APPDYNAMICS

Data Collection and Processing

Network Visibility

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 Network Visibility Software monitors the performance of the networking infrastructure that supports our customer's business application(s) by discovering and displaying application and network topology and interdependencies, tracking network KPIs including throughput, packet loss, and RT rates, and helping development teams troubleshoot and diagnose network related problems. The Network Visibility Software can be deployed to customers as either an on-premise installation or as software-as-a-service (SaaS).

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

What data does the Network Visibility Software collect?

Our Network Visibility Software is designed to collect the performance data about our customers' network infrastructure listed below. Which data types below are actually collected and processed by a customer's unique instance of our Network Visibility Software depends on how the customer has configured the Network Visibility Software and the monitored network infrastructure components.

Network performance metrics The following types of metric performance data can be collected by the Network Visibility Software: TCP connection information, link metrics, host level metrics on the network infrastructure components.

Source and destination machine IP addresses The Network Visibility Software can be configured to collect IP addresses associated with machines that are included within the monitored network infrastructure.

Packet information By default, the Network Visibility Software does not collect any parameter or payload values from within the network infrastructure components it is configured to monitor. Our customers' Network Visibility Software administrator may choose to change the default setting and enable the Network Visibility Software to collect packets transmitted over the monitored network infrastructure components by using the role-based access controlled settings within the Network Visibility Software user interface. If this setting is turned on, the packets are sent to storage of the customer's choice, are retained for the period set by the network admin, and we do not host nor process the data during such time.

Personal data collection and processing

The Network Visibility Software does not require the collection of personal data and does not collect personal data by default. Customer administrators of the Network Visibility Software can choose to configure the Network Visibility Software to collect packet information for remote storage (described above), but we do not store, nor do we process those data. As with all of our products, our customers can control whether the Network Visibility Software collects and processes personal data.

Where a customer administrator chooses to configure the Network Visibility 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* .

Where are data processed?

The Network Visibility Software leverages a co-located data center located in Chicago, IL, United States, as well as Amazon Web Services regions located in the United States. For customers based in Europe, we offer a version of the Network Visibility Software that uses Amazon Web Services located entirely within the European Union.

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 Network Visibility 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 Network Visibility 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* .