ADVANCED THREAT PREVENTION APPLIANCE

Product Overview

Advanced Threat Prevention Appliances are physical or virtual on-premises devices that combine advanced threat detection with consolidated security analytics to protect organizations from known and unknown cyberattacks while improving the productivity of security operations teams. Working with Juniper Networks SRX Series Services Gateways, ATP Appliances detect threats in Web, e-mail, and lateral traffic, blocking those threats if the firewall is deployed inline. ATP Appliances can also ingest logs from existing security devices and apply contextual analysis to provide a consolidated view of the threat landscape.

Product Description

Juniper Networks® Advanced Threat Prevention Appliances address the need for both on-premises physical and virtual threat detection and mitigation solutions.

Two hardware platforms are available—the JATP400 Advanced Threat Prevention Appliance and JATP700 Advanced Threat Prevention Appliance—which scale to support up to 130,000 processed files per day. The virtual version of the ATP Appliances, running on either VMware vSphere or ESXi, can be deployed with either 8 or 24 virtual CPU cores to process up to 116,000 files per day.

Juniper ATP Appliances collect web, e-mail, and lateral traffic using either the Juniper Networks SRX Series Services Gateways or its own built-in collector, making it an ideal fit for organizations employing multiple firewall solutions. Collected data is sent to an on-premises ATP Appliance for further processing by the ATP Appliance core, which identifies known and unknown threats and provides comprehensive analytics detailing the threat's progression within the environment by mapping detections to the attack kill chain. Once a threat is detected, the ATP Appliance sends firewall policy updates to the SRX Series firewalls. The ATP Appliance can also be configured to update policies on third-party firewalls from vendors such as Palo Alto Networks, Fortinet, and Cisco. Working with Juniper Networks EX Series Ethernet Switches, Juniper Networks QFX Series switches, or other third-party switches, JATP Appliances can also isolate threats and leverage one-touch mitigation to quarantine compromised hosts, limiting lateral spread.

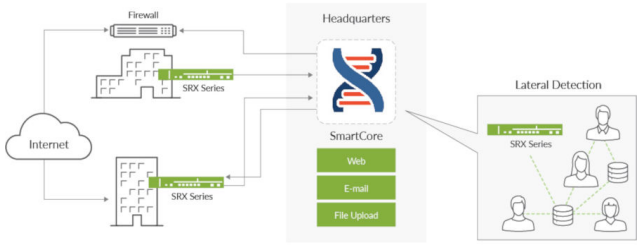

Figure 1: Juniper Networks ATP Appliance architecture

Architecture and Key Components

The on-premises ATP solution can use SRX Series firewalls as collectors for inline detection and blocking. JATP Appliances can also use their built-in collectors 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. For air-gapped environments, the Juniper ATP Appliance can run in private mode, which provides malware detection, mitigation, and even correlation when Internet access is not available.

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. The SRX Series firewalls can block threats detected by the SmartCore engine.

ATP Appliances can also ingest logs from other identity and security solutions such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. The logs can be ingested either directly from third-party devices, or they can be forwarded by existing security information and event management (SIEM)/syslog servers.

Table 1. Juniper Networks Advanced Threat Prevention Appliances Features and Benefits

Feature	Description	Benefits
Traffic Inspection	Protects multiple vectors, including Web, e-mail, and lateral spread	Provides a broad range of protocol support to cover the most common methods for malware and ransomware distribution
Inline Threat Mitigation	Offers inline blocking when an SRX Series firewall is deployed	Offers the ability to block known and unknown threats
Attack Analytics	Provides a real-time and historical view of the threat landscape across the network, including from third-party security solutions	Gives security operations employees visibility into correlated threat activity occurring inside their network, allowing them to quickly identify high-priority threats, understand how to respond, and/or quarantine to remediate the outbreak
Third-Party Interoperability	Includes comprehensive APIs and a custom log ingestion framework that easily integrate with third-party security devices, enabling threat log collection and aggregation from any security products already deployed	Ensures easy integration with third-party security devices using APIs and supports threat log collection and aggregation from any existing security products
Centralized Management	Includes Manager of Central Managers (MCM) functionality	Provides comprehensive, centralized, single-pane-of-glass management of clustered core appliances in large deployments requiring multiple cores
Flexible Deployment	Supports both physical and virtual on-premises deployments	Provides high-performance dedicated hardware for threat processing and analytics
Distributed Architecture	Leverages collectors that can be deployed at any number of network locations, all feeding into an analytics engine residing at headquarters or in the cloud	Increases threat coverage across your networks, including public and private clouds
Clustering	Allows clustering of multiple secondary cores via scalable architecture	Enables a quick increase in threat process capacity if more than a single appliance is required
Authentication	Supports access and authentication using SAML and RADIUS	Works with existing authentication solutions

Product Options

ATP Appliances are available in both physical and virtual form factors. The physical appliances—the 1 U JATP400 and the 2 U JATP700—can be deployed in all-in-one mode (SmartCore and Fabric Collector installed on the same physical appliance) or in distributed mode (SmartCore and Fabric Collector installed on separate appliances). Virtual appliances can be deployed in distributed mode.

Malware detection for MacOS is also supported. Customers are required to provide Mac mini hardware that can be deployed as a secondary core. The MacOS sandboxing image is available on the ATP Appliances' software downloads page.

Table 2. Hardware Appliance Performance

Product Name	Collector Performance	E-Mail MTA Receiver	Performance (Objects Detonations)[1]	Logging Performance
JATP400	1.5 Gbps	700,000	Up to 50,000 objects/day	1,500 events/second
JATP700	4 Gbps	2 million	Up to 130,000 objects/day	1,500 events/second

Table 3. Virtual Appliance Performance

Product Name	Virtual Memory/Disk	Collector Performance	E-Mail MTA Receiver	Performance (Objects Detonations)[1]
Virtual JATP Appliances solution (8-core CPU)	32 GB/1.5 TB	1.5 Gbps	720,000	Up to 46,000 objects/day
Virtual JATP Appliances solution (24-core CPU)	96 GB/1.5 TB	4 Gbps	2.4 million	Up to 116,000 objects/day

[1]Numbers based on a traffic mix that approximates real-world performance. Actual numbers may be different based on traffic mix, repeat objects, and other factors unique to user environments.

Table 4. Virtual Appliance Hardware Specifications

Product Name	Hypervisor Support	Versions
Virtual JATP Appliances	VMware vSphere, ESXi	vSphere (5.5, 6.0, 6.5), ESXi (5.5.1, 5.5)

JATP700

JATP400

Specifications

Specification	JATP400	JATP700
Weight	30.4 lbs (13.79kg)	42 lbs (19 kg)
Dimensions (WxHxD)	17.2 x 1.7 x 25.6 in (43.7 x 4.3 x 65 cm)	17.2 x 3.5 x 24.8 in (43.7 x 8.9 x 63 cm)
Form Factor	1 U (rack mountable)	2 U (rack mountable)
AC Power Supply	500 W high efficiency (94%+) AC-DC redundant power; AC input: -100 to -240 V, 50-60 Hz, 11-4.4 amp	920 W high efficiency (94%+) AC-DC redundant power; AC input: -100 to -240 V, 50-60 Hz, 11-4.4 amp
DC Power Supply	650 W high-efficiency redundant DC-to-DC power supply; DC input: 650 W; -44 to -74 VDC, 20 amp	850 W/1010 W high-efficiency redundant DC-to-DC power supply; DC input: 850 W; -35 to -42 VDC, 30-25 amp
Fans	1.6 x 1.6 x 2.2 in (4 x 4 x 5.6 cm) 13K-11K RPM counter rotating fan, RoHS/ REACH	1.6 x 1.6 x 2.2 in (4 x 4 x 5.6 cm) 13K-11K RPM counter rotating fan, RoHS/ REACH
Operating Temperature	50° to 104° F (10° to 40° C)	50° to 104° F (10° to 40° C)
Storage Temperature	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)
Relative Humidity (Operating)	8 to 90 percent noncondensing	8 to 90 percent noncondensing
Relative Humidity (Storage)	5 to 95 percent noncondensing	5 to 95 percent noncondensing
Altitude (Operating)	6500 ft max	6500 ft max
Altitude (Storage)	35,000 ft max	35,000 ft max
Safety Certifications	CAN/CSA-C22.2 No. 60950-1 Safety of Information Technology Equipment EN 60950-1 UL 60950-1 (2nd Edition) IEC 60950-1: 2005/A2:2013	CAN/CSA-C22.2 No. 60950-1 Safety of Information Technology Equipment EN 60950-1 UL 60950-1 (2nd Edition) IEC 60950-1: 2005/A2:2013
Emissions Certifications	47CFR Part 15, (FCC) Class A ICES-003 Class A EN 55022 Class A CISPR 22 Class A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 Class A CNS13438 Class A EN 61000-3-3 VCCI Class A KN22 Class A EN 61000-3-2 BSMI CNS 13438	47CFR Part 15, (FCC) Class A ICES-003 Class A EN 55022 Class A CISPR 22 Class A EN 55024 CISPR 24 EN 300 386 AS/NZA CISPR22 Class A CNS13438 Class A EN 61000-3-3 VCCI Class A KN22 Class A EN 61000-3-2 BSMI CNS 13438
NEBS	No	No
RoHS	Yes	Yes
CPU	10 cores	2x10 cores
Memory	32 GB	128 GB
Storage	8 TB (4 x 2 TB), RAID 6	8x900 GB 2.5 in 10K SAS, RAID 6
Traffic Ports	2xSFP+ 10GbE; 4xRJ-45 GbE	2xSFP+ 10GbE; 4xRJ-45 GbE

Ordering Information

Juniper Networks Advanced Threat Prevention Appliances support flexible deployment options. Required components vary based on the deployment model.

- **Physical deployments** require a physical ATP Appliance solution and an associated software subscription.
- **Virtual deployments** require a software subscription only.

Hardware

Product Number	Description
JATP700-AC-CORE	JATP700 appliance, AC power, core software installed
JATP700-AC-COL	JATP700 appliance, AC power, collector software installed
JATP700-AC-ALL	JATP700 appliance, AC power, all-in-one software installed
JATP700-DC-CORE	JATP700 appliance, DC power, core software installed
JATP700-DC-COL	JATP700 appliance, DC power, collector software installed
JATP700-DC-ALL	JATP700 appliance, DC power, all-in-one software installed
JATP400-AC	JATP400 appliance, AC power, single image installed (can be configured as all-in-one, core, or collector)
JATP400-DC	JATP400 appliance, DC power, single image installed (can be configured as all-in-one, core, or collector)

For information about the virtual ATP Appliance, software licensing, or answers to general ordering questions, please visit our How to Buy page at www.juniper.net/us/en/how-to-buy.

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