WiFi Monitoring Service

Service Overview

WiFi Monitoring Service (the "Service") provides wireless access to the network through Fortinet technology. We will monitor traffic across the Fortinet wireless networks.

Service Objectives: WiFi Monitoring service provides the customer with the following:

- 24x7 Monitoring of your WiFi traffic, blocking access to malicious, hacked or inappropriate websites
- 24x7 Service support with whitelist/blacklist capabilities, ticketing and alerting
- Event/Incident triage with security service support. Triage will work towards identification and remediation.
- SILVERSKY will provide alerting based on malicious behavior.

Service Deliverables: WiFi Monitoring service will deliver to the customer the following:

- Fortinet WiFi network enabled on Fortinet technology
- WiFi network monitoring, active directory integration
- Monitoring, Alerting, Blocking of malicious websites
- Bandwidth optimization when paired with Application Control
- Portal access with service ticketing

Service Description

WiFi Monitoring service is available as an add-on feature of the Managed Security Service through the FortiGate next generation firewall. No extra licenses are necessary, just SILVERSKY System's configuration and monitoring of your wireless network environment to ensure that the security fabric is well-protected through our use of Threat Intelligence and correlation with your existing firewall detection capabilities. WiFi-capable Fortinet technology will allow you to use active directory for secure wireless network implementations.

- Provides a secure wireless experience with the latest hardware integration
- Optimizes bandwidth usage on your network by prioritizing, de-prioritizing, or blocking traffic when paired with application control
- Customer is responsible for site survey, WiFi coverage ("dead spots")

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.