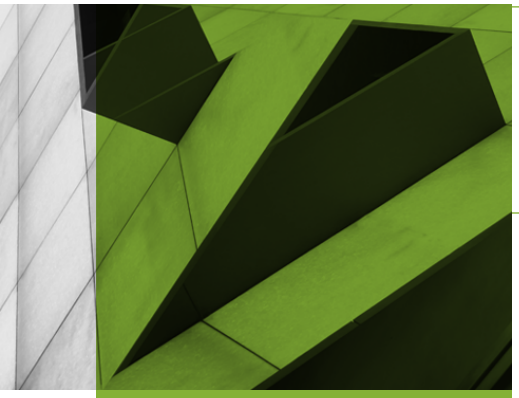

JUNIPER ADVANCED THREAT PREVENTION DATASHEET

Product Overview

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

Product Description

Customers looking to identify and block known and zero-day threats can add Juniper Networks® Advanced Threat Prevention (ATP) to their Juniper Networks SRX Series Firewalls. Juniper ATP uses machine learning to find and block known and zero-day cybersecurity threats by analyzing files and network traffic and 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 threats in their tracks by enforcing protection mechanisms at all network connection points.

Advanced Threat Prevention Cloud

ATP Cloud can be deployed as an add-on license to an SRX Series Firewall. It uses a combination of static and dynamic analysis and machine learning to quickly identify zero-day threats trying to infiltrate the network. ATP Cloud delivers a file verdict and risk score back to the SRX Series firewall to enable blocking at the network level.

In addition, ATP Cloud provides SecIntel security intelligence feeds 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 attack the organization successfully.

ATP Cloud also gives you crucial insights into DNS traffic on your network. ATP Cloud provides information to mitigate against attacks that leverage DNS for command and control or to deliver and exfiltrate data. ATP Cloud protects DNS-generating algorithms (DGA) and DNS tunneling threats. ATP Cloud can identify and classify IoT devices on the network to address security concerns due to the proliferation of IoT. With this information, ATP Cloud allows security operations teams to manage feeds for policy enforcement throughout the network and reduce the risk large IoT attack surfaces represent.

ATP Cloud includes its own management portal configuration management, licensing, and reporting.

Advanced Threat Prevention Appliance

The ATP appliance offering addresses on-premises deployments and is available as a virtualized version of Juniper ATP. It runs on either VMware vSphere or ESXi and 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 SRX Series firewalls or their 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 firewall vendors.

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. It works with Juniper Networks Policy Enforcer to integrate with Juniper Networks EX Series and QFX Series switches or NAC vendors 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 is 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's AI-Predictive Threat Prevention provides anti-malware capabilities at wire speed, ensuring that you don't have to compromise your throughput performance for better security, all while eliminating patient zero. Signatures generated by AI-Predictive Threat Prevention remain active for the entire attack lifecycle, instead of a mere 24 hours after discovering the malware like other technologies, and the active signatures provide effective protection against subsequent attacks.

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 is secure and 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 and the broader Juniper Networks privacy policy can be found on the product Web portal at https://www.juniper.net/us/en/privacy-policy.html.

Juniper ATP Cloud is available globally, with the service delivered from data centers in North America (U.S. and Canada), EMEA, and APAC. This widespread availability allows customers in these regions to benefit from cloud-based threat prevention and intelligence services while addressing customers' data localization and 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.

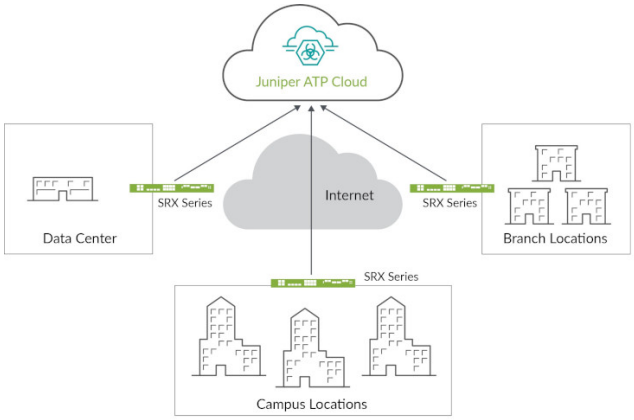

Figure 1: Juniper Advanced Threat Prevention Cloud architecture

Features and Benefits

Feature	Feature Description
Malware Analysis	Malware analysis consists of static and dynamic analysis of files downloaded from the Web or distributed over e-mail to identify malicious content and detect whether the file tries to contact a Command and Control (C&C) server to install a malicious payload. The file will be downloaded or delivered to the recipient if no threat is detected. 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 custom corporate Windows images can be uploaded 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	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 to combat the continuous onslaught of new threats. Adaptive Threat Profiling leverages Juniper Security Services to classify endpoint behavior and build custom threat intelligence feeds that can be used for further inspection or blocking at multiple enforcement points, giving organizations the power to respond to attacks in real time.
AI-Predictive Threat Prevention	AI-Predictive Threat Prevention predicts and prevents known and zero-day malware on the wire by using AI on packet snippets and reduces false positives by filtering out non-threatening activities, reducing the "noise." It helps human experts focus on more critical security tasks and discover the real, dangerous threats at line rate for the entire attack lifecycle–not merely 24 hours, like other technologies–keeping the network safe from initial and all subsequent attacks. Juniper understands that when there is an attack, every second counts.
Attack Analytics	The analytics view provides a window into what is happening. It lets security operations employees see correlated threat activity inside their network to identify high-priority threats quickly, understand how to respond, and/or potentially quarantine to remediate the outbreak.
DNS Security	Juniper Networks provides customers with advanced threat prevention for the growing number of attacks that leverage DNS. It can protect against DNS exploits for C&C communications, data exfiltration, phishing attacks, and ransomware that commonly exploit DNS using various techniques. ATP provides threat prevention from attacks that utilize DGA and DNS tunneling techniques.
IoT Threat Prevention	ATP Cloud allows customers to control the IoT attack surface on their network by providing an easy way to identify and categorize IoT devices. Security devices provide ATP Cloud IoT device information that includes traffic flow and metadata that can be used to create threat feeds to enforce security policies across IoT traffic in the network.
URL Filtering	URL Filtering prevents web-borne threats and unwanted browsing activity from taking place on a device. It provides web traffic categorizations that can be incorporated into the application. Juniper's URL Filtering supports over 200 languages and categories, making it easy to recategorize as needed, and eliminating frustration due to outdated or limited categories.
Prevention and Mitigation	Block malicious outbreaks in line with a physical or virtual SRX Series firewall or detect and log 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 is remediated to prevent the lateral spread of threats. Juniper's SecIntel threat feeds deliver regularly updated, actionable intelligence to SRX Series firewalls, MX Series routers and enforcement on Juniper wireless access points, 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 disparate systems rather than selecting individual policies on each device.

Advanced Threat Prevention Appliance

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

Files and related executables collected across the network are delivered to the SmartCore detection and analytics engine on an ATP virtualized appliance for further analysis. The Juniper ATP Appliance can run in private mode for air-gapped environments, providing malware detection, mitigation, and even correlation when Internet access is unavailable.

SRX Series firewalls can block threats detected by the SmartCore engine. To provide comprehensive attack analytics, the Juniper ATP Appliance ingests detection logs from other identity and security products such as Active Directory, endpoint antivirus, firewalls, Secure Web Gateways (SWGs), intrusion detection systems, and endpoint detection and response tools. Logs are ingested directly from third-party devices or forwarded from existing security information and event management (SIEM)/system logging servers.

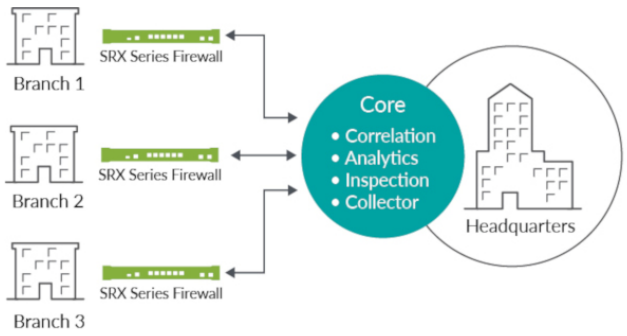

Figure 2: Juniper Advanced Threat Prevention on-premises architecture

Security Director Cloud

Security Director Cloud is Juniper's simple and seamless management experience delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, data, and infrastructure.

Organizations can secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and expand zero trust to all parts of the network from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Using Juniper Security Director Cloud, organizations can create policies once and apply them everywhere. Unified policy management ensures seamless security across all users, data, or devices wherever they are. Juniper meets our customers where they are on their journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

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	N/A	Cloud	Cloud	On-premises ATP Virtual Appliance
SecIntel feeds	Yes—MX240, MX480, MX960 (C&C, custom allowlist and blocklist only)	No. Enforcement point based on infected host feed	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 JATP 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	N/A	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	N/A	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

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

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