Forescout Assist for XDR Service Description

This document (**"Service Description"**) describes the 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 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 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

Term	Definition
	Medium/Low — Environment is not considered vulnerable or compromised based on the Service Context. One or more Detections may be falsely triggered, are informational, or benign in nature.
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 Customer's Environment.
Endpoint Count	The maximum number of Endpoints monitored by the 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.
Entity	An Entity can be an Endpoint or User.
Exploit	A method to use a Vulnerability to gain unauthorized access to functions, data, or privileges with malicious intent. An exploit can include a script or malware (virus, trojan, worm). An attack is the use of an Exploit. See below for examples of exploits: • A script refers to a document with steps to manually find and exploit vulnerabilities. A script is replicated by publishing it. • A virus refers to malicious software attached to a medium (e.g. files, removable media, and documents). A virus replicates using this medium. • A trojan refers to malicious software embedded in an application. The trojan will not replicate itself, as it spreads with the application. • A worm refers to a self-contained program (or set of programs) that spreads copies to other computers. A worm can spread through network connections and emails.
Health Detection	A Health Detection is triggered when a health event rule detects a Connector is offline or Forescout Cloud has stopped receiving Data Sources.
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, may not be enough to raise an alert or require a response, but it can contribute to a Detection.
Indicator-Detection Engine	Proprietary security analytics engine and a feature of Forescout Cloud for ingesting, enriching, correlating, and aggregating Logs into Indicators and Detections.

Term	Definition
Login	Email and password as a means of authentication to gain access to Forescout Cloud.
Security Incident	A Security Incident (also referred to as an **"Incident"**) may represent an attack or potential attack.
Security Incident Case	A Security Incident Case is defined as a case in Forescout Cloud created for a Suspicious Entity which tracks and drives the SOC Incident Handling Workflow (Appendix A).
Service Context	A set of documents uploaded to Forescout Cloud with version control containing information about Customer that Forescout uses for the provisioning and delivery of the Service. The Service Context is setup during deployment & onboarding and is updated as required during the monthly business review process between Forescout and the Customer. The Service Context may include one or more of the following: • Forescout Cloud Users with Admin role • Authorized contacts • Business critical assets • Custom threat intel sources/feeds • Escalation, notification and reporting procedures • List of all office campuses, sites, data centers, cloud service accounts, and software-as-a-service accounts where Endpoints are provisioned • Endpoint Count • Network topologies • Roles and responsibilities for any customized workflows
SOC Escalation Runbook	A Customer completed document which defines the decision tree for escalated Security Incident Case notifications.
Suspicious Entity	Suspicious Entity (also referred to as a **"Triage Card"**) is defined as a single Detection or a series of Detections that have been automatically aggregated and attributed to an Entity in Forescout Cloud.
Threat	A Threat is malicious code or activity executed by an internal or external actor who has attempted or who is attempting to for example: • Harm the Customer Environment • Exfiltrate or steal data from the Customer Environment • Use the Customer Environment to attack another environment. Examples of Threats may include the suspected: • use of an Exploit, or suspected presence of a Vulnerability in a configuration, software, firmware, application code, network, or platform. • infection by a worm or virus, or it can be a targeted attack.

Term	Definition
	• violation of an explicit or implied security policy. • attempts to gain unauthorized access. • unwanted denial of resources. • unauthorized use of systems. • execution of system changes without Customer's knowledge, instruction, or consent.
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.
Vulnerability	A weakness or defect of an Endpoint that can be exploited to gain access to data functions or privileges violating the intended authorization. Examples of Vulnerabilities can be defects: in application or system software (e.g., bugs), in the user administration (e.g., non-protected user accounts), in the configuration (e.g., unintended network or file access), in the policy and Rule Set definition (e.g., unrestricted open ports or exposed IP-addresses), etc. The combination of all vulnerabilities of a given system or infrastructure is the exposure.

2. Service Overview

Forescout Assist for XDR (**"FS Assist"**) is a Service that provides 24/7 cyber security monitoring, and human-led threat hunting. The FS Assist Service is powered by Forescout Cloud, which provides the foundation for delivery of the Service. The FS Assist Service is delivered remotely by our team of certified security experts (**"Forescout SOC"**).

FS Assist requires the Customer to have an Entitlement for Forescout Extended Detection and Response (**"FS XDR"**) .

3. Service Activities

The activities performed during Service delivery (**"Service Activities"**) depend on close collaboration between Forescout and the Customer. In many cases, coordinated action is required to provision or maintain the Service, and if a Customer fails to comply with their responsibilities, Forescout's ability to provide the Service may be adversely affected. The following outlines Customer and Forescout responsibilities that are applicable to specific Service Activities.

3.1. Discovery and Planning	
The purpose of this Service Activity is to conduct a kickoff call and a series of discovery and planning calls to gather information on the Customer's Environment along with relevant processes and procedures to define the Service Context and high-level deployment and onboarding plan.	
Forescout Responsibilities	**Customer Responsibilities**

3.1. Discovery and Planning	
• Schedule meeting(s), either in-person, by phone or by web conference, to plan the transition to the Service. • Define the high-level plan that describes the transition to the Service, milestones, and prerequisites, and establish a target date for deployment (**"Transition Plan"**). • Gather information to document the Service Context. • Identify the Customer's primary threat detection use cases and consult on the sensors and sources required to meet these goals. • Identify a single point of contact (SPOC) to engage with Customer during transition to the Service. • Perform any other tasks designated as Forescout's responsibility in the Transition Plan by the date specified in the Transition Plan • Review Forescout SOC Incident Handling Workflow (Appendix A)	• Provide the requested information to document the Service Context by the date in the Transition Plan. • Review and approve Transition Plan • Identify a SPOC to engage Forescout during transition to Service. • Perform tasks specified as Customer's responsibility in the Transition Plan by the date specified in the Transition Plan. • Obtain related internal compliance and governance approvals for data integration. • Work with Forescout to establish any exceptions to Forescout SOC Incident Handling Workflow (Appendix A) and provide escalation points of contact. • Provide Forescout with Customer contacts as needed for operational collaboration and incident escalations. Should these contacts change, the Customer must advise Forescout or update the necessary information via Forescout Cloud.

3.2. Deployment and Onboarding	
The purpose of this Service Activity is to assist with deploying the Connector (if required) and onboarding Data Sources.	
Forescout Responsibilities	**Customer Responsibilities**
• Assist the Customer with deploying at least one Connector (if required) in each Customer Environment to be used for receiving/pulling/forwarding Data Sources • Assist Customer with onboarding the Data Sources in scope for the Service. • Provide the Customer with secure access to Forescout Cloud. The Customer will be provided with an administrative login for provisioning subordinate accounts, as required, for their staff. • Assist Customer with uploading the Endpoint Count in Forescout Cloud. • Develop the required parsers and pullers for any unsupported Data Sources, which must provide security relevant data and be	• Provide Forescout the Endpoint Count or upload directly in Forescout Cloud. • Provide the necessary resources within Customer Environment such as connectivity, accounts, IP addresses, virtual machines (compute, memory, storage), credentials, OS, etc., as required to deploy Connector. • Work with Forescout to configure data pipeline for Data Sources ingestion from Customer network to Forescout Cloud (e.g. servers, firewalls, Active Directory, virtual private network (VPN), mail and web gateways and proxies). • Unless Forescout is providing the OS for the Connector (in the case when the Connector is distributed as a virtual appliance/OVA),

3.2. Deployment and Onboarding	
generated by a commercially available solution. • Work with customer to integrate any Customer exclusive Threat Intel feeds. • Provide the architecture guidelines for Data Sources ingestion and system requirements (e.g. CPU, RAM, storage, network connectivity, etc.) for compatibility with, and operation of, the Connector, if required. • Unless Customer is providing the operating system (**"OS"**) for the Connector, Forescout will remotely apply OS patches and upgrades at its discretion to help ensure the Connector remains up to date with important security patches.	Customer will apply OS patches and upgrades to help ensure the Connector remains up-to-date with important security patches. • Securely document and manage access credentials (e.g. username and password, or secret key pairs) to the virtual server(s) the Connector is deployed on.

3.3. Service Adjustment Period / Transition to Steady State and Tuning	
The purpose of this Service Activity is to tune the Indicator and Detection rules, validate the ingested Data Sources, learn the Customer's environment and gain some contextual awareness.	
Forescout Responsibilities	**Customer Responsibilities**
• Enable/disable Indicator and Detection rules to match Customer's use cases. • Provide Indicator and Detection rule tuning recommendations, and work with Customer to apply mutually agreed to whitelist and rule parameters to minimize false positives. • Validate ingested Data Sources is being parsed and transformed correctly. • Perform EDA on newly supported Data Sources to test various hypotheses for identifying potential Indicator and Detection rules.	• Review rule tuning recommendations and agree to mutually implement with Forescout. • Work with Forescout to resolve any Data Sources configuration issues preventing the required data fields from being ingested by Forescout Cloud.

3.4. Service Health Monitoring	
The purpose of this Service Activity is to monitor the availability of the Connector and the ingestion health of Data Sources.	
Forescout Responsibilities	**Customer Responsibilities**
• Monitor and investigate all Health Detections triggered by Forescout Cloud that indicate a health issue with the Connector or Data Sources source.	• Participate in troubleshooting to identify the source of a Health Detection. • Notify Forescout in advance of any maintenance updates or changes to

3.4. Service Health Monitoring	
• Determine the cause of a Health Detection through remote diagnosis, and initiate device troubleshooting to remedy the problem remotely. • Forescout will escalate the Health Detection to Customer via a **"Health Incident Case"** in Forescout Cloud if it cannot be resolved.	Customer's Environment that may trigger false positive Health Detections. • Take actions required to mitigate any Health Detections and notify if case is resolved.

3.5. Security Monitoring and Triage	
The purpose of this Service Activity is to monitor, and triage generated Suspicious Entities.	
Forescout Responsibilities	**Customer Responsibilities**
• Monitor all Detections and triage Suspicious Entities generated by the Forescout Indicator-Detection Engine, continuously 24/7. • Follow the Forescout SOC Incident Handling Workflow (Appendix A) for monitoring and triaging Suspicious Entities according to the **"Mean Time to Triage – Suspicious Entity"** Service Level Commitment defined in Forescout Assist SLA on https://docs.forescout.com/. • Create a Security Incident Case via Forescout Cloud for a Suspicious Entity that cannot be confirmed as benign true positive/false positive during triage to continue with the investigation.	• Contact Forescout if Customer believes a cyber-attack is in-progress or has occurred in Customer's Environment.

3.6. Threat Investigation	
The purpose of this Service Activity is to investigate Security Incident Cases to validate whether a Suspicious Entity is a confirmed Threat.	
Forescout Responsibilities	**Customer Responsibilities**
• Investigate Security Incident Cases to validate whether a Suspicious Entity is a confirmed Threat, and to identify Impact in accordance with the definitions in Appendix B • Document observations, attacker attributes, root cause, attack vector, attack campaign, infected Entities, malware capabilities and behavior and indicators of compromise (IOCs) as analysis in the Security Incident Case. • When a Security Incident is not fully discovered, is unknown or has insufficient	• Review Security Incident Case waiting on feedback from Customer and provide any additional context/Data Sources that can aid in an investigation, notify Forescout if it has been resolved, or resolve the case with the relevant reason code.

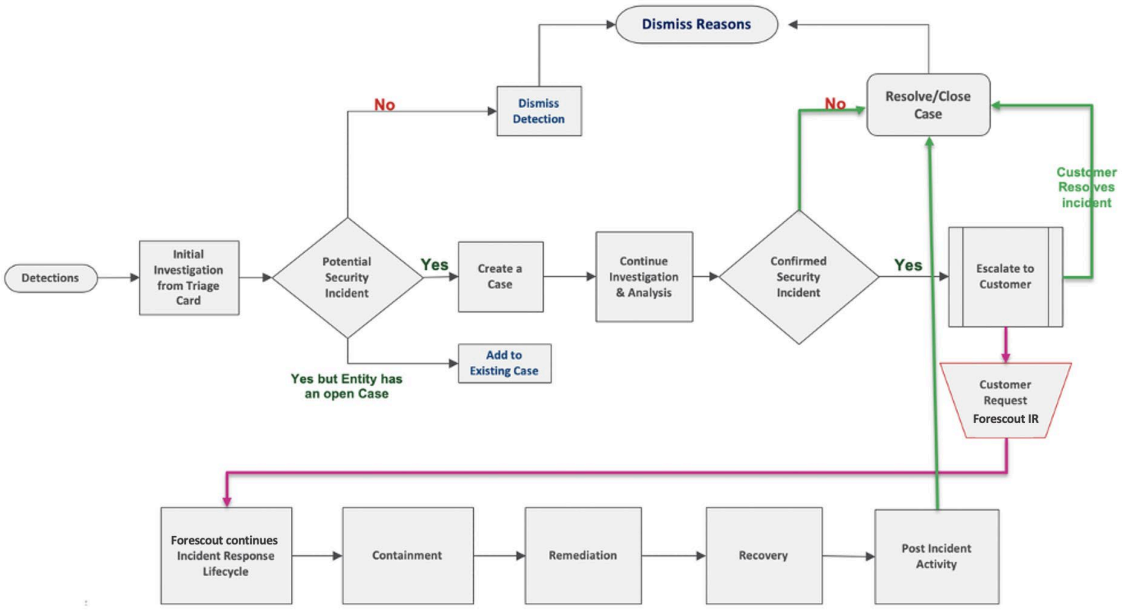
3.6. Threat Investigation	
information, recommend further investigation steps to Customer in the Security Incident Case and change its status to Waiting on Customer.	

3.7. Incident Management	
The purpose of this Service Activity is to provide end-to-end support once a Security Incident is confirmed.	
Forescout Responsibilities • Escalate a Security Incident Case once the Impact level is assigned (**"Confirmed Security Incident"**) in accordance with the definitions in Appendix B and in accordance with the **"Mean Time to Escalate – Security Incident"** Service Level Commitment defined in Forescout Assist SLA on https://docs.forescout.com/. Case escalation communication will be performed with Customers via email notifications generated by Forescout Cloud, when a Case is created and linked in Customer's integrated 3rd party case management system (where possible), or following Customer's preferred escalation procedure defined in the SOC Escalation Runbook. • Based on the nature of the Security Incident, provide containment and remediation guidance to stop and/or recover from an attack, if Customer requests it. • Recommend policy or security control changes to prevent similar Security Incidents from arising.	**Customer Responsibilities** • Review escalated Security Incident Case (Description, Incident Analysis, Recommendations sections) and notify Forescout if the incident has been resolved, or if Customer needs containment and remediation guidance. Also notify Forescout if the case was benign/false positive or resolve the case with the relevant reason code. • Resolve the escalated Security Incident Case with the appropriate resolve reason if it has been resolved. • If escalated Security Incident Case requires additional investigation or feedback has been provided by Customer, Customer will return the Case to the Forescout SOC. • Act on Forescout's recommendations or guidance and notify Forescout if Customer will not act on it.

3.8. Threat Hunting	
The purpose of this Service Activity is to provide tailored and proactive threat hunting.	
Forescout Responsibilities • Provide continuous monitoring and proactive investigation support for high-risk activities and IOCs that are not easily detected or prevented by security controls. • Support incident response activities by tracing all attack-related activities for	**Customer Responsibilities** • Provide feedback on which findings are normal and which are anomalous/benign in the escalated cases. • Provide feedback on prioritized assets and threats.

3.8. Threat Hunting	
containment and validating their mitigation during recovery. • Prioritize hunts based on Customer profile, critical assets, prevalent threat actors, current threat intelligence, high risk tactics, techniques, and procedures, and Customer input. • Escalate malicious findings to Customer via Security Incident Cases in Forescout Cloud.	• Work with Forescout as a partner by collaborating to provide a better understanding of Customer's security priorities and environmental norms.

Appendix A: SOC Incident Handling Process



Security Incident Case Status	Definition
Detection and Analysis	This is the initial case status when a new case is opened and Forescout SOC is still performing investigation and analysis
Escalated to Customer	Case status assigned when Forescout SOC completes an investigation and determines the case is a confirmed Security Incident and needs to be escalated to a customer
Waiting on Customer	Case is assigned to a case when waiting for additional information from a Customer to determine the validity of a Security Incident
Containment	Case status assigned when a Security Incident is in containment status of the IR life cycle
Remediation	Case status assigned when a Security Incident is in remediation status of the IR life cycle
Returned to SOC	Case status assigned when escalated Security Incident returned to Forescout SOC for follow-up
Post Incident Activity	Case status assigned when a Security Incident is in post incident activity status of the IR life cycle

Appendix B: Security Incident Case Impact Definitions

This Appendix describes the methodology and associated terminology used to define Security Incident Case Impact (**"Impact"**). A Security Incident Case Impact is classified according to the breadth of its impact on the Customer's business (the size, scope, and complexity of the Security Incident). Impact is a measure of the business criticality of a Security Incident, often equal to the extent to which it affects the availability of the Customer's Environment. There are 5 Impact levels:

Impact	Definitions
Sev-1	Severity 1 one impacts everyone or a very large number of customer's critical business operations. This indicates a high risk of compromise or potential disruption to customer's critical business operations or infrastructure (domain controller, patient accounting system, email systems) Examples include: Distributed Denial of Service (DDoS) attacks impacting customer business environment; enterprise wide malware outbreak and worm infections/ propagation impacting multiple business units, System or data compromises with potential reputational damage to a customer environment; **All Sev-1 incidents are considered major incidents**
Sev-2	Severity 2 impacts critical IT infrastructure, application, telecommunications or multiple end-users and/or multiple assets groups. These are high-risk events that have the potential to cause severe damage to a customer's environments. Examples include: Discovery of OWASP Top 10 vulnerability in a customer's environment actively exploited with potential impact; System or data compromises; privacy breaches; enterprise wide malware outbreak and worm infections/ propagation impacting single business unit; Ransomware infection on a single machine; significant Denial of Service (DoS) or; zero day threats that apply to a customer's infrastructure; creation of ID's with elevated privileges or adding elevated privileges to existing id's outside of approved change control processes; tampering of critical system files, application files, or databases that will impact system integrity; authorized (system) policy changes; and deletion of audit log files. **All Sev-2 incidents are considered major incidents**
Sev-3	Severity 3 may impact a business group, electronic assets, and/or an end-users' group. These incidents are typically unauthorized user activities that do not have ability to impact system performance or harm data but has lost efficiency. Examples include: Discovery of OWASP Top 10 vulnerability in a customer's environment NOT actively exploited; unauthorized local scanning activity; attacks targeted at specific servers or workstations; unauthorized creation of IDs on critical systems; user- caused contiguous failed/successful login attempts; failed attempts of tampering with critical systems, applications, audit log files, and databases; accessing critical systems or application files; malware outbreaks impacting a single

	business unit or a territory; uncleaned malware in a single user machine; phishing activity against a single user
Sev-4	Severity 4 impact a single end-user related, or non-critical business processes related. They do not directly impact business operations, but are necessary for the 'day- to-day' work and include unauthorized activity or policy violation Examples include: Script Kiddie scans, Discovery scanning; information gathering scripts; other reconnaissance probes; downloading of Unauthorized software; use of unauthorized P2P applications;
Sev-5	Severity 5 is usually informational alert as well as false positives. There is no impact to any operations.