
Forcepoint
Dynamic User Protection
Management of Personal Data

CONTENTS

© 2023 Forcepoint LLC. All Rights Reserved

Disclaimer

This document contains information regarding Forcepoint products and/or services. The information is Forcepoint's property. While every effort was made to ensure the content is up-to-date and accurate, the information is provided AS IS, without any representation or warranty, express or implied, and is subject to change without notice. Any references to future releases or functionality are forecasts and not intended to be commitments. Forcepoint assumes no liability for the use of this information.

©2023 Forcepoint. All Rights Reserved.

General

Document Purpose

This document is designed to answer the question: "What personal data is stored in Forcepoint Dynamic User Protection?" It is primarily intended for those involved in the procurement and privacy assessment of Forcepoint Dynamic User Protection.

Data Privacy Laws

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted on April 27, 2016 and came into effect on May 25, 2018. GDPR, along with other applicable data privacy laws, guide the principles that are incorporated in Forcepoint's privacy policies and processes, both internally and externally. Full details of the GDPR can be found in various sources, including https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Forcepoint Dynamic User Protection is designed to comply with applicable data privacy principles, including those contained in GDPR. Consistent with these principles, Forcepoint's customers are considered to be the sole data controller. Forcepoint is the data processor with respect to customer data transferred through or stored in Forcepoint Dynamic User Protection

Personal Data

This document adheres to the definition of personal data as defined in article 4.1 of the General Data Protection Regulation, which defines 'personal data' as any information relating to an identified or identifiable natural person ('Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Safeguarding Personal Data

Forcepoint uses industry-standard techniques to protect data held within the Forcepoint product, including personal data. Full details on Forcepoint's privacy policy and processes can be found at: https://www.forcepoint.com/forcepoint-privacy-hub.

TERMINOLOGY

Terms used in this document are as follows. Interested readers are required to familiarize themselves with these terms and their explanations before reading subsequent sections.

Term	Explanation
UIS	User Information Service – the micro-service that stores information imported from Directory Service and make it available for any product that likes to consume it
Device and System Properties	Consist of device metadata such as the host name, domain, device name, user signed in, OS, time zone, and device specs
Dynamic User Protection (DUP)	A solution that relies on Endpoint components to monitor the end user activities on Windows and macOS operating systems and reports Alerts to a Cloud Backend Storage. The Alerts are used to evaluate users' risk. Users and alerts can be investigated via a web user interface that runs in AWS cloud
Activity	Any operation performed by the end user or by an application in use by the end user Examples are: File copied to removable storage Email sent File printed File copied to a Network Share
Event	All activities on the endpoint are represented as events which are processed by the policy engine on the endpoint.
Alert	If an event matches a policy rule, then the policy rule engine may trigger an alert that is a form of message that is sent to the DUP cloud storage and which can be displayed to administrators that investigate risky users and alerts. Alerts are associated with a risk impact.
User	Any employee that access a computer system
Risky User	An employee that has performed one or more activities which generated alerts. The user risk is calculated based on the combination of the risk impact of alerts triggered by the user (it is not a sum, it is a mathematical formula that takes that takes into account multiple risk impacts and calculates the total risk score)

First Time Device Registration & Periodic Sending of Device (System) Properties

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Registration and Device and System Properties	The Device and System Properties consists of device metadata such as the host name, domain, device name, user signed in, OS, time zone, and device specs. The "user signed in" information contains the following: • user type - Domain if the logged in user was a Domain user or local if the user was a local user on the device in question. In the case of a local user, Neo will send the device's hostname as the domain or the custom domain name if configured by the Admin. • the user principal name (if available), and • the username used by the user when logging in, and • down level logon name consisting of the domain and the username	The software runs on the endpoint (Windows or MacOS) and calls to the AWS API gateway to register the device immediately after installation, and then sends Device and System Properties every 5 minutes to the cloud.	The device information is not pseudo anonymized presently. In the future, a feature that masks user information will be implemented.	This data is protected in transit and at rest. The device registration is sent by endpoint to DUP over an HTTPS secured connection (TLS 1.2). The registration process creates a device specific digital certificate (per endpoint) which the endpoint will use for all future communications with the Cloud backend. Then device properties are sent over MQTT secure communication that use the device specific digital certificate to secure the communication using TLS 1.2. The Device and System Properties are encrypted at rest using AES256.	Device and System Properties are retained in the Forcepoint AWS account until a system is deleted. Whenever a new user log to the system the logged-on user info is updated and the previous logged in user is overridden.

Reporting Alerts from Endpoint to Cloud Storage

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
Alerts contain information about the system on which the event triggered and the details of the user that performed the activities that lead to the alert System information relates to the device upon which the endpoint is installed. This typically includes: domain, hostname, OS and system information. User information relates to the currently logged in User at the time the Alert was generated. The information reported is consistent with the User information described in the *Registration and Device and System Properties* dataset described above.	The DUP endpoint software runs on Windows and macOS devices and monitors the activities on the system. All activities are sent to the policy engine locally on the endpoint in the form of events. The policy engine evaluates the events and triggers Alerts when a single (or multiple) events break the corporate policy. Note: User Activity or Device Control events are analyzed by the DUP policy engine. DLP events are analyzed by the DLP Policy Engine. If an event is related to both DLP and User Activity Monitoring or Device Control then an event can be analyzed multiple times in parallel. Alerts are sent to the DUP cloud storage and presented to the customer DUP admin who can investigate the Alerts via a web user interface (the DUP cloud console – note the customer DUP admin can be a full admin or an admin assigned to the Analyst role)	The purpose of the DUP solution is to monitor user activities and report alerts when a user performs an activity which is considered a breach of corporate policy. The purpose of an admin is to investigate users and suspicious activities to protect the organization against threats to the confidentiality of data, integrity of data, and availability of data.	No pseudo anonymization. The Alerts and Events data are stored as JSON files with include information about user that performed the activities and system on which the activities took place.	Alerts and Events are sent from endpoint to cloud over secure communication channel (MQTT) which utilizes TLS 1.2. The Alerts and Events data (JSON files) reside in the Alert data store which is encrypted at rest by AES256 and in the Archive. The Archive is also encrypted at rest by AES256. Each tenant has an alias which separates his data from other tenants (of the same customers and from tenants of other customers) alerts and events in order to prevent accidental access to other tenant's data.	Alerts and the supporting events (activity information that lead to the reporting of the alert) are stored for a period of 3 months in the Alert Data Store. In addition, the alerts are stored for a period of 12 months in the Archive.

Reporting Activity Counters from Endpoint to Cloud Storage

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The Counter itself is just a number that indicates how many activities the user (or applications) performed, and the total size of data that was involved.	Counters are plain numbers which count the number of activities that a user performs, for example how many files are copied to removable storage, how many emails are sent, or how many files the user prints. The counter metadata also includes the user identification (that performed the activities) and the computer activities on which the activities were performed. User information relates to the currently logged in user associated with the active record in the counters. The information reported is consistent with the User information described above in the *Registration and Device and System Properties* dataset.	The purpose of counters is to show as numbers (dashboards, histograms) the summary of user activities. In addition, the counters are used to build a baseline activity model of the user and help the anomaly detection engine to find significant deviations in user activity in order to report them as alerts.	No pseudo anonymization. The Counters data will be stored as JSON data and contain information about user that performed the activities and system on which the activities took place.	Counters information is sent to cloud via the same encrypted communication transport as events and alerts which uses TLS 1.2 and will be stored into Counters and Summary Data Store that is set to encrypt the data at rest by AES256.	Counters are sent to the cloud every hour and kept for a period of 3 months in the Counters and Summary Data Store.

© 2023 Forcepoint LLC. All Rights Reserved

Admin Login to Cloud Management Console

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The email address, first name and last name of each DUP customer admin are stored in a user-pool that is dedicated for the customer.	The data for login is the user email address and his password. Cognito stores the user first name, last name, and email address as well as the user password.	Administrators need to login into the Cloud management console to define policy rules and to investigate alerts and threats	The user (admin) information such first name, last name and email are not pseudo anonymized inside Cognito, but they are encrypted by AWS Cognito. For more details about Cognito and its security compliance see https://aws.amazon.com/cognito/details/	Cognito encrypts the users (admin) data at rest using AES256 and also encrypts the data in transit (TLS 1.2 or higher) in addition, Cognito is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.	The admin personal data – first name, last name and email address are stored in Cognito for the duration that the user is listed as an admin of the DUP application.

© 2023 Forcepoint LLC. All Rights Reserved

Administrator Investigating a Risky User

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The list of top risky users is displayed in the DUP management console. Shown below:	The user information including first name, last name, and email address. The alerts include the system information (computer name) User information relates to User information detected by the endpoint at user login and optionally information that is imported by the customer DUP Admin into the service. The information reported is consistent with the User information described above in the *Registration and Device and System Properties* dataset. If information is imported, it is automatically correlated / joined with the information detected by the endpoint during login events. Information imported can include the username – first name, last name, email address, and the User's manager. This information is entirely optional and typically used to enrich the default information detected by the endpoint.	Customer DUP Administrators invest most of their time reviewing risky users and investigating alerts that were triggered by users. The details displayed in the investigator help the customer DUP admins to determine if the Alert is indeed a threat.	Both User and Alert information are not pseudo anonymized presently. In the future, a feature that masks user information will be implemented.	The data is stored encrypted at rest in the respective data storage (the encryption is AES256 in both cases). All communication with the User Information Service (UIS) is encrypted in motion by using HTTPS and TLS 1.2	The user data is kept in the User Information Service (UIS) as long as the user is a member of the organization. The Alerts data is retained for a period of 3 months in the Alert Store and for 12 months in the Archive. The Archive data is not accessible to an admin, but access can be requested. The purpose of the Archive is to retain alert data for back up and long-term investigations. By default, the archive retains alert data for 12 months but is configurable upon request.

Administrator Investigating an Individual Alert

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow & Protection	Retention
The Alert data contains information about the activity that an end-user or application performed.	The alert contains the User information associated with the alert . The alerts also contain the computer details on which the activity was performed. User information relates to user information detected by the endpoint at user login and optionally information that is imported by the customer DUP Admin into the service. The information reported is consistent with the User information described above in the *Registration and Device and System Properties* dataset. If information is imported, it is automatically correlated / joined with the information detected by the endpoint during login events. The information imported will be consistent with the imported User information described above in the *Administrator Investigating a Risky User* dataset.	Customer DUP Administrators invest most of their time reviewing risky users and investigating alerts that were triggered by users. The details displayed in the investigator help the customer DUP admins to determine if the Alert is indeed a threat.	Alert information is not pseudo anonymized presently. In the future, a feature that masks user information will be implemented.	The Alerts information is sent over secured communication channel (TLS 1.2) to the cloud. The information is encrypted at rest inside the Alert Store by AES256.	The Alerts data is retained for a period of 3 months in the Alert Store and for 12 months in the Archive. The Archive data is not accessible to an admin, but access can be requested. The purpose of the Archive is to retain alert data for back up and long-term investigations. By default, the archive retains alert data for 12 months but is configurable upon request.

© 2023 Forcepoint LLC. All Rights Reserved