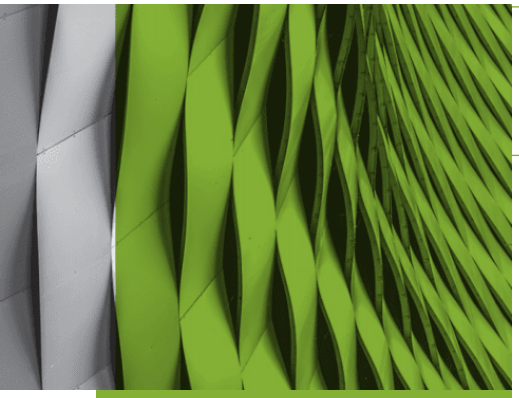

JUNIPER SECINTEL DATASHEET

Product Overview

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

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. SecIntel provides the threat intelligence to identify malicious endpoints, allowing firewall orchestration to enforce policy at every point of connection—including Juniper's patented one-click automation. 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 Firewalls, and non-security devices like 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), Juniper's cloud-based service, and third-party threat data and threat information. It covers industry-specific threats that customers can integrate into their solution. EX Series and QFX Series switches, and our Mist wireless solutions benefit from SecIntel's threat intelligence as these devices quarantine and mitigate risk based on policies shared over the network.

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, honeypots, security researchers, and analysts, our dedicated team of researchers offers 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.

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

Plus, Juniper gives you the most effective threat protection in the industry. When you purchase security technology, you trust that it will stop attacks. Juniper has been consistently validated by multiple third-party tests as the most effective security technology on the market for the past four years, with over 99.8% security efficacy across all use cases.

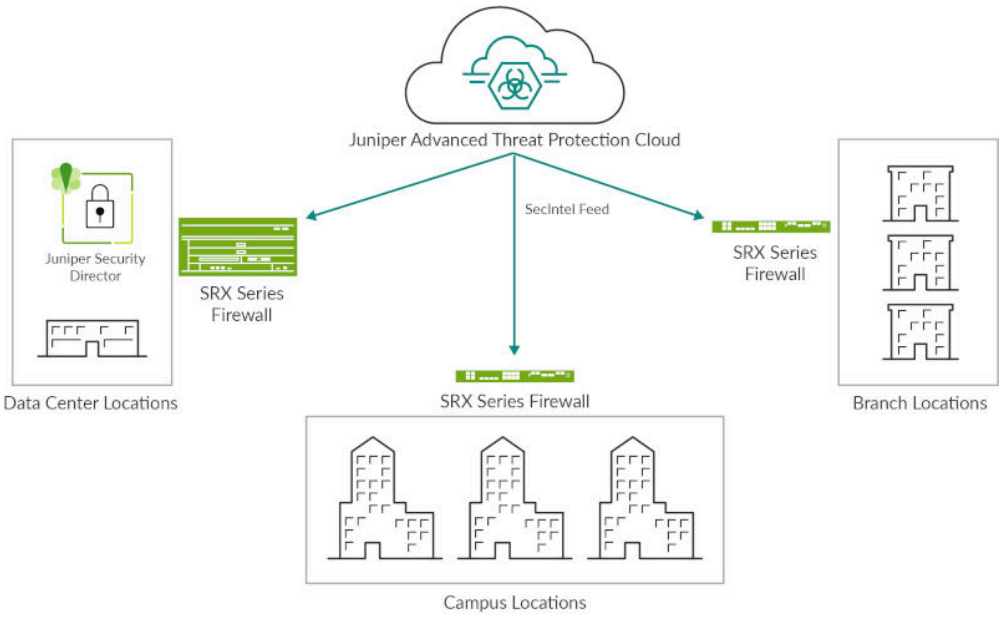

Figure 1: SecIntel on SRX Series firewalls

Architecture and Key Components

SRX Series firewalls use SecIntel threat feeds to offer traffic filtering at both the network and application layers, making identifying and acting upon known threats possible. 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. Configure SRX Series firewalls 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 allowlists and blocklists. 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 integrating 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 protects 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.

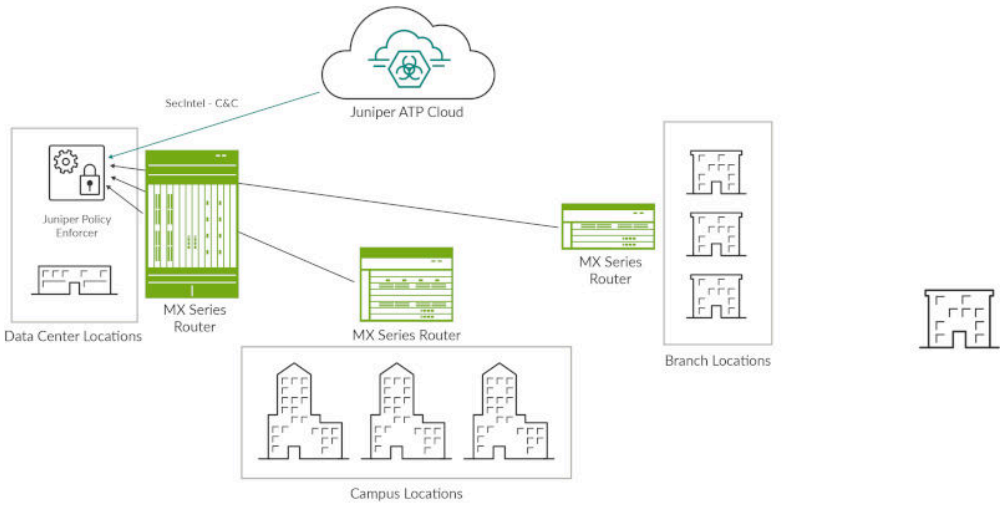

Figure 2: SecIntel on MX Series routers

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).

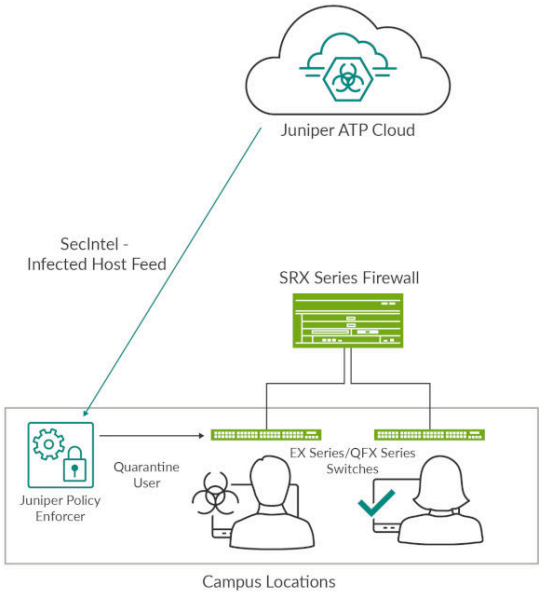

Figure 3: SecIntel on EX Series and QFX Series switches

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, certificate hashes 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 hunt down unknown threats proactively.
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 with 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 is 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 considered security devices as identification and enforcement points on the network.
Comprehensive threat logging and orchestration	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 Security Director Policy Enforcer. SecIntel helps to improve visibility and enable automated incident response.	Provides insights into ongoing threats within your business by correlating additional data points to discover unknown threats, quickly remediate them, and reduce the overall cost of a single breach.

Security Director Cloud

Security Director Cloud is Juniper's simple and seamless management experience delivered in a single UI to connect customers' current deployments with their future architectural rollouts. Management is at the center of the Juniper Connected Security strategy and helps organizations secure every point of connection on their network to safeguard users, data, and infrastructure.

Organizations can secure their architecture with consistent security policies across any environment—on-premises, cloud-based, cloud-delivered, and hybrid—and expand zero trust to all parts of the network from the edge all the way into the data center and to the applications and microservices. With Security Director Cloud, organizations have unbroken visibility, policy configuration, administration, and collective threat intelligence all in one place.

Juniper meets our customers where they are on their journey, helps them leverage their existing investments, and empowers them to transition to their preferred architecture at a pace that is best for business by automating their transition with Security Director Cloud.

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/form.html.

About Juniper Networks

At Juniper Networks, we are dedicated to dramatically simplifying network operations and driving superior experiences for end users. Our solutions deliver industry-leading insight, automation, security and AI to drive real business results. We believe that powering connections will bring us closer together while empowering us all to solve the world's greatest challenges of well-being, sustainability and equality.

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: +31.207.125.700

Juniper Networks | Driven by Experience™