

JUNIPER CONNECTED SECURITY IN ACTION

Enabling automated threat remediation without impacting business continuity

Challenge

Businesses need to continuously evolve to fight the increasingly sophisticated attacks threatening their networks. However, this focus on security is often at the expense of other important activities, triggering an on-going internal battle that pits business continuity against network security.

Solution

Businesses must take a synergistic approach that leverages network and security elements equally in an open, multivendor ecosystem with centralized policy, analytics, and management—to transform their traditional network into a threat-aware network.

Benefits

- Automate security coverage from endpoint to edge and every cloud in between
- See who and what is on your network and enforce policies across all connection points
- Employ granular quarantine capabilities enabled by a greater number of security enforcement points in the network
- Perform rapid and automated threat remediation
- Gain best-in-class networking

Network deployments have significantly changed over the past decade. Businesses are rapidly moving to the cloud and adopting new technologies such as Internet of Things (IoT) that are heavily dependent on the network.

These same enterprises are also increasing their spending on security to protect new and existing infrastructure, but the breaches continue unabated. Internal records and customer information are still being stolen and sold to the highest bidder, causing irreparable damage to corporate reputations. This begs the question—are these businesses missing something very fundamental in their approach to network security?

The Challenge

A number of highly effective security technologies and solutions are available today: next-generation firewalls, dynamic and static malware analysis, cloud access security brokers (CASB), security event and information management (SIEM), and endpoint protection, to name a few. However, a network is only as secure as its weakest link, and without deep collaboration and synchronization between all network elements, enterprises still have a gaping security hole that leaves them vulnerable to attack. Key stakeholders are faced with the realization that their considerable investments in popular security products have still not yielded the promised protection.

Threat Propagation in an Enterprise with Typical Infrastructure and Security Products

Let's take a look at a typical enterprise with clients, endpoints, access switches, and wireless access points. A next-generation firewall connected to an antimalware service is used at the enterprise perimeter to defend against threats in a north-south direction, as well as support security between internal segments across many clouds. Endpoint protection software may be available on clients, depending on their type or model. For IoT, network printers, or new types of endpoints, this protection is not available.

Network Compromise Workflow

Figure 1 shows a compromised network. These breaches typically follow a predictable pattern:

1. Client attempts to download an unknown malware.
2. The file is scanned at the perimeter firewall.
3. The firewall sends the file to an anti-malware service for analysis, which notifies

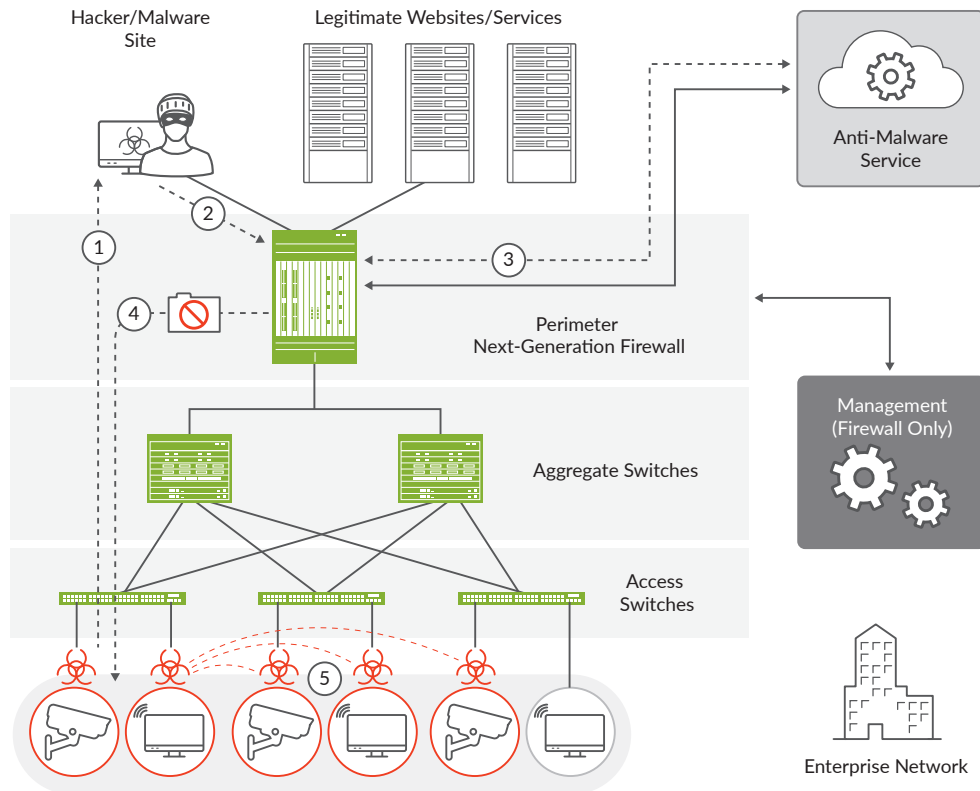


Figure 1: Network compromised in an agency with typical infrastructure and security products

the firewall that the file is malware.

4. The firewall blocks the file, preventing it from being downloaded.
5. However, if the client was compromised outside the corporate network (a “non-enterprise” environment) or by manual means, it will continue to infect all other reachable hosts in the network (based on the type of threat).

As a result:

- a. Simply preventing the client from reaching outside the corporate network is ineffective and does not protect against lateral threat propagation.
- b. The inability of security solutions to communicate with and leverage networking components reduces visibility and restricts the number of enforcement points.
- c. Failure to aggregate reports of abnormal behavior from different knowledge sources such as logging servers, endpoints, and other network elements is a significant weakness in the security strategy.
- d. Since the security strategy is heavily firewall focused, the complexity of firewall policies can easily overwhelm security teams; this problem is amplified when the enterprise has a global footprint.

Juniper Networks Connected Security

Juniper Networks® Connected Security helps organizations safeguard users, applications, and infrastructure by extending security to all connection points across the network and providing the ability to even use other vendors’ technologies. Juniper Connected Security combines policy, detection, and enforcement with a comprehensive product portfolio that centralizes and automates security.

Juniper Connected Security Building Blocks

Juniper Connected Security is built on the following components:

1. Sophisticated threat detection engine:
 - a. Juniper Advanced Threat Prevention (ATP) cloud-based malware detection solution is used to accurately detect known and unknown threats.
 - b. Juniper Networks® Advanced Threat Prevention Appliance is an on-premises analytics platform that detects sophisticated threats.
 - c. Known threats are detected by consolidating threat feed information from a variety of sources—command and control (C&C) servers, GeolP, third-party devices via REST APIs—as well as information acquired from in-house log servers.
 - d. Unknown threats are identified by Juniper ATP Cloud or ATP Appliance using technologies such as dynamic and static malware analysis, machine learning, and threat deception techniques.

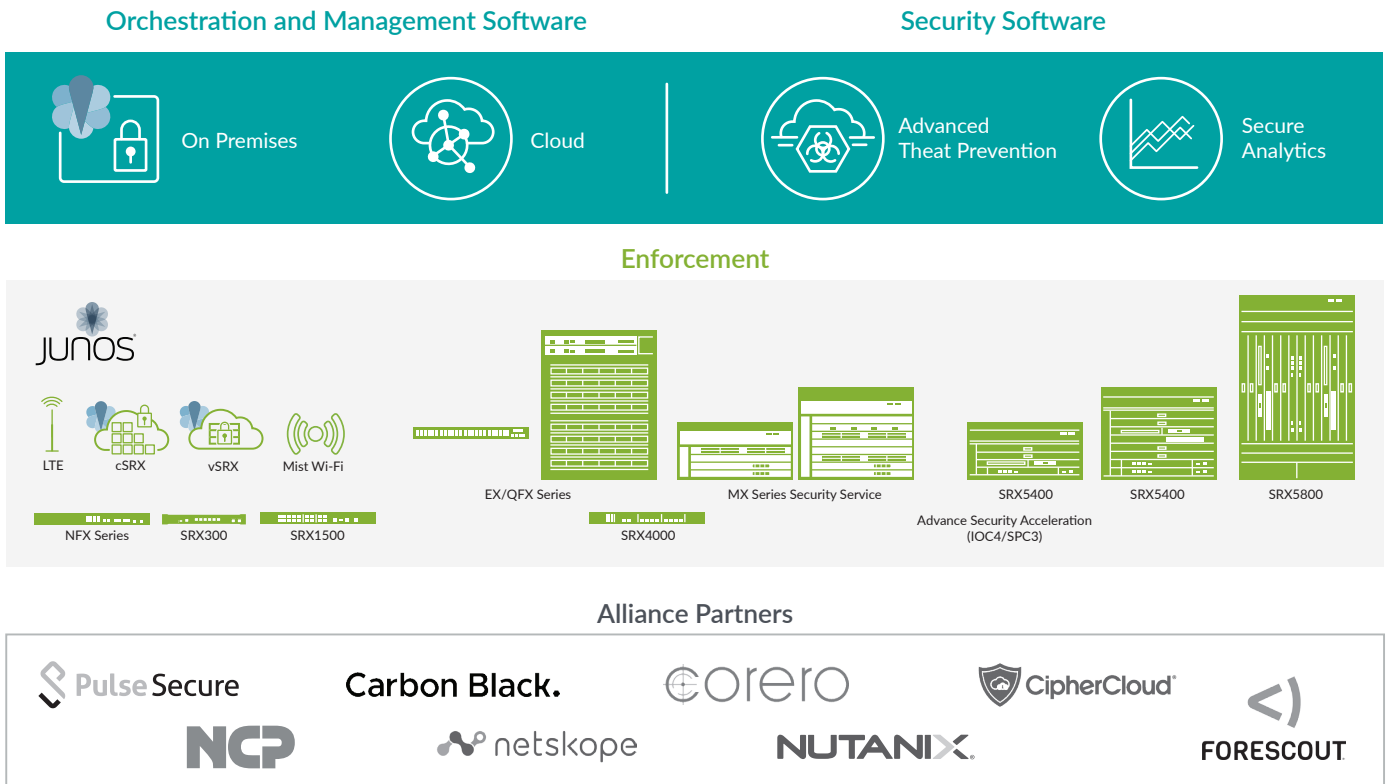


Figure 2: Connected Security Portfolio

2. Centralized management, policy, and analytics:
 - a. Juniper Networks Junos® Space Security Director delivers a scalable and responsive security management application that improves security policy administration through a single pane of glass.
 - b. Policy Enforcer, a component of Security Director, is a central intelligence module that provides:
 - Communication with multivendor network elements and security products such as next-generation firewalls to globally enforce security policies and provide analytics
 - Consolidation of threat intelligence from different sources within the premises
3. Enforce security everywhere:
 - a. Leverages any network element as an enforcement point.
 - b. Adopts an open, multivendor ecosystem to detect and enforce security across Juniper solutions, cloud, and thirdparty ecosystems.
 - c. Delivers the ability to rapidly block or quarantine threats to prevent north-south or east-west threat propagation.

Secure Network Deployment with Juniper Connected Security

Let's take a look at a Juniper Connected Security network that uses Juniper Networks SRX Series Services Gateways deployed as perimeter firewalls connected to Juniper ATP Cloud or ATP Appliance for anti-malware services. Security Director Policy Enforcer is the central intelligence component that communicates with different network elements, including next-generation firewalls, to globally enforce security policies.

Policy Enforcer's Feed Collector module consolidates threat feeds from the cloud and on-premises devices along with logging and in-house threat feeds. Clients/endpoints are connected to access switches or wireless access points with endpoint protection software. While IoT devices, printers, and new types of endpoints would not have this protection, Policy Enforcer can communicate with the access devices to share intelligence and enforce security where necessary.

Juniper Connected Security alters the security breach landscape considerably. Here's how two different scenarios play out when a Juniper Connected Security network is attacked.

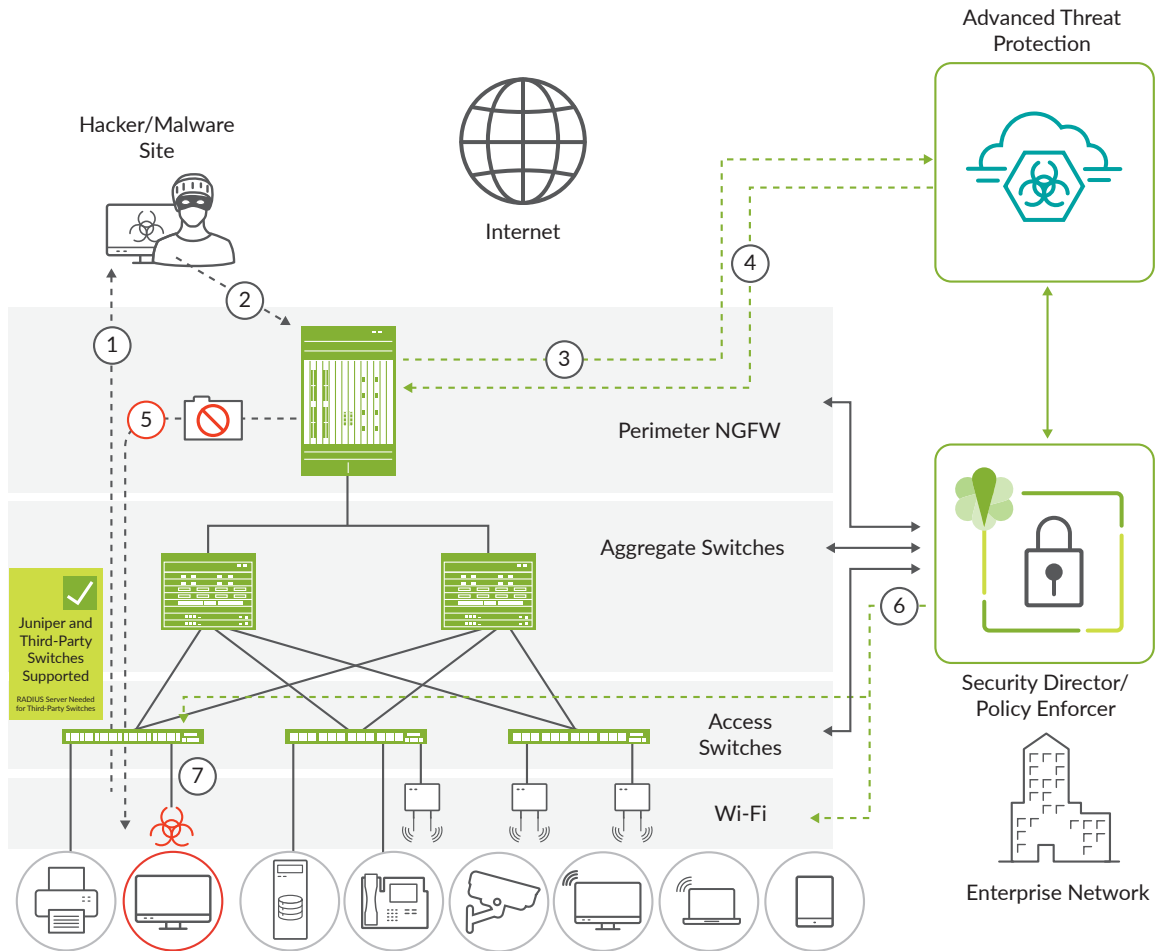


Figure 3: Secure network deployment with Juniper Connected Security and Juniper ATP Cloud

Workflow 1: Malware Download

1. A client attempts to download unknown malware.
2. The file is scanned by the perimeter SRX Series firewall.
3. The SRX Series firewall sends the file to Juniper ATP Cloud or ATP Appliance.
4. Juniper ATP Cloud or ATP Appliance determines the file is malware and notifies the SRX Series firewall and Policy Enforcer.
5. The SRX Series firewall blocks the file from being downloaded.
6. Policy Enforcer quarantines the host to a special VLAN (at the switch) until further investigation is possible. Policy Enforcer can also optionally disable the switch port or Wi-Fi access point that the client is connected to.
7. The targeted client is now prevented from infecting other hosts in the network. East-west and north-south malware propagation is halted. Policy Enforcer remembers the client, so even if it moves to another switch or Wi-Fi access point, Policy Enforcer recognizes the threat and blocks it from the network.

Workflow 2: IoT Malware Detection

1. An infected IoT device attached to the network attempts to download a restricted file or launches an attack on a critical infrastructure.
2. The unauthorized download attempt is detected by an SRX Series firewall, which sends the file to the Juniper ATP Appliance for further analysis.
3. If an IoT device tries to connect to a C&C server, the SRX Series firewall will detect the attempt and block the device.
4. Policy Enforcer automatically blocks or quarantines the host at the switch port or Wi-Fi access points.

If this attack on the network had happened in a different type of network security environment, the IoT device could have continued to access additional information; a traditional nextgeneration firewall would simply have prevented the IoT device from communicating outside the organization. If this were an internal attack where the attacker had physical access to the device, damage could be extremely high.

Features and Benefits

The Juniper Connected Security framework delivers the following benefits:

- **Pervasive security:** Juniper Connected Security extends security to every layer of the network, including switches, routers, and wi-fi access points, as well as the firewall layer. By supporting different deployment models ranging from on-premises physical deployment or private clouds (such as VMware NSX and Juniper Contrail) to public clouds (such as Amazon AWS and Microsoft Azure), Juniper Connected Security means customers don't have to compromise in their pursuit of robust security.
- **Open, multivendor ecosystem:** Most enterprises are multivendor environments. Any security solution that requires swapping out existing infrastructure during a refresh cycle, or locks customers into a single vendor, will impose significant restrictions with respect to introducing new capabilities and adopting new trends and technologies. Juniper Connected Security takes an open approach, allowing enterprises to keep most of their existing networking gear while transitioning to a more secure network. By partnering with other network and security vendors, Juniper Connected Security offers a truly collaborative and comprehensive approach to complete network security.
- **Global policy and security management:** Junos Space Security Director with the Policy Enforcer module allows users to enforce consistent security policies across the entire network, regardless of local or global footprint. Security administrators gain granular visibility into the system and enforcement at the network layer and in virtual environments, helping them optimize their security posture.

- **Dynamic, automated threat remediation:** The ability to quickly respond to threats is critical to network security. Threats are accurately and continuously detected by Juniper ATP Cloud, the ATP Appliance, in-house feeds, and third-party sensors. Policy Enforcer automatically takes corrective action against these threats, blocking or quarantining them almost immediately at the network layer. This reduces administrative overhead and facilitates a faster, more manageable approach to security as the network expands.

Summary

Juniper Connected Security combines network and security elements with centralized management and analytics to offer pervasive security and truly automated threat remediation. Juniper Connected Security's open, multivendor ecosystem support enables enterprises to use network and security elements already in their network to protect existing investments while ensuring business continuity.

Next Steps

For more information on Juniper Networks security solutions, 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

JUNIPER NETWORKS | Engineering
Simplicity

