Our POV: ESG Brief on Cybersecurity Vendor Consolidation Efforts

By Nir Zuk, Founder and CTO, Palo Alto Networks

In August 2020, analyst firm ESG published findings from a survey on enterprise-class cybersecurity vendor sentiment regarding vendor consolidation efforts.

What is in the report?

The ESG brief contains the analysis of organizational vendor consolidation efforts from the firm's enterprise-class cybersecurity vendor sentiment survey.

Why is it important now?

Enterprises today are confronted with massive tool sprawl, resulting in inefficiency, ineffectiveness, and additional risk that comes from failing to prevent, detect, and respond to attacks quickly. As many enterprises are undergoing network transformations, they're also reevaluating their current technology stack, seeking greater effectiveness and alignment with their transformed networks.

Key takeaways:

- **63% of survey respondents reported having more than 25 unique cybersecurity products currently in use.**
- **77% of survey respondents were actively consolidating the number of cybersecurity vendors they use as a means to address the current approach of disconnected point products.**
- **The top three most important attributes for a cybersecurity vendor, according to survey respondents, are:**
  - **» Industry-specific expertise (35%).**
  - **» World-class threat research and threat intelligence (31%).**
  - **» Broad portfolio of cybersecurity products (28%).**
- **The most important factor in deciding to purchase a product is its ability to prevent/detect threats (41%).**
- **ESG predicts that enterprise-class cybersecurity vendors will dominate the market and the remaining vendors will become ecosystem players, forming tight partnerships with the cybersecurity platform vendors.**
- **Organizations are looking for a platform: a tightly integrated suite of products from a single vendor with integration capabilities for third-party vendors and software developers.**

Our Advice for Leaders: Uncover Areas of Opportunity for Vendor Consolidation

Over the years, as new threats and threat vectors have arisen, large cybersecurity vendors have either ignored the growing challenges or failed to address them. Simultaneously, each new challenge has introduced a new set of vendors solely focused on addressing that specific problem. The result has forced security teams to deploy, manage, and manually stitch together alerts and insights from a growing set of individual products and varying data sources.

Today, ESG's research validates vendor consolidation as something organizations find value in and are actively pursuing. It has proven extremely beneficial in terms of efficacy and efficiency—but it's also extremely hard to do. There is a long history of older technologies embedded in the architecture that are challenging to rip and replace.

I am not suggesting that vendor consolidation is not the right path. On the contrary. Tool sprawl results in inconsistency and subpar security. My suggestion is that for organizations going through network transformations, there are areas of opportunity for vendor consolidation that make much more sense in terms of investment. The top three areas that are transforming and would benefit from a single-vendor platform approach are: cloud security, next-generation WAN, and next-generation SOC.

Cloud Security

As enterprises move more and more of their data centers to the cloud, they need to replicate what was done for enterprise security in cloud environments. This includes the risk, governance, and security functions. When evaluating your cloud architecture, there are three different paths you can take:

1. Use 25+ vendors to secure your cloud environments, the same approach taken for the network.
2. Use native cloud security, which lacks most of the necessary functions to secure your cloud environments and does not support a multicloud approach.
3. Use a cloud native product that provides all the functions in a single platform across all locations.

A vendor consolidation approach may be difficult in the traditional enterprise, but there is little excuse to repeat old mistakes for the cloud. This is an opportunity to do it properly because all enterprise cloud strategies are starting from scratch.

Next-Generation WAN

Traditionally, "access" meant access to applications in physical data centers. Enterprises would use MPLS for branch office access, remote access VPN or client VPN for user access, and clientless VPN and/or IPsec VPN for partner access. Now that applications are moving to the cloud, new technology is required. It no longer makes sense for these technologies to access the data center and move outwards to the cloud.

Similar to the cloud, this is an opportunity to rearchitect the WAN and do things right. You can purchase multiple solutions to secure access to the cloud for your branch office, user access, and partner access; or you can consolidate access for all of these users and locations into a single platform.

A multivendor approach does not provide consistency—using a single-vendor platform does. It provides the same security to all users, wherever they are in the world and for whatever they are trying to access, whether on traditional infrastructure or next-generation infrastructure, like the public cloud or SaaS.

Next-Generation SOC

The security operations center is yet another area that is ripe for being rearchitected to a single-vendor platform due to the need for automation. Automation for the SOC has two aspects: SOAR to automate playbooks and processes, and automating things that don't have procedures using machine learning.

For things that don't have procedures, the industry is going down a familiar path, requiring organizations to use machine learning across multiple tools, such as EDR, NTA, and UEBA. With these tools, machine learning is limited to the data available from an individual data source. To properly leverage machine learning and automation, a single-vendor platform is key because machine learning improves as it ingests more data from various sources. The need to rearchitect the SOC for improved machine learning and automation presents an opportunity to do what the ESG survey shows: consolidate vendors.

Capture the Opportunities Transformation Creates

For organizations currently undergoing network transformation to bring more and more into the cloud, continuing down a multivendor approach will result in inconsistent and subpar security that will cost far more than it should. If you're undertaking a transformation, consider the many business reasons for consolidating your vendors. These greenfield deployments present an opportunity to get better security and consistency from a platform approach that also enables easier management, compliance, and auditing.

See the full report

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