Data Collection and Processing

Mobile Real User Monitoring (MRUM)

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 Mobile Real User Monitoring software (MRUM 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 their monitored mobile applications.

The MRUM 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 versions of the MRUM Software; for on-premise deployments, AppDynamics does not have access to the data collected by the MRUM Software.

What data does the MRUM Software collect?

Our MRUM Software is designed to collect the types of performance data about our customers' browser-based applications listed below. Which data types set out below are actually collected and processed by a customer's unique instance of our MRUM Software depends on how the customer chooses to configure their MRUM Software and the nature of their monitored mobile application.

IP address for user device

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

Copyright © 2021 AppDynamics, LLC. All rights reserved.

Application infrastructure usage data

The MRUM Software can be enabled to collect information regarding the per- formance of infrastructure components that support the monitored mobile application during a user session. These performance data may include: operating system information (type, version), application information (type version), title of page visited, URL of page visited, and URLs of assets loaded on the relevant web page.

Metrics related to the session

The MRUM Software can be configured to collect the following session metrics: length of browsing session and time on a specific URL during session.

Crash reports and error reports

The MRUM Software customer administrator can enable the collection of call stacks of crashes and errors within the mobile application code.

Custom data collection

The customer's MRUM Software administrator may choose to enable the collection of customer parameter and/or payload information using the MRUM Software SDK by writing application code to collect any data that is accessible within the customer's mobile application.

Mobile screen shots

Screenshots of what a user viewed within a user's mobile application instance can be taken at the time of crash or error in the mobile application. The collection of mobile screenshots is disabled by default, and the MRUM Software customer administrator can choose to enable the collection of mobile screenshots using the RBAC supported configuration settings in the product UI.

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.

Copyright © 2021 AppDynamics, LLC. All rights reserved.

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

Copyright © 2021 AppDynamics, LLC. All rights reserved.

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.

Copyright © 2021 AppDynamics, LLC. All rights reserved.