Data Security Management of Personal Data

March 2026

Forcepoint

Table of Contents

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.

General

Document Purpose
This document is designed to answer the question: “What personal data is stored in Forcepoint Data Security?” It is primarily intended for those involved in the procurement and privacy assessment of Forcepoint Data Security.

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 Data Security is designed to comply with applicable data privacy principles, including those contained in GDPR. Consistent with these principles, Forcepoint’s customers are the sole data controller. Forcepoint is the data processor with respect to customer data processed through Forcepoint Data Security.

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.

Forcepoint Data Security

Solution Overview

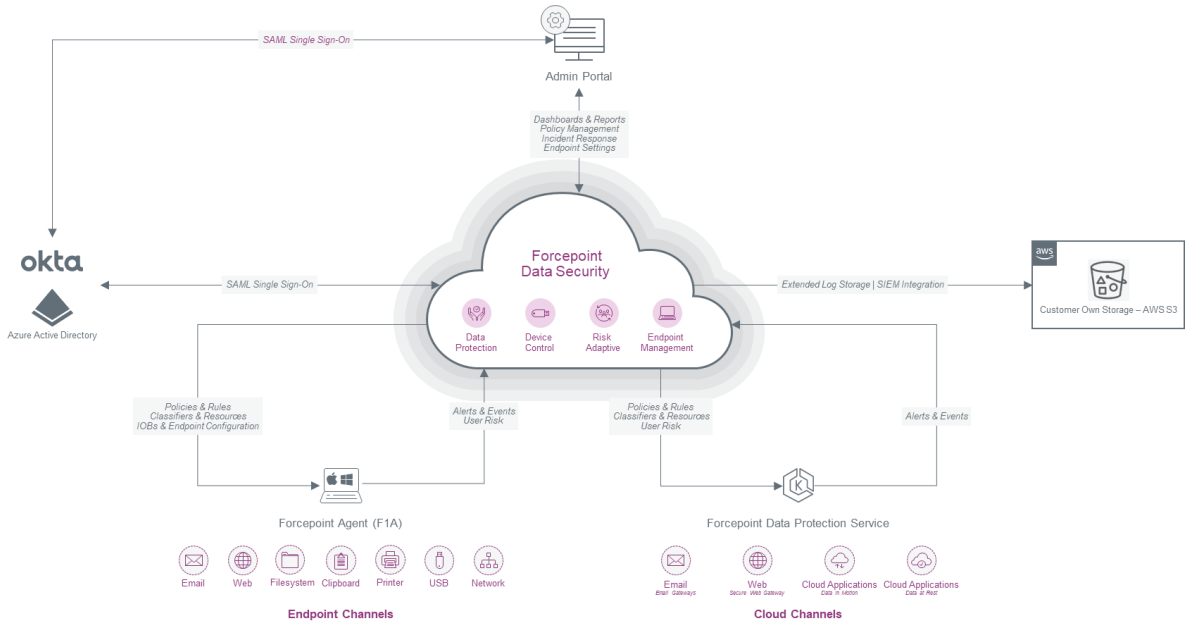

Image 1 – Solution Overview

Forcepoint Data Security combines Data Loss Prevention (DLP), device control, user activity monitoring and endpoint management delivered as part of Forcepoint Data Security Cloud. Designed to prevent sensitive data exfiltration across cloud, web, email and endpoint channels with consistent policy enforcement, it works by monitoring network and data security activities and reporting these activities to the policy engine, which identifies activities that the enterprise customer has determined should be assessed from a data protection and/or risk perspective. The Forcepoint Data Security policy engine is deployed across cloud Applications, web, email and endpoint channels as part of the Forcepoint Data Protection Service for integration with Forcepoint Cloud App Security, Forcepoint Web Security and Forcepoint Data Security for Email. The Data Security policy engine is also part of the Forcepoint endpoint agent for direct enforcement of organizations' data security policies across user endpoints. This ensures consistent data protection regardless of where data resides or how it moves.

The endpoint agent delivered as part of the solution can also optionally support web control and web traffic redirection to Forcepoint Web Security proxies (cloud web or hybrid web).

Activities are reported to the Forcepoint Data Security policy engine to identify activities that the enterprise customer has determined should be assessed from a data protection and/or risk perspective. Below are examples of activities:

- Endpoint Channel:
    - A file is copied to removable storage
    - A file is printed to a local printer
    - A new process starts
    - A new product is installed on the system
    - Windows security event logs are deleted
    - Printing of files
    - Access and use of USB removable media
- Email Channel: An outbound email is sent
- Web Channel: Content is posted or uploaded to an external website
- Cloud Applications: Content is uploaded to a monitored cloud application

The solution inspects the events and report ***alerts*** to a cloud management console when an activity (event) is performed that is defined as breaching the corporate policies such as data exfiltration, data protection or data exposure policy.

The corporate policy is a set of ***policies*** and ***rules*** that define which activities are considered as data exposure, data exfiltration or data protection breach.

Examples of alerts are:

- Suspicious number of files uploaded to a personal cloud storage (Data Exfiltration)
- Suspicious size of file(s) copied to removable storage (Data Exfiltration)
- Attempt made to kill the endpoint agent process, tamper or disable the endpoint agent product on macOS or Windows OS (Defense Evasion)
- Deletion of Windows security event logs to hide activities (Defense Evasion)
- Sharing of corporate OneDrive folder with unauthorized external recipients (Data Exposure)
- Saving of files to USB removable media wen the associated device control rules indicate that only read-only access is supported
- Attempt to print a document matching one or more data loss prevention rules

An alert can be a result of a single activity (event) or multiple activities (events). For example:

- Deletion of Windows security event logs to hide activities is a single event that is reported as an alert (Defense Evasion)
- A very large ZIP file copied to removable storage is a single event that is reported as an alert (Data Exfiltration)
- Uploading of 350 source code files to a personal Dropbox is 350 individual events (each file is an event) that together trigger an anomaly detection rule and report an alert due to suspicious number of files uploaded to personal cloud storage (Data Exfiltration)

Features

Data Protection allows the admin to define DLP policies and rules. It includes a set of **predefined data classifiers** which allow an admin to identify different types of sensitive data alongside a set of **predefined policies** enabling compliance for different use-cases including PII, PCI, PHI (e.g., HIPAA) and intellectual property. Admins can use these templates out of the box or as a starting point. Alternatively, admins can also define completely bespoke policies using the available data classifiers. Rules can also be specified to apply to **channels**. A channel identifies the means of the data exfiltration attempt and can be other Forcepoint products such as Forcepoint Cloud App Security, Forcepoint Web Security or Forcepoint Data Security for Email. A channel can also be the Forcepoint endpoint when data protection is enforced directly on user endpoints. In this way an organization has granular control over the types of data monitored and where this monitoring is applied, ensuring consistent protection across channels.

Device Control allows an admin to define a set of access control rules governing the use of USB removable media on devices where the Forcepoint endpoint agent is installed. Administrators can determine whether removable storage devices can be connected and whether users can only read from or write to them. In addition, content control allows for the inspection and management of data movement between endpoints and removable storage devices, providing enhanced security and data protection.

It automatically reports every removable storage device that is plugged into a system where the Forcepoint agent is running. This capability allows the Forcepoint Data Security admins to gain complete visibility to all the removable storage devices that have been used in the organization over the last 90 days.

In addition, an admin can see when each device was plugged in and the list of filenames (without content) of all files that were copied to the removable device (“potential exfiltration”), along with the filenames of all files that were copied from the removable device (“potential trouble coming in”).

Device Control also allows an administrator to create device control rules which can limit the access permissions of end users (or groups) to read or write from removable storage and can achieve the following use cases:

- Block/Allow all removable storage for all users or user groups on all systems
- Set all removable storage to read-only for specific user groups on specific systems
- Allow specific device based on device serial number or vendor ID (SanDisk) or Product ID (Cruzer Mini)
- Block specific device based on device serial number or vendor ID (SanDisk) or Product ID (Cruzer Mini)
- Set specific device to read-only based on device serial number or vendor ID (SanDisk) or Product ID (Cruzer Mini)

Risk Adaptive Protection is also specific to the Forcepoint Endpoint and comes with a set of **out-of-the-box rules** which are created by Forcepoint Research (including X-labs). The customer admin can edit and modify these rules so that they are enforced on specific endpoints, accounts or groups or edited to exclude specific endpoints, accounts or groups from being monitored by the rules. The feature continuously evaluates user behavior to build a dynamic individual risk profile, expressed as a dynamic risk score. Policies can then adjust their enforcement posture in real time based on that score — applying stricter controls to higher-risk activity and relaxing them where risk is low. This adaptive approach delivers more precise enforcement and materially reduces false positives compared to static, threshold-based rules.

Forcepoint Data Security includes an audit log to track the changes that admins perform and exercise appropriate governance on the administrator activities and policy implementation across all supported use cases.

When generating **alerts,** the solution if configured will report alert metadata to the cloud back-end storage. The organization's admin can also optionally configure the capture and reporting of **forensic data**. Forensic data in this case refers to the precise values that triggered the violation and capture of the actual file or email that triggered the alert (limited to a maximum file size of 20 MB).

Forensic data stored in the Forcepoint Data Security Cloud is subject to content encryption. When forensic data is securely received, the data is encrypted using a data encryption key that is generated for each individual alert. The data encryption key is unique to the individual tenant and to that transaction. The encrypted forensic data is then stored in the Forcepoint cloud. The data encryption key is then also encrypted using a tenant specific key that is unique to that tenant and stored alongside the forensic data. Access to forensic data is also strictly controlled and audited to ensure full data governance.

In addition to alerts, the system reports endpoint **system properties** such as the computer name, the IP address and the end user that is currently logged to the endpoint. The system properties are sent to the cloud back-end storage and visible to the administrator via the cloud management console (see image 3 in workflow 1 below).

In addition to system properties and alerts, the product also reports periodic **counters**, which are a form of telemetry that identifies the type and count of activities the endpoint or account has performed hour after hour. These counters are used to create a user activity model that helps the solution to identify abnormal user activity by looking for significant deviations in each individual user activity pattern.

When reporting events/alerts, the solution will include the **classification** of the data that was inspected by the event/alert. For example, if a user is copying source-code to removable storage, then the corresponding alert will inform the customer admin that the file copied included source-code.

The data classification can potentially identify personal information such as driver license, email address, first and last name or even drugs and diseases (personal health keywords that are part of the out-of-the-box classifiers) and credit card numbers which are identified by regular expressions. The solution can report the actual word or keywords that were matched as part of the forensic data captured. This is subject to administrative control and, if captured, is stored using content encryption. Administrative access to this data is also subject to RBAC and any access is recorded as part of the tenant's audit trail.

Web Control is a capability of the endpoint that allows it to act as the endpoint enforcer for Forcepoint Web Security, in cloud or hybrid mode. When active, the endpoint web control downloads configuration from the associated Cloud Security Gateway (CSG) portal and enforces it on the endpoint by redirecting web traffic of specified websites (URLs) to the Forcepoint web proxies, which determine whether to block the HTTP/S request or allow it.

The web proxy can also determine whether to inspect (in the web proxy itself) the content of the HTTP/S request, including AV scan or DLP scan, by integrating with the Forcepoint Data Protection Service.

Web functionality is not within the scope of this document. The endpoint agent's web control capability only focuses on determining which website's traffic should be redirected to the web service, and not on inspecting the content of the traffic.

Admin Roles and Pseudo Anonymization

The solution supports pseudo anonymization for information displayed through the cloud management console. It is only applied to the Analyst role. Four roles are supported today – Administrator, Investigator, Analyst and Helpdesk.

		Roles			
Function	**Purpose**	**Administrator**	**Investigator**	**Analyst**	**Helpdesk**
Getting Started					
Getting Started	General home page with quick links to endpoint download and what's new	Full	Full	Full	Full
Dashboards					
Users	Summary view of end user activities across the organization	Full	Full	Anonymized	None
Endpoints	Summary view of the status of Forcepoint endpoint agents across the organization	Full	None	None	Full
Devices	Summary view of the use of removable media devices on user endpoints running the Forcepoint agent	Full	Full	Anonymized	None
Investigation					
Users	View-per-user details on risk level of activities, most recent activity, alerts and other details.	Full	Full	Anonymized	None
Alerts	View detailed information on individual alerts as part of incident response	Full	Full	Anonymized	None
Alerts – Snippet Data	Can see **masked** snippet data or unmask to view the snippet data (Any request to unmask is tracked in the account's audit trail)	Full	Full	None	None
Alerts – Evidence File	Can **download** a decrypted copy of the evidence file stored in the Forcepoint cloud (Any request to download is tracked in the account's audit trail)	Full	Full	None	None
Devices	View-per-USB-removable-device usage details	Full	Full	Anonymized	None

		Roles			
Function	**Purpose**	**Administrator**	**Investigator**	**Analyst**	**Helpdesk**
Endpoint Management					
My Endpoints	View the status of all Forcepoint Data Security agents deployed across the organization	Full	None	None	Full
Profile	Manage configuration settings for the Forcepoint endpoint	Full	None	None	Full
Release Code	Generate master release code for agent uninstall and use of diagnostic tools	Full	None	None	Full
Policy					
Data Protection	Data Loss Prevention policy settings	Full	None	None	None
Device Control	USB Removal Media policy settings	Full	None	None	None
Activity Monitoring	Activity Monitoring policy settings	Full	None	None	None
Settings					
Admins	Manage Admin access to the management console	Full	None	None	None
Audit Log	View the audit log	Full	None	None	None
Advanced	Set up SAML SSO and AWS replication	Full	None	None	None

The remainder of this document will explore the data flows that report the above information to the cloud back-end storage.

System Component: Alerts, Forensic Data, Events and Counters

Following is a diagram of the high-level architecture of the Forcepoint Data Security platform which is the basis for the Web Control product capabilities. Each of the information data objects that are sent from the endpoint to the cloud or from Forcepoint Data Security for Email, Forcepoint Cloud App Security or Forcepoint Web Security can potentially contain private/personal information. The following sections will elaborate on each data flow between the client (endpoint or Forcepoint Data Protection Service) and the cloud components, with analysis from a data protection and privacy perspective.

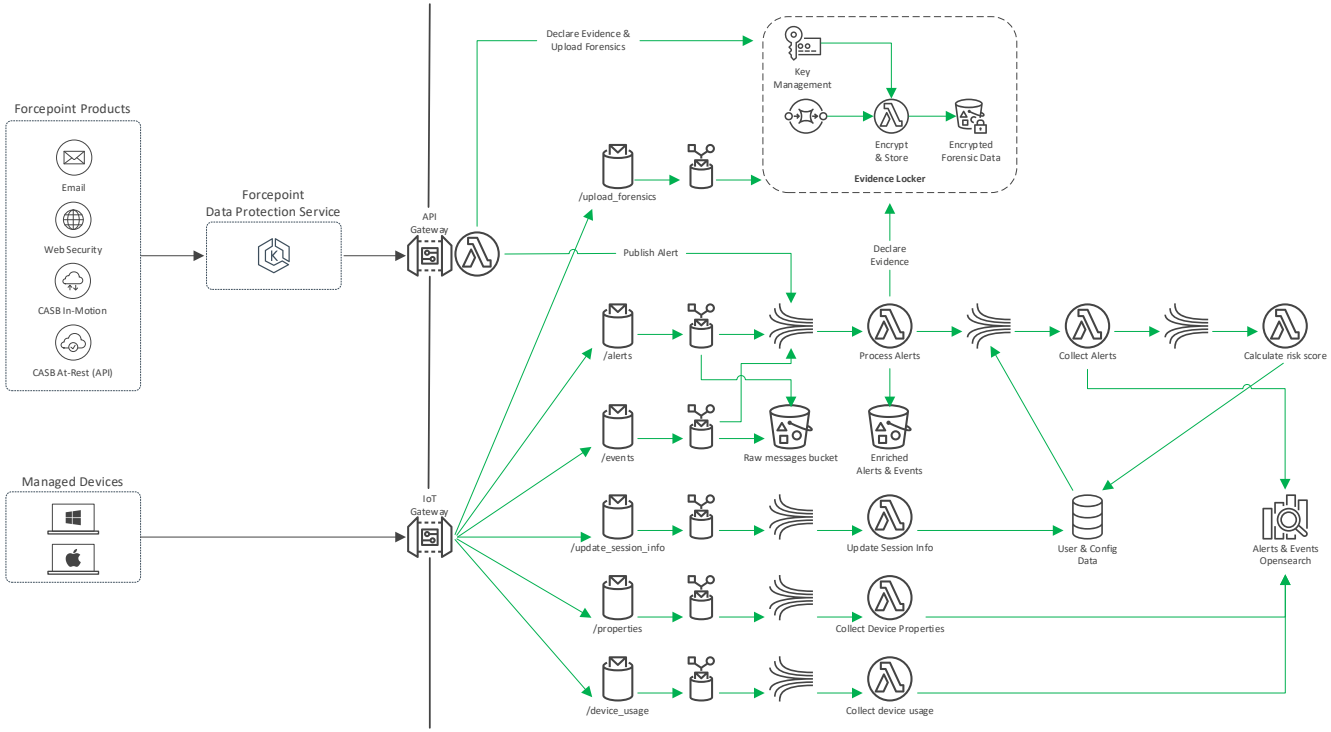

Image 2 – Alerts, Forensic Data, Events and Counters

Components

- **Forcepoint Data Protection Service** – A cloud-based deployment of the DLP policy engine that scans submitted content for the purpose of applying a customer's Forcepoint DLP policies. It enables integration between Forcepoint Data Security and other Forcepoint cloud products Forcepoint Cloud App Security, Forcepoint Web Security and Forcepoint Data Security for Email. These cloud products capture content that should be subject to DLP according to an organization's configured access policies (cloud application, web or email). When content is captured, it is forwarded over a secure channel to the associated DLP policy engine, which then applies the organization's DLP policies. The resulting verdict (allow/block) is returned to the client

product and, if configured, a resulting alert together with any forensic data is sent securely to the Forcepoint Data Security back end. The Forcepoint Data Protection Service allocates individual PODS (EC2 Instances) – DLP policy engines – for the processing of requests on a per-tenant basis. In this way all tenant information is fully isolated.

- **Managed Devices** for Windows and macOS – Devices running the Forcepoint endpoint, where the data is gathered and sent to the cloud. Endpoints communicate to the cloud back end over a secure communications channel that leverages TLS 1.2 and AES256 encryption.
- **IoT Core**, IoT Topics (Basic Ingest) and IoT Rules – Simply a data stream mechanism that redirects the data that is reported from the endpoints to the correct data storage.
- **Alerts and Events Analytics Storage (OpenSearch)** – Data storage that is used to keep and index alerts information as well as the events that caused the alert to trigger. The alerts and events are stored for a period of 3 months. Alerts and events include information that identifies the logged end user that performed the activities which caused the alert, as well as information about the endpoint system on which the alert was triggered.
- **Alerts and Events Archive Storage (S3)** – Storage that is used to keep alerts and events for a period of 12 months. The data is stored in the S3 bucket for the purpose of archiving in case an alert older than 3 months has to be investigated. Customers can also optionally configure their Forcepoint Data Security service to use the Amazon Replication Service to replicate alerts, event and or audit logs to a customer's own S3 bucket. If enabled, Forcepoint Data Security will replicate the identified objects to the configured bucket from this point. This can be used for long-term storage retention and external SIEM integration.
- **Evidence Locker** – A secure data storage layer that is used to store forensic data. Objects stored within the evidence locker are stored using content encryption, and each object is encrypted with a unique data encryption key. The data encryption key used is also encrypted using a tenant specific key and stored alongside the forensic object it was used to encrypt. Data held within the evidence locker is subject to a separate retention period of 30 days. Access to the data held within the evidence locker is also subject to roles-based access control and is audited as part of the tenant's audit trail.
- **User and Configuration Data (Aurora and DynamoDB)** – Storage that keeps Policy Configuration (Aurora) and counters and summary user data (Dynamo DB). Policy configuration refers to the Data Protection policies that the administrator defines. Counters and summary user data will typically include the count of activities that a user performs. The counter includes the number of activities that user performed (e.g., How many files did the user copy to cloud between 14:00 to 15:00?) and the total size of data that these activities included. The counter also includes the logged-in user identification information as well as the system information on which the activities were performed.

System Component: Portal Access

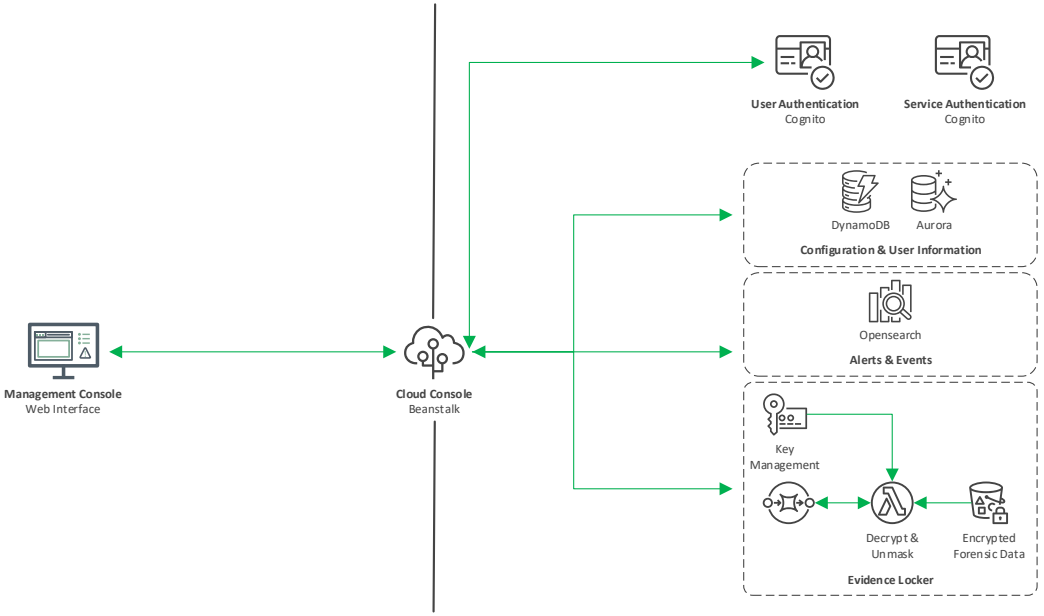

Image 3 – Portal Access

Components

- **Management Console (Beanstalk)** – A web user interface that provides the customer administrator the ability to search users, sorted by activity risk, and then investigate the activities (events and alerts) that led to this risk score.
- **User and Configuration Data (Aurora and DynamoDB)** – Storage that keeps Policy Configuration (Aurora) and counters and summary user data (Dynamo DB). Policy configuration refers to the data security policies that the administrator defines. Only correctly authenticated admins with the full administrator role have access to policy. Counters and summary user data will typically include the count of activities that a user performs. The counter includes the number of activities that user performed (e.g., How many files did the user copy to cloud between 14:00 to 15:00?) and the total size of data that these activities included. The counter also includes the logged-in user identification information as well as the system information on which the activities were performed. This information can be retrieved during investigation, but in this case only correctly authenticated users with the full Administrator or Investigator role can see the related user information. Admins with the Analyst role can see the same information, but in this case the device and user information is replaced with pseudo-anonymized data together with masking.
- **Alerts and Events Analytics Storage (OpenSearch)** – Data storage that is used to keep and index alerts information as well as the events that caused the alert to trigger. The alerts and events are stored for a period of 3 months. Alerts and events include information that identifies the logged-in end user that performed the activities which caused the alert, as well as information about the endpoint system on which the alert was triggered. In the context of the Management Console, authenticated admins with the appropriate role (Administrator, Investigator or Analyst) may retrieve alerts and Events from

- **Evidence Locker** – A secure data storage layer that is used to store forensic data. Objects stored within the evidence locker are stored using content encryption, and each object is encrypted with a unique data encryption key. The data encryption key used is also encrypted using a tenant-specific key and stored alongside the forensic object it was used to encrypt. Data held within the evidence locker is subject to a separate retention period of 30 days. Access to the data held within the evidence locker is also subject to roles-based access control and is audited as part of the tenant's audit trail. In this case, authenticated admins with the appropriate role (Administrator or Investigator) can choose to unmask forensic snippet data or download a decrypted copy of the evidence file. In either case, an entry is placed into the account's audit trail. Admins with a role of Analyst cannot unmask forensic snippet data or download evidence files.

System Component: Endpoint Device Registration and System Properties

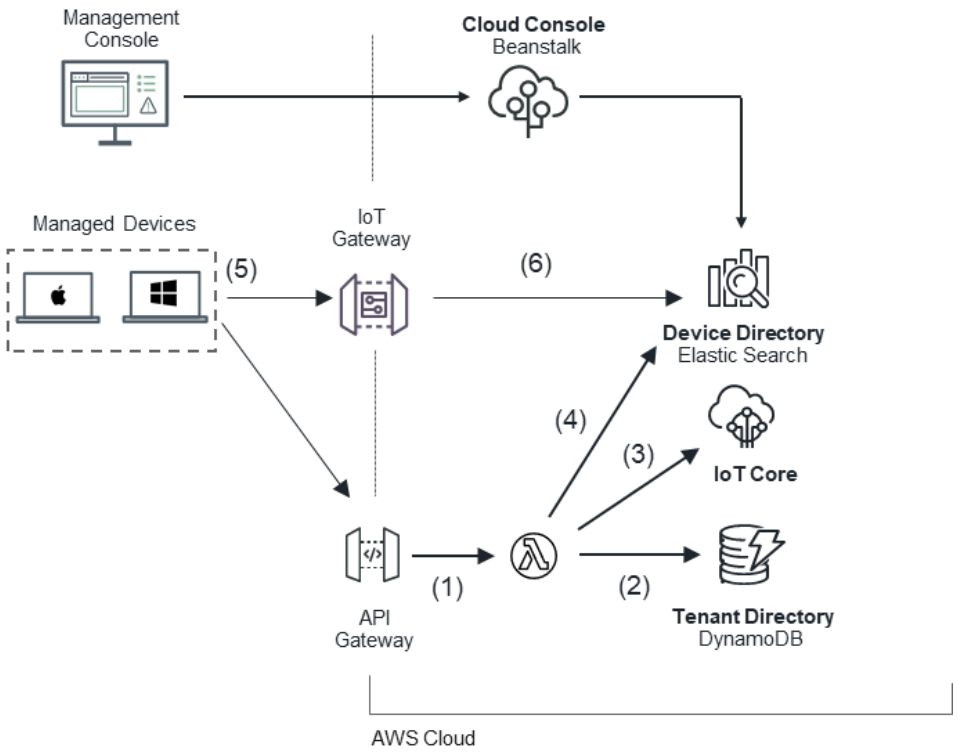

Image 4 – Endpoint Device Registration and System Properties

Components

- **Endpoints for Windows and macOS** – These devices on which the solution is installed perform a one-time device-registration to the cloud back end immediately after their installation. The device sends device identification and device hostname to the cloud back end for registration (see Flow 1 in the section below). Once the device registration is complete, a dedicated digital certificate is issued for each device and this digital certificate is used to secure all data-in-motion communications between the endpoint and the cloud back end using TLS 1.2.
- **API Gateway and Lambda** – A standard mechanism by AWS for the endpoints to call a remote REST API that will perform the one-time self-registration of the device. Upon registering the device, a representation of the device is stored in the device directory (Elasticsearch index).
- **Device Directory (Elasticsearch)** – Cloud storage that keeps a record per device including the system properties that the device reports periodically to the cloud.
- **Tenant Directory (DynamoDB)** – Each tenant has a record in the tenant directory, which does not hold any information about individual users nor devices.

General Data Processing Principles

- All data in motion is protected using TLS 1.2 on port 443.
- All data at rest is protected using AWS Server Side Encryption and AES256.
- Forensic data has additional AES256 content encryption applied. Each evidence file is encrypted with a unique per-file key (data encryption key). The data encryption key is also encrypted using a tenant-specific key. The encrypted data encryption key is then stored together with the forensic artifacts on an S3 bucket which is encrypted at rest (AES256).
- Processing of data is achieved using AWS Lambdas. Each Lambda invocation has a tenant-specific security context, (token) with the result that a tenant's data is always processed separately.
- Access to persistent data held in the underlying service databases uses row-level security. Processing of persistent data occurs in a tenant specific security context (token). This ensures that tenant data is only available to appropriately authorized clients.

Endpoint: First-Time Device Registration and Periodic Sending of Device (System) Properties

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Registration and device and system properties	The 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. 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 hostname as the domain or the custom domain name if configured by the admin. • The username used by the user when logging in. This can be the user principal name, email address and/or down-level logon name consisting of the domain and the username This information is collected in order to accurately identify the end user affected by any Data Security alerts.	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 at rest and stored in the tenant primary region (Europe – Germany, US – North Virginia, APAC – Mumbai or APAC – Singapore) and the information is encrypted at rest inside Elasticsearch using AES256. Information is anonymized when accessed via the cloud portal if the administrator is attached to the Analyst role. In this case, user information and computer information is replaced by terms such as user-01 and computer-01. Other information is also shown as obfuscated with *******. This affects the display of user information relating to display name, full name, local username, user groups, SAM account name if available; and system information relating to computer_hostname, domain, fully_qualified_domain_name and host_ips. Note that anonymization only applies to the Analyst role. Administrators with full privileges (Administrator or Investigator role) will see the information without anonymization applied.	The device registration is sent by the endpoint to cloud back end 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 back end. Then device properties are sent over MQTT. The communication is secured using TLS 1.2 and the device-specific digital certification. The device information (properties) is stored in Elasticsearch, which is encrypted at rest using a AES256 key provided by the AWS-managed Elasticsearch service.	Device and system properties are retained in the Forcepoint AWS account until a system is deleted. Whenever a new user logs in to the system, the user info is updated and the previously logged-in user is overridden. When the device is deleted from the management console (UI), the device properties including the logged in user info are deleted.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	All the information is stored in an Elasticsearch index (table) accessible by Forcepoint COPS employees. To access the Elasticsearch, a COPS engineer is required to get access permission via Forcepoint OKTA, which requires manager approval. An authenticated administrator can view device properties through the Forcepoint Data Security Cloud Management Console. The customer admin can also perform a search to find a specific device and then view its details.
SAR – Correction/Rectification	Not Available. The data is read-only information about the device and the Forcepoint software version that is installed on the device. The device information is updated every 5 minutes (re-sent from the endpoint to the cloud).
SAR – Right to be Forgotten	The endpoint (computer) data can be deleted via the user interface. But if an alert was triggered from the computer, then the alert (which also contains the computer name as well as the user information) will remain for 3 months in the live data (Elasticsearch) and for 12 months in the Archive (S3). Customers may request a smaller archive storage duration if required; this is handled in an ad-hoc fashion by modifying the retention policy on the S3 bucket associated with this customer tenant.
Data Storage / Localization	The device information is stored inside an Elasticsearch index. Each tenant (a sub-set of the customer organization that is treated as an isolated entity) has an alias which separates their data from other tenants (of the same customer or tenants that belong to other customers) for alerts and events. The purpose of the alias is to prevent accidental access to other tenant's data. The Elasticsearch is in the tenant primary region. Each tenant has only one primary region – for EU customers, their tenant's primary region is AWS eu-central-1 (Frankfurt). For US customers, the primary region is us-east-1 (North Virginia). For APAC customers, the primary region can be ap-south (Mumbai) or ap-southeast-1 (Singapore).

Data Protection Service: Reporting Alerts from Forcepoint Data Protection Service to Cloud Storage

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Alerts contain information about the system on which the event triggered and the details of the user that performed the activities that led to the alert Data captured can be specific to the source, such that emails will include subject and to/from email addresses. Cloud applications will contain the URL and the cloud application, etc. User information relates to the source user as identified by the source application. Alerts also contain metadata that describes the activity. This may include the DLP policies and rules triggered alongside the DLP classifiers matched and the number of matches. The alert may also result in the reporting of forensic data. This can include violation triggers, which are the actual snippets of text that triggered the policy and a copy of the content that was scanned.	Alerts include personal data in the form of username, user email and the names of the LDAP groups to which the user belongs. Some classifiers are looking for personal data such as first names, last names or social security numbers. If configured to include forensic data, then the alert can contain the actual text that triggered the Forcepoint DLP policy. This can include sensitive information but is typically required to understand the alert context. Forensic data can also include a file which is captured as part of the transaction. In this case, the file represents the actual data scanned and contain personal information.	The purpose of the Data Security solution is to monitor user activities and report alerts when a user performs an activity which is considered a breach of corporate policy. For example, Data Security will report alerts if 10 or more files that include source code have been copied to a removable storage or uploaded to a personal Gmail, as this may indicate intellectual property theft. Admins will typically enable the capture of forensic data for the most severe incidents. Forensic data is necessary to first triage the alert, establishing whether the alert is a false positive and gauging its seriousness. This information is necessary for Incident response purposes. Capture of an evidence file as part of the forensic data is also necessary for incident response and can be required should the incident lead to legal follow-up.	Alert and Event data stored as JSON files contain unredacted user and system activity information. The data is stored encrypted at rest (AES256). For users with Analyst role, the cloud portal anonymizes: • User data: display name, full name, local username, groups, SAM account (shown as user-01) • System data: hostname, domain, FQDN, IPs (shown as computer-01) • Other sensitive fields: masked with ******* Administrator/Investigator roles see unredacted data. Forensic data uses customer-specific content encryption instead of anonymization, with role-based access control and UI access auditing. Investigators or Administrators must request to unmask violation trigger data. An audit event is recorded for each unmask activity. Investigators or Administrators may download the evidence file. An audit event is recorded for each download.	Forcepoint cloud products (DLP for Email, Cloud App Security, Web Security) send DLP events to the Data Protection Service over secure channels, including user data and content for scanning. Data Protection processes events in isolated tenant nodes, applies customer DLP policies and returns verdicts to source products. When triggered: • Alerts are created with metadata (policy matches, user info, classifier data) • Forensic data includes violation triggers and scanned content, transmitted securely Data handling: • Data Protection temporarily stores encrypted forensic data until cloud transmission • Cloud applies per-transaction content encryption with tenant-specific keys • Only encrypted data is stored in the cloud Access control: • Analyst/Investigator/Admin roles can view alerts • Only Investigator/Admin roles can access forensic data	Data retention periods: • Alerts/events: 3 months in cloud analytics (Elasticsearch), 12 months in archive (S3) • Forensic data: 30 days, then auto-deleted Customer options: • Can use own S3 bucket for extended retention of alerts, events and audit logs • Extended forensic retention is not currently offered and is not included in the bring-your-own S3 bucket option Admins can request a shorter archive duration. Requests of this nature are handled in an ad-hoc fashion by modifying the retention policy on S3 bucket associated with this customer tenant.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	An authenticated administrator with the appropriate role can view alerts and events through the Forcepoint Data Security Cloud management console. The customer admin can also perform a search to find a specific user and then view its alerts and events. A customer administrator with a full Admin or Investigator role can access forensic data related to an alert – snippets and any evidence file captured. In this case, when viewing an alert, snippets are shown fully masked. The admin must click the unmask action to see the data. Clicking unmask results in an entry in the tenant's audit trail. Admins with either of these roles can also choose to download the evidence file. When downloading the evidence file, an unencrypted copy is downloaded in the usual fashion. Administrators without an Admin or Investigator role have no access to forensic data.
SAR – Correction/Rectification	The data is read-only.
SAR – Right to be Forgotten	The data is currently deleted automatically after 3 months from the analytics storage (Elasticsearch) and after 12 months from the archive. It is possible to delete the data from the database upon request (ad-hoc via Forcepoint support), but the option to do it is not exposed to the customer admin. Forcepoint support intervention is required to delete data of specific users from cloud storage prior to the automatic 3/12 months deletion. Forensic data is deleted automatically after 30 days. At this point, the forensic data is removed from the Forcepoint cloud and is no longer accessible.
Data Storage / Localization	The alerts and events information is stored inside an Elasticsearch index. Each tenant has an alias (row-level security), which separates their 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 tenants' data. The Elasticsearch and evidence locker is in the tenant's primary region (each tenant has only 1 primary region) – US, EMEA (Germany), APAC (Mumbai) or APAC (Singapore). Alerts, events and related forensic data is stored within this primary region.

Endpoint: Reporting Activity Counters from Endpoint to Cloud Storage

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and 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 that count the number of activities a user performs, such as 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.	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 find significant deviations in user activity in order to report them as alerts.	Counter data is stored as JSON files and contains unredacted user and system activity information. The data is stored encrypted at rest (AES256). For users with Analyst role, the cloud portal anonymizes: • User data: display name, full name, local username, groups, SAM account (shown as user-01) • System data: hostname, domain, FQDN, IPs (shown as computer-01) • Other sensitive fields: masked with ******* Administrator/Investigator roles see unredacted data.	Counter information is sent to cloud via the same encrypted communication transport as events and alerts (using TLS 1.2) and 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.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	An authenticated administrator with the appropriate role can view charts built from counter data through the Forcepoint Data Security Cloud management console. The customer admin can also perform a search to find a specific user and then view its activities and the total number of activities and total size of data involved (in a form of histograms that are built based on the counters).
SAR – Correction/Rectification	The data is read-only information and the customer admin has no options to modify this data, as the data represents end-user activities and must remain immutable.
SAR – Right to be Forgotten	The data is currently deleted automatically after 3 months from the DynamoDB table. Forcepoint intervention is required to delete data of a specific user from cloud storage prior to the automatic 3 months retention. This is available via an ad-hoc request.
Data Storage / Localization	The counters of all customers are stored in the same DynamoDB table with a partition key (row level security) that filters the data of one customer from another. The DynamoDB is in the tenant's primary region (each tenant has only 1 primary region) – US, EMEA (Germany), APAC (Mumbai) or APAC (Singapore).

Admin Login to Cloud Management Console

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
The email address, first name and last name of each admin are stored in a user pool that is dedicated for the customer.	The data for login is the user email address and password. AWS Cognito stores the user first name, last name and email address as well as the user password.	Administrators need to log in to the cloud management console to define policy rules and to investigate alerts and threats.	The user (admin) information configured name and email are not pseudo-anonymized inside Cognito, but they are encrypted by AWS Cognito. For more details about Cognito and Cognito 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.

How to Manage Subject Access Request (SAR)

SAR – Right to Access	The list of administrators is accessible by the customer admins that can create new administrators via the cloud management console.
SAR – Correction/Rectification	The data is editable and can be modified by the admin via the management console.
SAR – Right to be Forgotten	An administrator with the appropriate permissions can remove other administrators from the tenant through the Forcepoint Data Security Cloud management console. Removing an administrator deletes their record from the underlying identity store.
Data Storage / Localization	The administrator data is stored inside AWS Cognito. Information in Cognito is encrypted at rest using AES256.

Administrator Investigating User Activity

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
The list of users that have top risky activities or top number of alerts is displayed in the Forcepoint Data Security management console. When clicking on a specific user, the related user activities are displayed on screen. In addition, the user details are taken from the User Information Service (UIS) and displayed for context (manager, role, office location).	The alerts include the system information (computer name) as well as the type of information (classifiers) that were detected in the file/email that triggered the alert. Alerts reported by the Data Protection Service may continue forensic data including snippets of text that triggered the alert. The alert also contains user information related to the user associated with the alert. User information in this case is the user information reported by the endpoint or Data Protection Service and optionally information that is imported by the customer 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 reported by the Endpoint or the Data Protection Service.	Forcepoint Data Security administrators invest most of their time reviewing risky users and investigating alerts that were triggered by users. The details displayed under the investigation menu option help the admins to determine if the alert is indeed a threat to the organization or whether the user activity was legitimate or unintentional.	User and alert information is not anonymized; the data is stored encrypted at rest in the respective data storage (the encryption is AES256 in both cases). Information is anonymized when accessed via the cloud portal if the administrator is attached to the Analyst role. In this case, user information and computer information is replaced by terms such as user-01 and computer-01. Other information is also shown as obfuscated with *******. This affects the display of user information relating to display name, full name, local username, user groups, SAM account name if available; and system information relating to computer_hostname, domain, fully qualified domain name and host_ips. Anonymization only applies to the Analyst role. Administrators with full privileges (Administrator role or Investigator role) will see the information without anonymization applied.	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 Forensic data is available for alerts reported by the Data Protection Service. Forensic data is stored in the Evidence Locker associated with the customers tenant. The Evidence Locker stores all data using content encryption and an individual data encryption key per artifact.	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 backup and long-term investigations. By default, the archive retains alert data for 12 months but is configurable upon request. Forensic data held within the Evidence Locker is retained for 30 days, after which time it is no longer retained and is automatically deleted.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	To access alerts and investigation requires a Forcepoint Data Security admin permission. There can be multiple admins for a single customer. If a subject of investigation (i.e., the end user) would like to see the data, they can only get access via an authorized admin, who will show it to the end user or alternatively share screenshots of the user interface. If the customer has enabled use of the Amazon Replication Service and has chosen to replicate events and alerts to their own S3 bucket, then they can directly access related events and alerts and can provide this information directly to the end user without Forcepoint involvement. It should be noted that the service will only replicate events and alerts occurring after the replication is enabled, so in this case the replication must have been activated prior to the time period the user is requesting access to. Note also that this only refers to the alert metadata. If forensic data is available (applies to alerts related to the Data Protection Service only), then an admin with the appropriate privilege (Administrator or Investigator roles only) can choose to download the forensic artifact. This provides a copy of the data that was scanned to trigger the alert in the form of a .eml file. Any attempt to download evidence is logged in the account's audit trail.
SAR – Correction/Rectification	The user data is read-only and is modified only when the user information changes in the corporate Active Directory or user's directory from which the user information is imported. The alerts data is read-only and cannot be modified, but the user information is displayed from the Active Directory. If the user data is corrected in the Active Directory, it will show up corrected in the user interface.
SAR – Right to be Forgotten	User data stored as part of an event or alert will be automatically deleted after 3 months from the analytics store (Elasticsearch) and after 12 months from the archive (S3). Customers may request a smaller archive storage duration if required, and this is handled in an ad-hoc fashion by modifying the retention policy on the S3 bucket associated with this customer tenant. Forensic data captured as part of an alert is retained for 30 days, after which it is automatically deleted. User data stored in the user directory of the service remains until the tenant is deleted. Forcepoint intervention is required to delete data of a specific user from the cloud storage prior to the automatic 3/12 months retention and/or from the user directory. This is available via an ad-hoc request.
Data Storage / Localization	The user information data is stored inside DynamoDB in the customer primary region. The Alerts data is stored in Elasticsearch. Forensic data is held in the Evidence Locker. Both the Elasticsearch and Evidence Locker are hosted in the customer's primary data region.

Administrator Investigating an Individual Alert

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
The alert data contains information about the activity that an end user or application performed.	Alerts include personal data in the form of username, user email and the names of the LDAP groups to which the user belongs. Some classifiers are looking for personal data such as first names, last names or Social Security numbers. If configured to include forensic data (applies to the Data Protection Service only), the alert can contain the actual text that triggered the Forcepoint DLP policy. This can include sensitive information but is typically required to understand the alert context. Forensic data can also include a file which is captured as part of the transaction. In this case, the file represents the actual data scanned and may contain personal information.	Forcepoint Data Security administrators invest most of their time reviewing risky users and investigating alerts that were triggered by users. The details displayed under the investigation menu option help the admins determine if the alert is indeed a threat to the organization or whether the user activity was legitimate or unintentional.	User and alert information is not anonymized; the data is stored encrypted at rest in the respective data storage (the encryption is AES256 in both cases). Information is anonymized when accessed via the cloud portal if the administrator is attached to the Analyst role. In this case, user information and computer information is replaced by terms such as user-01 and computer-01. Other information is also shown as obfuscated with *******. This affects the display of user information relating to display name, full name, local username, user groups, SAM account name if available; and system information relating to computer_hostname, domain, fully qualified domain name and host_ips. Anonymizations also only applies to the Analyst role. Administrators with full privileges (Administrator role or Investigator role) will see the information without anonymization applied.	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. Forensic data is available for alerts reported by the Data Protection Service. Forensic data is stored in the Evidence Locker associated with the customer's tenant. The Evidence Locker stores all data using content encryption and an individual data encryption key per artifact. Display of forensic data through the cloud portal is subject to RBAC. Only Administrators or Investigators may access. Violation trigger data is always shown masked and any requests to unmask or to download the forensic artifact are logged in the account's audit trail.	The user data is kept in the User Information Service (UIS) as long as the user is a member of the organization. The alert 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. Forensic data held within the Evidence Locker is retained for 30 days, after which time it is no longer retained and is automatically deleted.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	Alerts are accessed via the Investigation menu option in the Forcepoint Data Security cloud console. An admin permission with an Administrator, Investigator or Analyst role is required to access. There can be multiple admins for a single customer. If a subject of investigation (i.e., the end user) would like to see the data, they can only get access via an authorized admin, who will show it to the end user or alternatively share screenshots of the user interface. If the customer has enabled use of the Amazon Replication Service and has chosen to replicate events and alerts to their own S3 bucket, then the customer can directly access related events and alerts and can provide this information directly to the end user without Forcepoint involvement. It should be noted that the service will only replicate events and alerts occurring after the replication is enabled, so in this case the replication must have been activated prior to the time period the user is requesting access to. Forensic data (snippets and any evidence file captured) can only be accessed via the admin portal in the content of the alert that they are related to. Admins with the Administrator role or Investigator role can see the snippets and can download the evidence file. Admins with the Analys role cannot view snippets or download the evidence file. Admins with the Helpdesk role have no access to alerts or forensic data. Forensic data is not part of the Amazon Replication Service. Forensic data is only held in the Forcepoint Evidence Locker and is deleted after 30 days.
SAR – Correction/Rectification	The alert data is read-only and cannot be modified, but the user information is displayed from the Active Directory. If the user data is corrected in the Active Directory, it will show up corrected in the user interface
SAR – Right to be Forgotten	The alert data is deleted after 3 months from the analytics store (Elasticsearch) and after 12 months from the archive (S3). Customers may request a smaller archive storage duration if required; this is handled in an ad-hoc fashion by modifying the retention policy on the S3 bucket associated with this customer tenant. User data stored in the user directory of the service remains until the tenant is deleted. Forcepoint intervention is required to delete data of a specific user from the cloud storage prior to the automatic 3/12 months retention and/or from the user directory. This is available via an ad-hoc request. Forensic data (snippets and any evidence file captured) are deleted after 30 days. Afte this time, the data is no longer available in the Forcepoint service.
Data Storage / Localization	The user information data is stored inside DynamoDB in the customer primary region. The alert data is stored in Elasticsearch. Forensic data is held in the Evidence Locker. Both the Elasticsearch and Evidence Locker are hosted in the customer’s primary data region.

Endpoint: Endpoint Reporting Peripheral Device Usage

Data Set	What Personal Data is Used?	Purpose	Is Pseudonymization Possible?	Storage, Flow and Protection	Retention
Every 1 hour, if peripheral device activities occur such as copying files to/from removable storage, the filenames are sent to the Forcepoint Data Security cloud storage. The device usage data is stored inside Elasticsearch.	The device usage data contains filenames that were copied from/to removable storage and the file classification (containing PCI, source code, etc.). Actual file content is not shared with the cloud.	Forcepoint Data Security administrators often ask the question: how many files, and which files have people copied to removable storage devices? The device usage message that the Forcepoint agent sends to the cloud aims to answer this precise question and provide admins visibility into how users are using removable storage devices in the organization. This supports decisions about creating rules to block (or set to read-only) removable storage devices for individuals or groups of employees.	Device usage data is not anonymized at rest. This includes information about the user that performed the activities and the system on which the activities took place. The data is stored encrypted at rest using AES-256 encryption. Information is anonymized when accessed via the cloud portal if the administrator is attached to the Analyst role. In this case, user information and computer information is replaced by terms such as user-01 and computer-01. Other information is also shown as obfuscated with *******. This affects the display of user information relating to display name, full name, local user name, user groups, SAM account name if available; and system information relating to computer_hostname, domain, fully_qualified_domain_name and host_ips. Note that the anoymization only applies to the Analyst role. Administrators with full privileges (Administrator role) will see the information without anonymization applied.	Device usage messages are sent from endpoint to cloud over a secure communication channel (HTTPS). Device plug/unplug alerts are sent from endpoint to cloud over secure communication channel (MQTT). The alerts (device plug/unplug) stored in Elasticsearch are encrypted at rest by AES256. The device usage files are stored in S3 bucket that is encrypted at rest by AES256 as well.	Device usage data is stored in Elasticsearch and is automatically deleted after 3 months. Device usage data stored in Archive (S3) is automatically deleted after 12 months. Customers may request a smaller archive storage duration if required; this is handled in an ad-hoc fashion by modifying the retention policy on the S3 bucket associated with this customer tenant.

How to Manage a Subject Access Request (SAR)

SAR – Right to Access	Device usage information and device plug/unplug alerts are displayed via the Investigation screens in the Forcepoint Data Security cloud console. The investigator requires a Forcepoint Data Security admin permission with an Administrator or Analyst role. There can be multiple administrators for a single customer. If a subject of investigation (i.e., the end user) would like to see this data, they can only get access via an authorized operator, who will show it to the end user or alternatively share screenshots of the user interface. If the customer has enabled use of the Amazon Replication Service and has chosen to replicate events and alerts to their own S3 bucket, then they can directly access related device usage events and can provide this information directly to the end user without Forcepoint involvement. It should be noted that the service will only replicate events and alerts occurring after the replication is enabled, so in this case the replication must have been activated prior to the time period the user is requesting access to.
SAR – Correction/Rectification	The device usage data is read-only and cannot be modified.
SAR – Right to be Forgotten	The data is deleted after 3 months from the analytics store (Elasticsearch) and after 12 months from the srchive (S3). Customers may request a smaller archive storage duration if required; this is handled in an ad-hoc fashion by modifying the retention policy on the S3 bucket associated with this customer tenant.
Data Storage / Localization	The device plug/unplug alert data is stored in Elasticsearch, while the device usage data is stored in S3. Both the Elasticsearch and Evidence Locker are hosted in the customer's primary data region.

Appendix A

Terminology

Term	Explanation
Forcepoint Data Security	Forcepoint Data Security is a cloud-native, unified DLP solution that safeguards sensitive data, prevents breaches and ensures global compliance. With 1,800+ out-of-the-box policies and templates, rapid deployment and centralized policy management, it streamlines data protection across cloud apps, web, email and endpoints – with high availability on AWS, enabling people to work anywhere, with data everywhere. Featuring AI-powered data classification for high-accuracy policy enforcement, USB device control and Risk-Adaptive Protection (RAP), it dynamically adjusts security policies based on user behavior. This enables smarter enforcement, reducing false positives and ensuring security doesn't disrupt work, while also lowering costs and risks, increasing productivity and streamlining compliance audits.
UIS	User Information Service – The micro-service that stores information imported from Directory Service and makes it available for any product that likes to consume it.
Device and System Properties	Consists of device metadata such as host name, domain, device name, user signed in, OS, time zone and device specs.
DUP	Dynamic User Protection – 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 backeend 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 sent to the Forcepoint Data Security cloud storage and which can be displayed to administrators, who investigate alerts and security risks resulting from users' activities.
User	Any employee that accesses a computer system.
Risky User	An employee who has performed one or more activities that generated alerts. The 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 considers multiple risk impacts and calculates the total risk score).

Forcepoint

About Forcepoint

Forcepoint enables Self-Aware Data Security, an AI-native approach that helps enterprises and governments know their data everywhere, adapt to evolving risks and regulations in real-time, and protect at scale with a unified, single-policy framework. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, LinkedIn, Instagram and YouTube.

[FP Data Security Management of Personal Data] 30Mar2026