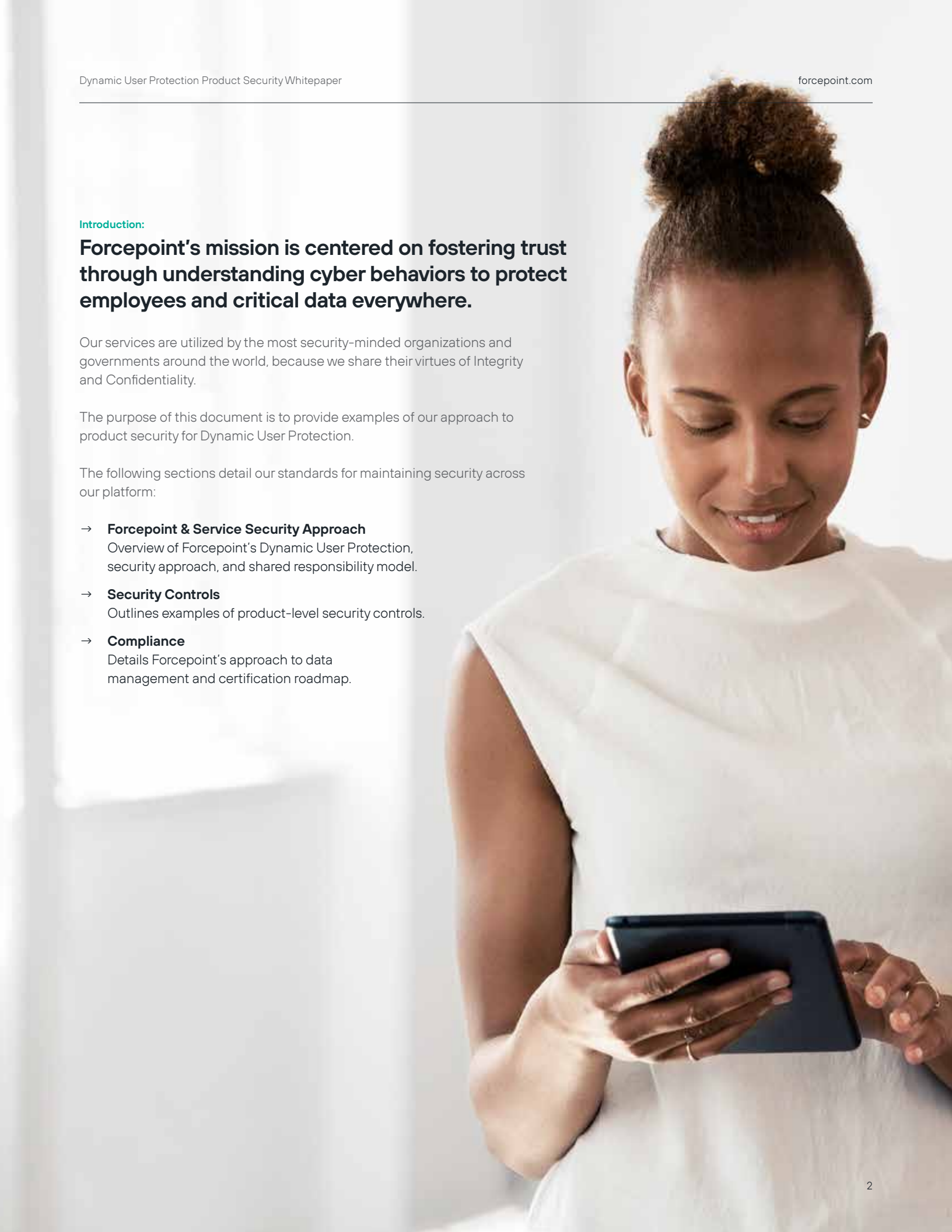
Dynamic User Protection

Product Security Whitepaper

Forcepoint

Whitepaper

Table of Contents



Introduction:

Forcepoint's mission is centered on fostering trust through understanding cyber behaviors to protect employees and critical data everywhere.

Our services are utilized by the most security-minded organizations and governments around the world, because we share their virtues of Integrity and Confidentiality.

The purpose of this document is to provide examples of our approach to product security for Dynamic User Protection.

The following sections detail our standards for maintaining security across our platform:

- → **Forcepoint & Service Security Approach**
  Overview of Forcepoint's Dynamic User Protection, security approach, and shared responsibility model.
- → **Security Controls**
  Outlines examples of product-level security controls.
- → **Compliance**
  Details Forcepoint's approach to data management and certification roadmap.

Forcepoint & Service Security

About Forcepoint

Forcepoint is on a mission to reshape security by focusing on what matters most: people.

Dynamic User Protection

Our Dynamic User Protection (DUP) platform shifts the focus from events to behaviors by tailoring policy and enforcement to each user's risk level.

Designed with a cloud-native and multi-tenant architecture, ensuring high availability, scalability, and security.

Pre-configured Autopilot—out of the box 100-point risk assessment leads to quick time to value.

With privacy and GDPR top of mind, user event data resides on the endpoint, and only leaves the device when an alert is triggered.

Continuous user monitoring enables risk-based prioritization, reducing analyst time spent per investigation by up to 70%.

The lightweight and autonomous agent radically decreases setup and maintenance.

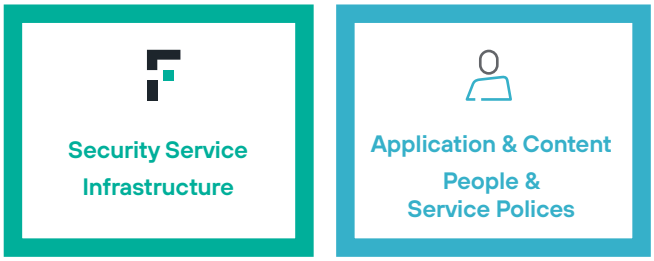
Forcepoint's Approach to Security

Security is in our DNA and is perpetuated through every facet of our platform to provide the utmost integrity and confidentiality.

In order to deliver our cloud services, we rely on a shared security responsibility model.

Shared security responsibility model
Industry leaders like AWS rely on the shared responsibility framework to clearly define the line between customer and service provider:

- → Forcepoint is responsible for the security of the cloud.
- → The customer is responsible for the security in the cloud.



Forcepoint's responsibility
Forcepoint is responsible for the security of the cloud infrastructure. The section below on Forcepoint Security Controls provides a detailed look at controls and procedures we've implemented to protect your data.

Your responsibility
Customers utilizing our service are responsible for securing access within the application, such as managing account permissions, authentication policies, password security, etc.

Principle of least privilege
Forcepoint sees the principle of least privilege as a guiding principle that is perpetuated throughout our organization. In order to receive access to any data, infrastructure, or application, explicit business requirements must be aligned. Additionally, core operational duties are delegated among multiple teams. Cloud operations teams are responsible for monitoring production environments and deployments, while engineering teams that develop the code are confined to test environments. This example of separation of duties prevents any single employee from pushing code to production. Any and all privileged or elevated access relies on least privilege to ensure administrators are equipped with the minimum privilege required to accomplish their tasks.

Security Controls

As a SaaS provider, Forcepoint is responsible for securing the underlying infrastructure up to the application itself.

Examples of the controls we use include:

→ Secure Software Development

→ Service-Level Security

→ Infrastructure / Physical Security

Secure Software Development

Forcepoint blends innovation with secure procedures through the use of Scrum/Agile in our software development lifecycle.

The foundation of this Agile framework is built around delivering the highest value possible through iterative cycles made up of the following steps: Planning, Development, Testing, and Demoing.

Planning
During this step, engineering and product management teams partner with our architecture board to ensure security controls/ practices are standardized across the platform.

Development
Every Forcepoint software developer follows secure development procedures and is equipped with secure tools to ensure security is not sacrificed for speed.

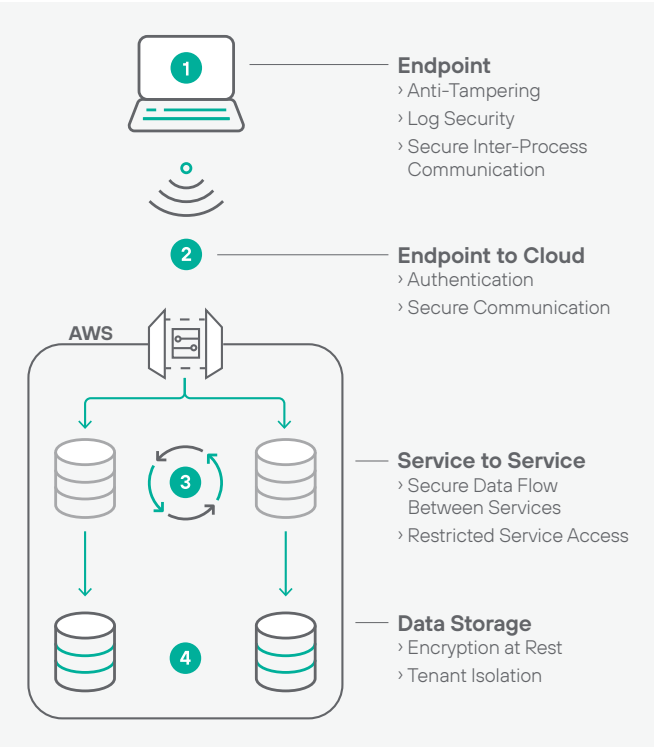
Testing
Developers are required to peer review and unit test their code before it can be merged. Additionally, before the release, critical functionality code must undergo both static and dynamic analysis.

Demoing
To complete the cycle of rapid iteration, features are prototyped and demoed at the conclusion of each sprint to ensure all functional/non-functional and security requirements are met.

Service-Level Security

Service-level security controls are layered across the platform and continuously validated by our internal Product Security Team.

Security architecture



1 Endpoint

Local security controls on the endpoint that provide anti-tampering and secure process communication.

Anti-tampering
In order to prevent user intervention, the following resources are protected:

PROTECTED RESOURCE	PREVENTED ACTIONS
Files and Folders	Delete, Create, Write, Change Permission
Processes	Kill, Injection, Start, Restart
Registry (Windows)	Delete, Add, Change
Property (Mac)	Plist Modification

Security Benefits
› Endpoint agent is resilient.
› Provides operational integrity.

Log security

Logs can contain confidential information. Rather than storing this data in clear text, logs are preprocessed using WPP (trace preprocessor) which stores logs in a binary format, rendering the logs unreadable.

Security Benefit

› Confidential data is not stored in clear text on the endpoint.

Secure inter-process communication

Local endpoint processes such as data collection and risk computation communicate via a message bus. In order to secure these messages, we utilize authentication and encryption:

→ Authentication: Each process requires a certificate to be authenticated to access the message bus

→ All messages between processes are encrypted using TLS 1.2

Security Benefits

› Only trusted processes can send messages.

› Data in transit is secured with strong encryption.

2 Endpoint to Cloud

Secure data transmission between device and cloud.

Authentication

As soon as the Neo agent is installed on the endpoint, the device registration process begins. Each endpoint is issued a certificate which is mutually authenticated with the AWS service. Once the device is registered, it is able to securely transmit user activity data to the cloud.

Security Benefits

› Mutual authentication ensures data is transmitted between trusted services.

Secure communication

When data is in motion between the endpoint and the cloud, it is encrypted using TLS 1.2.

Security Benefits

› Mutual authentication ensures data is transmitted between trusted services.

3 Service to Service

Secure communications between AWS managed services.

Secure data flow between services

AWS natively secures data flow between its managed services through TLS encryption.

Security Benefits

› Confidential data is transported using strong encryption.

Restricted service access

Forcepoint adheres to the principle of least privilege wherever possible. When it comes to communications between services, IAM (Identity and Access Management) roles are implemented to dictate the minimum action each service can and cannot take.

Security Benefits

› IAM roles perpetuate least privilege.

› Ensures secure processing of data between services.

4 Data Storage

Data at rest within AWS services.

Encryption at rest

Wherever applicable, data is encrypted at rest using Amazon's default AES-256 symmetric encryption.

Security Benefits

› Confidential data is encrypted at rest.

Tenant isolation

When accessing tenant data, queries are restricted to the specific tenant ID using Row Level Security.

Security Benefits

› Tenant data is logically separated to ensure secure and private access.

Product Security Team
To augment the security controls discussed above, we maintain a commitment to continuously monitoring and evaluating our security posture. This is overseen by our highly skilled Product Security Team whose focus is to identify and manage vulnerabilities.

Examples of their responsibilities include:

- → Incident Response – partnering with various technical stakeholders to discover, triage, and remediate vulnerabilities.
- → Product Security Testing – internal testing conducted through the use of dynamic and static tools.
- → Penetration Testing – conducting internal penetration testing, as well as enlisting third parties to perform assessments.
- → Consultation – acting as a resource to development teams to ensure secure architecture practices are followed.
- → Threat Research – continuous exploration into the latest threats and vulnerabilities.

Infrastructure / Physical Security

Infrastructure security
After weighing in on the top infrastructure providers, Forcepoint chose to partner with Amazon Web Services. Their industry-leading commitment to operational excellence, innovation, and security aligns with our values.

Our utilization of AWS means:

- → Workloads are run on AWS
- → We benefit from AWS infrastructure and native security
- → AWS controls are configured and tuned to maximize security
- → On top of AWS's measures, we instrument additional service-level controls

Physical security
Data Centers
AWS's physical infrastructure resides in discrete unmarked buildings around the world. Access to these buildings is highly controlled through the use of security personnel, video surveillance, and other cutting-edge security systems. Additionally, access entails strict logging and audit procedures.

Forcepoint Offices
Within Forcepoint's globally distributed offices, there are strict policies in place including:

- → Employees are required to have badges visible
- → All major entrances require proximity cards with different levels of access
- → Video monitoring of all egress points
- → On-site security staff
- → Employee awareness security training

After weighing in on the top infrastructure providers, Forcepoint chose to partner with Amazon Web Services. Their industry-leading commitment to operational excellence, innovation, and security aligns with our values.

Privacy & Compliance

GDPR

The General Data Protection Regulation (GDPR) is a significant source for the privacy principles that guide 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_en

Forcepoint Dynamic User Protection is designed with technical and organizational controls to meet GDPR compliance. See the User Data Management section below for examples.

User Data Management

ENDPOINT	
Data Location	Endpoint
Data Type	User activity data is monitored by the local Windows or Mac endpoint based on pre-configured policies. The data may vary by platform (Windows vs. Mac), but generally includes: → Web → Email → File → Printer → Clipboard → Process → Registry → Event Log
Purpose	As activity data is collected, it is filtered into meaningful events. The events are then processed in the policy engine. The policy engine evaluates the events and triggers alerts when an event (or multiple events) breaks corporate policy. This computation results in an impact to the user's risk score.
Storage, Flow, Protection	The data is protected using multiple, layered security controls: → Anti-Tampering – prevents user intervention/access to resources including: Files/Folders, Processes, Registry (Windows), Plist (Mac) → Inter Process Communications – local processes communicate securely via a message bus that requires certificate authentication and all messages in transit are secured using TLS 1.2 → Log Security – Logs are preprocessed using WPP so that they are stored in binary format, rather than clear text
Retention	User activity data is retained on a rolling 30-day basis, meaning day 31 overrides day 1.

ENDPOINT TO CLOUD	
Data Location	In-Transit between Endpoint and Cloud Services
Data Type	Event data is stored locally on the endpoint until an alert is triggered. When an alert is triggered, the alert and associated events are sent to the DUP cloud storage. Alerts and Events include information that identifies the user who performed the activities which caused the alert, as well as information about the endpoint system on which the alert was triggered. Counters are baseline counts of average user activity that are regularly sent to the cloud, regardless of alerting.
Purpose	Event and Alert data are used for the purpose of analyst investigation. Counters are used to establish a baseline of normal user behavior which are used for anomaly detection and to provide context for investigations.
Storage, Flow, Protection	Data traveling between the endpoint and cloud services is not stored until it resides in the cloud. To secure data in-transit: → Authentication – devices are issued certificates that are mutually authenticated with the AWS service → Encryption – All data sent between the endpoint and cloud are encrypted using TLS 1.2
Retention	N/A

SERVICE TO SERVICE	
Data Location	In-Transit: between AWS Services At-Rest: Counters and Summary Data Store Alerts and Events Store Alerts and Events Archive Store
Data Type	Counters are a count of the number of activities a user performs which results in a baseline of normal activity. Alerts indicate a policy was triggered that impacts the risk score. Events are only sent to the cloud when they are associated with an alert.
Purpose	Counters and Summary Data Store — storage that keeps the count of activities that a user performs, which is used for anomaly detection and analyst investigations. Alerts and Events Store — information that identifies the end user that performed the activities which caused the alert, as well as information about the endpoint system that the alert was triggered on. Alerts and Events Archive — a cold storage that is used to keep Alerts and Events for a period of 12 months. The data is stored for the purpose of archiving in case an alert older than 3 months needs to be investigated.
Storage, Flow, Protection	To secure data in-transit: → IAM Roles — each service has specifically defined permissions which limit actions based on the principle of least privilege → Encryption — all data sent between the managed services are natively encrypted using TLS 1.2 To secure data at-rest: → Encryption — data stored in AWS is secured using AWS default AES-256 symmetric encryption
Regionality	Each tenant belongs to a primary region Current AWS regions include US-east-1, EU-central-1, and EU-west-1. All traffic and data belonging to the tenant is routed through and stored in its specific region.
Access	Forcepoint employee access to production accounts is limited to the Cloud Operations Team, only under specific access permission. Any data that is to be accessed by Forcepoint researchers must receive explicit permission and is anonymized/pseudonymized.
Retention	Counters and Summary Data: → 3 months Alerts and Events: → Events (associated with an alert) – 3 months → Alerts – 3 months Alert and Event Archive: → Events/Alerts (Archived) – 12 months

Certification Roadmap

Forcepoint has a wealth of experience building products that meet and exceed industry certification standards. The AWS services utilized by Dynamic User Protection are ISO-certified. We will to receive specific certification for our service. See AWS ISO Certifications here: https://aws.amazon.com/compliance/iso-certified/

For DUP, we aim to achieve the following certifications by 2021:

→ ISO 27001

→ Cyber Essentials PLUS

Appendix: Resources

https://aws.amazon.com/compliance/shared-responsibility-model/ https://aws.amazon.com/compliance/data-center/controls/
https://aws.amazon.com/compliance/iso-certified/ https://docs.aws.amazon.com/iot/latest/developerguide/transport-security.html
https://aws.amazon.com/blogs/database/multi-tenant-data-isolation-with-postgresql-row-level-security/
https://docs.aws.amazon.com/apigateway/latest/developerguide/data-protection-encryption.html

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.