tasks have a minimum duration of thirty (30) minutes ● Where travel is required, travel time is billed at one-half (0.5x), and includes door-to-door travel ● Time is accounted for in real (elapsed) time, with appropriate multipliers applied to determine billable hours ● Abnormal work requirements are billed at rate of one and one-half (1.5x). This includes: <ul style="list-style-type: none"> ○ Work on designated holidays ○ Work on weekends ○ Work overnight (more than four (4) hours outside normal shift) ○ Work above eight (8) hours in a single stretch ○ Any period where a resource needs to be available
<u>Billable and Nonbillable hours</u>	<ul style="list-style-type: none"> ● Billable Hours include: <ul style="list-style-type: none"> ○ Customer meetings ○ Customer meetings, when customer does not show-up or cancels with less than twenty-four (24) hours advance notice (billed for thirty (30) minutes) ○ Internal ThousandEyes meetings, only if customer-specific ○ Travel to/from customer site (for onsite services) ○ Engagement specific tasks. Examples include but are not limited to: <ul style="list-style-type: none"> ■ Configuration tasks ■ Customer training ■ Offline work including research, analysis and testing ■ Creation of written assessments or report ■ Account health checks ■ Solution integration ● Non-Billable Hours include: <ul style="list-style-type: none"> ○ Certain administrative tasks <ul style="list-style-type: none"> ■ Time used to fill out information in task management tracking system

	<ul style="list-style-type: none">■ Time used to track the customer down (mostly applies to onboarding)■ Scoping of additional packages
--	--

General Professional Services Policies

- All fixed-fee or custom (hourly) services have an expiration period. The services shall expire, even if unused, one (1) year from the beginning of the service start date as set forth in the applicable Order Form.
- Licensing - All engagements which require ThousandEyes Professional Services to create code for the Client are licensed under the Client's MSA with ThousandEyes. If open source software is required, ThousandEyes will notify Client of such inclusions and document it appropriately in the final report.
- Access - Customers are required to provide access to systems and key personnel required to complete any service.
- All services are performed remotely, unless explicitly agreed to as part of a custom service.

EXHIBIT A



Service Level Agreement

This Service Level Agreement (“SLA”) applies to the ThousandEyes Cloud Service (referred to herein as the “Cloud Service”) as set out in the Product Description at [ThousandEyes \(cisco.com\)](#). If capitalized terms are not defined in this SLA, then they have the same meaning as under the Product Description.

1. Service Level

Cisco will use commercially reasonable efforts to deliver the Cloud Service so that the Core Services meet or exceed the performance standards described below (“Service Level”). Subject to the terms of this SLA, You can get Service Credits if Cisco fails to meet the Service Level.

1.1 Service Level

Service Level	During each Measurement Period, the Availability of the Core Services will be 99.5% or greater.
Measurement Period	One calendar month

“Availability” is calculated as follows and converted into a percentage:

$$\frac{\text{Total Service Time} - \text{Total Outage Time}}{\text{Total Service Time}}$$

“Core Services” means the app.thousandeyes.com and api.thousandeyes.com monitored properties of the Cloud Service.

“Qualifying Outage” means the time that one or more of the Core Services do not meet the following criteria: (a) packet loss from at least 70% of the >29 reporting global monitoring points targeting the Core Service is measured at less than 50%, and (b) at least 70% of reporting global monitoring points targeting the Core Service return an expected HTTP response code (HTTP/200). Service Level measurements will be conducted from multiple nodes worldwide (and ThousandEyes may change the set of nodes used to calculate Service Level from time to time in its sole discretion).

“Service Credits” means (i) credits Cisco will issue that may be used towards the purchase of additional Units, or (ii) if You have exceeded Your monthly quantity of purchased Units in a given month, credits that may be used towards such excess usage. The applicable Service Credit type and amount is listed in the table in Section 2.

“Total Service Time” means the total number of minutes in a Measurement Period (calculated by multiplying 60 (minutes) by 24 (hours) by the number of calendar days in the Measurement Period).

“Total Outage Time” means the aggregate total time for all Qualifying Outages during a Measurement Period (rounded upward to the nearest minute). To calculate Total Outage Time, each Qualifying Outage will:

- (i) Begin when Cisco logs an incident ticket based on our own identification of a Qualifying Outage or upon confirming a Qualifying Outage; and

EXHIBIT A

(ii) End when the Core Services are restored.

2. Service Credits.

2.1 If Cisco fails to meet the Service Level for a given Measurement Period, Cisco will issue You a Service Credit consistent with the table below.

Service Credits Table.

Availability Percentage	Amount Credited and Type
For each one full percent (1%) of Total Outage time below the Service Level. Service Credits in any month will not exceed one hundred percent (100%) of monthly fees.	(1%) of such month's fees

2.2 Service Credit Limitations

2.2.1 The aggregate maximum Service Credit for any Measurement Period will be a credit for the value of 100% of the fees (based on subscription fees paid to us for the applicable Measurement Period), excluding excess usage.

2.2.2 These Service Credits are Your only remedy if the Core Services do not meet the Service Level.

3. Claims Procedure.

3.1 To receive a Service Credit, You must:

- (a) be up to date on payment of all applicable fees;
- (b) promptly notify Cisco of a Qualifying Outage when You become aware of or reasonably suspect one; and
- (c) request Service Credits no more than 20 days after the end of the applicable Measurement Period.

3.2 You must submit a claim via Email to support@thousandeyes.com.

3.3 If You purchased the Cloud Service from a Cisco Partner, You may claim Service Credits or the Cisco Partner may claim them on Your behalf.

3.4 If there is a dispute about whether a Qualifying Outage has occurred, Cisco will decide in good faith based on our system logs, monitoring reports, and configuration records. If You have supporting information for Your claim that You want Cisco to consider, You should provide this information with Your claim.

4 Issuance.

4.1 Review. Cisco will use commercially reasonable efforts to review and issue earned Service Credits within 30 calendar days of Cisco confirming that You are entitled to Service Credits.

5 Non-Qualifying Outages.

It is not a Qualifying Outage and You will not earn Service Credits if Cisco fails to meet the Service Level for any of the following reasons:

EXHIBIT A

- (a) Scheduled maintenance or emergency maintenance (emergency maintenance is where Cisco performs work to prevent or mitigate an outage or degradation of the Cloud Service or to prevent or mitigate a security incident) that is less than 4.5 hours per Measurement Period;
- (b) Due to Your integrations or modifications or any applicable third-party software, hardware, network connections or services not provided by Cisco;
- (c) You are using a beta, limited preview, evaluation, or trial version of the Cloud Service;
- (d) Your failure to (i) use the Cloud Service or perform responsibilities in accordance with Your applicable agreement (e.g. EULA or General Terms), Offer Description, or the Documentation, or (ii) apply updates or upgrades when made available; or
- (e) Factors outside of Cisco's reasonable control, such as events described as Force Majeure in Your applicable agreement, Internet outages, pandemics, acts of government, industry-wide shortages, failures, or delays of common carriers.