Forescout Cloud Services Description

This document (**"Service Description"**) describes the Cloud Services (as defined below) being provided by Forescout Technologies, Inc., (**"Forescout"**) to Customer (**"Customer"**) pursuant to the terms of the Forescout End User License Agreement (**"Agreement "**), available here: www.forescout.com/eula. Capitalized terms used but not defined herein shall have the meaning ascribed to them in the Agreement or related addendum. This Service Description may be revised from time to time by Forescout and will be effective upon posting at https://www.forescout.com/company/legal/.

1. Definitions

Term	Definition
Connector	Connector is a virtual appliance or agent which provides an encrypted conduit for the secure transfer of Data Sources from Customer's Environment to Forescout Cloud.
Customer's Environment	The Customer's on-premise, hosted, network, and cloud information technology infrastructure/assets.
Data Sources	A Data Source is any Customer-designated source, including third-party products and services that generates data. Data Sources can include security and non-security related data, e.g., Firewall, IPS/IDS, SIEM, applications, databases, Microsoft Office 365, Microsoft Active Directory, AWS CloudTrail, Google Cloud Platform Audit, Azure Monitor/Activity Cloud, DNS, web proxy, VPN, DHCP.
Detection	A Detection is a high-confidence, high-fidelity set of logically grouped Indicators, generated by Forescout's proprietary Indicator-Detection Engine, enriched with contextual data, correlated to Threat Intelligence, and attributed to an Endpoint or User that indicates a potential threat.
Endpoint	An Endpoint means any physical or virtual IP-addressable device, such as, a computer, server, laptop, desktop computer, tablet, mobile, network switch, network router, PLC, container or virtual machine image which connects to the Customer's Environment.
Endpoint Count	The maximum number of Endpoints monitored by the Cloud Service and licensed to Customer, as specified in the Entitlement.
Enriched Logs	An Enriched Log (also referred to as an **"Event" or "Alert"**) is defined as follows: An Enriched Log is indexed in Forescout Cloud after an observable occurrence in a Data Source that occurred at some point in time and can be security related, non-security related, or a system event.
Indicator	An Indicator is a single Enriched Log, a sequence or aggregation of Enriched Logs, or an analytics model result based on many Enriched Logs that indicates possibly malicious activity but also possibly legitimate activity. An Indicator, by itself, is not normally enough to raise an alert or

Term	Definition
	require a response, but it can contribute to a Detection. This drastically reduces false positives.
Indicator-Detection Engine	Proprietary security analytics engine and a feature of the XDR Service for ingesting, enriching, correlating, and aggregating logs into Indicators and Detections.
Login	Email and password as a means of authentication to gain access to Forescout Cloud.
Threat Intelligence	Strategic, tactical and operational intelligence used to develop applied Detection algorithms, and perform security incident correlation, so that only threats that pose a significant risk are identified.

2. Cloud Service Overview

The Forescout® Cloud (**"FS Cloud"**) is a unified SaaS platform for security visibility, risk, and operational management. FS Cloud continuously discovers and analyzes all cyber assets, whether they are managed or unmanaged for IT, OT/ICS, IoMT, IoT and cloud. The FS Cloud platform provides the foundation for the delivery of the following ("**Cloud Services**"):

- Forescout® Risk and Exposure Management (**"FS REM"**)
- Forescout® Extended Detection and Response (**"FS XDR"**)

Each Cloud Service is licensed on a subscription basis by Endpoint. If Customer uses a Cloud Service beyond the Entitlement ("Overage"), Customer's Forescout Partner may invoice Customer for such Overage. In addition, in the event of an Overage, Forescout may institute controls to limit the Cloud Service to the licensed Endpoint Count.

The Customer has the option to copy data stored in FS Cloud to storage media in the Customer's environment, at the Customer's expense, if the Customer notifies Forescout in writing seven (7) days prior to the Cloud Service termination date.

Customer's use of the Cloud Services shall be in accordance with and subject to the Agreement and the Service Description.

2.1. Forescout REM

The Forescout® Risk and Exposure Management Cloud Service ("FS REM") 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. FS REM supports flexible data collection options (passive sensor, active probe, and API).

- SKUs: FS-SUB-A-REM-100-1-USA, FS-SUB-B-REM-100-1-USA
- Endpoint data retention in FS Cloud is 90 days.
- Ingested endpoint data will be removed from storage and permanently deleted after 90 days has elapsed from the date of ingestion.

- Audit logs recorded for Customer's FS Cloud activity will be deleted after 365 days has elapsed from the date of creation.

2.2. Forescout XDR

The Forescout® Extended Detection and Response Cloud Service ("FS XDR") automatically and intelligently correlates threat signals across the entire enterprise to quickly generate high-fidelity, high-confidence detections for analyst investigation. It can be used standalone, or combined with other Forescout Products, to continuously assess and significantly reduce the risk of an attack, providing the ability to deliver automated response actions to every network and every single device on those networks.

FS XDR includes a maximum allowed aggregate average of 0.6 Events per Second (**"EPS"**) per Endpoint per calendar month (**"Aggregate EPS Cap"**). If a Customer's monthly aggregate average EPS per Endpoint exceeds the Aggregate EPS Cap for 3 consecutive months, Forescout reserves the right to invoice for the Overage, pursuant to the terms of the Agreement.

2.2.1. Essentials license tier retention configuration

- SKUs: FS-SUB-A-XDR-100-1-USA, FS-SUB-B-XDR-100-1-USA, FS-SUB-A-XDR-100-1-CAN, FS-SUB-B-XDR-100-1-CAN, FS-SUB-A-XDR-100-1-UK, FS-SUB-B-XDR-100-1-UK, FS-SUB-A-XDR-100-1-GER, FS-SUB-B-XDR-100-1-GER
- Enriched Logs recorded in FS Cloud are immediately searchable for up to 7 Days after the ingestion date.
- After 7 Days, Enriched Logs are archived and can be searched for up to 31 Days after the ingestion date following a restore from the archive.
- Enriched Logs restored from the archive are immediately searchable for up to 7 Days after restoration.
- Enriched Logs will be removed from storage and permanently deleted after 31 Days has elapsed from the date of ingestion.
- Indicators, Detections, and cases recorded in FS Cloud will be removed from storage and permanently deleted when the Customer cancels the Cloud Service.
- Audit logs recorded for Customer's FS Cloud activity will be deleted after 365 Days has elapsed from the date of creation.

2.2.2. Essentials Plus license tier retention configuration

- SKUs: FS-SUB-A-XDRPLUS-100-1-USA, FS-SUB-B-XDRPLUS-100-1-USA, FS-SUB-A-XDRPLUS-100-1-CAN, FS-SUB-B-XDRPLUS-100-1-CAN, FS-SUB-A-XDRPLUS-100-1-UK, FS-SUB-B-XDRPLUS-100-1-UK, FS-SUB-A-XDRPLUS-100-1-GER, FS-SUB-B-XDRPLUS-100-1-GER
- Enriched Logs recorded in FS Cloud are immediately searchable for up to 7 Days after the ingestion date.
- After 7 Days, Enriched Logs are archived and can be searched for up to 365 Days after the ingestion date following a restore from the archive.

- Enriched Logs restored from the archive are immediately searchable for up to 7 Days after restoration.
- Enriched Logs will be removed from storage and permanently deleted after 365 Days has elapsed from the date of ingestion.
- Indicators, Detections, and cases recorded in FS Cloud will be removed from storage and permanently deleted when the Customer cancels the Cloud Service.
- Audit logs recorded for Customer's FS Cloud activity will be deleted after 365 Days has elapsed from the date of creation.
- Customer has the option to purchase additional Enriched Log retention beyond 365 days.

2.2.3. Professional license tier retention configuration

- SKUs: FS-SUB-A-XDRPRO-100-1-USA, FS-SUB-B-XDRPRO-100-1-USA, FS-SUB-A-XDRPRO-100-1-CAN, FS-SUB-B-XDRPRO-100-1-CAN, FS-SUB-A-XDRPRO-100-1-UK, FS-SUB-B-XDRPRO-100-1-UK, FS-SUB-A-XDRPRO-100-1-GER, FS-SUB-B-XDRPRO-100-1-GER
- Enriched Logs recorded in FS Cloud are immediately searchable for up to 31 Days after the ingestion date.
- After 31 Days, Enriched Logs are archived and can be searched for up to 365 Days after the ingestion date following a restore from the archive.
- Enriched Logs restored from the archive are immediately searchable for up to 7 Days after restoration.
- Enriched Logs will be removed from storage and permanently deleted after 365 Days has elapsed from the date of ingestion.
- Indicators, Detections, and cases recorded in FS Cloud will be removed from storage and permanently deleted when the Customer cancels the Cloud Service.
- Audit logs recorded for Customer's FS Cloud activity will be deleted after 365 Days has elapsed from the date of creation.
- Customer has the option to purchase additional Enriched Log retention beyond 365 days.