ThousandEyes

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").

1. Overview of The ThousandEyes Service Capabilities

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.

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	• 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
Usage Information Collected by Endpoint Agent	• IP address and logged-in username for the end user computer where endpoint agent is installed • Computer hostname	• 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)	• 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)	• 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

3. Cross-Border Transfers

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, Bulgaria, Ireland, Singapore, Slovenia, 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:

- EU Binding Corporate Rules
- EU Standard Contractual Clauses
- APEC Cross Border Privacy Rules
- APEC Privacy Recognition for Processors

4. Access Control

ThousandEyes and ThousandEyes's customers can access personal data as described in the table below.

Personal Data Category	Who Has Access	Purpose of the Access
Registration Data/Support Information	• Customer Administrator • ThousandEyes	• 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	• Customer Administrator • ThousandEyes	• Measure network performance against either internal or public internet-based network assets

5. Data Portability

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

6. 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; screenshots from web transaction tests deleted after 45 days	To allow customer to authenticate and use the service, as well as, to address any billing related issues

7. 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.

8. Third Party Service Providers (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. A list of third-party service providers having access to personal data is available at https://thousandeyes.com/subprocessors. If you would like to receive notifications when this list is updated, please email dpa@thousandeyes.com.

9. Information Security Incident Management

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. 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 RSSfeed). 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.

10. Certifications and Compliance with Privacy Laws

The Security and 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. Cisco and its underlying processes are designed to meet Cisco's obligations under the EU General Data Protection Regulation and other privacy laws around the world. Cisco leverages the following privacy transfer mechanisms related to the lawful use of data across jurisdictions. See Section 3, above. In addition to complying with our stringent internal standards, Cisco also maintains third-party validations to demonstrate our commitment to information security.

11. General Information and GDPR FAQ

For more general information and FAQs related to Cisco's Security Compliance Program, please visit The Cisco Trust Center.