Automated Threat Containment with Cyphort and SRX Series Firewalls

Eliminating the chasm between threat detection and mitigation

Challenge

Discovering that a cyberattack is underway is only half the battle. A true security solution not only detects an attack but allows the target to rapidly take action to mitigate and contain the attack before any serious damage is done.

Solution

Cyphort and Juniper have jointly developed a solution that allows customers to automatically publish threat containment data from the Cyphort solution directly to SRX Series Services Gateways. This minimizes the impact of intrusive attacks and enables a safe and secure environment.

Benefits

- Quickly contain the most dangerous threats
- Block advanced persistent threats (APTs)
- Reduce the number of blocking devices required at the network perimeter
- Reduce the costs associated with cyber incident response
- Protect the entire organization, not just targeted segments, from APTs

When it comes to dealing with advanced and persistent threats, discovering that an attack is underway is only the beginning. For a security outcome to be considered successful, the threat must be identified, isolated, and dealt with quickly and efficiently by an incident response team in order to neutralize the risk and minimize the exposure. Cyphort and Juniper Networks have joined forces to develop and deliver a comprehensive solution that increases the velocity at which cyberthreats are identified and contained, enabling customers to maintain a safe and secure network environment.

The 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. Threat detection, however, is typically performed by one solution, while the threat mitigation and containment is performed by another. Working together, Cyphort and Juniper Networks have delivered a comprehensive security solution that leverages the best of both product portfolios to protect today’s enterprise networks from intruders.

The Juniper Networks-Cyphort Security Solution

The joint Cyphort and Juniper Networks solution allows customers to automatically publish threat containment data from the Cyphort Advanced Threat Defense Platform directly to the Juniper Networks® SRX Series Services Gateways, enabling them to quickly act to mitigate and contain malicious activity.

The Cyphort solution continuously monitors network traffic for threat activity and generates threat containment data such as which IP addresses to block, the intrusion prevention system (IPS) signatures of malicious traffic, and Web URLs that may be involved in disseminating malware or acting as an endpoint for command and control traffic. Open API access to this data enables it to be published to existing network security infrastructure—including firewalls such as the SRX Series Services Gateways.

Customers can create a dynamic address group on their SRX Series firewalls and use that information to source containment IP addresses from Cyphort Core. This integration not only creates a highly scalable open policy enforcement approach, it is also the fastest way to deliver threat intelligence data to enforcement points, enabling customers to contain advanced threats before they can cause any damage.

Protecting the Entire Enterprise

Typical APT defenses are normally deployed inline to block malware traffic. While this approach works well for the network segment being protected, it leaves other segments such as branch offices and other campuses vulnerable. With the joint Juniper Networks-Cyphort solution, the Cyphort platform can publish threat containment data simultaneously to SRX Series devices deployed throughout the entire organization, protecting all users—not just those at the location where the malware was originally detected.

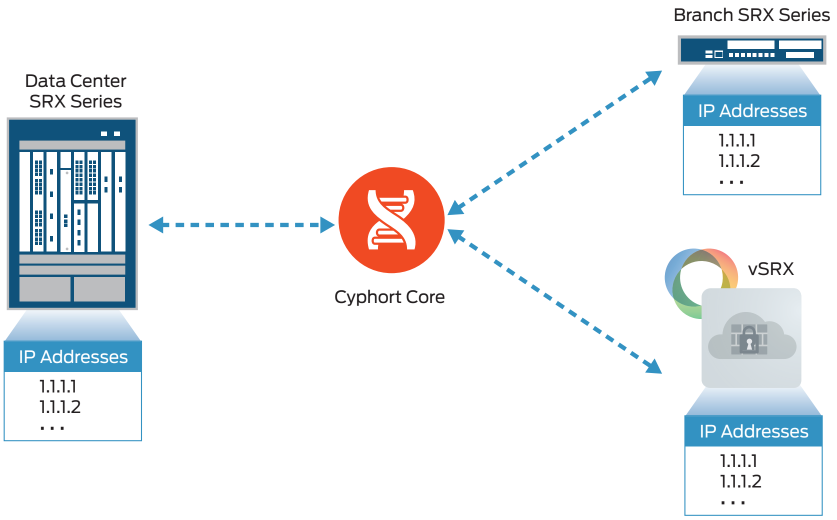

Figure 1: The Cyphort-Juniper automated threat containment solution

Summary—Reducing the Cost of Cyber Incident Responses

With this joint solution, customers can quickly contain the most dangerous threats. By automatically forwarding Cyphort-collected threat containment data directly to Juniper Networks SRX Series firewalls and using them for APT containment, customers can also save on the capital and operational costs related to dealing with advanced attacks. APT defenses using traditional blocking, appliance-based solutions have to deploy appliances at every gateway on the network perimeter. With the joint Cyphort-Juniper solution, customers can use their existing SRX Series platforms for effective APT defense, while keeping incident response costs low thanks to automation.

About Cyphort

Cyphort is an innovative provider of ATP solutions that deliver a complete defense against current and emerging advanced persistent threats, targeted attacks, and zero day vulnerabilities. The Cyphort Platform accurately detects and analyzes next-generation malware, providing actionable, contextual intelligence that enables security teams to respond to attacks faster, more effectively, and in as surgical a manner as their attackers. Cyphort's software-based, distributed architecture offers a cost-effective, high-performance approach to detecting and protecting an organization's virtual, physical, and cloud infrastructure against sophisticated attacks. Malware detection for Windows, OSX, and Linux allows businesses to extract maximum value from IT assets without compromising the security of an organization. Founded by experts in advanced threats from government intelligence agencies and premier network security companies, Cyphort is a privately held company headquartered in Santa Clara, California. For more information, please visit: www.cyphort.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