JUNIPER ADVANCED THREAT PREVENTION CLOUD

Product Overview

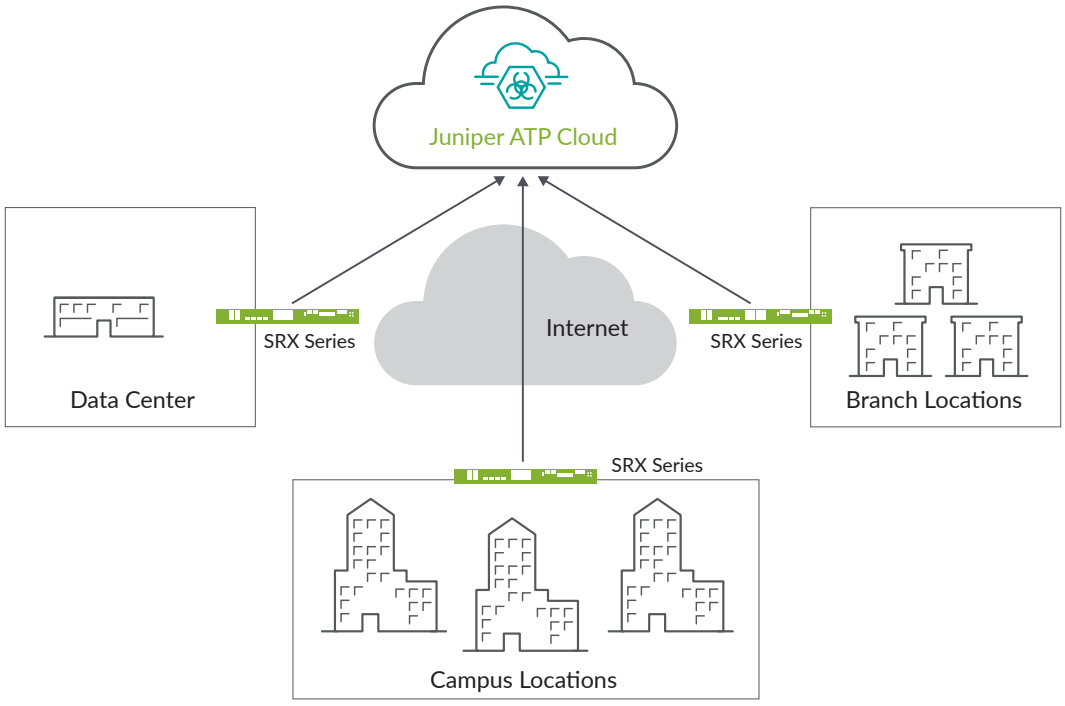
Juniper Networks® Advanced Threat Prevention is a cloud-based service that provides complete advanced malware protection, detection, and prevention. When integrated with Juniper Networks SRX Series Services Gateways, Juniper ATP Cloud delivers threat intelligence and malware analysis capabilities leveraging static, dynamic, and machine learning identification to safeguard your users, applications, and infrastructure.

Juniper ATP Cloud helps customers:

- Identify and defend against new zero-day malware and targeted attacks
- Mitigate risks by updating existing security controls to defend against identified and unknown threats
- Reduce the time and cost to resolve advanced threats
- Reduce exposure to advanced threats

Key Advantages of Juniper ATP Cloud

- Delivers a cloud-based and scalable solution
- Offers zero-day threat protection
- Integrates with SRX Series next-generation firewalls
- Supports inline blocking and blocking of files with unknown verdict
- Offers unique deception and provocation techniques
- Detects IoT malware with support for executable and linkable format (ELF) file types
- Provides network behavioral analysis and machine learning to determine if an SSL/TLS connection is benign or malicious without the heavy burden of full decryption with Encrypted Traffic Insights Analysis
- Quickly identifies unknown threats at the network level using static and dynamic analysis and machine learning
- Automatically blocks C2 communications with SecIntel
- Includes its own management portal for configuration management, licensing, and reporting



Juniper ATP Cloud solution

Juniper ATP Cloud Identification Technology

Juniper ATP Cloud leverages Juniper's next-generation SRX Series firewalls for traffic routing and visibility while offering cloud management of threats, configuration, and reporting.

The Juniper ATP Cloud identifies web-based or e-mail borne threats. Using the SSL decryption capabilities of the SRX Series firewalls, any malware transmitted in encrypted sessions can be easily identified. Support for SMTP and IMAP email protocols allow Juniper ATP Cloud to examine emails for malicious attachments and quarantine emails that might pose a threat to the end user.

Juniper ATP Cloud Features and Benefits:

Capabilities	Features and Benefits
Malware Analysis	Malware analysis consists of both static and dynamic analysis of files downloaded from the Web or distributed over e-mail in order to identify malicious content and detect whether the file tries to contact a Command and Control (C&C) server to install a malicious payload. If no threat is detected, the file will be downloaded or delivered to the recipient. If malware or grayware is detected, the SRX Series firewall can block the download or prevent the e-mail from being delivered. Juniper ATP can analyze files and executables for Windows Versions 7 and 10, Mac, Linux, and Android. Customers who create their own custom corporate Windows images can upload those images to the JATP Appliance.
Encrypted Traffic Insights	Encrypted Traffic Insights restores visibility lost due to encrypted traffic, without the heavy burden of full TLS/SSL decryption. SRX Series firewalls collect the relevant SSL/TLS connection data, including certificates used, cipher suites negotiated, and connection behavior. This information is processed by Juniper ATP Cloud, which uses network behavioral analysis and machine learning to determine whether the connection is benign or malicious. For encrypted traffic identified as malicious, policies configured on the SRX Series firewall can be used to block those threats.
SecIntel	SecIntel provides curated security intelligence in the form of threat feeds that include malicious domains, URLs, and IP addresses used in known attack campaigns. SecIntel also enables customers to feed and distribute their own threat intelligence for in-line blocking. This information is provided to an SRX Series firewall and, in some cases, Juniper Networks MX Series Universal Routing Platforms and Juniper Networks EX Series and QFX Series switches to identify and block known threats.
Adaptive Threat Profiling	To better combat the continuous onslaught of new threats, organizations can use ATP Cloud's Adaptive Threat Profiling to automatically create security intelligence threat feeds based on who and what is currently attacking the network. Adaptive Threat Profiling leverages Juniper Security Services to classify endpoint behavior and build custom threat intelligence feeds that can then be used for further inspection or blocking at multiple enforcement points, giving organizations the power to respond to attacks in real time.
Attack Analytics	The analytics view provides a window into what is happening, letting security operations employees see correlated threat activity occurring inside their network to quickly identify high-priority threats, understand how to respond, and/or potentially quarantine to remediate the outbreak.
Prevention and Mitigation	Malicious outbreaks can be blocked inline with a physical or virtual SRX Series firewall or detected and logged via a network tap with third-party firewalls. To prevent the lateral spread of threats, Juniper ATP integrates with existing network access control (NAC) solutions to quarantine an infected host or drop it from the network until the infection can be remediated to prevent the lateral spread of threats. Additionally, Juniper ATP's SecIntel threat feeds can also integrate with MX Series routers and EX Series and QFX Series switches.
Automation	To help security operations personnel reduce the manual load of host or endpoint identification, Juniper ATP can triangulate IP addresses with media access control (MAC) addresses to identify the infected machine or host. To automate prevention capabilities, Juniper ATP can integrate with third-party firewalls, switches, and wireless technology to block users or quarantine hosts until the threat can be neutralized. This feature applies to SRX Series firewalls, MX Series routers, and EX Series and QFX Series switches. Automation simplifies deployment by allowing organizations to set and define policies across a group of disparate systems rather than setting individual policies on each device.

Next Steps

A free version of Juniper ATP Cloud is available for existing customers of supported SRX Series devices with a valid software support contract. The free download supports executable processing only. For customers who do not currently have an SRX Series device, a free trial of the vSRX Virtual Firewall that supports Juniper ATP Cloud is available. To download the free trial version of the vSRX, visit www.juniper.net/us/en/dm/free-vsrx-trial/.

For more information on Juniper ATP Cloud, visit www.juniper.net/us/en/products-services/security/advanced-threat-prevention/.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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: +31.207.125.700
Fax: +31.207.125.701

Juniper Networks | Driven by Experience™

9040110-006-EN Jan 2022