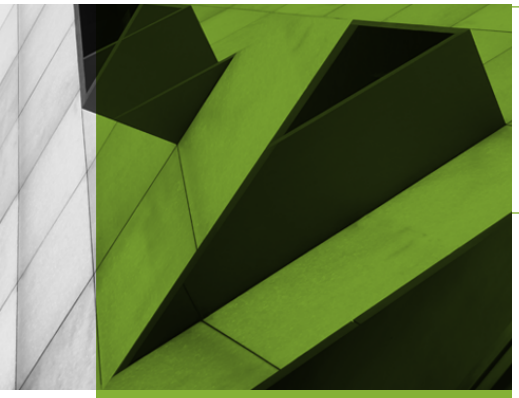

JUNIPER ADVANCED THREAT PREVENTION

Product Overview

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

Product Description

Customers looking to identify and block known and unknown threats can add Juniper Networks® Advanced Threat Prevention (ATP) to their Juniper Networks SRX Series Services Gateways. Juniper ATP uses machine learning to find and block both known and unknown cyberthreats, analyzing files and network traffic looking for signs of malicious behavior. ATP can uncover zero-day malware threats and malicious connections, including botnets and C&C servers hiding in encrypted traffic. Using SecIntel, Juniper's curated security intelligence feeds, ATP stops these threats in their tracks by enforcing protection mechanisms at all network connection points.

Advanced Threat Prevention Cloud

Deployed as an add-on license to an SRX Series Services Gateway, ATP Cloud uses a combination of static and dynamic analysis and machine learning to quickly identify unknown threats, either downloaded from the web or sent via e-mail, and delivers a file verdict and risk score back to the SRX Series firewall to enable blocking at the network level. In addition, ATP Cloud delivers SecIntel security intelligence consisting of malicious domains, URLs, and IP addresses gathered from file analysis, Juniper Threat Labs research, and highly reputable third-party threat feeds. These feeds are collected and distributed to SRX Series firewalls and Juniper Networks MX Series Universal Routing Platforms to automatically block command-and-control communications, making it more difficult to wage a successful attack on the organization. ATP Cloud includes its own management portal configuration management, licensing, and reporting.

Advanced Threat Prevention Appliance

To address the needs for on-premises and virtual deployments, the ATP offering is also available on two hardware-based platforms: the Juniper Networks JATP400 and JATP700 Advanced Threat Prevention Appliances.

- **JATP400**: The JATP400 is a 1 U appliance that delivers up to 50,000 object detonations per day. It's purpose-built for organizations that need distributed detection of Web, e-mail, and lateral threats across the enterprise.
- **JATP700**: The JATP700 is a 2 U appliance for larger, centralized environments with high-performance security demands requiring up to 130,000 object detonations per day.

Virtual versions of Juniper ATP, running on either VMware vSphere or ESXi, can be deployed with 8 or 24 virtual CPU cores, enabling it to process up to 116,000 object detonations per day.

Juniper ATP Appliances collect web, e-mail, and lateral traffic using either SRX Series firewalls or their own built-in collectors, making it an ideal fit for organizations employing multiple firewall solutions. Collected data is sent to an on-premises Juniper ATP Appliance for further processing by the ATP Appliance core, which identifies known and unknown threats and provides comprehensive analytics detailing the progression of the threat within the environment by mapping detections to the attack kill chain.

Once a threat is detected, the Juniper ATP Appliance sends firewall policy updates to the SRX Series firewall. The Juniper ATP Appliance can also be configured to update policies on third-party firewalls from vendors such as Palo Alto Networks, Fortinet, and Cisco.

The Juniper ATP solution also works with Juniper or third-party switches to quarantine threats, leveraging one-touch mitigation to isolate compromised hosts and limit the lateral spread of the infection. Juniper ATP builds a list of infected hosts based on its detections and works with Juniper Networks Policy Enforcer to integrate with Juniper Networks EX Series and QFX Series switches, or NAC vendors such as ForeScout, to block or quarantine compromised hosts on the network.

Architecture and Key Components

Advanced Threat Prevention Cloud

Juniper ATP leverages Juniper's next-generation SRX Series firewalls for traffic routing and visibility while offering cloud management of threat, 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 also be easily identified. Support for SMTP and IMAP e-mail protocols allows Juniper ATP Cloud to examine e-mails for malicious attachments and quarantine e-mails that might pose a threat to the end user.

Juniper ATP Cloud utilizes public cloud infrastructure to deliver flexible and scalable file analysis and threat identification. All communications between the SRX Series firewall 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. A detailed description of the Juniper ATP Cloud privacy policy, as well as the broader Juniper Networks privacy policy, can be found on the product Web portal at www.juniper.net/us/en/privacy-policy/.

Juniper ATP Cloud is available globally, with the service delivered from data centers in North America (U.S. and Canada), EMEA, and APAC. This allows customers in these regions to benefit from the cloud-based threat prevention and intelligence services while addressing customers' data localization and data privacy concerns. Data submitted in a particular region will be processed in that region and will not leave its geographic boundaries. Customers have greater control over the location of the data, helping them comply with regulatory and privacy requirements.

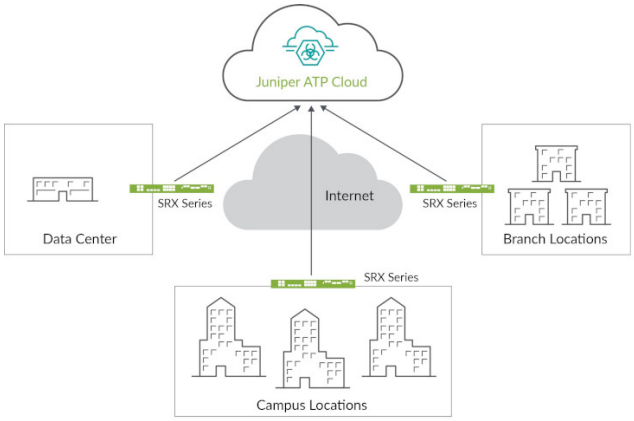

Figure 1: Juniper Advanced Threat Prevention Cloud architecture

Juniper Advanced Threat Prevention Features and Benefits

Feature	Feature Description
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.
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 to 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 that was 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.
Attack Analytics	The analytics view provides a window into what is happening, letting security operations employees see correlated threat activity occurring inside their network in order 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. 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 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.
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.

Advanced Threat Prevention Appliance

The on-premises Juniper ATP Appliance can use the SRX Series firewalls as collectors for inline detection and blocking, or it can use its own built-in collector for use with third-party firewalls. For MSSP environments, the ATP Appliance can be deployed as a separate collector and core supporting multi-tenancy, where a collector is deployed at each customer location and all traffic is analyzed by a core or cluster of cores.

Files and related executables collected across the network are delivered to the SmartCore detection and analytics engine on a JATP400 or JATP700 appliance for further analysis. Threats detected by the SmartCore engine can be blocked by SRX Series Firewalls. To provide comprehensive attack analytics, the Juniper ATP Appliance also ingests detection logs from other identity and security products such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. Logs can be ingested directly from third-party devices, or they can be forwarded from existing security information and event management (SIEM)/system logging servers.

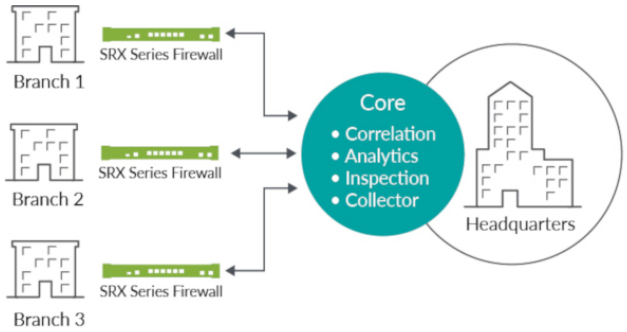

Figure 2: Juniper Advanced Threat Prevention on-premises architecture

Ordering Information

Juniper Advanced Threat Prevention

License Options	MX Series Routers	EX/QFX Series Switches	SRX Series Firewalls	Juniper ATP Cloud	Juniper ATP Appliance
Deployment of ATP and SecIntel features	Cloud	Cloud	Cloud	Cloud	On-premises (requires JATP400, JATP700, or ATP Virtual Appliance)
SecIntel feeds	Yes—MX240, MX480, MX960 (C&C, custom whitelist, and blocklist only)	Yes-infected host feed only	Yes	Yes	Yes
Dynamic Analysis	No	No	No	Yes	Yes
Adaptive Threat Profiling	No	No	Yes	Yes	No
Encrypted Traffic Insights[1]	No	No	No	Yes	No
Firewalls/collectors	N/A	N/A	SRX Series firewalls	SRX Series firewalls	SRX Series firewalls or JATP400, JATP700, or ATP Virtual Appliance
Threat analytics	No	No	No	Yes	Yes[2]
Third-party threat detection log ingestion	No	No	No	No	Yes[2]
Requires Policy Enforcer	Yes	Yes	No	No	No
License type	S-MX(Model)-CSECINTEL	S-(EX or QFX)-CSECINTEL	Premium 1, 2, or 3	Requires SRX Premium 1, 2, or 3	Standard 1 or 2; Advanced 1 or 2
License duration	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year

[1] Encrypted Traffic Insights requires Junos OS 20.2 and later

[2]. These options are only available when an Advanced-1 or Advanced-2 license is purchased for the ATP Appliance

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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

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

Juniper Networks | Engineering Simplicity