Forescout XDR Service Description

This document (**"Service Description"**) describes the Cloud Service (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 which provides an encrypted conduit for the secure transfer of Data Sources from Customer's Environment to Forescout Cloud.
Customer Environment	The Customer's network, cloud services and/or information technology infrastructure and 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 Entity that indicates a potential Threat. **Detection Severity Classification** Classification — Condition Critical — One or more Detections are identified as an attack, or attempted attack that may result in damage or unauthorized access to a device or application. The cause may render Customer's Environment vulnerable or compromised. High — One or more Detections are identified as a known attack, attempted known attack, or reconnaissance effort. Customer's Environment is not considered vulnerable or compromised based on the Service Context.

Term	Definition
	Medium/Low — One or more Detections may be falsely triggered, are informational, or benign in nature.
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.
Entity	An Entity can be an Endpoint or User.
Health Detection	A Health Detection is triggered when a health event rule detects a Connector is offline or Forescout Cloud has stopped receiving Data from a Data Source.
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 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 Forescout XDR 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

Forescout XDR (**"Cloud Service"**) is an extended detection and response solution that automatically and intelligently correlates threat signals across the entire enterprise to quickly generate high-fidelity, high-confidence detections for analyst investigation. Combined with other Forescout Products, it can 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.

Forescout XDR is licensed on a subscription basis by Endpoint Count. Forescout XDR includes a maximum allowed aggregate average of 1.2 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 Customer for the Overage, pursuant to the terms of the Agreement. .

Forescout XDR provides the right to access a cloud-native, cyber security console (**"Forescout Cloud"**). Forescout Cloud is a SaaS-based solution for security visibility and operational management.

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

3. Maintenance Policy

In order to make Forescout XDR highly available and secure, as well as deliver the latest feature enhancements, Forescout XDR has three types of maintenance windows:

1. **"Platform Updates"**
    a. *Purpose:* Performed to deliver the latest features to customers
    b. *Frequency:* At most once per week
    c. *Notification:* Release notes posted in Forescout Documentation Portal: https://docs.forescout.com/en-US/
    d. *Performance:* During Platform Updates, ingest, login and search services may be degraded for a short period of time
2. **"Planned Maintenance"**
    a. *Purpose:* Performed to deliver non-feature related enhancements
    b. *Frequency:* Limited to a maximum of 2 hours per calendar month
    c. *Notification:* Forescout will notify customer at least 72 hours prior to Planned Maintenance
    d. *Performance:* During Planned Maintenance, ingest, login and search services may be degraded or unavailable for a short period of time. Logs forwarded during Planned Maintenance are cached and indexed at the end of Planned Maintenance.
3. **"Emergency Maintenance"**
    a. *Purpose:* Performed when immediate attention is required to stabilize Forescout Cloud.
    b. *Frequency:* Unscheduled, as needed under exceptional circumstances
    c. *Notification:* Forescout will make commercially reasonable efforts to notify Customer of Emergency Maintenance in advance
    d. *Performance:* During Emergency Maintenance, ingest, login and search services may be degraded or unavailable for a short period of time

4. Data Retention

Data retention in Forescout Cloud is driven by the Forescout XDR subscription Customer purchased, as described below:

A. Forescout XDR

- SKUs: FS-SUB-A-XDR-100-1, FS-SUB-B-XDR-100-1
- Enriched Logs recorded in Forescout Cloud are immediately searchable for up to 3 Days after the ingestion date.
- After 3 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 7Days after restoration

- Enriched Logs will be removed from storage and permanently deleted after 31 Days has elapsed since ingestion date.
- Indicators, Detections, and cases recorded in Forescout Cloud will be removed from storage and permanently deleted when the Customer cancels the Cloud Service.
- Audit logs recorded for Customer's Forescout Cloud activity are deleted after 365 Days has elapsed since the audit log was created.

B. Forescout XDR Professional

- SKUs: FS-SUB-A-XDRPRO-100-1, FS-SUB-B-XDRPRO-100-1
- Enriched Logs recorded in Forescout 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 since ingestion date.
- Indicators, Detections, and cases recorded in Forescout Cloud will be removed from storage and permanently deleted when the Customer cancels the Cloud Service.
- Audit logs recorded for Customer's Forescout Cloud activity are deleted after 365 Days has elapsed since the audit log was created.
- Customer has the option to purchase additional Enriched Log retention beyond 365 days.

The Customer has the option to copy stored data 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 Cloud Service termination date.