Application Control Service

Service Overview:

Application Control Service (the "Service") improves security and meets compliance with easy enforcement of your acceptable use policy through control of the applications your users are running. With Application Control, you can create policies to allow, deny, or restrict access to applications or entire categories of applications.

Service Objectives: Application Control service provides the customer with the following:

- Privacy and security of data used by and transmitted between applications
- Controls input, output, and/or access from, to, or by an application or service
- Service support 24x7 with online ticketing
- Monitors and potentially blocks the input, output, or system service calls that do not meet the configured policy of the firewall

Service Deliverables: Application Control service will deliver to the customer the following:

- Monitoring and blocking of applications that do not meet the configured firewall policy
- Quarantine and Allowance of user-defined applications
- Online ticketing support for change management and reporting

Service Description

Application Control service is available as part of the NGFW service through the FortiGate next generation firewall. Conventional firewalls that only identify ports, protocols, and IP addresses can't identify and control applications, but your next generation firewall can use application control to keep malicious, risky, and unwanted applications out of your network through control points at the perimeter, in the data center, and internally between network segments traversing the firewall.

- Protects your organization better by blocking or restricting access to risky applications
- Optimizes bandwidth usage on your network by prioritizing, de-prioritizing, or blocking traffic based on application

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.