ADVANCED THREAT PREVENTION APPLIANCE

Advanced threat and malware detection, consolidated security analytics, and quick threat mitigation

Challenge

Organizations in sensitive or regulated industries that rely on first-line-of-defense security solutions are facing considerable risks. They need a new type of on-premise solution that can provide shared threat intelligence from the cloud.

Solution

An advanced threat detection appliance, deployed locally and offering flexible deployment options, dynamic advanced attack analytics, and anti-malware techniques provides comprehensive protection against a sophisticated, ever-changing threat landscape.

Benefits

- *Works across multiple locations, managed as a single system*
- *Protects against Web, e-mail, and lateral threats*
- *Correlates and aggregates events and logs from multiple sources to add context*
- *Provides a consolidated view of every incident and related events affecting targeted hosts*
- *Offers one-touch mitigation to block attacks and isolate infected hosts*

The definition of a comprehensive security intelligence solution that detects, analyzes, and remediates advanced cybersecurity threats has changed in recent years. Organizations not only need deep and real-time visibility into their environment to detect cybersecurity attacks, their security teams must also be able to rapidly take remedial action to mitigate or eliminate discovered threats across the network.

These organizations realize that network complexity and a lack of real-time security analytics influence the time it takes to respond effectively to detected threats. Traditional inline security devices, which use rules and signatures to make allow/block decisions, and systems that generate large numbers of alerts from several security devices negatively impact the effectiveness and productivity of security teams, increasing security risk levels. What's needed are systems that continually learn about new threats and provide comprehensive and consolidated security analytics that allow security teams to detect and react to attacks faster, and with a better understanding of what they are facing.

It's equally important that customers have the flexibility to deploy solutions that best suit their needs. Customers who value the privacy of data and are reluctant to upload sensitive documents for analysis should have the option to deploy advanced threat solutions on-premise.

The Challenge

Sophisticated cyber criminals continue to evolve their techniques. In fact, most malware is seen only once, showing how quickly hackers modify their code packaging to make it look different enough to avoid detection by inline defenses that rely on rules and signatures to identify malicious code that has been seen and disseminated repeatedly. Attackers only have to succeed once to be successful, making it essential to empower security analysts and incident responders with the best defense strategies.

According to the Verizon 2017 Data Breach Investigations Report, 75% of data breaches are attributed to external actors, while 73% of attacks were financially motivated. Cyber attackers continue to employ evasive, multipronged attacks that security teams can't respond to quickly because they lack a holistic view of events.

Their options are limited. They can continue relying on traditional inline systems, but that means there is a good chance that they will miss critical threats and alerts. If they perform deeper threat inspection, they introduce significant latency to the process, increasing the risk to the organization and compromising user experience and productivity.

The Juniper Networks Advanced Threat Prevention Appliance

Juniper Networks® Advanced Threat Prevention Appliance is an open, scalable software platform, available in 1U (JATP400), 2U (JATP700), and virtual form factors, that works with the security products you already have in place to accelerate the productivity of security analysts and incident responders. Deployed quickly and easily, the ATP Appliance bolsters your organization's security posture by offering advanced threat detection, consolidated security analytics, and one-touch threat mitigation to defend against advanced threats.

The ATP Appliance improves the productivity of security teams by detecting threats across Web, e-mail, and lateral traffic, ingesting logs from security devices throughout the network to present a consolidated view of all threats in the environment. The system collects information from multiple attack vectors, then uses advanced machine learning and behavioral analysis technologies to discover advanced threats. Detected threats are combined with data ingested from other security tools, analyzed, correlated by an internal analytics engine, and then presented to security analysts with a consolidated timeline view of all events related to the infected host. Once threats are discovered, "one-touch" policy updates are pushed to inline tools, strengthening them against a recurrence of advanced attacks.

The ATP Appliance solution features three key components:

1. **Detection**: The ATP Appliance monitors network traffic to identify external and internal threats such as exploits, malware downloads, and command and control (C&C) communications as they progress along the kill chain. It uses a multistage threat analysis process that includes static analysis, payload analysis, machine learning, and behavior and malware reputation analysis. The threat analysis process continuously adapts to the changing threat landscape using Juniper Global Security Services (GSS), which is updated with threat detection and mitigation data produced by Juniper ATP Labs, a team of security researchers, data scientists, and ethical hackers.
2. **Advanced Threat Analytics**: The ATP Appliance provides a holistic view of identity information and threat activity gathered from diverse sources such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. By looking at the data, identifying advanced malicious traits, and correlating the events, the ATP Appliance provides complete visibility into the threat kill chain. A host and user timeline provides an overview of the events that have occurred on the host or to the user, focused around the day-to-day workflow of Tier 1 and Tier 2 security analysts who work on triaging and investigating malware incidents.
3. **Mitigation**: The ATP Appliance's one-touch mitigation capability, performed through Juniper Networks SRX Series Services Gateways, gives organizations the ability to automatically mitigate threats inline and isolate infected hosts. The ATP Appliance also provides the ability to automatically quarantine e-mails on Google and Office 365 using REST APIs. Communications between an infected endpoint and the command and control servers are blocked by pushing malicious IP addresses to firewall devices. The appliance can also work with SRX Series firewalls to isolate infected hosts. The ATP Appliance's open API architecture allows it to integrate with other security vendors to automatically mitigate threats.

Figure 1: Juniper Networks Advanced Threat Prevention Appliance components

Capabilities, Features, and Benefits

Table 1: ATP Appliance Features and Benefits.

Capabilities	Features and Benefits
Multivector traffic inspection	• Inspects traffic across multiple vectors such as Web, e-mail, and lateral spread
File upload	• Inspects and analyzes files uploaded through the Web console
Key operating systems supported	• Supports Windows, MacOS
Multiple file type analytics	• Analyzes multiple file types including executables, DLL, Mach-o, Dmg, PDF, Office, Flash, ISO, ELF, RTF, APK, Silverlight, Archive, JAR
Effective detection techniques	• Includes detection techniques such as exploit detection, payload analysis, C&C detection, YARA, and SNORT rules
Extensive data correlation	• Correlates events across kill chain stages to monitor threat progress and risk
Contextual threat prioritization	• Prioritizes threats based on risk score calculated from threat severity, threat progress, value of asset, and other contextual data
Host behavior timeline	• Provides timeline view of host to offer context about malware events that have occurred
Comprehensive third-party API support	• Includes comprehensive and well-documented APIs that allow easy integration with third-party security devices
Extensive automatic threat mitigation	• Automatically works with most security vendors to block malicious IP addresses and URLs
E-mail security on Office 365 and Gmail	• Automatically quarantines e-mails on Office 365 and Gmail
Endpoint integration	• Uploads files from Carbon Black Response and Carbon Black Protect
Reporting	• Produces executive reports to help CISOs understand the overall malware activity within the enterprise • Provides detailed technical reports to track security incidents and infected hosts

Use Cases

The following three key use cases demonstrate how the ATP Appliance can protect your organization.

Use Case 1: Advanced On-Premise Threat Protection for Highly Distributed Organizations

Most large organizations have employees spread across multiple office locations, making it difficult for security teams to build a distributed, multisite security architecture that can be managed as a single system. This use case looks at how the ATP Appliance protects distributed organizations against advanced attacks that elude the first line of defense.

Advanced Cyber Attacks and Their Growing Damage: Security teams are hard-pressed to stop advanced malware attacks, especially when trying to protect thousands of employees across multiple locations. Each location has different requirements when it comes to form factor and available resources, and such practical considerations must be taken into account to ensure that all locations are protected. Cyber attackers look for the weakest link to penetrate a network; most often, malware is delivered via e-mail or Web traffic (or a combination of both) and quickly spreads laterally once a host is compromised. Eventually, communications with a C&C server are established, enabling attackers to pursue their objectives of surveillance and theft.

The Juniper Solution: The ATP Appliance is an innovative, distributed, software-layer solution that safeguards your organization and addresses the critical detection gaps in your security architecture. The appliance collects, correlates, and analyzes Web, e-mail (including cloud-based), and lateral-spread traffic throughout the network, using advanced detection technology to quickly alert security teams. The ATP Appliance includes a multistage detection engine with payload analysis (powered by machine learning and behavioral detection), heuristic-based exploit detection, and ransomware-focused threat identification, giving users the ability to customize detections via Snort and YARA rules.

The ATP Appliance also features a distributed architecture and centralized management, giving you the flexibility to leverage VMs, commercial servers, and cloud resources to ensure that all locations and users are protected.

Use Case 2: Advanced Threat Protection for Enterprise E-Mail

E-mail continues to be the go-to delivery vehicle for cyber attacks. Whether your organization use an on-premise or cloud-based e-mail system, these channels need to be secured. This use case shows how the ATP Appliance, with its integrated advanced threat detection fabric, helps you defend against these attacks to maintain productivity, establish comprehensive and advanced protection, and ensure that compliance obligations are being met.

Continued Dependence and Dangers Associated with E-Mail: While many aspects of IT have experienced a fundamental paradigm shift in recent years, one reality remains: e-mail continues to be the primary tool for personal and business communications. Organizations typically employ inline security

tools that rely on static, rules-based approaches to protect on-premise e-mail systems. Without a solution that can correlate intelligence across multiple threat vectors such as endpoints, Web, and e-mail to quickly respond to threats, security teams must perform deep inspection which introduces considerable latency, increases security risks, and compromises productivity.

The Juniper Solution: The ATP Appliance detects malicious attachments and URL links and can automatically quarantine dangerous e-mails in near real time. Its flexible implementation allows it to integrate easily with any existing cloud-based e-mail system, including Microsoft Office 365 or Google Gmail, without having to change any network or e-mail infrastructure, including routing and mail exchanger (MX) records.

The rich intelligence correlation on the ATP Appliance gives your team a single management console for viewing and tracking threats, including those coming through e-mail and Web traffic. The ATP Appliance also delivers robust scalability, with a capacity to process up to 2.4 million e-mails a day.

Use Case 3: Advanced Threat Analytics for Insight into Compromised Users and Endpoints

For many security teams, fighting cyber attacks is only part of the battle; they also struggle with their current tools and their limited expertise. This use case shows how the ATP Appliance aggregates distributed security intelligence gathered throughout the network to gain a unified, contextual view and timeline of all activities related to advanced attacks on users and endpoint devices, reducing workloads for second-level staff and maximizing existing investments.

Demand for Unified Visibility and Context: Organizations spend considerable time manually collecting, aggregating, and correlating data from different tools and resources. When threats are detected, teams are forced to scramble to answer critical questions such as which host and user were infected, did any device block the threat, and whether the threat has spread. Not only do security teams dedicate a lot of time and effort to these activities, they lack any threat context or alert prioritization, placing an additional burden on the staff to optimize their ability to analyze and respond to security alerts.

The Juniper Solution: The ATP Appliance provides a holistic view of threat activity from diverse sources such as Active Directory, endpoint antivirus, firewalls, secure Web gateways, intrusion detection systems, and endpoint detection and response tools. The ATP Appliance fully automates the collection, correlation, and analysis of logs, events, and alerts, providing response teams with rich data that includes the threat context, the host identity, and the end-user identity—with no manual data aggregation and analysis required. The ATP Appliance includes a host and user timeline that includes the evolution and the correlation of advanced threats. With this view, Tier 1 teams now have the information they need to determine the exact nature of the threat and whether it

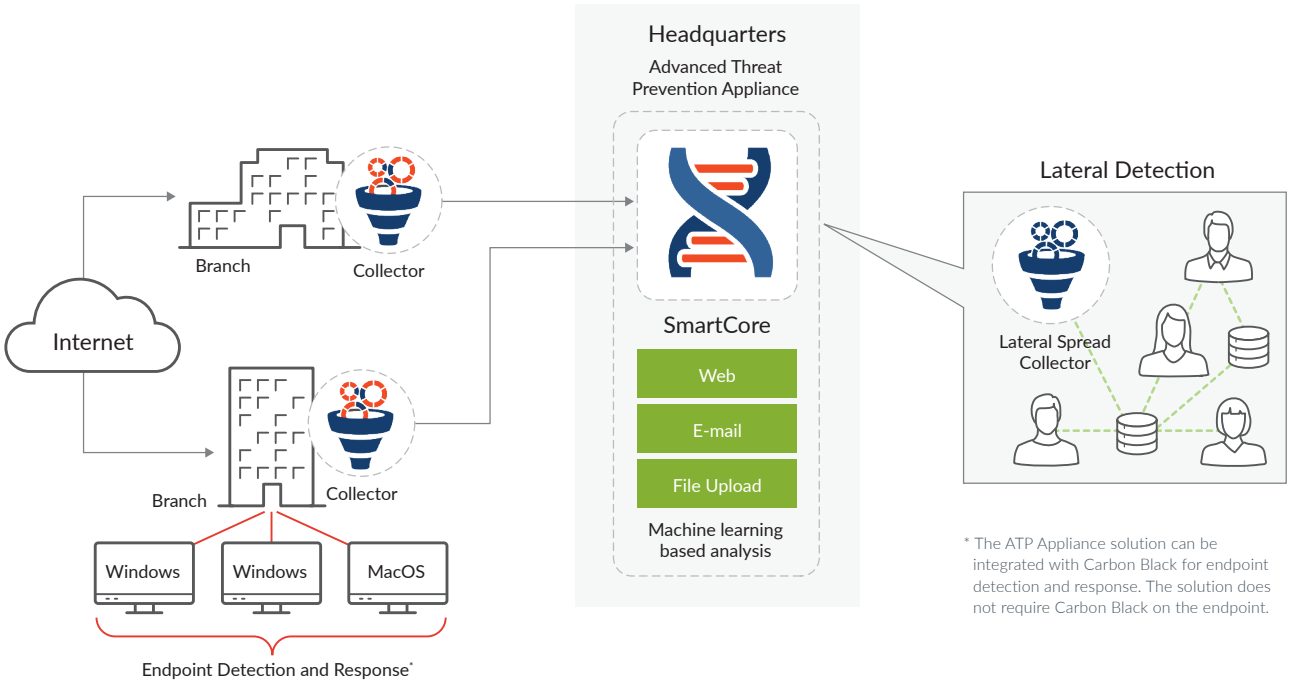

Figure 2: Deployment Option 1—Standalone Advanced Threat Prevention Appliance

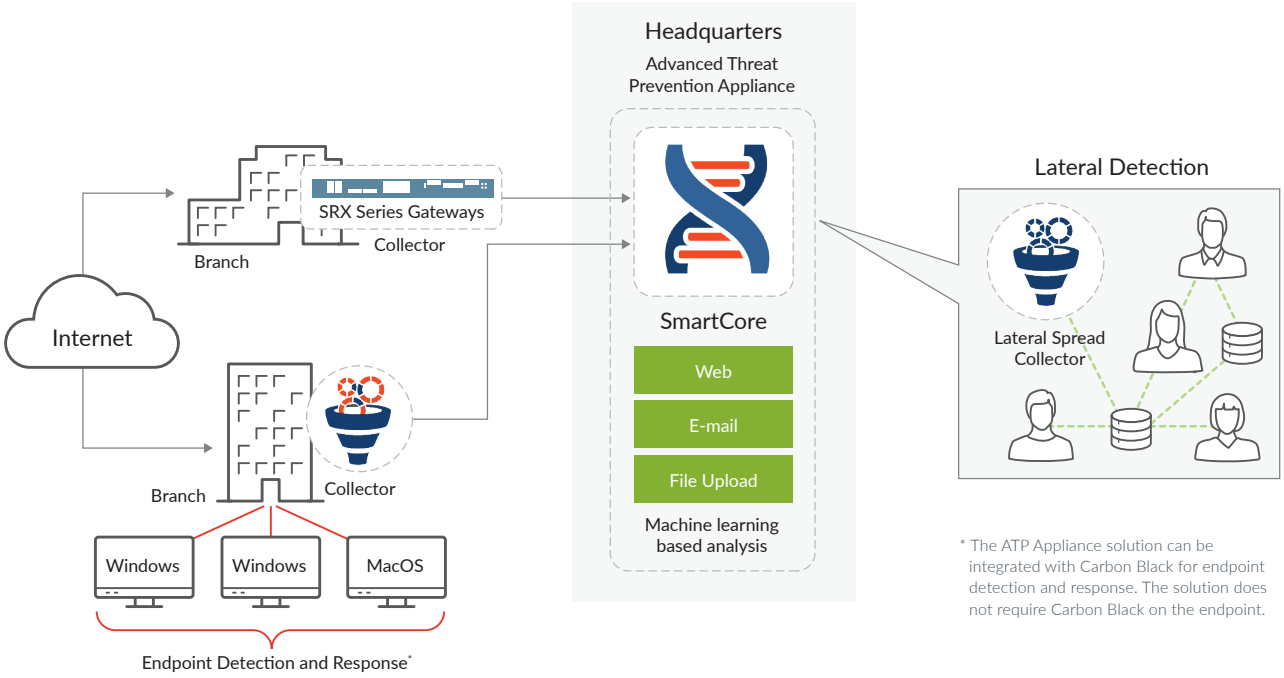

Figure 3: Deployment Option 2—ATP Appliance with SRX Series Services Gateways as collectors

requires escalation to a Tier 2 team for mitigation. The ATP Appliance easily integrates with security information and event management (SIEM) platforms through its open API, allowing you to use your SIEM for prioritization and incident handling while leveraging the ATP Appliance to provide complete context of advanced threats.

Deployment Options and Solution Components

The Juniper Networks Advanced Threat Prevention Appliance can be deployed in two different modes, each requiring certain components.

ATP Appliance in Standalone Mode

When deployed in standalone mode, the ATP Appliance is ideal for organizations that struggle to gain network-wide visibility into existing or potential threats due to the large number of point products, a lack of data correlation and actionable intelligence, limited expertise, and the number of steps required to identify and mitigate threats. The ATP Appliance is a distributed software platform that combines advanced threat detection, consolidated security analytics, and one-touch threat mitigation to protect organizations from advanced threats and improve the productivity of security teams. The ATP Appliance detects threats across Web, e-mail, and lateral traffic, ingesting logs from security devices to present a consolidated view of all threats within the environment.

The following components are required for this deployment mode:

- **Collectors**: The ATP Appliance architecture consists of collectors that are deployed at critical points in the network, including remote locations, where they capture Web, e-mail, and lateral traffic data.
- **SmartCore Management and Analytics**: Data and related executables continuously collected across the fabric are delivered to ATP Appliance SmartCore, which is the analytics engine, as well as the management platform.

Along with traffic from native collectors, the ATP Appliance can also ingest 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 directly ingested from third-party security devices or forwarded from existing SIEM/system logging servers.

With data collected from various sources, the SmartCore analytics engine performs the following multistage threat analysis.

Table 2: SmartCore Multistage Threat Analysis

Function	Description
Static analysis	• Applies continuously updated rules and signatures to look for 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 which would otherwise target Windows, OSX, or Android endpoint devices.
Machine learning and behavioral analysis	• Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such as multicomponent attacks over time) to quickly detect previously unknown threats.
Malware reputation analysis	• Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.
Prioritization, risk analysis, correlation	• After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain. For example, high-severity Windows malware landing on a Mac is given a lower risk score than 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 plotted on a host timeline. This enables security teams to assess the severity of a threat, as well as determine if a threat requires attention. It also allows security teams to go back in time to look at all the malicious events that occurred on an infected host.

ATP Appliance with SRX Series Services Gateways as Collectors

When using SRX Series Services Gateways as collectors, the ATP Appliance is ideal for organizations that have already deployed, or are planning to deploy, SRX Series firewalls in their environment and are specifically looking for an on-premises solution for advanced threat detection and analysis. Unlike standalone mode, in this deployment the SRX Series firewalls act as collectors, decrypting traffic and uploading suspicious files and decrypted traffic to the SmartCore analytics engine for inspection. Standalone collectors are optional and can be deployed in conjunction with those running on the SRX Series gateways. In this mode, the ATP Appliance also provides threat intelligence to the SRX Series firewalls to block callbacks to malicious C&C servers. The ATP Appliance also sends a list of infected hosts requiring immediate attention so the SRX Series firewalls can isolate those devices. By operating in inline blocking mode, the SRX Series devices can also detect previously seen threats. The SRX Series device and security policies can be configured on Juniper Networks Junos Space® Security Director to quarantine or block identified threats.

The following components are required for this deployment mode:

- **SRX Series Firewalls:** Juniper's physical SRX Series gateways provide next-generation firewall (NGFW)-level protection with integrated application awareness, intrusion prevention, and role-based user controls, plus best-in-class unified threat management (UTM) to protect and control business assets. This solution is centrally managed using Junos Space Security Director.

  To learn more about the SRX Series NGFWs, visit www.juniper.net/us/en/products-services/security/srx-series/.

- **Junos Space Security Director:** With Juniper's scalable and intuitive Security Director solution, enterprises can make precise security decisions and achieve end-to-end visibility into applications, users, and threats through their SRX Series devices. Offering a holistic view, rich security feature set, and easy-to-use actionable intelligence such as threat intelligence received from Juniper Sky ATP and ATP Appliances, Security Director lets you create security policies that allow you to immediately take remedial action and block high-risk applications and threats. With a single pane-of-glass management solution, an easy-to-use intelligent security rule creation wizard, and an auto-rule placement, you can create less complex security policies faster.

  To learn more about Security Director, visit www.juniper.net/us/en/products-services/security/security-director.

Summary—A Local, Highly Effective Threat Intelligence and Security Solution

Virtually every enterprise security architecture begins with a strong first line of defense. As threats evolve, however, it is getting more difficult for traditional "first line of defense" solutions to effectively defend the network. As effective as these tools are, none of them can fully protect you against the advanced threats targeting your network. Once these threats gain access to internal resources, they can operate in stealth mode for months undetected. By the time the breach is discovered, the damage is already done.

The Juniper Networks Advanced Threat Prevention Appliance provides comprehensive, local threat intelligence, detection, and protection against today's continuously evolving threats. Compared to traditional inline products, the ATP Appliance correlates and aggregates threat intelligence from multiple sources,

adding context to threats and protecting your organization from Web, e-mail, and lateral threats. Flexible deployment options, dynamic advanced threat analytics, and extensive one-touch threat mitigation capabilities on the ATP Appliance allow you to adapt to the ever-changing threat landscape.

Next Steps

For more information on Juniper Networks Advanced Threat Prevention Appliance, please visit us at www.juniper.net/us/en/products-services/security and contact your Juniper Networks representative.

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
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: +31.0.207.125.700
Fax: +31.0.207.125.701