You Can't Stop What You Can't See

ADAM GELLER

Vice President Of Product Management, *Palo Alto Networks*

Adam Geller is an accomplished technology leader with over 15 years of experience in information security. As vice president of product management for Palo Alto Networks, Adam leads the company's strategy and roadmap virtualization as well as securing public and private clouds.

MILIN DESAI

Vice President, Product Management, *NSBU VMware*

Milin Desai started network virtualization at VMware and leads a team that sets the product direction and roadmaps for VMware NSX. With a global responsibility and perspective, he is responsible for taking customer input and steering NSX to address the market's biggest demands.

TAKING AN INTEGRATED APPROACH TO SECURITY PROVIDES VISIBILITY WHILE DELIVERING VALUABLE ANALYTICS AND ENABLING AUTOMATION FOR GREAT BUSINESS AGILITY.

As cloud converges with the ongoing digital transformation, keeping pace with technology—and competitive forces—is a constant challenge. Unfortunately, with each technology evolution, the sophistication level of hackers intensifies. This means organizations need to make necessary adjustments, moving away from inconsistent, often manual approaches that leave them unnecessarily vulnerable to costly attacks. Adam Geller and Milin Desai explore why an integrated approach to security is the answer.

How is the security landscape evolving, and what does this mean to today's enterprise?

Adam Geller: There's a significant faction who wonder if prevention is even possible or if it's more important to focus efforts entirely on detection and remediation. The Palo Alto Networks position is that prevention is too critical to give up on, especially since it's essential to achieve a holistic security strategy. After all, if you have a breach and information leaves your network, there's no way to get it back. Without investing in prevention, you aren't even giving yourself a chance. Nor are you reducing the surface area of attack for detection purposes. You need a consistent security posture both at the network perimeter and within the data center to do the important job of prevention.

Milin Desai: Prevention is a big piece of the puzzle, and it starts with visibility. VMware NSX enables visibility and enforcement for east-west traffic patterns and alongside Palo Alto Networks enables full visibility throughout the infrastructure. Together, we have a set of policies across all traffic flows to ensure prevention and enable analytics to, for instance, determine disallowed communications. As a result, you can enforce very robust security postures.

What are some of the challenges around point-based security solutions?

A.G.: Point-based solutions have limited contextual awareness to deal with a diverse range of security threats. As a result, you have limited visibility, allowing for potentially dangerous blind spots. However, with our ability to inspect east-west traffic flows between data center servers,

> "Point-based solutions have limited contextual awareness to deal with a diverse range of security threats."
>
> – Adam Geller

You Can't Stop What You Can't See

we enable visibility into places not seen with traditional perimeter solutions. Visibility enables you to reduce the surface area of attack and filter out what doesn't belong. Point-based solutions also struggle to detect unknown malware, which can only be detected with in-depth content analysis and recognition of malicious behavior. A prevention mindset starts with identifying new and unknown malware and defining advanced security measures that can be automatically pushed out to the firewall to ensure that malware can never come through again.

M.D.: Security threats are changing and a single vendor approach is not always 100 percent effective. However, multiple vendors working together raises the bar. VMware NSX provides a platform that enables us to work in conjunction with Palo Alto Networks VM-Series virtualized next-generation firewall to share real-time information on applications that provides context for tighter security. VMware knows what workloads are running and where they are installed—information that is shared with Palo Alto Networks to prevent rogue application behavior.

> "Prevention is a big piece of the puzzle, and it starts with visibility."
>
> – Milin Desai

How does an integrated approach to security address the limitations in point solutions?

A.G.: With an integrated security approach, you can significantly improve the security posture because an attacker has to be successful in multiple stages (i.e., breaching the perimeter, delivering the malware, exfiltration, etc.). Point products focus on one phase of the attack lifecycle; that gives you little chance to succeed, especially when it's a new form of attack. However, with an integrated approach, you have multiple opportunities to prevent damage.

There is also added advantage of security policy consistency and automation. Specifically, if a policy is in place to secure a particular traffic flow—for instance, from a web tier to a database tier—once it's defined it shouldn't matter if there are five or 50 web servers. The scale challenge shouldn't require any rule changes. Our integrated approach allows information sharing and automatic updates to the security policies. This is valuable because we can tell VMware when a specific webserver has been compromised, allowing for quarantine and prompting other actions to remediate the issue.

M.D.: It can take significant time to implement security, which slows down business. However, if we can operationalize security, businesses can be more agile and competitive, resulting in the delivery of applications faster. Given NSX's unique position next to the application, we are able to provide visibility and control points aligned to applications. Historically we were siloed boxes coming together, capturing only glimpses into the data center. With our integration, virtualized next-generation security deployment and operations is now automated, and the appropriate application traffic can be steered transparently—with no network configuration changes.

What can organizations expect when engaging with the VMware and Palo Alto Networks team?

A.G.: The level of interaction we have creates a seamless workflow for managing security risk within an organization. And the shared success that comes with it is hard to achieve with informal arrangements. As such, security is not an afterthought that's simply bolted on, but delivered with the required native integration. Without it, artificial humps exist; people don't do it, or do it in an inefficient way that heightens the risk. This teamed approach toward managing risk results in significant business benefits.

M.D.: When businesses are looking at IT as a whole, automation is always top of mind, and the driver behind that is time to market. But what often slows a business down is delivering a security model to fit. Integration without security is hard to accomplish. Because of the relationship between VMware and Palo Alto Networks, we can uniquely deliver on the goal of security with automation, allowing businesses to meet their needs to competitively deliver applications with agility.