Forescout Cloud Security and Data Privacy Brief

Forescout Cloud Security and Data Privacy

Forescout Technologies' cloud-based service protects customer data with robust, global, information security and data privacy programs. This data sheet 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. Like every Forescout product, security is built into every step of the workflow. Privacy by Design principles and technical and organizational measures are engineered into the cloud product for protection, trust, accountability and compliance.

Product Summary & Services

Forescout Cloud is part of the Forescout Continuum Platform, the industry's first automated cybersecurity platform that continuously manages the risk posture of assets across an enterprise's digital terrain, providing complete coverage of IT, OT, IoT and IoMT devices.

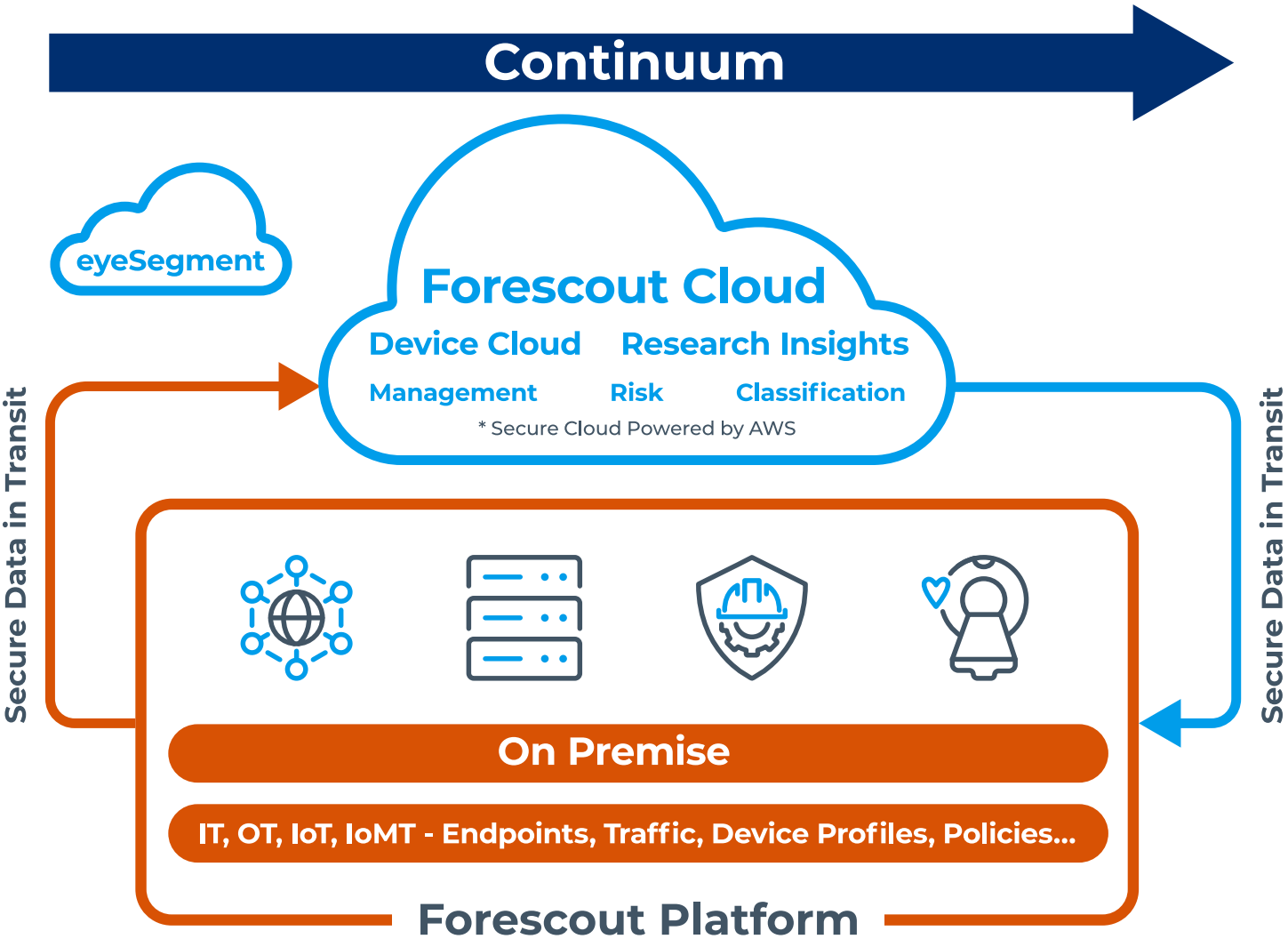
Forescout Cloud is a cloud-based automated security platform integrated with customer's on-premises deployments. Forescout Cloud provides enterprise services such as Asset Management, Classification and Risk. Forescout Cloud is an evolving product offering additional services aimed to enrich on-premises capabilities, as well as new services over time. Services include:

Management

Enables continuous data collection from Forescout on-premises appliances to be leveraged by cloud services for data-powered insights and automated decision-making; drives down costs through cloud-enabled administration interfaces and easy-to-use programming interfaces for large-scale administrative tasks

Risk

Brings together factors through Scoring Services related to the function, behavior and configuration of assets and traffic from the endpoint to generate risk scores that enable high-quality, easy decision-making to securely manage network and asset governance



Classification

Uses machine learning to further improve Forescout's ability to automatically classify assets.

Continuum refers to the overall platform that delivers all Forescout cloud-based services

eyeSegment

is a secure, cloud-driven application that provides visual representation of network traffic flows and dependencies between endpoints, users and services.

Device Cloud

is a secure cloud-based asset repository.

Research Platform

is a centralized repository that enables customer-focused analysis for cyber insights and continuous improvements to services offering. Personal identifiable information (PII) data are anonymized in this environment.

Security

The Forescout Cloud solution is based on a multi-tenant architecture that separates data between customers. Forescout appliances initiate HTTPS connections to the Forescout Cloud Service. All data in transit and at rest are secured using encryption technologies such as TLS V2 and higher and AES-256. Any data stored on or processed by Forescout is secured with state-of-the-art technologies, and we operate rigorous technical and organizational security controls. Forescout maintains certifications or conforms to the standards associated with Common Criteria; United States Department of Defense Approved Product (DoDin); UL CSA/UL 69050 (Safety); FCC Part 15, Class A, CREST Certified Penetration Testing; CIS Security Technical Implementation Guide (STIG); OWASP Software Assurance Maturity Model; and SANS Critical Security Controls. Refer to AWS's Security & Compliance documentation.

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 Privacy by Design 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. We create value for our customers by regularly releasing new products and product versions in response to the evolving risk landscape. Please refer to the more detailed information and table below for more detailed information about how personal data is collected, transferred, stored, processed and retained by the Forescout cloud-based service.

Compliance with Privacy Laws and Regulations

Forescout complies with international, federal, state and local privacy regulations. Privacy compliance is holistically baked in as we process technical and personal data for legitimate business purposes to ensure device and information security. Forescout has certified its compliance with the EU-U.S. Privacy Shield and Swiss-U.S Privacy Shield Frameworks. In addition, Forescout utilizes Data Processing Addendums for its vendors and customers that incorporate the Standard Contractual Clauses (SCCs) as approved by the European Commission. Forescout is a service provider, and we do not sell or share personal information. Forescout holds all service providers, affiliates, employees and independent contractors to strict confidentiality and data protection legal standards.

Transfer and Storage

Forescout Cloud hosts data in Amazon Web Services (AWS) in the United States. 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. Additionally, data access is monitored and logged. Authorized Forescout Customer Support personnel access data within your account exclusively for troubleshooting purposes only when a support case is opened by the customer and only if the customer enables access. Authorized Forescout data scientists' access to data in the research environment is limited to customer-focused security insights and product improvements. Within the research environment, IP addresses, MAC addresses, usernames and host names are fully anonymized. Data collected from the Active Directory plugin is not shared with the research environment.

Data Retention Schedule

Forescout Cloud retains customer data for purposes of operational support, backup, audit and compliance as needed to provide services and to comply with our legal or contractual obligations.

Data Deletion

Customers may request that data be deleted by submitting a written request to Forescout Support and following the instructions found here: https://www.forescout.com/support-hub/customer-support/. Upon submission of a request, Forescout will purge the requested data from its systems to the extent permitted by applicable law and may retain your administrative data required for legitimate business purposes (e.g., billing or contractual records). Upon deletion of data, you will be notified via reply email. The data purge process is permanent and cannot be reversed.

About This Technical Brief

Forescout Security and Privacy documents are reviewed and updated on 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.

Table: Information Collected and Processed

DATA CATEGORY	TYPE OF INFORMATION	EXAMPLE(S)	PURPOSE OF PROCESSING	MANAGE-MENT	RISK AND CLASSIFI-CATION	RESEARCH AND INSIGHTS
Account Information	▸ Tenant ID (numeric)	▸ 82da848b	▸ Activation of service ▸ Billing/invoicing ▸ Ongoing service ▸ Future notification of features/updates ▸ Support	Yes	Yes	Yes
Endpoint Characteristics ("What the endpoint IS")	▸ Username (String) ▸ Mac address (12 Dig Hex) ▸ IP address (4 8-bit numeric) ▸ 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)	Yes	Yes	Yes. IP addresses, MAC addresses, usernames and host names are anonymized. Data collected from Active Directory plugin is not shared with the research platform.
Endpoint Behavior (What the endpoint DOES)	▸ Source and destination IP ▸ (4 8-bit numeric) ▸ Port and protocol (string/number) ▸ Time stamp (Unix time) ▸ Occurrences (numeric)	▸ 10.20.10.10 (Private range), 12.5.6.55 (Internet), 224.0.0.37 (multicast) ▸ https/443 (TCP), 17 (UDP) ▸ 1611431404 ▸ 55	▸ Providing information on endpoint communication behavior for policy development and management ▸ Internal business and product analysis and insights to drive product improvements (research platform)	Yes	Yes	Yes. IP addresses, MAC addresses, usernames and host names are anonymized. Data collected from Active Directory plugin is not shared with the 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)	Yes	No	Yes
System Events	▸ Tenant ID (numeric) ▸ Device type ▸ Event type ▸ Time ▸ Severity	{ "syslogSeverity": 7, "eventSubType": "EXPORT", "eventType": "SYSTEM", "outcome": "FAILURE", "tenantId": "test-tenant", "timestamp": 1598353401247, "specialCode": "12F443S", "eventParams": "addional }	Monitor the performance and health of the system	No	No	Yes. IP addresses, MAC addresses, usernames and host names are anonymized. Data collected from Active Directory plugin are not shared with the research platform.
Audit Events	▸ Tenant ID (numeric) ▸ Device type ▸ Event type ▸ Time ▸ Severity ▸ Reason	{ "syslogSeverity": 1, "eventType": "AUDIT", "outcome": "SUCCESS", "tenantId": "test-tenant", "timestamp": 1598353401247, "specialCode": "12F443S", "eventParams": "addional info for adding dashboard", }	Store the events of the system for compliance and traceability	No	No	Yes. IP addresses, MAC addresses, usernames and host names are anonymized. Data collected from Active Directory plugin is not shared with the research platform.

Note: Alphanumeric identifiers are auto generated and random.

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