SOLUTION BRIEF

Automated Threat Containment using Anti-SIEM and Juniper SRX Firewalls

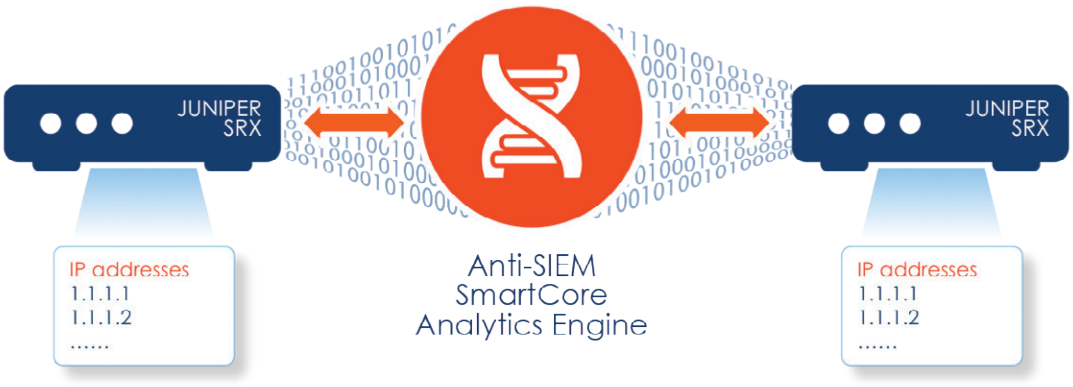
Key Benefits

- Quick containment of most dangerous threats
- Use Juniper SRX Firewalls to deal with APTs
- Reduction in blocking devices at the network perimeter
- Reduce incident response time and cost

Eliminating the Chasm Between Threat Detection and Containment

When dealing with advanced threats, discovering an attack is only one side of the coin. A good security outcome depends equally on the velocity at which an incident response team can deal with the threat and minimize the exposure. Cyphort provides continuous insight and analysis of web, email, and lateral-spread traffic to quickly discover and prioritize advanced threats early in their life-cycle. Once malicious traffic is identified, Anit-SIEM generates threat containment data, e.g., IP Addresses to block IPS signatures of malicious traffic and web URLs that may be involved in either disseminating malware content or maybe acting as an endpoint for command & control traffic. Open API access to this data enables publishing of this data to the existing network security infrastructure including: Firewalls, IPS appliances and Web Security Gateways.

Cyphort and Juniper Networks have created a joint solution that allows customers to automatically publish threat containment data from Cyphort's Anti-SIEM SmartCore analytics engine, directly to the Juniper Networks SRX Firewalls. Customers can create a Dynamic Address Group on their SRX appliances and use that to source containment IP addresses from SmartCore. This integration creates a more scalable open policy enforcement approach. It is also the fastest way to deliver threat intelligence to the enforcement points, enabling customers to contain advanced threats before they can cause damage.



Protection for the Entire Enterprise, Not Just the Segment Where a Threat was Discovered

Typical APT defense appliances need to be deployed in-line to block malware traffic. This approach works for the network segment that is protected by the appliance that was monitoring the identified malware traffic, however other network segments. remain unprotected. Cyphort provides a distributed software security layer that stops threats undetectable by traditional in-line security tools. Cyphort and Juniper Networks joint solution, can publish threat containment data simultaneously to the entire organization, thus protecting all the users not just the ones that happened to be at the location of original malware detection.

Cyphort's Anit-SIEM and Juniper Networks joint solution, can publish threat containment data simultaneously to the entire organization, thus protecting all the users not just the ones that happened to be at the location of original malware detection.

Reduced Costs of Cyber Incident Response

By automating the flow of threat containment data directly to the Juniper Networks SRX Firewalls and using existing firewalls for APT containment, customers can save on both the capital and operational costs of dealing with advanced attacks. With this joint solution, customers can use existing Juniper SRX platform for effective APT defense while also keeping their incident response costs low thanks to the automation.

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

About Juniper Networks

Juniper Networks (NYSE:JNPR) delivers innovation across routing, switching and security. From the network core down to consumer devices, Juniper Networks' innovations in software, silicon and systems transform the experience and economics of networking. Additional information can be found at Juniper Networks (www.juniper.net) or connect with Juniper on Twitter and Facebook.