Forescout Cloud Security and Data Privacy Brief for Cloud Services

Forescout Technologies' cloud-based service protects customer data with robust, global, information security and data privacy programs. This brief describes how the cloud-based service architecture protects personal information from collection, transfer, storage, processing and retention through deletion. At its core, Forescout Cloud is a security platform 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 technical and organizational measures are engineered into the cloud product for protection, trust, accountability and compliance.

Summary

Forescout Cloud is a cloud-native, SaaS-based solution for security visibility and operational management. It is an evolving offering with additional services aimed at enriching on-premises capabilities, as well as new services over time.

Services currently provided by Forescout Cloud:

Threat detection and response

Provides the ability to monitor, detect, investigate and respond to cybersecurity threats. Integrates, correlates and contextualizes events and alerts from multiple data sources to identify threats and then automate the incident response process.

Risk and exposure management

Discovers all cyber assets to provide visibility to continuously assess and quantify the attack surface presented by these endpoint assets, mitigating risk and compliance exposure through prioritized remediations and automated enforcement.

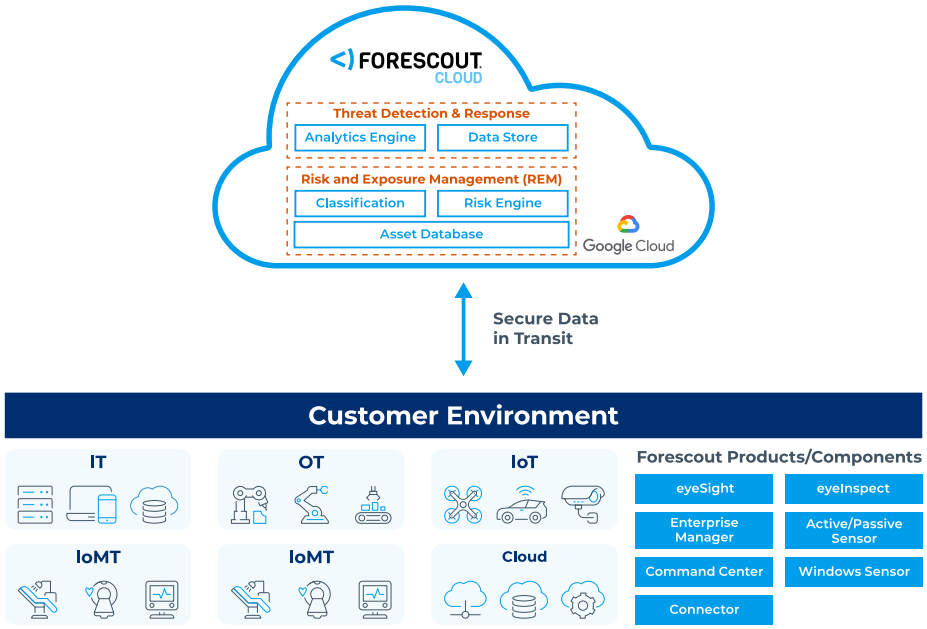

Figure 1: Data Flow Diagram

Security

Forescout Cloud is based on a multi-tenant architecture and separates data between customers. All data in transit and at rest are secured using encryption technologies such as TLS v 1.2 and higher and AES-256. Any data stored on or processed by Forescout Cloud is secured with state-of- the-art technologies, and we operate rigorous technical and organizational security controls. Forescout maintains a SOC 2 Type 2 certification for Forescout XDR.

Data Privacy

Data processing for customers

Forescout is committed to maintaining the highest levels of protection for private information when processing our customers' data. We take privacy seriously through the product development lifecycle and integrate PbD principles and technical and organizational measures in order to safeguard the privacy of personal information in the cloud. Personal data is used only as necessary to perform contractual obligations and for purposes compatible with those services. Forescout monitors, detects and evaluates security threats. The technical data and relatively small amount of personal information Forescout collects is used to deliver customer-specific insights, improve the quality of services, ensure network and information security, and not for advertising.

Compliance with privacy laws and regulations

Forescout Cloud maintains SOC2 Type 2 certification. SOC, in this instance, stands for "system and organization controls" and was developed by the American Institute of Certified Public Accountants (AICPA) to provide a way to address growing concerns around data privacy and security. SOC 2 Type 2 certification demonstrates that an independent firm has audited and tested an organization's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality and privacy.

Transfer and storage

Forescout Cloud hosts data in Google Cloud Platform (GCP) in the United States, Montreal (Canada), Frankfurt (Germany) and London (United Kingdom) regions. Forescout XDR service is available in all Forescout Cloud regions; Forescout Risk & Exposure Management is available in the United States region. Customer data is stored in a supported region of the customer's choice. Data in transit is protected using TLS 1.2 or higher, and data at rest is encrypted using the AES-256 algorithm.

Access and disclosure

Access to raw data stored in the Forescout Cloud is strictly limited to Forescout's internal technical team and only on a need-to-access basis. Authorized Forescout data scientists' access to data is limited to customer-focused security insights and product improvements such as ensuring proper data transformation and rule logic tailored to your environment.

Data retention schedule

Forescout Cloud retains customer data for purposes of operational support, backup, audit and compliance as needed to provide services. Data is retained for the retention periods outlined in the Forescout XDR Service Description and Forescout Risk & Exposure Management Service Description.

Data deletion

Customer data will be rolled off from storage and permanently deleted when a customer cancels their subscription for a service powered by the 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.

Data segregation

Customer data is segregated to its own index/table. Customer data is not mixed within indices or the same table. User access to data is restricted to the index/table for which the user is granted view/edit permission.

Data collected and processed

Data collected and processed depends on what customer data sources are configured to be sent to the Forescout Cloud. Network telemetry includes data elements such as source/destination IP address, browser, browser plugins and URL. Endpoint telemetry sources include data elements such as source/destination IP address, hostname, MAC address, username. Forescout Cloud does not take any information from the customer's environment without having set up and configured the data source as required for function within Forescout Cloud. Table 1 defines types of data collected & processed.

Table 1: Example Data Collected & Processed

Data Category	Type Of Information	Example(s)	Purpose of Processing
Account Information	▸ Tenant ID / Account Number (numeric)	▸ 82da848b	▸ Activation of service ▸ Billing/invoicing ▸ Ongoing service ▸ API calls ▸ Future notification of features/updates ▸ Support
Endpoint Telemetry	▸ Username (String) ▸ Mac address (12 Dig Hex) ▸ IP address (ipv4, ipv6) ▸ First Name, Last Name ▸ Connection Type (wireless, ethernet) ▸ Device type ▸ (printer, thermostat) ▸ Firmware (type, version) ▸ 802.1 SSID ▸ Encryption enabled ▸ Classification (OS type version) ▸ Forescout Zone (group and segment) IDs (numeric) ▸ Optional DNS name (string.string.string...)	▸ 139128496003412 ▸ foo.bar.acme.com	▸ Providing information on endpoint context for policy development and management ▸ Internal business and product analysis and insights to drive product improvement (research platform)
Network Telemetry	▸ Source and destination IP ▸ Port and protocol (string/number) ▸ Time stamp	▸ 10.20.10.10 (Private range), 12.5.6.55 (Internet), 224.0.0.37 (multicast) ▸ https/443 (TCP), 17 (UDP)	▸ Providing information on endpoint communication behavior for policy development and management ▸ Internal business and product analysis and insights to drive product improvements (research platform)
Deployment Configuration Data	▸ Appliance ID (numeric) ▸ Appliance list (numeric list) ▸ Flow source type (string) ▸ Forescout zone (segment or group) ID structure (numeric list) ▸ Policy information (name, structure, conditions, actions)	▸ 223950159931206 ▸ 322395015993120, 582605362940965,...} ▸ Flow, packet engine, AWS ▸ {139128496003412, 55826053629409,...}	▸ Support ▸ Internal business and product analysis and insights to drive product improvements (research platform)
System / Security / Audit Events	▸ Tenant ID / Account Number (numeric) ▸ Device type ▸ Event type ▸ Event description ▸ Time ▸ Severity	{ "syslogSeverity": 7, "eventSubType": "EXPORT", "eventType": "SYSTEM", "outcome": "FAILURE", "tenantId": "test-tenant", "timestamp": 1598353401247, "specialCode": "12F443S", "eventParams": "additonal" }	▸ Monitor the performance and health of the system

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®

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