

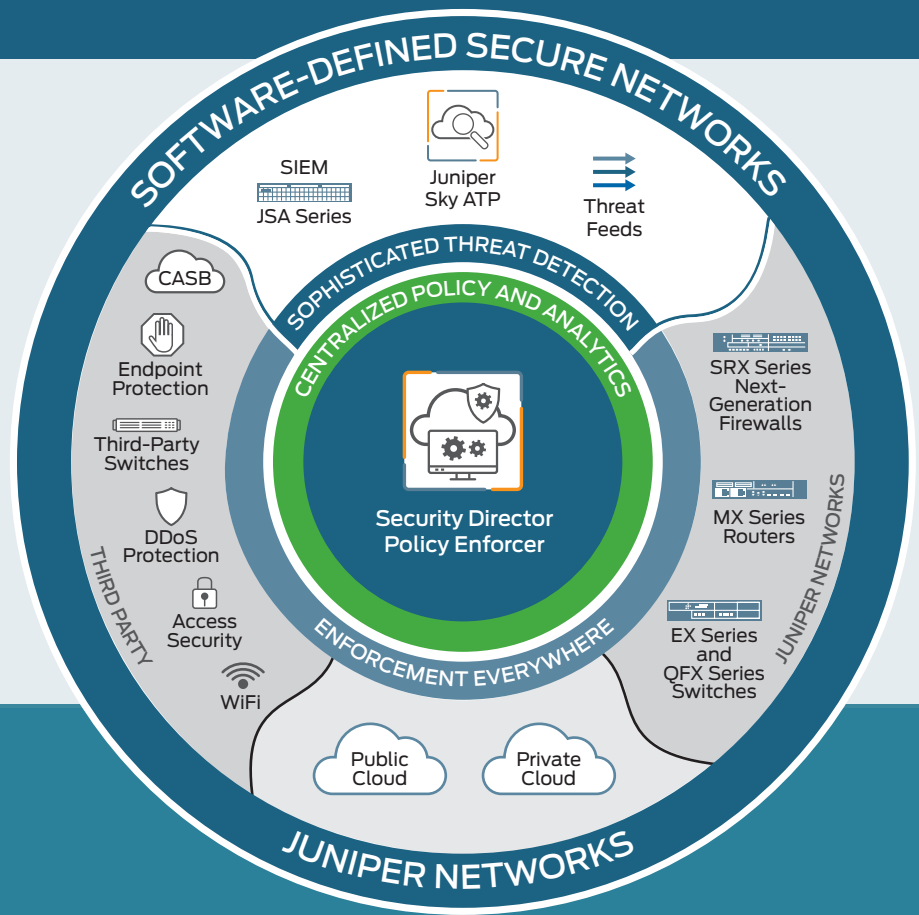
SDSN: Software-Defined Secure Networks

What is SDSN? How does it work?

SDSN is Juniper's cyber security platform that integrates, centralizes, and automates defense from today's sophisticated threat landscape. SDSN automatically and dynamically detects and responds to threats as a whole ecosystem rather than as an individual entity.

SDSN has three fundamental premises:

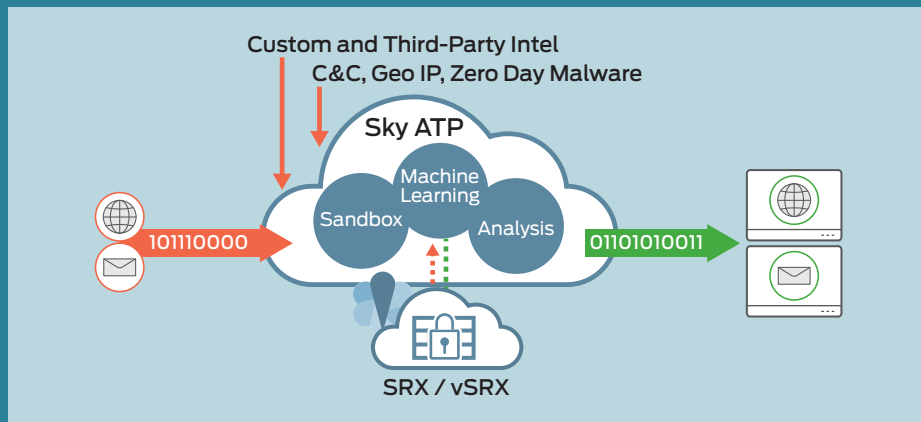
- POLICY** User intent-based system to create security policies to be enforced in the network.
- DETECTION** Gather and distribute threat intelligence, from multiple sources — leverage cloud economics for real time analysis.
- ENFORCEMENT EVERYWHERE** Adapt and enforce policy in real time across the network.



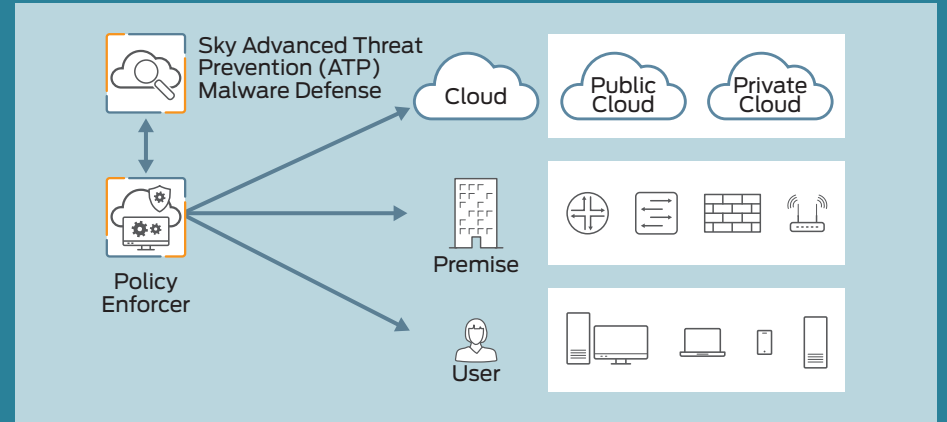
Centralize and Automate Security

Juniper Networks provides the essential building blocks for the foundation of SDSN – so you can start building secure networks and not just talking about network security. Here's how:

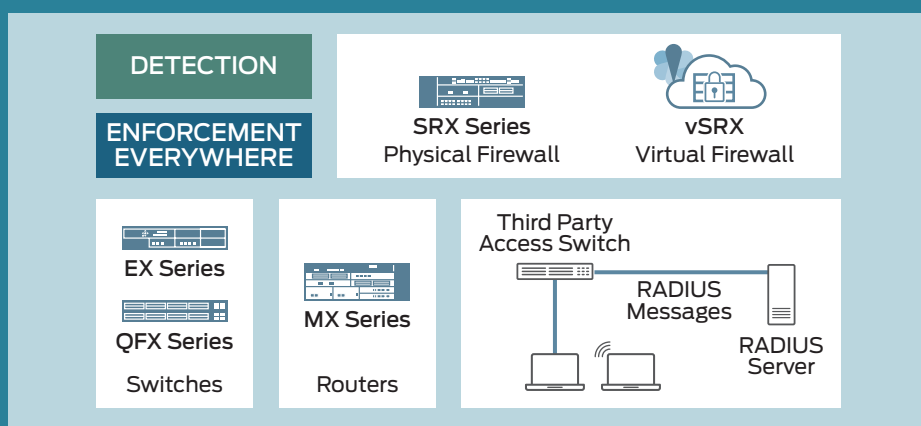
Sky Advanced Threat Prevention, the cloud-based malware detection solution, accurately detects and consolidates known threat information from in-house logging, cloud feeds from command and control (C&C) – both Geo-IP and third-party via REST API, and unknown threats from sandboxing, machine learning, and deception.



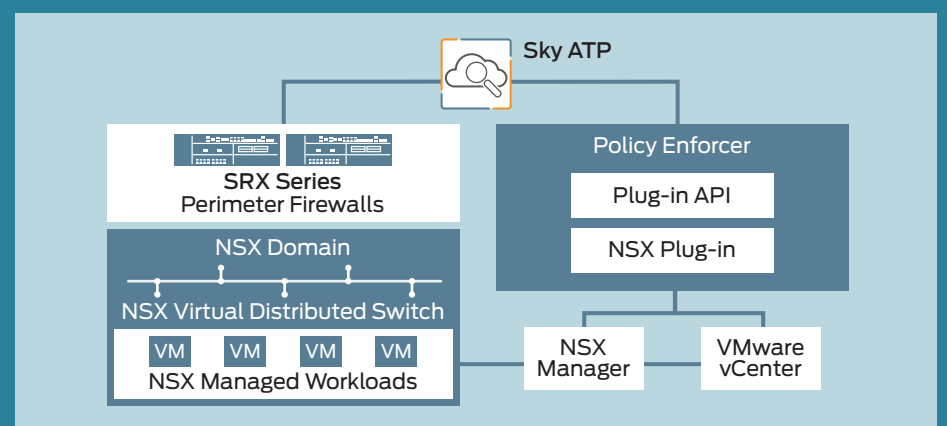
SDSN automates threat remediation workflows and real-time remediation of infected hosts with policy enforcers. Policy enforcers provide communication with multivendor network elements and next-generation firewalls to globally enforce security policies and provide analytics.



SDSN's open, multivendor ecosystem detects and enforces security across Juniper solutions, clouds, and third-party ecosystems by delivering the ability to rapidly block or quarantine threats to prevent further propagation.



The auto-provisioning of vSRX on NSX hosts provides micro-segmentation for private cloud workloads in NSX domain by ensuring advanced security (a Level 7 firewall and IPS) and consistent management experience for North-South or East-West traffic.



Four Steps Toward Deploying SDSN

1. **Upgrade your perimeter** to make it adaptable. The SRX Series is a complete NG firewall that's available today. Simplify and remove niche appliances. Use vSRX for your virtual needs.
2. **Start using cloud economics** for instant threat intelligence and more effective detection, such as Juniper's Sky ATP and Spotlight Secure.
3. **Get visibility into your network** with Juniper Security Director. It can view and analyze your security policies all within a customizable user interface – watch your defense work and learn from it.
4. **Start the transition to the new world** where security policy will be created through an intent-based policy engine with enforcement across all network elements, even third-party vendor elements.

For additional technical resources, please visit: www.juniper.net/documentation/



SDSN Landing Page
Access to resources, news, white papers, and more.
<http://www.juniper.net/us/en/solutions/software-defined-secure-networks/>



SDSN Solution Brief
SDSN in action with the financial services industry.
<https://www.juniper.net/assets/us/en/local/pdf/solutionbriefs/3510608-en.pdf>



SDSN Blogs
Great "Security Now" blogs in the forum pages.
<http://forums.juniper.net/t5/tag/SDSN/tg-p/tag-id/13361/category-id/blogs>

DAY ONE POSTER

SDSN: Software-Defined Secure Networks

Juniper Networks Information and Learning Experience (iLX)