

Data Collection and Processing

Application Performance Management (APM)

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 Application Performance Management software (APM Software) monitors the performance of our customers' business applications by delivering application mapping, dynamic baselining, and code-level diagnostics. Our customers can use the APM Software to map their application environment, see how components are connected, baseline performance within the application environment, and obtain code-level diagnostics to support root cause analysis and troubleshooting for business-critical applications.

Our APM Software currently supports monitoring of applications written in a variety of application programming languages. The APM Software can be deployed to our customers as an on-premise installation or consumed by our customers as software-as-a-service (SaaS).

The information below addresses SaaS versions of the APM Software; for on-premise deployments, we do not have access to the data collected by the APM Software.

What data does the APM Software collect?

By default, the APM Software does not collect any payload or parameter data in the application(s) it is configured to monitor. Our customers' APM Software administrator may choose to collect parameter and/or payload information using the role-based access controlled data collector settings within the APM Software user interface.

Our APM Software is designed to collect the types of performance data from our customers' application(s) as listed below.

Business transaction name

A "business transaction" is a process identified within their application(s) that the customer chooses to monitor (e.g., "log in," "check out," or "search for flights"). The APM Software can auto-discover certain common business transactions and name them accordingly; but a customer can always choose to apply a custom name to any business transaction they identify and choose to monitor

using the RBAC-supported configuration management functionality available within the APM Software.

Business transaction snapshot data

Our APM Software monitors every execution of a business transaction in the instrumented environment, and the collected metrics reflect all such executions. However, for troubleshooting purposes, AppDynamics takes snapshots of specific instances of a transaction. A transaction snapshot gives the customer a cross-tier view of the processing flow for a single invocation of a business transaction. Snapshot data may include call entry and exit points (e.g., URLs or queue names), call stacks, and error details (if the snapshot is associated with an error).

URLs associated with a business transaction

Business transactions utilize networked infrastructure for execution and data transmission. The APM Software collects URLs that are utilized in supporting the business transactions that a customer chooses to identify and monitor.

Performance metric data

These data consist of numeric information representing the resource utilization of a customer's application while executing a business transaction. Metrics include average end-to-end latency, number of slow end-to-end messages, and number of slow end-to-end latency times.

Agent logs

These files can help a customer administrator resolve configuration and instrumentation issues within the APM Software. Agent logs are configurable by the customer administrator and may include the following information: APM Software agent version and build date, application runtime metadata (e.g., for Java applications, the JVM runtime version), configuration changes, backend detection, exceptions, and output from logging session requests.

Personal data collection and processing

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/trust-center/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/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.

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. 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/security>.

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

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