Data Collection and Processing

Browser Synthetic 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 Browser Synthetic Monitoring software (Synthetic Moni- toring Software), one of our end user monitoring (EUM) products, allows our customers to use synthetic traffic as a proxy to understand and analyze the performance of their browser-based applications. With our Synthetic Monitoring Software, our customers can see how a real user experiences the performance of a web application vis-a-vis synthetic traffic that simulates a real user's device during a browsing session with the monitored application.

The Synthetic Monitoring 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?

The Synthetic Monitoring Software generates simulated user traffic from geographic locations selected by our customer and then makes requests to the monitored application. This traffic-request simulation emulates the traffic load that a real user from the same geographic location would place on the monitored application. The Synthetic Monitoring Software then collects and processes metric performance data related to the relevant traffic-request simulation.

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

Application infrastructure usage data

The Synthetic Monitoring Software can be configured to collect information regarding the performance of infrastructure components that support the monitored application during a user session. These performance data may include: web browser information (type, version), title of page visited, URL of page visited, and URLs of assets loaded on page.

Resource timing aggregation data

This data class includes: webpage element load times, and timing of response from the application to relevant web servers.

Metrics related to the session

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

Script crash logs & error reports

The Synthetic Monitoring Software administrator can enable the collection of script crashes and scripting errors executed within the synthetic agent for the monitored application.

Monitored application screenshots

A screenshot of the viewable area is captured for each URL test or page within a synthetic session.

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.