Forescout Cloud Services

Data Security and Privacy Brief

1. INTRODUCTION

1.1. Purpose of the Document

Forescout® Cloud protects your data with robust information security and data privacy programs. This brief describes how the architecture of Forescout Cloud Services protects your Customer Data and Personal Data from collection, transfer, storage, processing and retention through deletion. At its core, Forescout Cloud Services are a cybersecurity technology stack designed by security professionals for security professionals. As with every Forescout product, security is built into every step of the workflow. Privacy-by-design (PbD) principles and comprehensive technical and organizational measures are engineered into the cloud product for protection, trust, accountability and compliance.

1.2. Overview of Forescout Cloud Services

Forescout Cloud Services are cloud-native SaaS (Software as a Service) technologies designed to deliver cybersecurity outcomes and operational management for the Forescout 4D Platform™, its Products, and Cloud Services. By unifying threat detection, exposure management, and automated enforcement in the cloud, Forescout helps organizations continuously monitor, assess, and secure their entire cyber asset landscape. The Forescout Cloud seamlessly integrates hybrid environments, leveraging modern authentication and data encryption mechanisms for secure communications and data transport, ensuring confidentiality, integrity and availability of Customer's Data.

Forescout Cloud Services are hosted on **Microsoft© Azure.** This architecture leverages Azure Kubernetes Service (AKS) for containerized workflows and Azure ADX for data storage.

1.3. Forecout Cloud Services

1.3.1. eyeScope

Forescout eyeScope provides a unified console that simplifies enterprise management by delivering real-time asset visibility, health monitoring, and operational efficiency. It streamlines security oversight with intuitive dashboards, automated insights, and executive-level reporting that supports well-informed decision-making. With consolidated asset visibility, eyeScope enhances asset management and ensures a resilient, well-managed security posture at any scale.

1.3.2. eyeAlert (Formerly Threat Detection and Response – TDR/XDR)

Forescout eyeAlert converts telemetry and logs into high fidelity, SOC-actionable threats. It automates and accelerates the process of detecting, investigating, hunting for and responding to advanced threats across the entire enterprise. From cloud, campus, remote and datacenter environments to IT, OT/ICS, IoT and IoMT devices, Forescout eyeAlert combines essential SOC technologies and functions into a unified, SaaS experience.

1.3.3. eyeFocus (Formerly Risk and Exposure Management – REM)

Forescout eyeFocus is a comprehensive asset intelligence tool that provides the foundation for understanding the security posture of your attack surface. eyeFocus tracks the effectiveness of response actions across the security ecosystem to reduce your risk posture and exposure state using an automated risk-based approach to remediate vulnerabilities.

1.3.4. eyeSegment

Forescout eyeSegment provides real-time visibility into network traffic and simulation of logical segmentation policies that can be used to design and enforce dynamic zero trust policies across hybrid environments. eyeSegment enables enterprises to achieve granular control over network traffic while simplifying the complexity of segmentation. Forescout eyeSegment operates with a hybrid architecture, leveraging both an on-premises console for operational functionalities and cloud-based data processing for advanced network analytics.

2. DATA SECURITY

Forescout Cloud Services are designed with industry-leading security controls to ensure the confidentiality, integrity, and availability of Customer Data and Personal Data. Our comprehensive data security approach includes data segregation, encryption at rest and in transit, security of data transmissions, and compliance with SOC 2 Type 2 standards to protect sensitive information and maintain trust.

2.1.1. Data Segregation

- Forescout enforces strict multi-tenant data isolation, ensuring that Customer Data remains logically separated within our cloud infrastructure.
- Access control policies and role-based access management (RBAC) prevents unauthorized access and enforces least privilege principles.
- Audit logging monitors unauthorized access attempts.

2.1.2. Encryption at Rest

- All stored data, including logs, cases, configurations, and asset information, is encrypted using AES-256 encryption, consistent with industry best practices.
- Encryption keys are managed through a security key management system (KMS) with automatic rotation policies.

2.1.3. Data in Transit

- All communications between on-premises appliances (physical & virtual), data collectors, data connectors and Forescout Cloud Services are secured using TLS 1.2+ encryption.
- API requests and responses are authenticated and secured using OAuth 2.0 and JWT-based authorization mechanisms.
- Mutual TLS (mTLS) is enforced for security data exchanges between Forescout Cloud Services, on-premises appliances, and 3rd party integrations.

2.1.4. SOC 2 Type 2 Compliance & Continuous Monitoring

- Forescout Cloud Services maintain SOC 2 Type 2 certification, ensuring rigorous security, availability, and privacy controls are in place and independently audited.
- Continuous security monitoring and logging provide real-time detection of potential threats and anomalous activities.
- Regular penetration testing, vulnerability assessments, and compliance audits ensure adherences to the highest security standards.

3. DATA PRIVACY

At Forescout, safeguarding Customer Data and Personal Data and ensuring strict privacy controls are at the core of our cloud security strategy. We are fully committed to transparency, accountability, and compliance, ensuring that your data is handled with high standards for security and privacy. Our approach follows Privacy by Design PbD principles**,** embedding technical and organizational safeguards throughout the product lifecycle.

3.1.1. Commitment to Responsible Data Processing

Forescout Cloud Services process Customer Data only to deliver and enhance Cloud Services. Forescout collects the data necessary to provide asset discovery, threat detection, security orchestration & response, deployment health, compliance and risk assessment and network traffic analysis, ensuring that:

- Customer maintains control over data collection, processing and retention;
- Customer Data is processed solely to fulfill contractual obligations and enhance service quality; and
- Privacy safeguards are continuously enhanced to meet evolving compliance and security requirements.

3.1.2. Purposes of Data Processing

Forescout processes Customer Data strictly for the authorized purposes defined below:

- Delivery of the Forescout Products and Services
- Provision of Forescout Support Services
- Improvement of the Products and Services
- Administration of the Forescout End User License Agreement, or similar agreement executed between you and Forescout governing your use of the Forescout Products and Services
- Compliance with applicable data protection laws
- To otherwise act in accordance with explicit, written Customer instructions

In addition, Forescout may access, process and use Personal Data collected as part of Customer Data during the provisioning and use of the Forescout Products in accordance with applicable privacy and data protection laws. Forescout's Customer Data Protection Agreement ("DPA") is available here: https://trust.forescout.com/home.

3.1.3. Strict Compliance and Security Certifications

To provide customers with confidence in our data handling practices, Forescout undergoes independent security audits and maintains certifications that validate our privacy and security controls:

- SOC 2 Type 2 Certification – Ensures compliances with rigorous security, availability, processing integrity, confidentiality, and privacy standards.
- Global privacy & security frameworks – Our practices align with leading regulatory standards, including GDPR, and other international data protection laws. For additional compliant frameworks, see https://trust.forescout.com/home.

3.1.4. Subprocessors: Secure and Transparent Data Processing

Forescout partners with trusted, security-vetted subprocessors to support cloud operations while ensuring compliance with Forescout's security requirements. A comprehensive list of subprocessors, including their data processing functions, is available here: https://www.forescout.com/company/legal/subprocessors/.

3.1.5. Cross-Border Data Transfers & Regional Data Storage

Forescout lawfully transfers and stores Customer Data in compliance with global data sovereignty regulations such as the EU-US Data Privacy Framework.

Forescout's Cloud Services support regional data processing & hosting. Customers can choose to store their data in one of six secure cloud regions:

  - Virginia, United States
  - Toronto, Canada
  - Frankfurt, Germany
  - Dubai, U.A.E

  - New South Wales, Australia
  - London, United Kingdom

3.1.6. Data Access & Strict Role-Based Controls

Forescout enforces stringent access controls to ensure that only authorized personnel can access Customer Data only when necessary:

- Need-to-know basis – Internal access to Customer Data is strictly limited to Forescout's internal technical and support teams for:
  - **Support, troubleshooting and required maintenance** - Customer Data may be accessed to diagnose, resolve, and prevent technical issues that impact system performance, stability, and security. This includes investigating software malfunctions, connectivity issues, and system failures to ensure optimal functionality.
  - **Enhancing threat detection analytics and data transformation** - Customer Data is used to refine and improve security analytics, vulnerability identification, machine learning models, and data transformation (normalization/parsing/deduplication) processes. This helps identify and mitigate cybersecurity threats more effectively, strengthening overall network security.
  - **Improving asset identification & classification** - By analyzing network and device data, Forescout enhances its ability to accurately classify and profile assets. This improves visibility into IT and OT environments, ensuring more precise security controls and policy enforcement.
  - **Product usage & adoption** - Aggregated and anonymized Customer Data is leveraged to analyze product utilization trends, assess feature adoption, and identify opportunities for user experience enhancements. This insight drives continuous product improvements and better alignment with customer needs.
- Role-based access control (RBAC) – Customers define and control who within their organization can view, modify, or manage data.
- No unauthorized data sharing – Forescout does not share, sell, or use Customer Data for advertising, marketing, or unauthorized secondary uses.

3.1.7. Data Aggregation Functions

Customers may opt in to data-aggregation functions that allow a subset of their anonymized Customer Data to be used for threat research, aggregated analytics, and threat intelligence services. This data is aggregated and anonymized to ensure that individual customer identities remain undisclosed, with no direct attribution to specific organizations. The aggregated data contributes to broader security insights, including threat and risk landscape assessments across industry sectors and geographic regions. By participating in this data-aggregation function, customers also receive tailored and customized threat intelligence, enhancing their security posture with actionable insights specific to their industry or geographies. Customers retain full control over their participation and may manage their data-sharing preferences at any time.

3.1.8. Data Retention

Forescout retains Customer Data for purposes of operational support, backup, audit and compliance as needed to provide Cloud Services. Data is retained for the retention periods outlined in the respective Forescout Cloud Service Description, located here: https://www.forescout.com/resources/forescout-cloud-services-description/.

3.1.9. Secure Deletion Policies

Customer Data will be rolled off from storage and permanently deleted within 30 days following deactivation of customer's subscription for a service powered by Forescout Cloud. Customers have the option to copy stored data to storage media in the customer's environment if notification is given seven days prior to subscription cancellation.

3.1.10. Privacy and Security for AI Features

For customers who opt-in to product features powered by AI, inputs, outputs, embeddings and Customer Data, including Personal Data, are not made available to other customers. This information is not used to improve any AI model, is not available to third party products or services that provide trained models for Forescout AI usage and are not used by third-party products or services to improve models used by Forescout AI and AI-generated content does not leave the system boundary.

4. DATA COLLECTED AND PROCESSED

Forescout processes Customer Data only for authorized purposes (see Section 3) and may handle certain Personal Data based on Customer configured data sources. The table below outlines important data source categories, associated Cloud Services, and processing purposes.

Data Source Category	Examples (included but not limited to)	Data Category	Purpose of Processing	Cloud Service
Tenant Information	• Account Name • Account Number • Tenant ID • Tenant Name	• Registration information • Customer identification	• Onboarding, provisioning & entitlement • Enable product operations and functionality • Technical support	• eyeAlert • eyeFocus • eyeScope • eyeSegment
User Information / External Identity Store	• Certificate • City • Country • Department • Email Address • First Name • IP Address • Job Title • Last failed login IP address • Last Name • Last successful login IP address • MAC Address • Office Location • Postal Code • Request login/display name • User Groups • User-Principal-Name • Username	• Registration information • Host and usage information	• Authentication • Authorization • Technical support • Enable product operations and functionality • Technical support	• eyeAlert • eyeFocus • eyeScope • eyeSegment
Endpoint Telemetry	• Appliance ID • Category • City • Country • Vulnerability • Device Criticality • Device ID • Device Location • Device Type • Enterprise Manager ID • Event Type • Exploitability • Firmware • FQDN • Function • Group Description • Group Name • Host FQDN • Host Name • Identity Group • Interface • IP Address • Last Seen Online	• Host and usage information • Endpoint information • Customer identification	• Asset identification • Asset classification • Compliance • Incident response • Threat detection • Risk assessment • Product improvement • Technical Support	• eyeAlert • eyeFocus • eyeScope

Data Source Category	Examples (included but not limited to)	Data Category	Purpose of Processing	Cloud Service
	• MAC Address • Manufacturer • Medical Equipment Function • Model • Network Group • OS • OS Architecture • OS Name • OS Version • Path • Policy Name • Port Protocol • Property Name • Protocol • Segment Name • Serial Number • Service Name • Switch IP • Switch Location • Switch Port Alias • Switch Port VLAN • Tenant ID • Tenant Name • User Domain • User ID • Username • Vendor • Vulnerability Description • Vulnerability ID			
Endpoint Security Telemetry	• Action • Application Category • Application Name • Authentication Type • ASN • Client Application • Command Line • Direction • DNS Query • Domain Name • Event Category • Event Description • Event ID • Event Time • Event Type • File Path • HTTP Method • HTTP Status • ICMP Code • ICMP Type • Identity • Latitude • Longitude • Message • Module	• Host information • Endpoint information	• Compliance • Incident response • Threat detection • Product improvement • Technical Support	• eyeAlert

Data Source Category	Examples (included but not limited to)	Data Category	Purpose of Processing	Cloud Service
	• Process Call Trace • Process ID • Process Name • Process Path • Provide Name • Reason • Request URL • Response Name • Response Code • Resource Type • Rule ID • Rule Name • Service Name • Severity Level • Tags • Terminal Session ID • Thread ID • User SID • User Agent • User Mail • VM Name • Zone			
Network Telemetry	• Appliance Name • Appliance ID • ASN • ASN Organization • Bytes • City • Country • Direction • IP • Port • Host Name • Event Description • Event ID • Event Time • ICMP Code • ICMP Type • Latitude • Longitude • Message • Protocol	• Host information	• Threat detection • Network traffic analytics • Network traffic visualization • Technical Support	• eyeAlert • eyeFocus • eyeScope • eyeSegment
System / Audit Telemetry	• Appliance ID • Appliance Name • Connector ID • Device • Device Type • Event Type • Event Description • Event Time • Plugin Name • Severity	• Usage information	• Uptime and performance monitoring • Technical Support	• eyeAlert • eyeFocus • eyeScope • eyeSegment

About This Technical Brief

Forescout security and privacy documents are reviewed and updated on an as-needed basis. Please note that the information provided with this paper concerning technical or professional subject matter is for general awareness only, may be subject to change and does not constitute legal or professional advice, warranty of fitness for a particular purpose or compliance with applicable laws.

Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com