Juniper Sky Advanced Threat Prevention

Product Overview

Sky Advanced Threat Prevention is a cloud-based service that provides complete advanced malware protection. Integrated with SRX Series Services Gateways and the Spotlight Secure threat intelligence platform, Sky Advanced Threat Prevention delivers a dynamic anti-malware solution that can adapt to an ever-changing threat landscape.

Your ideas. Connected.™

Product Description

As malware evolves and becomes more sophisticated, it grows more difficult for conventional anti-malware products to effectively defend against these types of attacks. Juniper Networks® Sky Advanced Threat Prevention delivers advanced anti-malware protection against sophisticated "zero-day" and unknown threats by monitoring ingress and egress network traffic looking for malware and other indicators of compromise. Using a pipeline of technologies in the cloud, Sky Advanced Threat Prevention delivers progressive verdicts that assess the risk level of each potential attack, providing a higher degree of accuracy in threat prevention. Hosted securely in the cloud, Sky Advanced Threat Prevention integrates with Juniper Networks SRX Series Services Gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Sky Advanced Threat Prevention's identification technology uses a range of techniques to quickly identify a threat and prevent an impending attack. These range from rapid cache lookups to identify known files to dynamic analysis using unique deception techniques applied in a sandbox environment to trick malware into activating and self-identifying. Machine learning algorithms allow Sky Advanced Threat Prevention to adapt and identify new malware in the ever-changing threat landscape.

Using evolving techniques that take into account multiple attributes and behaviors of large datasets, Sky Advanced Threat Prevention can also identify zero-day attacks and eliminate threats before an attacker infiltrates the network. Once identified, the malware's signature is recorded in the lookup cache to immediately stop similar attacks in the future.

Architecture and Key Components

Sky Advanced Threat Prevention leverages Juniper's newest SRX Series firewall platforms and a cloud-based service component for all management, configuration, and reporting.

Sky Advanced Threat Prevention's progressive pipeline analysis engine starts with a cache lookup against a database of known threats, which is accomplished in under two seconds. Suspicious files are subjected to a series of deeper inspection steps that attempt to positively identify malware. Static analysis combined with processing through multiple antivirus engines attempts to identify the threat; if a file is identified as malware through analysis, its signature is added to the cache to ensure immediate identification of recurring threats in the future.

Finally, dynamic analysis is applied in a sandbox environment, where the threat is "detonated" and observed. Unique deception techniques are employed to elicit malware response and self-identification. Threats that slip by during the more extensive analysis stage are identified, logged, reported, and can be easily mitigated by security operations staff. Infected hosts are automatically isolated and blocked from outbound network access.

Features and Benefits

Integrating with SRX Series firewalls for detection and enforcement allows Sky Advanced Threat Prevention to provide dynamic, automated protection against known malware and advanced zero-day threats, resulting in instant threat response.

Features and capabilities include:

- Extracting compromised files and sending them to the cloud for deep inspection and analysis. Using a pipeline of technologies to analyze the content, Sky Advanced Threat Prevention uses everything from fast methods that quickly identify known threats to advanced approaches that get deeper into the files, looking for more sophisticated and evasive malware.
- Quickly identifying malware (fast verdict) and instantly communicating that information to the SRX Series firewall to block the malicious traffic.
- Sending more sophisticated malware for deeper analysis to observe behavior during file execution in a controlled, dynamic environment—a sandboxing technique that uses dynamic analysis and "detonation."
- Managing the service, including product licensing, configuration, and detailed reporting through a web-based portal. A rich set of reports and analytics provides customers with improved visibility into what threats are entering their network and which hosts within the organization might be compromised.
- Tight coupling with the Spotlight Secure threat intelligence platform, allowing compromised host information to be cascaded to SRX Series gateways for immediate action as specified by the customer. Providing a list of Command and Control (C&C) servers to the SRX Series firewalls prevents compromised internal systems from communicating with these devices.
- Alerting via the SRX Series firewalls to warn the Sky Advanced Threat Prevention service when internal hosts are attempting to communicate with compromised servers, providing organizations with a wealth of data on various "indicators of compromise" within the organization.
- Analyzing and correlating data via analytics capabilities, which allow administrators and security personnel to identify compromised systems and feed this information to SRX Series gateways to quarantine compromised systems.

Product Options

Sky Advanced Threat Prevention is licensed as both a free version and a premium service. The free version of Sky Advanced Threat Prevention analyzes basic file types (.exe only) and provides the full complement of Sky Advanced Threat Prevention anti-malware techniques, including anti-virus analysis, static analysis, and dynamic analysis of suspect files with detailed reporting.

The premium service provides expanded file support (.exe, .pdf, and MS Office suite files including .doc, .ppt, .xls, etc.), along with detailed reporting and the entire Sky Advanced Threat Prevention anti-malware identification stack, including static and dynamic analysis. Enhanced, detailed reporting makes it easy for security operations personnel to mitigate any infected hosts identified by Sky Advanced Threat Prevention's advanced identification techniques. The premium version also quarantines infected hosts and blocks communication with C&C servers.

Specifications

Sky Advanced Threat Prevention requires an SRX Series firewall running the latest version of Juniper Networks Junos® operating system (15.1). Support is included for the Juniper Networks SRX1500 Services Gateway platform at release and is planned for vSRX and all other SRX Series platforms in a future release.

.Ordering Information

Please contact your sales associate for further information on ordering Sky Advanced Threat Prevention.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1000549-001-EN Sep 2015