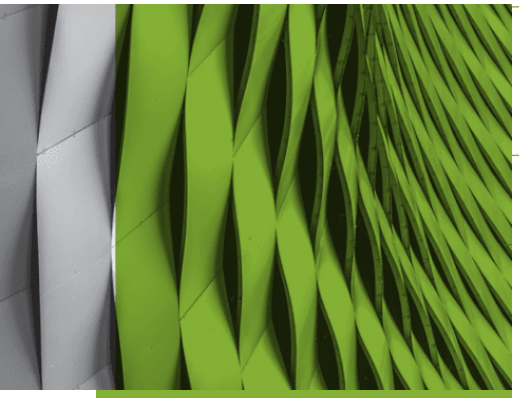

JUNIPER SECINTEL

Product Overview

Juniper SecIntel provides threat intelligence to all points of connection across the network to block malicious traffic, creating a threat-aware network. To reduce risk, SecIntel can be deployed at the WAN edge, across wired and wireless LANs to increase threat visibility, and at enforcement points within the network.

Product Description

Juniper® Connected Security provides visibility into threats from the network and cloud; analyzes, deciphers, and prioritizes those threats; and pushes recommended actions to Juniper firewalls, switches, and routers. This gives customers a complete view of their network and cloud, allowing them to create a threat-aware environment.

At Juniper, we believe that a truly secure network must be threat-aware. Threat-aware networks require both deep network visibility and the ability to enforce policy at every connection point. Firewall orchestration—including Juniper's patented one-click automation—is one example of a simple management option that allows administrators to safeguard users, applications, and infrastructure by enabling the automatic creation and distribution of policies that can block traffic at the port level. That is the power of Security Intelligence (SecIntel).

SecIntel provides security threat intelligence feeds that aggregate data from multiple sources, including Juniper devices, to deliver curated, consolidated, actionable intelligence. These feeds are delivered to Juniper Networks SRX Series Services Gateways, as well as non-security devices such as Juniper Networks MX Series Universal Routing Platforms, Juniper Networks EX Series and QFX Series switches, and our Mist wireless solutions deployed across the organization. These threat intelligence feeds include threat information curated by Juniper Threat Labs and accessed via Juniper Advanced Threat Prevention (ATP) cloud-based service, as well as third-party threat data and threat information covering industry-specific threats that customers can integrate into their solution.

Being able to identify and shut down attacks across the network before they can do any damage protects users, applications, and infrastructure—including subscriber networks—from compromise, and it turns connectivity layers into security layers without additional infrastructure.

Juniper Threat Labs provides dynamic and automatic updates for SecIntel. With a large global presence of sensors, security researchers, and analysts, our dedicated team of researchers provides rapid and actionable insights about emerging threats and new infiltration techniques. Juniper Threat Labs also maintains and integrates our threat intelligence ecosystem by working with many other security vendors, alliances, and partnerships.

Verified by NSS Labs during the recent Data Center Security Gateway Test, Juniper achieved a recommended rating and scored greater than 99% for exploits and 100% on evasions identified and blocked. Juniper ATP Cloud, which includes SecIntel, goes through quarterly testing by ICSA Labs for Advanced Threat Defense, where Juniper is achieving nearly 100% catch rates on the latest malicious threats.

SecIntel threat feeds can be used to filter traffic and orchestrate automated incident response. These threat feeds are an important component of a threat-aware network, allowing IT teams to improve visibility and security while continuing to reduce risk.

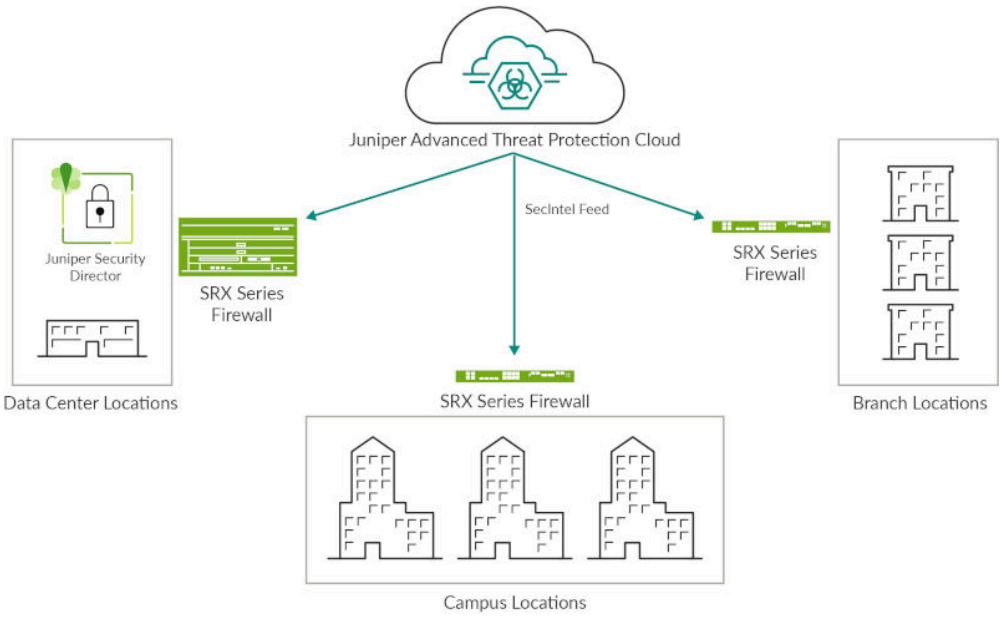

Figure 1: SecIntel on SRX Series firewalls

Architecture and Key Components

SRX Series firewalls make use of SecIntel threat feeds to offer traffic filtering at both the network and application layers, making it possible to identify and act upon known threats. The threat intelligence provided through SecIntel from ATP Cloud includes attacker IPs, Command and Control (C&C), GeoIP, infected hosts, dynamic address groups, global as well as custom allowlists, and blocklists consisting of file hashes, domain names, IP addresses, malicious URLs, code signing certificates, and signer organizations. SRX Series firewalls can be configured to passively monitor and alert, or to monitor and block threats detected using SecIntel (see Figure 1).

MX Series routers also use the SecIntel threat feeds, providing an additional layer of network security by identifying and blocking C&C traffic provided by Juniper ATP Cloud, along with custom whitelists and blacklists. This feature evolves the role of the router from a simple connectivity layer into a threat-aware network device.

Threat-aware networks actively participate in their own defense, and the integration of SecIntel threat feeds into MX Series routers gives organizations an automated defense layer without adding hardware. Threat-aware MX Series routers block threats before they even get to the firewall. This reduces the load on the firewall, which is typically more computationally expensive, and potentially offers protection to data flows that would otherwise go unprotected. Like the SRX Series firewall, the MX Series router can be configured to passively monitor and alert or monitor and block detected threats using SecIntel (see Figure 2).

Routers and firewalls are typically found at the network's edge. However, information security best practices call for enforcing policy as close to the point of compromise as possible. SecIntel for EX Series and QFX Series switches allows organizations to identify and block—or quarantine—compromised hosts anywhere on the network, protecting you against lateral threat propagation.

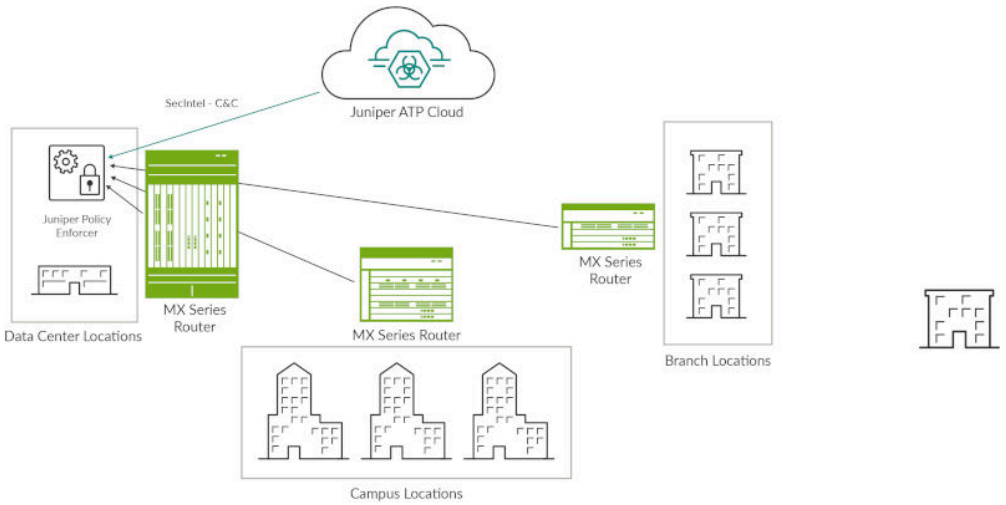

Figure 2: SecIntel on MX Series routers

EX Series and QFX Series switches use SecIntel's Infected Host Feed, which is dynamically updated via ATP Cloud, to quickly identify compromised hosts and automatically quarantine or block the host from accessing the network. This extends policy enforcement to every point of connection throughout the network, providing the deep network visibility required to build a threat-aware network (see Figure 3).

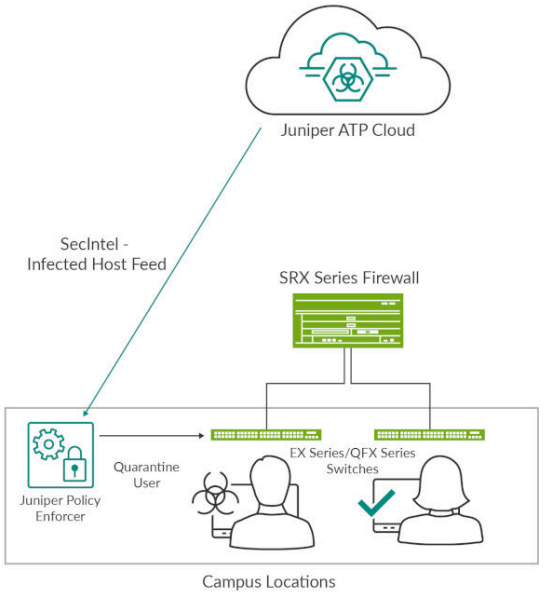

Figure 3: SecIntel on EX Series and QFX Series switches

Features and Benefits

Feature	Description	Benefits
Curated threat intelligence	SecIntel uses curated threat feeds provided by Juniper Threat Labs, including malicious IPs, malicious URLs, malicious domains, and GeoIP. The information included within SecIntel is scrubbed and validated while being constantly updated in real time by Juniper Threat Labs.	Delivers constantly updated and curated threat data to increase threat coverage and reduce false positives. Mitigates the risk of a breach by blocking known avenues of attack with the latest threat data, leaving more time for your security teams to proactively hunt down unknown threats.
Infected host feeds	SecIntel uses infected host and custom threat feeds. Infected Hosts is a threat feed provided by Juniper ATP Cloud, which contains a list of all known infected hosts on your network.	Automates detection and mitigation for security events and identifies and blocks those events closer to the source.
Custom threat intelligence	Custom threat feed allows organizations to add data sources of their choosing, such as industry-specific threat mitigation and prevention input by third parties.	Provides the Security Operations team a flexible input to add specific threat intelligence provided by industry-specific third parties.
Identification and blocking of recognized threats across the network	SecIntel provides the ability to identify and either passively monitor or block known threats. This can be done at the network edge, throughout the network core, and at the access layer (including both wired and wireless networks).	Allows for the addition of security to the networking stack—not as an add-on, but natively within the network infrastructure. Leverages other network resources typically not thought of as security devices as identification and enforcement points on the network.
Comprehensive threat logging and orchestration	To improve visibility and enable automated incident response, threat logs from SecIntel can be sent to security information and event management (SIEM), log management tools such as Juniper Networks Secure Analytics, or to orchestration platforms such as Junos Space Security Director Policy Enforcer.	Provides insights into ongoing threats within your business by correlating additional data points to not only discover unknown threats but quickly remediate them and reduce the overall cost of a single breach.

Ordering Information

To order a Juniper SecIntel license, or to access software licensing information, please visit the How to Buy page at https://www.juniper.net/us/en/how-to-buy/.

Juniper SecIntel License Overview

	MX Series Routers	EX Series and QFX Series Switches	SRX Series Firewalls
SecIntel feed source	ATP Cloud	ATP Cloud	ATP Cloud
SecIntel feed types	Attacker IPs, C&C, custom allowlists and blocklists	Infected hosts	Attacker IPs, C&C, GeoIP, infected hosts, dynamic address groups, custom allowlists and blocklists, third party
Requires Juniper Policy Enforcer	Yes	Yes	No
License duration	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year	Subscription: 1, 3, or 5 year

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