Gaining Total Visibility

Campus IT needs a consistent view into how data flows through the network, cloud and endpoints; otherwise, security will continue to be a hit-and-miss remedy.

Hunter Ely
Security Strategist, Palo Alto Networks

SECURITY THREATS IN HIGHER EDUCATION today are only becoming more automated and obfuscated, making point solutions or the old notion of "best of breed" woefully inadequate. The proliferation of cloud computing, web-based applications and services, not to mention the need to be more flexible in remote work and learning environments, requires the IT organization to come up with a new philosophy for securing assets both on the network and off. After all, traditional firewalls can only see traffic that flows through them. Traditional VPN technologies either hairpin all the traffic back to the firewall, thereby causing bottlenecks and bandwidth concerns, or compromise security through a split tunnel approach.

Neither approach solves the problem of encrypted traffic or provides the granularity to meet specific security requirements for the litany of diverse use cases: the HR department using Azure for its employee system; central IT using AWS to augment the datacenter; increased demand by research for resources to participate in federated projects

To get a taste of the dilemma, one question I often ask campuses is this: "Do you know all of the cloud services that your faculty, staff and researchers are using?" In almost every instance, the institution is a multi-cloud or hybrid-cloud user, and IT doesn't necessarily have a consistent way to secure all of that. Like other aspects of security, every cloud provider has a robust set of security tools, but they're all implemented in wildly different ways. And cloud is just one facet of the challenge.

An Integrated Solution

We can no longer piece together a set of disparate tools to solve acute security or compliance issues. Really, the only way forward is to use a mix of integrated security technologies that deliver, first, a view into traffic and, second, a flexible enforcement model that relies on artificial intelligence and machine learning to identify attacks.

The solution starts and ends with visibility. The goal is to understand how data flows through the network, cloud and endpoints so that IT can provide a consistent security view no matter how services are being used. It's important to understand how your users are tapping those services and to surface those things that traditional tools can't see. As one example, we have a service called **Xpanse**, which will take an outside-in view of the network and start to build relationships, looking at how endpoints are interacting with other endpoints that are outside of the network, contributing to the building of a map showing how the institution is connected to the rest of the world.

Once there's visibility, AI and ML can stitch systems together from a threat perspective. Think about all of your various security measures as sensors. The more sensors you have, the richer the picture you can build. Then you can layer on things like automation to contextualize those threats, understand how they're flowing through the network and take action in an automated way. AI and ML can take the flows, make sense of them and respond accordingly.

> We can no longer piece together a set of disparate tools to solve acute security or compliance issues. Really, the only way forward is to use a mix of integrated security technologies that deliver, first, a view into traffic and, second, a flexible enforcement model that relies on artificial intelligence and machine learning to identify attacks.

Vetted Tools

One of the reasons I love working with colleges and universities is because of their openness and willingness to share what they've learned. The Internet2 NET+

program creates a forum to share experiences, learn from each other and provide access to folks that have solved or need to solve similar technical challenges. To effect change in the security arena, the **University of Nebraska-Lincoln**, under the sponsorship of Chief Information Security Officer Rick Haugerud, brought us into Internet2's NET+ program, sponsoring our work in a **service validation effort**. For the last year we've been working with a handful of institutions, both big and public and small and private, to vet Palo Alto Networks products for fit and to negotiate terms and conditions that are good for the community. That work was recently completed.

The total solution consists of **Prisma Access**, **Prisma Cloud**, **Prisma SaaS and Cortex XSOAR, all supported by Cortex Data Lake**. These solutions address four major facets of security:

- Cloud-native security, to secure campus workloads in the mixed cloud;
- Secure remote access, for learning and working;
- Advanced threat detection, to protect against emerging threats; and
- Automated security operations, to make security modernization easier.

The use of a portfolio approach protects on numerous fronts. Prisma Cloud maintains configuration management across cloud providers, protects workloads in a dynamic way, secures the internal cloud network and keeps tabs on administration entitlement so users can do their jobs while maintaining a compliant and secure environment. Prisma SaaS protects dozens of SaaS services using a similar API approach. Integration of those tools with Prisma Access delivers secure remote connectivity and extended detection and response for endpoint, network and cloud. And the addition of Cortex Data Lake enables all of the alerts and logs generated by Prisma to be processed and normalized in an integrated manner, to develop a holistic view across the network, cloud and beyond.

The big result is that the IT security team gains the visibility and flexibility it needs to support all the various use cases for students, faculty, administration and research teams. Plus, some of those common issues like responding to phishing and other kinds of malware or other frequent attacks can be automated, freeing up the security staff to focus on the harder stuff.

Hunter Ely *is security strategist for Palo Alto Networks and a former assistant vice president for information security at Tulane University.*

Comprehensive Cloud Native Security
With Prisma™ Access

paloalto NETWORKS

paloaltonetworks.com/prisma/access