SilverSky Managed Services

Threat Feed Engine

SilverSky has implemented a one-touch solution to enable your firewalls to block malicious activity detected by our analysts in our Global Security Operations Center (SOC). Our Threat Feed Engine (TFE) protects our customers by activating a blocking response via API to your firewalls, without the need for SilverSky to have administrative access to that device. After several months of beta testing, and implementing TFE on all of our managed devices, we are rolling out this capability to all of our Lightning Managed Detection and Response customers.

This new feature is available without a contract change nor increase in cost. Once TFE is enabled, there is no action that customers need to take to receive TFE benefits.

TFE is an IP blocking list that is updated daily based on

- SilverSky SOC detections of malicious activity across our customer base
- Global threat intelligence feeds
- Technology vendor updates
- Law enforcement and cyber industry sources

Customers who activate our TFE receive rapid blocking of malicious activity – one change cascades to all devices subscribed to the TFE. This eliminates the need for our SOC to contact customers to participate in a response action for known threat activity. SilverSky SOC analysts can also create a customer-specific list that will be populated based off their device alerting, should customers want to tailor a response to certain devices. .

Our TFE current supports

- Fortigate
- Cisco FMC
- Palo Alto, Sonicwall (v6.5 and above)
- pfSense
- OPNSense

Additional firewall devices, which have API supported by the device manufacturer, will take a bit of time to test and develop documentation.

Activating the TFE on your firewall is a simple API configuration change. Your SilverSky team can provide the documentation on how to configure the API. To get started, we need a list of your firewall devices and along with a list of every public IP address that could potentially access the TFE (including all WAN IPs for failover scenarios or SDWAN). You can either upload the list to the Files repository on Lightning customer portal (outSOC) or email the information to us. If the latter, please send a firewall device inventory (manufacturer, model and operating system) along with the list of public IP addresses to Customer_Care@SilverSky.com with “TFE for <Tag ID customer name>” in the subject line.

Many of our customers can take these steps without working with our team. But we're here to help and can schedule a short call with your IT team to step through the API configuration for TFE at a time that works best for you

We are encouraging all our Lightning MDR clients to take advantage of this enhancement, so please contact us today.