ThousandEyes

This Privacy Data Sheet describes the processing of personal data (or personally identifiable information) in the ThousandEyes service ("ThousandEyes Service") by ThousandEyes, LLC and its affiliates (collectively, "Cisco").

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

Cisco will process personal data from the 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 to provide the ThousandEyes Service functionality. It the Customer's responsibility to ensure that its use of the ThousandEyes Service is in accordance with applicable legal requirements, including but not limited to, providing any required notice to Customer's end users and obtaining any required consents.

Note: This Privacy Data Sheet is a supplement to the Cisco Online Privacy Statement.

1. Overview

ThousandEyes Service. 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 collects network metadata, not content payload data. The ThousandEyes Service may collect personal data using the following components, depending on which components are selected/deployed by the customer.

A. Web Platform: The ThousandEyes Service web platform is the primary user interface for the ThousandEyes Service.

B. Cloud Agents: Cloud Agents are testing agents deployed by ThousandEyes 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.

C. Enterprise Agents: Enterprise Agents are equivalent to Cloud Agents but are deployed by customers in customer-controlled environments. Customers can 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.

D. Endpoint Agents: Endpoint Agents are testing agents deployed by customers on devices within their organization to help troubleshoot network and application performance. There are multiple tiers of Endpoint Agents, see the Endpoint Agent Licensing documentation. Customer's administrators configure 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 Service. If so configured by a customer, Endpoint users may also manually record data performance metrics by targeting a specified domain.

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

1. Automatic browser data collection: The Endpoint Agent will gather performance data associated with the end-user's browsing session when the device is operating within networks selected by customer administrators, and the end-user visits a website which is selected for monitoring by customer administrators.

2. Automatic application data collection: The Endpoint Agent may be configured by customer administrators to collect data about network and application performance when operating certain applications (as defined by the customer administrators). For example, Meeting IDs could be collected when the end user uses a video conferencing program.

3. Automatic session tests: The Endpoint Agent may be configured to collect data about network and application performance to specified destinations when certain conditions occur. For example, the Endpoint Agent can monitor when a Webex Meeting starts and then perform regular tests to the Webex service. These tests are at regular intervals, as defined by the customer's administrator. The trigger for each automated session test will vary based on the application being used.

4. Manual data collection: The end-user can initiate data collection using Google Chrome and Microsoft Edge by clicking the ThousandEyes logo in the extension toolbar. (The ThousandEyes extension must be first deployed by the customer's administrator.) When the Endpoint Agent is recording the browsing session, the top of the webpage will show a banner indicating that the ThousandEyes Service Endpoint Agent is debugging the tab. To stop recording, the end user may click the ThousandEyes logo in the toolbar or click the Cancel button on the banner.

5. 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.

6. 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 the same as a scheduled test.

E. Endpoint Agent Pulse: Endpoint Agent Pulse is typically used by customers to troubleshoot connectivity into unmanaged networks, such as their client sites, kiosk devices, 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, etc.) are uploaded to the customer's account on the ThousandEyes platform.
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 the same as a scheduled test.

F. WAN Insights: WAN Insights is an optional product of the ThousandEyes Service that enables customers to improve quality of experience of applications in their Cisco SD-WAN network. The solution uses network data from Cisco SD-WAN 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.

The WAN Insights component processes the Cisco SD-WAN vAnalytics data if enabled by the Customer administrators. Customer may only use the WAN Insights Functionality (as defined in the ThousandEyes Product Description) for the number of applications or application categories set forth in the Product Description. The applications or application categories may be pre-defined in WAN Insights or imported by Customer as permitted by the Application-Aware Routing Policy from vManage. Please see the SD-WAN Cloud Privacy Data Sheet for details regarding processing of personal data by the Cisco vAnalytics feature.

Collection of Log Data. To troubleshoot issues with the Enterprise or Endpoint Agents, Cisco may need local device logs. Local device logs can include network connectivity information and, in the case of Endpoint Agents, detailed information about the

device, users of the device, browser data, operating system information and application log data. If needed, Customer can upload local device logs or Cisco can initiate an automated collection process. The collection process will only be initiated by Cisco in connection with a support case, part of a services engagement, or part of an escalation from the customer for investigation. Customer can disable the automated collection of the local device logs for its organization by raising a Cisco support ticket.

Integrations. ThousandEyes integrates with various Cisco products including, but not limited to, those referenced below. If a Customer elects to enable or leverage integration between Cisco ThousandEyes and another Cisco cloud service or feature, then the Customer should also review the data sheet of such other cloud service or feature for information regarding the personal data collected, processed, and stored by that product, cloud service or feature by visiting the Cisco Trust Portal. Cisco ThousandEyes also integrates with various third-party systems. Each Customer is responsible for ensuring it has the proper data protection agreement(s) in place with any third parties to whom it elects to send data.

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	Type of Personal Data	Purpose of Processing
Registration Data	• User email address • User first and last name • User Password • User IP address • Billing contact name	• Activation of service • Billing/invoicing • Product notifications • Technical support • Authentication/Authorization • Activity logs
Support Information	• First name, last name, email, Phone number of the individual opening the service request • Customer account information	• Technical support • Review of the support service quality • Troubleshooting • Analysis of service
Application Credentials	• Credentials used by Cloud and Enterprise Agents to execute web transaction tests	• Authentication by the application being tested
Web Platform	• User login credentials including usernames, email addresses, and passwords • IP addresses • PII provided in the data sent from the Agents	• Operation of the Service • Authentication/Authorization • Security auditing
Information Collected by Cloud Agents	• Cloud Agents are generally used to monitor the public internet, but may process personal information if tests configured by the customer include personal data	• Operation of the ThousandEyes Service
Information Collected by Enterprise Agents	• Enterprise Agent may process personal information if tests configured by the customer include personal data	• Operation of the ThousandEyes Service
Information Collected by Endpoint Agents	• IP addresses for the end-user device (including metro area location information derived from the IP address) • Username of the logged in end-user • End-user Device host name • SSID Geolocation data for Endpoints	• Operation of the ThousandEyes Service • Measure network performance against either internal or public internet-based network assets
Additional Usage Information Customer Can Configure Endpoint Agent to Process	• Administrator-selected website page names, object names on target pages (for load time monitoring) • Local device logs (which may contain, for example: information on the device, users of the device, browser data, operating system information and relevant application data) • Device information which may include device hardware and software information, serial number, resource utilization and wireless access points	• Operation of the ThousandEyes Service • Measure network performance against either internal or public internet-based network assets

	• Meeting identifiers including MeetingID, Meeting URL, participants, meeting subject, and attendees. • Personal information included or resulting from customer-configured tests	
Any category of information displayed on a web page being tested during a screenshot capture (if any)	• 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	• Troubleshooting and monitoring script execution
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)	• Source IP address • Destination IP address (IP addresses of end-user devices are hashed to deliver the WAN Insights service.)	• Operation of the ThousandEyes Service

3. Data Center Locations

Cisco leverages the third-party cloud hosting providers listed below to provide the ThousandEyes Service. Not all ThousandEyes Service features or products may be available in all datacenter locations. If customer requires that a certain Primary Region Location to be used for their deployment, the customer must reach out to their account manager.

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

4. Cross-Border Data Transfer Mechanisms

Cisco 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

Customer support 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.

5. Access Control

The table below lists the personal data used by Cisco to provide the ThousandEyes Service, who can access that data, and why.

Personal Data Category	Who has Access	Purpose of the Access
Registration Data	• Customer Administrator • Cisco	• Modify and control certain administrative information • Provision customer's account • Billing/invoicing • Supporting the service in accordance with Cisco's data access and security controls process
Support Information		

Application Credentials	• Customer Administrator • Cisco	• Operation of the ThousandEyes Service • Measure network performance against either internal or public internet-based network assets
Web Platform		
Information Collected by Cloud Agents		
Information Collected by Enterprise Agents		
Information Collected by Endpoint Agents		
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)		
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)		

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 and Retention

A customer may request deletion of personal data by submitting the Data Subject Rights and Privacy Request Form at https://privacyrequest.cisco.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). In the absence of any such deletion request, the table below describes the retention period and the business reasons that the ThousandEyes Service retains the personal data.

Type of Personal Data	Retention Period	Reason for Retention
Registration Data	Data is deleted upon request.	• To allow Customer to authenticate and use the service, as well as, to address any billing related issues
Support Information		
Application Credentials	While You are an active customer, usage data is retained for 90 days before being overwritten; provided, however, (i) Cloud Agent and Enterprise Agent screenshots from web transaction tests are deleted after 45 days, (ii) Endpoint Agent Advantage data is deleted after 30 days, (iii) Endpoint Agent Essentials data is deleted after 14 days, and (iv) Endpoint Agent Embedded data is deleted after four days. Local device logs will be deleted within 180 days of collection.	• To allow Customer to authenticate and use the service, as well as, to address any billing related issues. • Post subscription termination, data is retained for the stated duration to allow the customer a grace period in case they mistakenly did not renew their subscription on time.
Web Platform		
Information Collected by Cloud Agents		
Information Collected by Enterprise Agents		
Information Collected by Endpoint Agents		
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)	If Customer terminates its subscription, then its authentication and configuration data will be deleted within 180 days of Customer's subscription terminati on.	
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)		

8. Personal Data Security

Cisco 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 data is always encrypted in transit over untrusted networks.

Personal Data Category	Security Controls and Measures
Registration Data	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Support Information	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Application Credentials	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Web Platform	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Information Collected by Cloud Agents	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Information Collected by Enterprise Agents	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Usage Information Collected by Endpoint Agents	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Additional Usage Information Customer Can Configure Endpoint Agent to Process	• 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)	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum
Cisco SD-WAN network traffic metadata (if WAN Insights is being used)	• See ISO 27001, 27701, 27018 certification • SOC2 Type 2 • Data Protection Addendum

9. Sub-processors

Cisco partners with service providers that act as sub-processors of personal data and contract to provide the same level of data protection and information security provided to You by Cisco. Cisco 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.

As indicated in Section 3, the ThousandEyes Service is currently available in two regions: USA and EU. If customer requires that a certain Primary Region Location to be used for their deployment, the customer must reach out to their account manager.

ThousandEyes Instance	Sub-processor	Personal Data	Service Type	Location of Sub-processor Data Center

USA & EU	**Salesforce.com, Inc.** 1 Market Street San Francisco, CA 94105 USA	• Registration Data • Support Information	Salesforce	USA[1]
USA & EU	**Amazon Web Services, Inc.** 1200 12th Avenue South, Suite 1200 Seattle, WA 98144 USA	• Registration Data • Support Information • Application Credentials • The data collected by the Agents and sent to the Platform, as described in Section 2 • Any category of information displayed on a web page being tested during a screenshot capture (if any)	Amazon Web Services	**USA Instance:** Primary – USA Disaster Recovery – USA OR **EU Instance:** Primary – Germany Disaster Recovery – Ireland
USA only	**Google, LLC** 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	• Registration Data • Support Information	Google Cloud Platform	USA
USA & EU	**MongoDB, Inc.** 1633 Broadway, 38th Floor New York, NY 10019 USA	• Registration Data • Support Information • Application Credentials • The data collected by the Agents and sent to the Platform, as described in Section 2 • Any category of information displayed on a web page being tested during a screenshot capture (if any)	MongoDB Atlas	**USA Instance:** Primary – USA Disaster Recovery – USA OR **EU Instance:** Primary – Germany Disaster Recovery – Ireland
USA & EU	**Snowflake, Inc.** 450 Concar Drive San Mateo, CA 94402 USA	• Registration Data • Support Information	Snowflake Data Platform	USA[1]
USA & EU	**Fivetran, Inc.** 1221 Broadway, Suite 2400 Oakland, CA 94612	• Registration Data • Support Information • Application Credentials	Fivetran Database Replication	**USA Instance:** USA OR **EU Instance:** Germany[2]
USA & EU	**OwnBackup, Ltd.** 940 Sylvan Avenue Englewood Cliffs, NJ 07632 USA	• Registration Data • Support Information	OwnBackup CRM Backup	USA[1]
USA & EU	**Okta, Inc.** 100 1st Street San Francisco, CA 94105	• Application Credentials • Support Information	Otka MFA	USA[1]

10. Information Security Incident Management

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.

[1] ThousandEyes uses the sub-processor's standard offering and thus the sub-processor controls the country in which data is stored. The country indicated above is the sub-processor's primary business location.

[2] For the EU Instance, Billing Information is also processed in the USA by FiveTran.

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:

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

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 Autoritiet Persoonsgegevens.

13. General Information

For more general information and FAQs related to Cisco's Security and Privacy 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.