Data Collection and Processing

Log Analytics

Product Overview

At Cisco AppDynamics, we offer enterprise-grade software that enables our customers to monitor and analyze the performance of their business applications and supporting infrastructure. Our Log Analytics Software enables our customers to collect and analyze both structured and unstructured data stored within log files associated with the customer's monitored application(s) and supporting machines to gain real-time visibility into physical, virtual, or cloud infrastructure. The Log Analytics Software can be deployed to customers as either an on-premise installation or as software-as-a-service (SaaS).

The information below addresses SaaS versions of the Log Analytics Software; for on-premise deployments, we do not have access to the data collected by the Log Analytics Software.

What data does the Log Analytics Software collect?

Our Log Analytics Software is designed to analyze data contained within the log files from within our customers' application infrastructure, including log files from instrumented and non-instrumented applications, as well as machine log files. The data types are actually collected and processed by a customer's unique instance of our Log Analytics Software depends on how the customer has configured the Log Analytics Software, what information the customer has chosen to include in the relevant log files, and whether the customer administrator has chosen to utilize the masking functionality (described below) to exclude certain information within the relevant log files from being sent to our SaaS infrastructure.

Personal data collection and processing

The software customer administrator can choose to configure the Software to collect and process payload and parameter information within their application(s), which may contain this information. Therefore, our customer controls whether the AppDynamics Software collects and processes personal data.

The Log Analytics Software requires the collection of log files identified by the customer for processing and analysis, but it does not require the collection or processing of personal data, and the product does not collect personal data by default. Customer administrators of the Log Analytics Software must configure the Log Analytics Software to collect the log files that it wants to analyze, and the contents of such files are fully controlled and managed by the customer, using the customer's internal logging practice and policies. Therefore our customer controls whether the Log Analytics Software collects and processes personal data contained within log files.

For example, if a customer has written the log limits for a relevant log file to include "username" and "user-email" as fields within the resulting log files, then, the resulting log files will likely contain personal data in those fields. If the customer administrator has configured their instance of the Log Analytics Software to collect and process those log files, any personal data contained in those log files will be transferred to our SaaS infrastructure for processing.

To help customers manage the type of data they pass to us in log files, we offer customers a UI-based "field masking" functionality that identifies and masks parameter values within the log files that a customer does not want to send to our SaaS infrastructure. In the example above, the fields "username" and "user-email" could be masked within the log files by a customer administrator. The masking, once configured, occurs in the customer's datacenter, and the masked data is sent and written to disk within our SaaS infrastructure.

Cisco AppDynamics adheres to Cisco Online Privacy Statement. To learn more about the Cisco Online Privacy statement and how we process our customers' personal data, please visit https://www.cisco.com/c/en/us/about/legal/privacy-full.html

How is access to data controlled?

We use industry-standard techniques designed to restrict access to and to prevent unauthorized use of our information systems. We require the use of individual user accounts to maintain the integrity of audit trails. User and group management is centralized using single-sign-on systems and access to systems is subject to management approval. Access to all systems that process or store customer data are reviewed and re-approval is required periodically.

How long is data retained?

Information about data retention is set out in the relevant License Entitlement located at: https://docs.appdynamics.com/latest/en/appdynamics-licensing/license-entitlements-and-restrictions.

Can I delete or rectify data?

Our customers may request information regarding the deletion of data, or make specific requests to have certain data deleted from our systems and records, by opening a ticket with our support teams.

AppDynamics Software collects data from various sources as described above. If the source data are incorrect then the collected data will be incorrect. It is not possible to correct the data within the product. Customers can submit deletion requests for inaccurate data.

Is the data encrypted?

Yes; our SaaS software products support encryption of customer data in transit and at rest, including backups.

How secure is the data?

We are committed at all levels to the security of customer data. We have developed a comprehensive security program and organization that is supported by leadership who are committed to proactively managing cybersecurity risk. By focusing on a secure-by-design approach, we seek to weave security into our development practices early and layer security across our architecture to protect its corporate services, supply chain, software distribution, and customer-facing services.

We implement process, and technical controls designed to manage cybersecurity risks. Controls may be physical, technical or administrative in their operation, and they may be preventative, detective, corrective, deterrent or recovery focused in their intent. Controls may include hardware and software functions, processes, and procedures, as well as organizational and managerial structures. Controls are reviewed periodically to ensure they are still appropriate.

We maintain a SOC 2 Type II certification. For more information please visit https://www.appdynamics.com/trust-center/security.

Third parties

We engage third-party service providers to help us provide our products and related services. More information about our third parties and a description of their activities is available at https://www.appdynamics.com/trust-center/privacy#subprocessors.