ADVANCED THREAT PREVENTION APPLIANCE

Product Overview

Juniper Networks Advanced Threat Prevention Appliance is a distributed software platform that combines advanced threat detection, consolidated security analytics, and one-touch threat mitigation to protect organizations from cyber attacks and improve the productivity of security teams. The ATP Appliance detects threats across web, e-mail, and lateral traffic. Additionally, it can ingest logs from security devices and apply contextual analysis to present a consolidated view of all threats in the environment.

Product Description

Organizations worldwide face security and productivity challenges every day. Zero-day malware often goes undetected because traditional security devices, which rely on signature-based detection, can't see it. Adding to the problem, security teams—overwhelmed by large volumes of alerts—often fail to recognize and act on critical incidents.

The Juniper Networks® Advanced Threat Prevention Appliance provides continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network. It collects information from multiple attack vectors, using advanced machine learning and behavioral analysis technologies to identify advanced threats in as little as 15 seconds. Those threats are then combined with data collected from other security tools in the network, analyzed, and correlated, creating a consolidated timeline view of all malware events related to an infected host. Once threats are identified, "one-touch" policy updates are pushed to inline tools to protect against a recurrence of advanced attacks.

The detection component of the ATP Appliance monitors network traffic to identify threats as they progress through the kill chain, detecting phishing, exploits, malware downloads, command and control communications, and internal threats. A multistage threat analysis process, which includes static, payload, machine learning, and behavior, as well as malware reputation analysis, continuously adapts to the changing threat landscape leveraging Juniper's Global Security Service, a cloud-based service that offers the latest threat detection and mitigation information produced by a team of security researchers, data scientists, and ethical hackers.

The threat analytics component of the ATP Appliance offers a holistic view of identity and threat activity gathered from a diverse set of sources such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. The analytics component looks at data from these sources, identifies advanced malicious traits, and correlates the events to provide complete visibility into a threat's kill chain. Security analysts receive a comprehensive host and user timeline that depicts how the events that occurred on a host or user unfolded. The timeline enhances the productivity of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents.

The ATP Appliance can integrate with other security devices to mitigate threats, giving users the ability to automatically quarantine e-mails on Google and Office 365 using REST APIs. Communications between the infected endpoint and the command and control servers are blocked by pushing malicious IP addresses to firewall devices. Integration with network access control devices can isolate infected hosts. The ATP Appliance's open API architecture also allows it to integrate with a number of third-party security vendors such as Cisco, Palo Alto Networks, Fortinet, Bluecoat, Check Point, Carbon Black, and Bradford, among others.

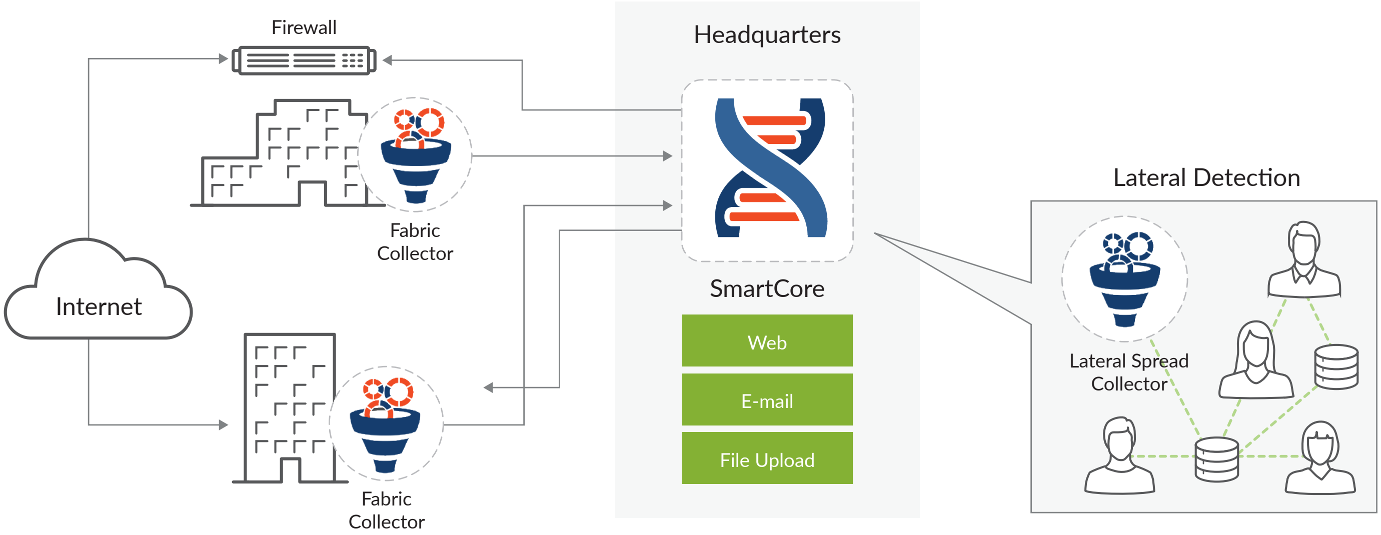


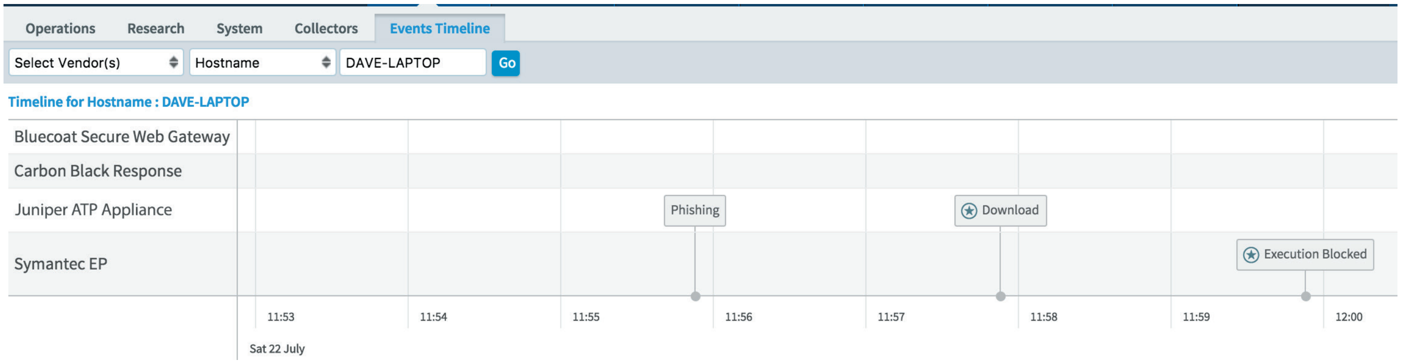
Figure 1: Juniper Networks ATP Appliance architecture

Architecture and Key Components

The architecture of the ATP Appliance consists of collectors deployed at critical points in the network, including remote locations. These collectors act like sensors, capturing information about Web, e-mail, and lateral traffic. Data and related executables collected across the fabric are delivered to the SmartCore analytics engine, which is fully integrated with the Juniper Networks SRX Series Services Gateways. When an SRX Series firewall is deployed as the collector, the solution can operate in an inline threat-prevention mode. Along with traffic from the native collectors, the ATP Appliance also ingests 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. The logs can be ingested directly from third-party devices, or they can be forwarded from existing SIEM/syslog servers.

Armed with data collected from various sources, the SmartCore analytics engine performs the following multistage threat analysis processes:

- **Static analysis**: Applies continuously updated rules and signatures to find known threats that may have eluded inline devices.
- **Payload analysis**: Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content that would otherwise target Windows, OSX, or Android endpoint devices.
- **Machine learning and behavioral analysis**: Employs patent-pending technologies to recognize the latest threat behaviors (such as multicomponent attacks over time) and quickly detect previously unknown threats.
- **Malware reputation analysis**: Compares analysis results with similar known threats to determine whether a newly detected threat is a variant of an existing issue or something completely new.
- **Prioritization, risk analysis, correlation**: Prioritizes threats based on threat severity, asset targets in the network, endpoint environment, and the threat's progression along the kill chain. For example, a high severity Windows malware landing on a Mac receives a lower risk score than a medium severity malware landing on a protected server. All malware events from the ATP Appliance and other security devices are correlated based on endpoint hostname and time and then plotted on a host timeline, allowing security teams to assess the risk of a threat and whether it requires immediate attention. For example, a threat detected by the ATP Appliance but missed by the antivirus solution receives a higher risk score. This allows security teams to go back in time and review all malicious events that have occurred on an infected host.



Hostname: DAVE-LAPTOP

Timeline for Hostname : DAVE-LAPTOP

Figure 2: ATP Appliance events timeline

Features and Benefits

The ATP Appliance includes the following features and benefits:

- Inspects traffic across multiple vectors such as Web, e-mail, and lateral spread
- Uploads suspicious files through the Web UI for processing
- Supports Windows 7 and OSX 10.10 operating systems
- Integrates fully with the SRX300, SRX4000, and SRX5000 lines, as well as the SRX550M and SRX1500; Junos 18.1 is the minimum supported release for SRX Series integration
- Operates in inline blocking mode when used with an SRX Series firewall in inline mode
- Analyzes multiple file types, including executables, DLL, Mach-o, Dmg, PDF, Office, Flash, ISO, ELF, RTF, APK, Silverlight, Archive, and JAR
- Includes detection techniques such as exploit detection, payload analysis, command and control (C&C) detection, YARA, and SNORT rules
- Provides comprehensive and well-documented APIs that allow easy integration with third-party security devices
- Integrates with Juniper Networks, Palo Alto Networks, Checkpoint, Cisco, Fortinet, and Bluecoat solutions to automatically block malicious IP addresses and URLs
- Automatically quarantines Office 365 and Gmail e-mails
- Integrates with Carbon Black Protect and Response (endpoint solution) to allow upload of binaries executed on endpoints
- Allows clustering of multiple secondary cores via scalable architecture, increasing processing capacity
- Includes Manager of Central Managers (MCM) functionality to enable centralized, single-pane-of-glass management in large deployments requiring multiple cores
- Supports access and authentication using SAML and RADIUS
- Correlates events across kill chain stages to monitor threat progress and risk
- Visualizes malware activity and groups malware traits to help incident response teams better understand malware behavior
- Prioritizes threats based on risk calculated from threat severity, threat progress, asset value, and other contextual data
- Provides timeline host view to obtain complete context about malware events that have occurred on the host

Product Options

The ATP Appliance is available in both physical and virtual form factors. The physical appliances—the 1U JATP400 and 2U JATP700—can be deployed in all-in-one mode (SmartCore and Fabric Collector are installed on the same physical appliance) or in distributed mode (SmartCore and Fabric Collector are installed on separate appliances). Virtual appliances can be deployed in distributed mode only. Malware detection for MacOS is also supported. Customers will be required to provide Mac mini hardware that can be deployed as a secondary core. The MacOS sandboxing image is available on the JATP software downloads page.

Physical

All in One

Product Number	Performance (Objects Detonated)[1]	Performance
JATP400	Up to 25,000 objects/day	1 Gbps
JATP700	Up to 61,000 objects/day	2.5 Gbps

SmartCore

Product Number	Performance (Objects Detonated) [1]	Logging Performance
JATP400	Up to 50,000 objects/day	1500 events/second
JATP700	Up to 130,000 objects/day	1500 events/second

[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.

Collector

Product Number	Performance
JATP400	1.5 Gbps
JATP700	4 Gbps

E-mail MTA Receiver

Product Number	Maximum E-mails per Day
JATP400	700,000
JATP700	2 million

Virtual

Supported Hypervisor

Product Number	Versions
VMware vSphere ESXi	5.5, 6.0

Virtual SmartCore

Product Number	Performance (Objects Detonated)	Virtual CPU	Virtual Memory	Virtual Disk
vSC-8	Up to 46,000 objects/day[1]	8	32 GB	1.5 TB
vSC-24	Up to 116,000 objects/day[1]	24	96 GB	1.5 TB

Virtual Collector

Product Number	Performance	Virtual CPU	Virtual Memory	Virtual Disk
FC-v500M	500 Mbps	4	16 GB	512 GB
FC-v1G	1 Gbps	8	32 GB	512 GB
FC-v2.5G	2.5 Gbps	24	64 GB	512 GB

Virtual E-Mail MTA Receiver

Product Number	Maximum E-mails per Day	Number of vCPU	Virtual Memory
vMTA-M	720,000	8	16 GB
vMTA-L	1.4 million	16	16 GB
vMTA-XL	2.4 million	24	32 GB

JATP700

JATP400

JATP700 Specifications

Specification	JATP400	JATP700
Weight	30.4 lbs (13.79kg)	42 lbs (19 kg)
Dimensions (WxHxD)	17.2"x1.7"x25.6"	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: -100-240 V, 50-60 Hz, 11-4.4 Amp	920 W high efficiency (94%+) AC-DC redundant power; AC Input: -100-240 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; -44Vdc to -74Vdc, 20A	850 W/1010 W high-efficiency redundant DC-to-DC power supply; DC Input: 850 W; -35Vdc to -42Vdc, 30-25A
Fans	5x 40x40x56 mm 13K-11K RPM fans	3x8 cm 7 K RPM, 4-pin PWM fans
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

Specification	JATP400	JATP700
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	32GB	128 GB
Storage	8TB(4 x 2TB), RAID 6	8x900 GB 2.5" 10K SAS, RAID 6
Traffic Ports	2xSFP+ 10GbE; 4xRJ-45 GbE	2xSFP+ 10GbE; 4xRJ-45 GbE

Ordering Information

The Juniper ATP Appliance supports flexible deployment options. The components required vary based on the deployment model.

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

The software subscription licenses are offered in two feature packages, summarized in the table below.

Feature Package	Included Features
Standard(STD)	North-South Web traffic, Auto Mitigation, Analytics, Email (BCC), manual upload
Enterprise(ENT)	All Standard features, Lateral traffic (SMB), Email(MTA)

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 AIO, Core, or Collector)
JATP400-DC	JATP400 appliance, DC power, single image installed (can be configured as AIO, Core, or Collector)

Software Subscription Licenses

The subscription licenses are throughput/bandwidth-based. The supported throughput levels are 100 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps,and 10 Gbps.

Note: Integration with SRX Series firewalls requires the AppSecure feature to be installed on the SRX Series device. A separate license may be required, depending on the platform model number.

Product Number	Description
JATP-100M-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 100 Mbps, 1 year term. Support included.
JATP-500M-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 500 Mbps, 1 year term. Support included.
JATP-1G-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 1 Gbps, 1 year term. Support included.
JATP-2G-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 2 Gbps, 1 year term. Support included.
JATP-5G-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 5 Gbps, 1 year term. Support included.
JATP-10G-STD-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 10 Gbps, 1 year term. Support included.
JATP-100M-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 100 Mbps, 3 year term. Support included.
JATP-500M-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 500 Mbps, 3 year term. Support included.
JATP-1G-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 1 Gbps, 3 year term. Support included.
JATP-2G-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 2 Gbps, 3 year term. Support included.

Product Number	Description
JATP-5G-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 5 Gbps, 3 year term. Support included.
JATP-10G-STD-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 10 Gbps, 3 year term. Support included.
JATP-100M-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 100 Mbps, 5 year term. Support included.
JATP-500M-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 500 Mbps, 5 year term. Support included.
JATP-1G-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 1 Gbps, 5 year term. Support included.
JATP-2G-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 2 Gbps, 5 year term. Support included.
JATP-5G-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 5 Gbps, 5 year term. Support included.
JATP-10G-STD-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Standard feature package, up to 10 Gbps, 5 year term. Support included.
JATP-100M-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 100 Mbps, 1 year term. Support included.
JATP-500M-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 500 Mbps, 1 year term. Support included.
JATP-1G-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 1 Gbps, 1 year term. Support included.
JATP-2G-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 2 Gbps, 1 year term. Support included.
JATP-5G-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 5 Gbps, 1 year term. Support included.
JATP-10G-ENT-1	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 10 Gbps, 1 year term. Support included.
JATP-100M-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 100 Mbps, 3 year term. Support included.
JATP-500M-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 500 Mbps, 3 year term. Support included.
JATP-1G-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 1 Gbps, 3 year term. Support included.
JATP-2G-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 2 Gbps, 3 year term. Support included.
JATP-5G-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 5 Gbps, 3 year term. Support included.
JATP-10G-ENT-3	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 10 Gbps, 3 year term. Support included.
JATP-100M-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 100 Mbps, 5 year term. Support included.
JATP-500M-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 500 Mbps, 5 year term. Support included.
JATP-1G-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 1 Gbps, 5 year term. Support included.
JATP-2G-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 2 Gbps, 5 year term. Support included.
JATP-5G-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 5 Gbps, 5 year term. Support included.
JATP-10G-ENT-5	Software Subscription for the Advanced Threat Prevention Appliance – HW or virtual. Enterprise feature package, up to 10 Gbps, 5 year term. Support included.

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

Engineering
Simplicity

EXPLORE JUNIPER
Get the App.
JUNIPER 1ON1
Available on the App Store
ANDROID APP ON Google Play

Copyright 2018 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.