Disparate Security Vendors and Too Many Tools

Niall Browne and Janice Tung of Palo Alto Networks discuss how organizations can accelerate cybersecurity transformation with consolidation.

Niall Browne is the Senior Vice President and Chief Information Security Officer (CISO) at Palo Alto Networks. Niall leads the security team that is responsible for helping secure the company's services. Before joining Palo Alto Networks, Niall was the Chief Security Officer (CSO) and Chief Trust Officer at Workday.

Janice Tung is the SVP, Finance for Palo Alto Networks, responsible for managing and driving the company's financial results. Before joining Palo Alto Networks, Janice was the Vice President of Worldwide Sales Finance at VMware, where in addition to her responsibilities of overseeing the financial activities for the global sales organization and driving top-line growth, she also led cross-functional efforts in policies, processes and systems to enable the company's transformation to SaaS.

Today's cyberthreats occur with more frequency and severity than ever before. 96% of CXOs have experienced at least one breach in the past year. The latest attacks target vulnerabilities in networks, cloud and endpoints, using tools like AI to bypass traditional cyber defenses. But most organizations are ill-equipped to manage a sophisticated cyberattack, with an array of disparate point solutions scattered throughout their environment. To stay on top of emerging threats, organizations need to consolidate their security and implement a holistic platform approach.

In this interview, Niall Browne and Janice Tung of Palo Alto Networks discuss the evolving threat landscape and recent security trends as well as recommendations for how organizations should approach security consolidation to accelerate cybersecurity transformation. The conversation was moderated by Tony Goblirsch, VP – U.S. CSP Sales at Palo Alto Networks.

The importance of simplicity

TONY GOBLIRSCH: Let's start with a discussion about the importance of consolidation. Why is it more important now than ever before for organizations to streamline and simplify their cybersecurity environment?

NIALL BROWNE: Over the last number of years, there's been a tremendous number of acquisitions across the industry. Everyone has an array of different security tools. One of the things I've learned about security is you can't protect everything if your attack surface is too wide. If you've got too many tools, if there are too many "front doors into your castle," so to speak, you are leaving yourself open to intrusion and theft. I've always firmly believed that the biggest "bang for your buck" that any CISO can deliver is partnering with the financial team to consolidate tools and reduce the attack surface, making it much more difficult for attackers to compromise your environment.

NIALL: We can all agree that choice is good. But sometimes too much choice is bad. No CISO has ever said, "I'm doing a great job because I've got a lot of cybersecurity tools." They always complain about having too many tools. Across all industries, most CISOs are running about 75-85 security tools. That creates absolute chaos in most organizations. Imagine 75 people in a room speaking 75 different languages trying to communicate with each other. As you reduce the amount of tools and technologies that you're leveraging, you get way more efficient in securing your infrastructure and your environment.

NIALL: The other problem with having too many tools is the vast amount of time required to run them. That's literally all cybersecurity teams are doing sometimes. Are they detecting the bad guys? Are they stopping them from getting in? The answer for the most part is "no," because they're continuously updating and patching security tools. It's very, very easy for CISOs to fall into the trap of perpetually running tools and technologies rather than solving security problems.

> As you reduce the amount of tools and technologies that you're leveraging, you get way more efficient in securing your infrastructure and your environment.
>
> **— Niall Browne, CISO, Palo Alto Networks**

The financial impact of consolidation

TONY: When organizations are searching for opportunities to save on operational and capital expenses, what areas should be considered investment areas versus just keeping the lights on?

JANICE TUNG: In terms of investment areas, I would first look at things that drive the overall shareholder value and long-term growth or benefits for the company. Even if that means investing in something currently where you don't see immediate results, but it's something that would pay off in the long run. When it comes to keeping lights on, there are certain things that we have to do that are foundational to keeping the business going. Those are operational activities where you want to look for efficiencies. How do you get the most bang for your buck? How do you become more productive and more efficient? Keep the lights on, but find efficiency over time.

TONY: What are some of the data points that you consider when you look at evaluating budgets?

JANICE: First, I look at what kind of business outcome we're trying to drive in terms of investments. We evaluate multiple solutions with different vendors to determine what will help us achieve better business outcomes and drive results through consolidation. It's important to ask, "Do we have to do everything right now? Or can we do it over a period of time?" Making these types of decisions requires a well-thought-out business proposal that examines not just the technology but also the financial impact.

> It's important to ask, 'Do we have to do everything right now? Or can we do it over a period of time?' Making these types of decisions requires a well-thought-out business proposal that examines not just the technology but also the financial impact.

— Janice Tung, SVP – Finance, Palo Alto Networks

The benefits of a platform approach

TONY: What are the benefits of consolidating security vendors and moving away from point tools and manual processes to a more integrated security platform?

NIALL: I think the big one is communications. When an attacker comes in, they'll move laterally across the network. They may touch 20 tools. Imagine 20 people shouting at you that something is wrong. The SOC is going to get overwhelmed with all the alerts and events. They're not going to be able to understand and analyze an attack from just general comms. It's going to cause chaos. When you have that many tools, the problem is they're not communicating back and forth. There are no integrations, and they don't want to speak to each other. Most security tools are not designed to integrate with other tools.

NIALL: A platform is one infrastructure, one environment and one single pane of glass with clear visibility. When an attacker starts to move laterally, now instead of 20 tools shouting at me, I've got one platform that's detecting it and blocking it every single step along the way. That's extremely powerful. It costs less, it's less data to manage, and it's a single platform that you can respond to. No matter where your users are, at the headquarters, at home on a mobile device or working from a branch, the platform provides the same level of security across the board. With only two or three disparate protection products in your environment, your headquarters might have great security, but then users at home might have terrible security. That's why most organizations see the platform approach as the way forward from an engineering and security perspective. There is no alternative. Reduce the sprawl, save costs. It's a great opportunity for security teams to partner directly with finance because at the end of the day it's two parties going in the same direction.

JANICE: Consolidation and simplification while getting to a more finite number of vendors in a platform approach also makes a lot of sense from a business perspective. Consolidating our contracts and having better negotiation power drives better financial outcomes. With our sourcing department, only having to negotiate a couple contracts versus 20 or 30 different contracts drives a lot of operational efficiencies both from a business perspective and from a financial perspective. Limiting your purchasing to one vendor or a few vendors delivers hard cost savings. Our research shows that organizations can reduce their total cyber spend by up to 30% through consolidation.

Making a plan for consolidation

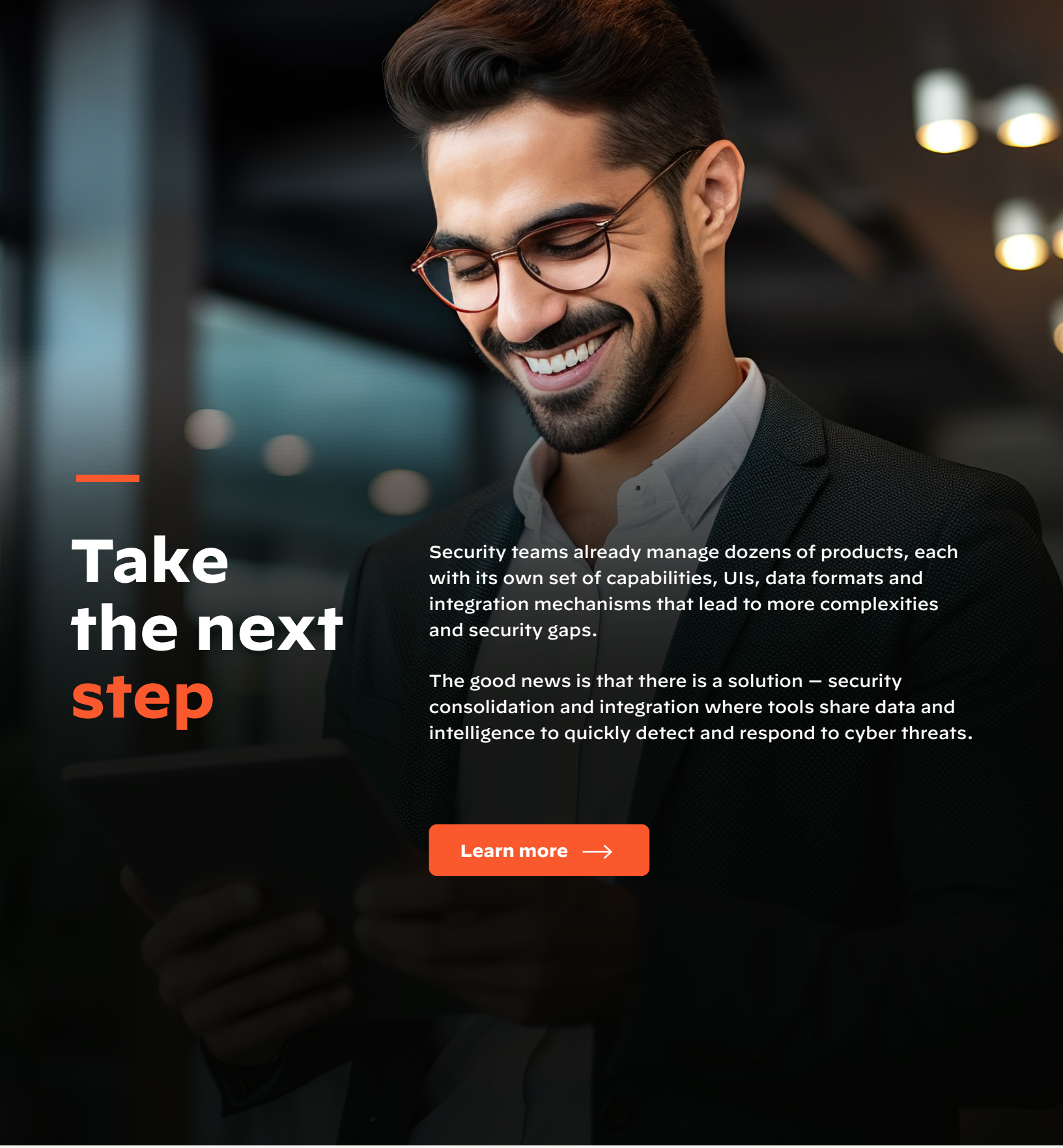
TONY: How can security teams build a business case for consolidation that they can take back to their leadership? What are the most important questions, considerations and recommendations when evaluating cybersecurity partners?

JANICE: I would say it all starts with the business outcome. What is the ultimate goal that you're trying to achieve? Be upfront as to what problem you're trying to address. Read the technology reviews. Perform the appropriate testing and evaluation that validates your desired business outcome. Understand the financial impact and the operational impact this could potentially have for the company. You also have to ask the right questions. What risk are you mitigating? What problem are you trying to solve? What happens if you don't do this, what kind of impact could it have? What are things that we can phase out as part of this process? When it comes to a vendor, you need to think about whether or not that vendor is going to be around for the long term. What does the journey with this vendor look like?

JANICE: In addition to understanding the desired business outcome that you're trying to drive, you have to understand all the tools you already have deployed. How much are you spending on those things? What is the cost benefit of consolidating? You also need to be able to clearly articulate how this consolidation will take place. It's not just about timing. You're most likely not going to do it all in one shot, so how do you phase it in efficiently? You need to develop a methodical way to approach the project and then bring in both the business outcome and the financial impact.

NIALL: Effective consolidation is not a "one and done" effort. Cybersecurity must be continuously evaluated if it is to be effective. It's important to think about consolidation as part of a larger cybersecurity review process that incorporates examining IT spend as well as the current risk landscape. Consolidation is vital not just from a security perspective but also as part of any organization's business and technical strategy.

NIALL: With a platform approach, people will soon realize that they don't need all those point solutions anymore. But you have to negotiate with the cybersecurity owners in parallel as you migrate to a platform approach, because they were probably the ones who made the decision to buy these tools in the first place. It's not going to happen overnight, but I would say within a year, the organization will have started to make significant inroads to reducing their point solutions. Start with the tools you haven't logged into in six months. That might be almost half of them. The executive buy-in is easy, but if you can get the practitioners to get on board as a partnership, it's going to be a much easier transition.



Take the next step

Security teams already manage dozens of products, each with its own set of capabilities, UIs, data formats and integration mechanisms that lead to more complexities and security gaps.

The good news is that there is a solution — security consolidation and integration where tools share data and intelligence to quickly detect and respond to cyber threats.

Learn more →

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com