Data Collection and Processing

Internet of Things (IoT) Monitoring

Product Overview

At AppDynamics, we offer enterprise-grade software that enables our customers to monitor and analyze the performance of their business applications and supporting infrastructure. Our Internet of Things Monitoring software (IoT Software), one of our end user monitoring (EUM) products, monitors the performance of our customers mobile applications through the lens of a user's journey and interaction with the monitored applications running on an internet-enabled device.

The IoT Software can be deployed to our customers as a fully on-premise installation, consumed by our customers as software-as-a-service (SaaS), or made available as a "hybrid deployment" where the customer's on-premise AppDynamics software controller instance leverages our SaaS-based EUM Collector and EUM Cloud services (both discussed below) for temporary data processing.

The information below addresses SaaS and "hybrid deployment" versions of the Synthetic Monitoring Software; for fully on-premise installations, we do not have access to the data collected by the Synthetic Monitoring Software.

What data does the Synthetic Monitoring Software collect?

By default, our IoT Software does not collect any data at all, and the customer's IoT Software administrator must configure the IoT Software agent (or leverage our IoT SDK or REST API) to collect any of the types of performance data about an application running on a user's internet-enabled device listed below. Which data types set out below are actually collected and processed by a customer's unique instance of our IoT Software depends on how the customer chooses to configure their IoT Software and the nature of their monitored application.

IP address for internet-enabled device

.By default, the IoT Software collects the geographic location of an internet- enabled device at the time the device makes a connection to the monitored application. To resolve the location data, the internet-enabled device IP address is combined with geo-location data. The resolved geo-location data is sent to our SaaS infrastructure. By default, the IP address of the relevant internet-enabled device is discarded by our SaaS infrastructure and not retained. But the customer's IoT Software administrator can choose to change the default setting and configure their IoT Software settings to retain the user device IP address from the data beacon that is sent to our SaaS infrastructure for processing.

Application infrastructure usage data

The IoT Software can be configured to collect information regarding the perfor- mance of infrastructure components that support the monitored application during a user session, including firmware version and OS version.

Metrics related to the session

The IoT Software can be configured to collect the following session metrics: length of device activity stream and time on a specific URL during a session.

Crash reports and error reports

The IoT Software administrator can enable the collection of call stacks of crashes and errors within the monitored application code.

Custom data collection

The customer's IoT Software administrator may choose to enable the collection of customer parameters and/or payload information from within the monitored application by writing instrumenting through our SDK or REST APIs that instruct the IoT Software to collect any data that is accessible within the customers' application code.

Personal data collection and processing

AppDynamics Software does not require the collection of personal data and does not collect personal data by default. 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.
For more information about our privacy practices and how we process our customers' personal data, please visit our Privacy Center at https://www.appdynamics.com/privacy.

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/display/latest/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 emailing privacy@appdynamics.com or 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 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/security

Third parties

We engage third-party service providers to help us provide our products and related services. We maintain an up-to-date list of such third parties and a description of their activities at https://www.appdynamics.com/privacy/subprocessors.