Cloud Services Description

This document ("**Cloud Services Description**") describes the Cloud Services (as defined below) being provided by Forescout Technologies, Inc., ("**Forescout**") to 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 Cloud Services 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.

"Customer Environment" means the Customer's on-premise, hosted, network, and cloud information technology infrastructure and/or assets.

"Data Source" means any Customer-designated source, including third-party products and services that generates Customer Data. Data Sources may 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.

"Endpoint" means any physical or virtual IP-addressable device, such as, a computer, server, laptop, desktop computer, tablet, mobile phone, network switch, network router, PLC, container or virtual machine image which connects to the Customer Environment directly or through specific gateways.

"Endpoint Count" means the maximum number of Endpoints to be monitored by the Product, as specified in the Entitlement.

"Enriched Logs" means a log that 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; "Enriched Logs" may also be referred to as an "**Event**" or "**Alert**".

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 products ("**Cloud Services**"):

- Forescout® Risk and Exposure Management ("**FS REM**")
- Forescout® Threat Detection and Response ("**FS TDR**")
- Forescout® eyeSegment ("**FS Segment**")

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 Cloud Services Description.

2.1. Forescout REM

The Forescout® Risk and Exposure Management Cloud Service 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).

- 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.
- FS REM hosts data in the United States, Canada, Germany, Qatar, Australia and United Kingdom.

2.2. Forescout TDR

The Forescout® Threat Detection and Response Cloud Service 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.

- After the ingestion date Enriched Logs recorded in FS Cloud are immediately searchable for the number of days as specified by each SKU ("**Immediate Search Term**").
- After the Immediate Search Term, Enriched Logs are archived and can be searched for the number of days as specified by each SKU following a restore from the archive ("**Archive Search Term**").
- 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 the Archive Search Term has lapsed.
- 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.
- FS TDR hosts data in the United States, Canada, Germany, Qatar, Australia and United Kingdom.

Offerings	Immediate Search Term	Archive Search Term
Threat Detection & Response Core	7 Days	31 Days
Threat Detection & Response Plus	7 Days	365 Days
Threat Detection & Response Professional	31 Days	365 Days

2.3. Forescout eyeSegment

The Forescout® eyeSegment Cloud Service is a zero trust solution that simplifies the design, planning, and deployment of network segmentation across an organization's environment, enabling visualization of traffic flows, policy simulation to provide granular enforcement to reduce cyber risk and operational complexity.

- Flow and utilization data retention in FS Cloud is 90 days.
- Ingested flow and utilization data will be removed from storage and permanently deleted after 90 days has elapsed from the date of ingestion.
- FS Segment hosts data in the United States, Germany and United Kingdom.