PREVENT THE SPREAD OF LATERAL THREATS WITH LEVERAGED INTELLIGENCE

Reduce the noise from multiple security solutions and spot threats faster using machine learning and threat analytics.

Why Preventing the Lateral Spread of Threats Is Important

Security engineers are buried in an avalanche of alerts from multiple—and possibly overlapping—solutions. The Juniper Networks® Advanced Threat Prevention Appliances use machine learning and threat analytics data to consolidate and prioritize alerts from multiple threat detection solutions, enabling engineers to deal with what's most important first and moving them from simply managing security to improving it.

Juniper Advanced Threat Prevention

There is a way to harness all the raw data from multiple security solutions and turn it into actionable information, providing critical insights the team can use to quickly identify and mitigate threats. While it may not be possible to prevent a zero-day attack from occurring, a single pane-of-glass view and one-touch mitigation capabilities that aggregate and synthesize data from multiple sources help you identify and stop threats early, before they can do any serious damage.

This is where JATP Appliances come in. Available as a physical platform or in a virtual form, JATP Appliances collect raw data from existing security solutions and use that information to identify threats at different points in the kill chain. Once a threat has been identified, one-touch mitigation can be activated to stop it in its tracks.

JATP Appliances are easy to deploy and do not require existing Juniper infrastructure; in fact, they are entirely hardware- and software-agnostic. JATP Appliances work with your current infrastructure, including existing security products, to provide rich security data. No rip-and-replace is required.

What are the Benefits of JATP Appliances?

When a threat gains access to the network, it spreads fast. This is known as "lateral spread," and this is where the JATP Appliances deliver their greatest benefits.

- *Using machine learning and behavioral analysis*, JATP Appliances detect and analyze threat data by continuously collecting information from Web traffic and e-mail, enabling them to spot lateral threats which have eluded first-line security defenses.
- The JATP Appliances' *analytics engine* correlates and consolidates threat information with event data, presenting a timeline view of the complete security incident.
- The solution's open *architecture* allows for logs to be collected from multiple sources, allowing nonintegrated security products to work together. Collected information is correlated and analyzed by the JATP SmartCore Engine.
- Finally, JATP Appliances allow the creation of *mitigation* policies that strengthen inline security tools against future attacks while isolating infected hosts. These policies are enforced through *one-touch mitigation*.

Because JATP Appliances act as a central point for correlating and analyzing data from multiple sources, they reduce the amount of work required for the security team to spot and mitigate threats entering the network. This, in turn, speeds up mitigation and resolution, allowing the team to focus on making the organization more secure.

- Mitigation and enforcement are accomplished by generating and publishing blocking data to existing firewalls, intrusion prevention systems (IPS), and secure Web gateways, either manually or via APIs.
- Suspect traffic is verified and contained at endpoints before publishing clean data to third-party solutions, including Carbon Black.

Conclusion

Companies struggling to deal with the sheer volume of threat data requiring analysis need a solution that lets them quickly identify and mitigate risks while allowing security engineers to focus on improving security rather than just managing it.

JATP Appliances provide this laser focus on security data using advanced machine learning and analytics across multiple security solutions, showing not only when a threat is spreading across the network but how it gained access and where it can be stopped effectively.

For more information on Juniper Advanced Threat Prevention Appliances, please go to: www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

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