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, Sky Advanced Threat Prevention delivers a dynamic anti-malware solution that can adapt to an ever-changing threat landscape.

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. Patented 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 and widely propagated to stop similar attacks in the future.

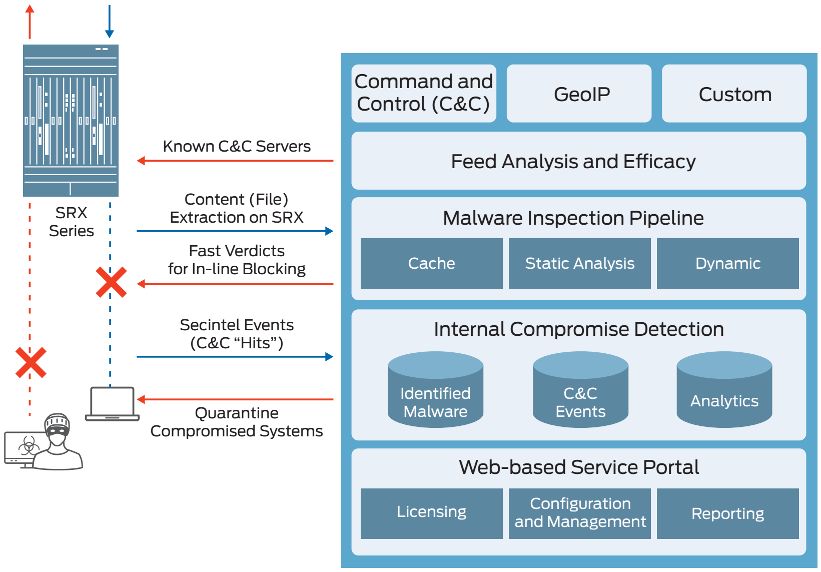

Figure 1: Juniper's Sky Advanced Threat Prevention solution.

Architecture and Key Components

Sky Advanced Threat Prevention leverages Juniper's next-generation 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. This is accomplished in near real time and facilitates inline blocking of malicious content. 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 by delivering an "infected host" feed to the SRX Series device.

Sky Advanced Threat Prevention utilizes public cloud infrastructure to deliver a flexible and scalable solution. All communications between the SRX Series device and the cloud are secure, conducted over encrypted connections on both sides. Files uploaded to the cloud for processing are destroyed afterward to ensure privacy.

Features and Benefits

Integrating with next-generation 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 nearly instantaneous threat responses.

Features and capabilities include:

- Windows 7, Windows 10, and Android operating system support
- Deep analysis and sandboxing support for multiple file types including executables, PDFs, MS Office files, archives, and Flash
- Support for HTTP and HTTPs protocols
- Comprehensive logging and integration with Juniper Secure Analytics (JSA) and IBM QRadar SIEMs allows rapid threat analysis and incident response
- Integration with Junos Space Security Director Version 16.1 simplifies security policy management and monitoring using an intuitive centralized interface
- Fast verdict capability that enables the SRX Series firewall to block malicious traffic in inline blocking mode
- Scalable secure cloud infrastructure that, when a threat is discovered, shares updates globally among customers in near real time to block additional attacks
- Patented pipeline of technologies to analyze sophisticated malware, "detonate" files in a controlled sandboxing environment, and identify zero day threats
- Comprehensive API support to programmatically deliver dynamic threat intelligence feeds and upload files for analysis
- Rich set of curated threat feeds, provided by the Spotlight Secure threat intelligence platform, to proactively block outbound command and control (C&C) communication
- Full-featured, web-based portal to provision, monitor, and manage services, as well as a rich set of reports and analytics to provide customers with deep visibility into threats and potentially compromised hosts
- Ability to upload suspicious files through the Web UI for processing
- Deep analytics that identify compromised systems; this information is propagated to SRX Series firewalls via infected host feeds to quarantine compromised systems in near-real time

Product Options

Sky Advanced Threat Prevention is available in both free and premium versions; Table 1 below shows the key differences between the two. Both versions support inline blocking and provide the full Sky Advanced Threat Prevention anti-malware identification stack with detailed reporting.

Table 1: Sky Advanced Threat Prevention versions

	Free	Premium
Licensing	Available to all SRX Series customers with a valid software support contract; no additional license purchase required.	Requires purchase of a subscription license
File types	Executables	Executables, PDF, MS Office, archives, java, active media, dlls, mobile applications, audio/video, source code*
Feeds	Infected host	Infected host, C&C, GeoIP

* A complete list of supported file types can be found in the Sky Advanced Threat Prevention administrator's guide.

SRX Series Platform Support

Sky Advanced Threat Prevention supports a variety of platforms. Table 2 summarizes the platforms supported and the minimum required Junos release.

Table 2: Sky Advanced Threat Prevention supported platforms

Platform	Supported Junos Release
SRX340, SRX345	15.1X49-D60 or later
SRX550M	15.1X49-D60 or later
SRX1500	15.1X49-D40 or later
SRX4000 line	15.1X49-D65 or later
SRX5000 line	15.1X49-D50 or later
vSRX	15.1X49-D60 or later

Please contact your Juniper sales representative for additional information.

Ordering Information

Product Number	Description
SRX340-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX340
SRX340-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX340
SRX340-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX340
SRX345-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX345
SRX345-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX345
SRX345-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX345
SRX550-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX550M
SRX550-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX550M
SRX550-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX550M
SRX1500-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX1500
SRX1500-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX1500
SRX1500-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX1500
SRX4100-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX4100
SRX4100-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX4100
SRX4100-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX4100
SRX4200-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX4200
SRX4200-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX4200
SRX4200-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX4200
SRX5400-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX5400
SRX5400-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX5400
SRX5400-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX5400
SRX5600-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX5600
SRX5600-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX5600
SRX5600-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX5600
SRX5800-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on SRX5800
SRX5800-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on SRX5800
SRX5800-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on SRX5800
VSRX-10M-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-10M-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-10M-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on 10Mbps vSRX
VSRX-100M-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on 100Mbps vSRX
VSRX-100M-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on 100Mbps vSRX
VSRX-100M-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on 100Mbps vSRX
VSRX-1G-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-1G-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-1G-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on 1Gbps vSRX
VSRX-2G-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-2G-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-2G-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on 2Gbps vSRX
VSRX-4G-ATP-1	One Year Subscription for Sky Advanced Threat Prevention on 4Gbps vSRX
VSRX-4G-ATP-3	Three Year Subscription for Sky Advanced Threat Prevention on 4Gbps vSRX
VSRX-4G-ATP-5	Five Year Subscription for Sky Advanced Threat Prevention on 4Gbps vSRX

Note:

Sky Advanced Threat Prevention requires the AppSecure functionality to be available. In addition to the standalone Sky Advanced Threat Prevention license, individual SRX Series platforms might require additional licenses as described below.

- On the SRX550M, SRX5000, and vSRX platforms, the AppSecure license is available for purchase a la carte or through a bundle SKU that includes the license.
- The SRX340 and SRX345 are available with a JSE bundle that includes AppSecure. AppSecure can also be purchased a la carte if JSE is not purchased.
- On the SRX4000 platforms, the JSE software bundle includes a license for AppSecure
- The SRX1500 requires a mandatory purchase of the JSE bundle, which includes the AppSecure license. Consequently, the standalone Sky ATP license will suffice.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

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