VECTRA®

JUNIPER NETWORKS

Juniper and Vectra create a new class of Advanced Persistent Threat defense

Data science, machine learning and behavioral analysis combine to detect targeted attacks

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

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

BENEFITS

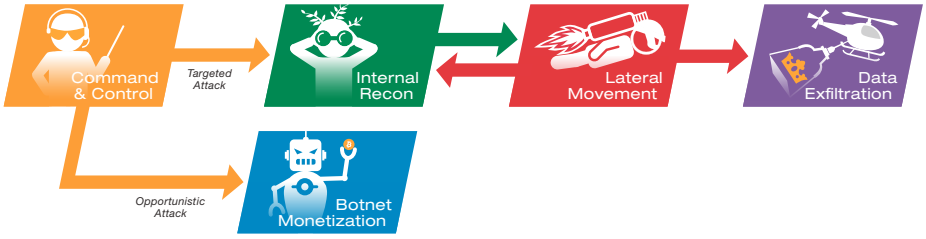
The combination of Vectra and Juniper technology picks up where perimeter security leaves off by providing deep, continuous analysis of both internal and Internet network traffic to automatically detect all phases of an attack as hackers attempt to spy, spread, and steal within your network.

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.

The Vectra-Juniper APT solution

Vectra® has teamed with Juniper Networks to provide inside-the-network threat detection as a next layer of defense in today's security infrastructure. The Cognito™ automated threat detection and response platform from Vectra brings an added layer of security, analyzing internal network traffic to reveal all phases of an active cyber attack, including hidden command and control (C&C) communications, internal reconnaissance, lateral movement, botnet fraud, and data exfiltration.



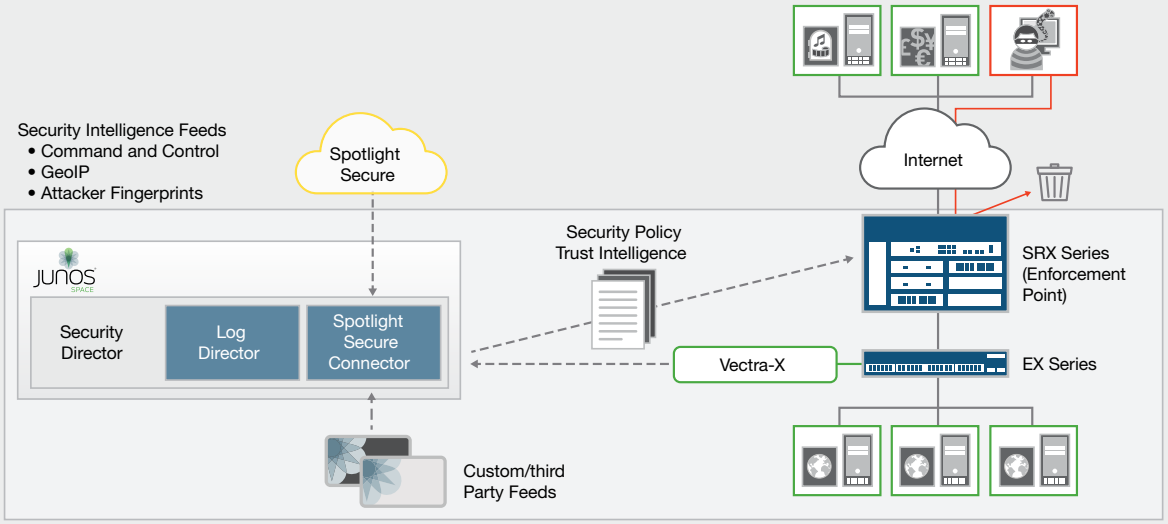
Cognito detects active cyber threats in every phase of the attack kill chain – automatically and in real time

Once Cognito 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 Cognito, 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.

Cognito 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.



The Juniper SecIntel framework

Spotlight Secure provides an API that allows Cognito 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 cyber attacks
- 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

Solution components

- Cognito threat detection and response platform
- Juniper Networks SRX Series Services Gateways
- Juniper Networks Spotlight Secure Connector
- Juniper SecIntel framework

Summary – A new class of APT defense

With this joint solution, Vectra and Juniper 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, Cognito analyzes internal network traffic to reveal all phases of an active cyber attack, 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 SecIntel framework, where the SRX Series Services Gateways can retrieve and apply feed information to firewall policies.

Using artificial intelligence, Cognito 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.

About Vectra

Vectra® is an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 168X. Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint, NAC, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper 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.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai