Juniper and Vectra Networks Add New Class of Advanced Persistent Threat (APT) Defense

Combining Data Science and Machine Learning to Detect Advanced Malware

Challenge

Protecting networks against malicious attacks requires constant vigilance. Network traffic must be continuously monitored for threat activity. Once potential attacks are identified, the threat must be contained and malicious activity blocked.

Solution

Juniper and Vectra's joint solution adds a new class of advanced persistent threat (APT) defense, delivering real-time detection and analysis of active network breaches so that they can be stopped in their tracks.

Benefits

The combination of Juniper and Vectra technology picks up where perimeter security leaves off by providing deep, continuous analysis of both internal and Internet network traffic to automatically detect all phases of a breach as attackers attempt to spy, spread, and steal within your network.

The Challenge

As the scale and sophistication of network threats continues to increase, businesses need greater insight into attackers, threats, and the devices used in attacks. Next-generation security has to be built on automated and actionable intelligence that can be quickly shared to meet the demands of modern and evolving networks. SRX Series Services Gateways offer high-performance network security with advanced integrated threat intelligence, delivered on the industry's most scalable and resilient platform.

The Juniper Networks-Vectra Networks APT Solution

Juniper Networks has teamed with Vectra Networks to provide inside-the-network threat detection as a next layer of defense in today's security infrastructure. The Vectra® Networks Automated Threat Management solution brings an added layer of security, analyzing internal network traffic to reveal all phases of an active cyberattack, including hidden Command and Control (C&C) communications, internal reconnaissance, lateral movement, botnet fraud, and data exfiltration.

Once Vectra identifies an infected node, its IP address and threat certainty are pushed to Juniper's Security Intelligence (SecIntel) framework, enabling SRX Series Services Gateways to quarantine the infected device, stop communication with a C&C server, and prevent data exfiltration.

There are two methods to bring feeds into the internal database of Juniper's SecIntel framework where the SRX Series Services Gateways can retrieve and apply the feed information to firewall policies.

- The first is a list of IP addresses or ranges of addresses, without an associated threat score. These are typically used in blacklist or whitelist applications, where a threat level is inferred from the application. Blacklist entries are assumed to be "Bad," while whitelist entries are assumed to be "Good."
- The second data format, used by Vectra, is an IP address with an associated threat level. These mimic the format used by Juniper's own threat feeds. The entries are typically used with SecIntel policies on the firewall, and the threat levels allow a more granular application of the rules. Vectra seamlessly integrates with the Spotlight Secure Connector, giving the SRX Series gateways the necessary intelligence to prevent infected nodes from gaining Internet access, moving laterally, and exfiltrating valuable company data.

Spotlight Secure provides an API that allows Vectra to push data directly into Spotlight Secure Connector. This enables the SRX Series to quarantine the infected device and stop communication with a C&C server.

Features and Benefits

- Delivers real-time detection and deep analysis of active network breaches
- Uses continuous malware threat monitoring to instantly identify any phase of an attack
- Learns new malware threat behaviors and adapts to an ever-changing network and threat landscape

VECTRA® Security that thinks.™

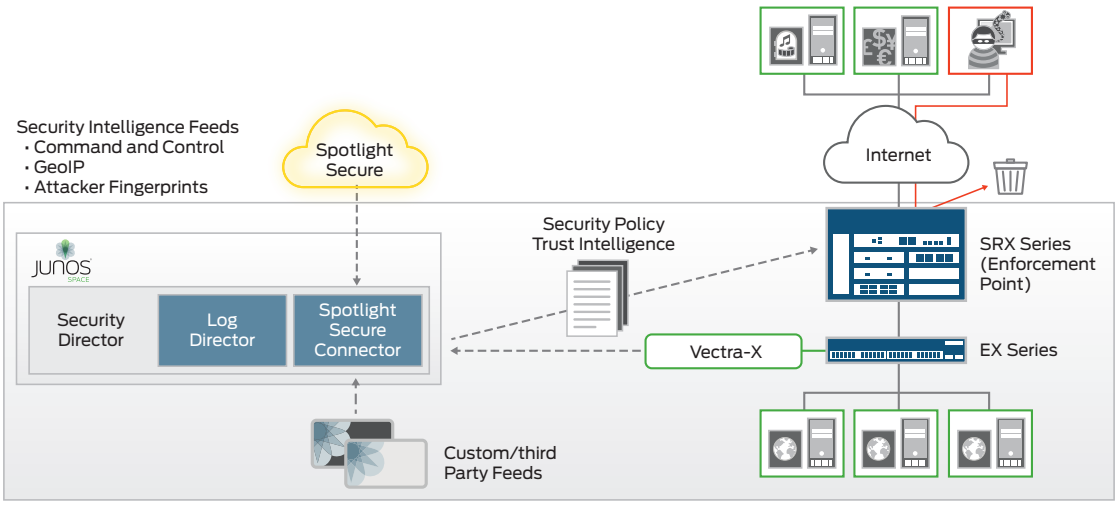

Figure 1: Security intelligence framework

Solution Components

- Juniper Networks SRX Series Services Gateways
- Juniper Networks Spotlight Secure Connector
- Juniper's Security Intelligence (SecIntel) framework
- Vectra Networks Automated Threat Management solution

Summary—Introducing a New Class of APT Defense

With this joint solution, Juniper and Vectra have created a new class of APT defense. By combining data science and machine learning, it provides inside-the-network threat detection as a next layer of defense in today's security infrastructure. Using the Spotlight Secure Connector API, Vectra's Automated Threat Management solution analyzes internal network traffic to reveal all phases of an active cyberattack, including hidden C&C communications, internal reconnaissance, lateral movement, botnet fraud, and data exfiltration. It then feeds this information into the internal database of the open and scalable Security Intelligence (SecIntel) framework, where the SRX Series Services Gateways can retrieve and apply feed information to firewall policies. Vectra's deep and broad network intelligence enables the high-performance SRX Series to quarantine an infected device and stop communication with a C&C server, providing a foundation that secures against the broadest spectrum of threats.

Next Steps

To explore ways that your organization could benefit from the Juniper-Vectra joint security solution, please contact your Juniper Networks representative for more information.

About Vectra Networks

Vectra Networks is the leader in real-time detection of in-progress cyberattacks. Our Automated Threat Management solution continuously monitors internal network traffic to pinpoint cyberattacks inside networks as they happen. Vectra prioritizes attacks that pose the greatest business risk so organizations can quickly mitigate or prevent data loss. www.vectranetworks.com.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

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

3510563-001-EN Dec 2015