Managed Gateway Anti-Virus

Service Overview

Managed Gateway Anti-Virus (the "Service") is provided on Fortinet next generation firewall appliance with 24x7x365 proactive administration and monitoring of your Fortinet firewall appliance. Certified security experts will perform all activities necessary to keep the Managed Gateway Anti-Virus enabled Fortinet appliances operating at peak performance. The Security Operations Center (SOC) is trained to handle the management of your Anti-Virus protection and contact the customer based on predefined incident handling policies.

Service Objectives: Managed Gateway Anti-Virus service provides the customer with the following:

- Protection from malware, viruses, spyware and other content-level threats
- Service support 24x7 with online ticketing
- Signature database can be configured for updates hourly, ensuring the latest possible coverage
- Advanced detection engines can analyze and detect unknown threats before they infect the network.

Service Deliverables: Managed Gateway Anti-Virus service will deliver to the customer the following:

- Defined custom A/V signatures
- Monitoring and reporting of Gateway A/V events that trigger an alert
- Management of A/V signature and policy tuning and updates
- Online ticketing support for change management

Service Description

A proprietary threat intelligence platform provides the foundation for delivery of our Managed Gateway Anti-Virus service. Managed Gateway Anti-Virus protects against the latest viruses, spyware, and other content-level threats. The best way to protect your organization is to keep malware out, and Managed Gateway Anti-Virus uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and accessing its invaluable content.

The Managed Gateway Anti-Virus service is available through FortiGate next generation firewalls and includes:

- Scanning of encrypted files traversing the firewall for viruses

The scanning of encrypted files reduces the risk of data breach or damage caused by malware with highly effective antivirus protection delivered through multiple control points. It protects against the latest malware variants with proactive technologies able to block previously unknown threat variants.

Other Services

Any other services are out-of-scope. Upon request, SilverSky may provide out-of-scope technical support on a time and materials basis pursuant to a separate service description or statement of work ("SOW"). 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., antivirus software; web reporting software)
- Custom analysis and/or custom reports
- Forensics
- Any change requests not specified above
- Rule set design, validation, and troubleshooting
- 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 firewall hardware and service necessary for SilverSky to deliver the Service. Additionally, the Customer is responsible for ensuring that their hardware/software stays within Fortinet's supported versions. SilverSky System's SLAs will not apply to platforms that are end of life, end of support, or are otherwise not receiving updates by Fortinet.

Support Contracts

Customer is responsible for maintaining appropriate levels of hardware support and maintenance for the Customer-owned firewall and connectivity to prevent network performance degradation and maintain communications between the customer's contracted firewall 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 SilverSky SMC customer 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