Data Collection and Processing

Cisco Secure Application

Product Overview

Cisco Secure Application delivers security to applications at runtime, by bringing together AppDynamics application insight and Cisco security knowledge, products and services to bridge the knowledge gap between application and security teams. Cisco Secure Application enables continuous vulnerability assessment and protection by scanning code execution to prevent possible exploits. Cisco Secure Application empowers AppDynamics customers by packaging Cisco Secure Application extensions with AppDynamics Performance Monitoring (APM) to provide proactive, runtime-aware security controls embedded in a single agent, brings security and application teams together, addressing their needs: maximize speed, performance, and uptime while minimizing security risk.

Data collected by Cisco Secure Application

Cisco Secure Application is accessible as part of the AppDynamics user interface and provides a real-time dashboard visibility on the security health of customer's applications. Cisco Secure Application software is designed to collect security events and buffer them during the duration of a transaction. Non-business events such as application runtime and execution behaviors that are not triggered by an inbound transaction can also be enabled to monitor situations to help application housekeeping functions.

Cisco Secure Application does not collect any privacy data and uses Business Transaction correlation and APM collected data through the APM agents. The data types listed below are collected and processed by a customer's unique instance of Cisco Secure Application software and collection is dependent on how the customer has configured the Cisco Secure Application software, APM agent and the nature of their monitored application(s).

AppDynamics Business Transaction with Security Vulnerabilities

The Cisco Secure Application maps security vulnerability events to applications, tiers, and nodes. To get more specific information about the business risk of the events, Cisco Secure Application correlates vulnerabilities to business transactions being monitored by AppDynamics.

Cisco Secure Application does not collect any privacy data for Business Transaction correlation and solely relies on APM collected data to provide different context for vulnerability impact if any for this specific Business Transaction.

Application Library Composition

Cisco Secure Application agent can be activated as part of AppDynamics APM agent installation by the Customer Application Administrator to monitor applications and report any vulnerable application library/code dependencies. Cisco Secure Application backend utilizes public databases to track vulnerabilities in open-source libraries. If and when the agent detects these vulnerabilities in the application or in the dependencies / libraries that the application is using, Cisco Secure Application reports these to the customer using the web-based dashboard.

Security Attack & Observation (Events)

Cisco Secure Application provides predefined fully configurable security policies to track and monitor certain system and application activities called events. You may consider an event as an application / system transaction (i.e. file processing, SQL execution, URL parsing etc.) Cisco Secure Application marks these events as an observation or attack based on policy configuration or associated risk and captures certain data points based on the event;

- Network event: source / target IP address, port number, requesting application or process etc.
- File processing event: file name, file path, requested operation, operation status etc.
- SQL transaction event: SQL query being executed, parameters used etc. (by default SQL queries are scrubbed)
- URL parsing event: URL & its parameters associated with application calls.
- Security snapshot / Stack trace: Any application failure, security events details and complete stack trace

Agent logs

Agent logs capture what changed within the target application, including configuration changes and application events. This helps the Cisco Secure Application User perform root cause analysis on failures and issues within the target application performance.

Snapshot data with Security Incident

Snapshot data captures any error or failure of the Target Application. This allows the Cisco Secure Application to perform and support root cause analysis of security failure in the Target Application.

URLs Associated with the Security Incident

The Cisco Secure Application can be configured to collect the URLs used within the application's functional calls, these URLs can be used to identify the business transaction(s) being performed.

Personal data collection and processing

Cisco Secure Application leverages data collected by AppDynamics APM agent and does not require the collection of personal data for any above-mentioned data types. Cisco Secure Application customer administrator can choose to disable the service on an app, tier or node level as well as specific policy on an app or tier level to manage the data collection, therefore, are in full control of data sharing with the Cisco Secure Application Software.

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.

Data Processing Locations

Cisco AppDynamics offers number of geographic hosting options where the Cisco AppDynamics controller is deployed in Infrastructure as a Service provider locations worldwide. For a list of the current deployment locations, please reference the Privacy Data Sheet on the Trust Portal at https://www.appdynamics.com/trust-center/privacy.

Cisco AppDynamics complies with applicable law when international transfers of its customers' personal data are made. Where a customer's use of Cisco AppDynamics products and services requires the transfer of personal data to a location outside the European Economic Area, Cisco AppDynamics employs Standard Contractual Clauses (also commonly referred to as EU Model Clauses) as a legally recognized data transfer mechanism.

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 for the Cisco Secure Application Software 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.

The Cisco Secure Application 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 but if the source data is corrected, the next time the product collects the data, it will be accurate. 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/privacy.

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 the https://www.appdynamics.com/trust-center/privacy#subprocessors