Managed Security Premier

Service Description

Service Overview:

Managed Security Premier provides 24x7x365 proactive administration of your network security infrastructure. This package provides principle network security controls in a single bundled package. This bundle includes Managed Firewall, Intrusion Detection Prevention Services (IDPS), Web Content Filtering, Gateway AV and remote access that includes two factor SSL VPN. SilverSky provides full management, monitoring and response for the services. These services are deployed on our industry standard and proprietary platforms.

Managed Security Premier service provides the customer with the following:

- Customer portal with reporting functionality on firewall and Intrusion Detection Prevention System (IDPS) logs (SMC Portal)
- Service support 24x7 with online ticketing and customizable alerts through the customer portal
- Threat intelligence correlation across the customer firewall and IDPS to protect against threats
- Event/Incident triage with security service support. Triage will work towards identification and remediation.
- Hardware or software user security tokens to support remote user access.
- Signature and policy tuning of the firewall hardware prior to shipment.

SERVICES PROVIDED

The following service components are included with Managed Security Premier Services:

- Device availability monitoring
- Security Event Monitoring
- Upgrade and Patch Management
- Change Management
- Gateway Anti-Virus
- Web Content & URL Filtering (WCF)

Device Availability Monitoring

SilverSky must be able to connect to the device via the Internet using SSH, SNMPv3, HTTPS & IPSEC protocol.

SilverSky will perform availability monitoring of the device. SilverSky monitors availability via periodic polling of the device. If periodic polling checks indicate that the device has become unavailable, an automatic alert is sent to SilverSky which then generates a ticket for the customer to view on the SMC Portal.

If the root problem of device failure is customer related, such as a network change, outage, or customer-managed device, SilverSky will provide customer with troubleshooting information upon customer request but SilverSky is not responsible for troubleshooting issues that are not directly related to the device under SilverSky management.

Security Event Monitoring

Device log data is gathered, parsed, correlated, and prioritized by SilverSky. The relevant security events, if any, are categorized by SilverSky based on the severity level. Malicious and unknown events are correlated and alerts are presented to Customer via the SMC Portal.

The SMC Portal provides customers with a secure, web-based method to monitor the environment, generate security reports and update escalation procedures.

Following deliverables are associated with Security Event Monitoring

- SMC Portal access for ticket requests and reporting capabilities.
- Ongoing security event aggregation and reporting for devices during the service term.

Incident response, forensics and ticket requests associated with security event analysis are not included in security event monitoring.

Software Upgrade and Patch Maintenance

As security related software patches and upgrades are released by the device vendor, SilverSky assesses the applicability of each release to Customer’s environment. SilverSky will work with Customer to schedule any necessary remote upgrades if necessary.

In cases where support for a particular product or product version is being discontinued by the vendor or by SilverSky, SilverSky will communicate new platform migration options, if any. In order to be assured of uninterrupted service, Customer must complete the migration process within sixty (60) days notification by SilverSky. Customer bears any costs relating to procuring new hardware or components and to re-provisioning any devices.

Change Management

Customer may submit change requests to SilverSky via the SMC portal. SilverSky requires that the change request is made by an authorized Customer contact. SilverSky will contact Customer via email or customer portal to clarify requests as needed. The Change Management request could be on any of the following features of the device.

Firewall

SilverSky will manage the policy on the device.

The following defines what is considered to be a policy change:

• Adding, deleting, or modifying up to three individual Network Address Translations (NAT) (incoming, outgoing and loop-back) including object creation

• Adding, deleting, or modifying up to two access control list changes (such as permit or deny changes) Including the creation of up to 6 policy objects creation (Hosts, Groups, Networks, Ranges and Service objects)

• Adding, deleting, or modifying up to two individual network routes within the firewall

Standard policy change may comprise one or more of the above bullets. Any change request that is not specifically listed above may be completed by SilverSky on a time and materials basis. SilverSky reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.

SilverSky does not design or validate rule sets or provide troubleshooting related to rule sets as part of the Service.

Intrusion Detection and Prevention System

SilverSky manages the policy on the device. Policies are updated regularly as updates are released by Fortinet and reviewed by SilverSky.

The following defines what is considered to be one policy change:

• Adding, deleting, or modifying IDPS signatures, not including routine signature updates

Any change request that is not specifically listed above may be completed by SilverSky on a time and materials basis. SilverSky reserves the right to determine, within its reasonable discretion, whether a change falls within the scope of Customer's service.

Gateway Anti-Virus support

SilverSky includes Gateway Anti-Virus functionality on Managed Security Premier Fortinet devices. As a component of this service, SilverSky will work with Fortinet to update anti-virus signatures/policies regularly when updates are released by Fortinet and reviewed by SilverSky.

Security relevant AV events are logged to the SilverSky SMC portal. These events will not result in ticket creation or viewing by a SilverSky SOC Analyst.

Web Content Filtering (WCF) support

SilverSky also includes Web Content Filtering (WCF) with the Managed Security Premier bundle. WCF as a licensed option is included in purchase of this bundle, SilverSky shall deploy the default categorization policy by zone or internet protocol ("IP") range as specified by the Customer. Web sites that are accessed that are within an enabled category shall be blocked. Customers who wish to challenge a categorization shall contact SilverSky SOC directly.

Customers can request, via the SilverSky SMC Portal, a change of website category. This is equated to a standard policy change request. Requests for whitelisting or blacklisting of domains are permitted under a standard policy change request and made possible within the SilverSky SMC portal. User authentication for WCF service is not supported.

Other Services

Any other services are out-of-scope. Examples of such out-of-scope support include but are not limited to:

- On-site installation and provisioning of device.
- Integration of complementary products that are not managed by SilverSky (e.g., encrypted email; web reporting software).
- Custom analysis and/or custom reports.
- Forensics.
- Any change requests not specified above.
- Configuration of any tunnel end point that is not terminated on a SilverSky-managed device.
- Rule set design, validation, and troubleshooting.
- Firewall policy auditing, policy/rule utilization, and security best practice consulting

CUSTOMER REQUIREMENTS

Customer agrees to perform the following obligations and acknowledges and agrees that SilverSky System’s ability to perform its obligations, and its liability under the SLAs below, are dependent upon Customer’s compliance with the following:

Hardware/Software Procurement

The Customer is responsible for purchasing the device and service necessary for SilverSky to deliver the Service. Additionally, the Customer is responsible for ensuring that their hardware/software stays within SilverSky’ supported versions of the device. SilverSky System’s SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updates by the device manufacturers.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned devices and connectivity to prevent network performance degradation and maintain communications between the customer’s contracted devices and SilverSky System’s security operations centers (Secure Operations Centers” or “SOC(s)”).

RMA Responsibilities

The Customer is responsible for initiating and fulfilling the return materials authorization (“RMA”) process directly with SilverSky in the event that the hardware/software being managed by SilverSky is determined to be in a failed or faulty state and requires replacement.

Connectivity

Customer will provide access to Customer-premises and relevant appliance(s) necessary for SilverSky to manage and monitor the contracted firewall devices. Additionally, Customer should communicate any network or system changes that could impact service delivery to the SOC via a ticket in the SMC Portal. Service activation which may require device downtime will depend on customer deliverables such as on-site assistance with initial configuration of the appliance to get connectivity between Fortinet appliance and SilverSky data centers. SLAs will not apply to devices that are experiencing Customer-caused connectivity issues.