APPDYNAMICS

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 IoT Software; for fully on-premise installations, we do not have access to the data collected by the IoT Software.

What data does the IoT 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 prior to any data beacon being sent to our SaaS infrastructure. The resolved geo-location data – without the IP address of the internet-enabled device – are sent to our SaaS infrastructure. By default, the IP address of the relevant internet-enabled device is not sent to our SaaS infrastructure for processing. But the customer's IoT Software administrator can choose to configure their IoT Software to include the internet-enabled 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 performance 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 parameter 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

The IoT Software does not require the collection of personal data and does not collect personal data by default. Customer administrators of the IoT Software must choose to configure the IoT Software to collect and process any data from within their monitored IoT application, and therefore our customer controls whether the IoT Software collects and processes personal data.

Where a customer administrator chooses to configure the IoT Software to collect and process personal data, we comply with applicable law when we make international transfers of such personal data. For international transfers, we employ the following legally-recognized data transfer mechanisms: the EU-US Privacy Shield, the Swiss-US Privacy Shield, and Standard Contractual Clauses (also commonly referred to as EU Model Clauses).

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* .

Does the IoT Software "track" my customers around the internet?

The IoT Software is designed to monitor an application associated with an internet-enabled device via the performance metrics noted above. All of these data help a customer understand how a real user experiences the monitored application. The IoT Software does not track our customer's application users around the internet as those users visit third-party sites and applications via their internet-enabled device. But, the AppDynamics IoT Software customer administrator can choose to configure the IoT Software to track device activity stream over time across the customer's monitored application. In order to provide this functionality (i.e., the ability to identify that the same device or set of devices experienced a crash/problem or series of crashes/problems with the same instance of the monitored application or across multiple instances of the monitored application), the IoT Software can be configured to use a technology that attaches a globally-unique identifier ("GUID") to each instance of the monitored application. The GUID is generated by the customer's development team and is attached to the performance data package as it leaves the monitored application and is sent over the internet to the nearest EUM Collector (described below). If a customer chooses to use the GUID user device identification method, the customer maintains the key needed to match the GUID with a specific user/device profile; this key is not stored within our SaaS infrastructure by default.

Where are data processed?

Data are collected by the AppDynamics IoT Software javascript agent (which is installed in the customer's monitored mobile application code) and the data are sent to the AppDynamics EUM software collector service (the EUM Collector). The EUM Collector is hosted in Amazon Web Services (AWS) in AWS edge regions around the world in order to provide low-latency connections to each customer device. The performance data are sent from the EUM Collector to the "EUM Cloud" where the data from worldwide EUM Collectors are aggregated. The AppDynamics controller downloads the aggregated data from the EUM Cloud once every minute for final processing, storage, and viewing by the customer.

For SaaS deployments, the the AppDynamics controller resides in our co-located data center located in Chicago, IL, United States, and leverages Amazon Web Services regions located in the United States as well as our EUM Collector and EUM Cloud services. For customers based in Europe, we offer a version of the IoT Software that utilizes Amazon Web Services located entirely within the European Union and the EUM Collector and EUM Cloud services.

For "hybrid deployments," the AppDynamics controller resides in the customer's datacenter and leverages our EUM Collector and EUM Cloud services.

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 are data retained?

Information about data retention for the IoT Software 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* .

The IoT 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 are corrected, the next time the product collects the data, it will be accurate. Customers can submit deletion requests for inaccurate data.

Are 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* .