REDUCING THE BUSINESS RISKS OF CYBERTHREATS:

Make Smart Investments in Next-Generation Security

Executive Summary

Your organization's approach to cybersecurity can either securely enable your business to innovate and make use of transformational technologies, like the cloud, or it can introduce unnecessary risk and complexity. In this era of advanced threats and mega-breaches, organizations face an increasingly sophisticated adversary, aided by automation and the power of the cloud. Those companies still relying on largely manual methods to deal with such threats are now seeking ways to adjust to the changing landscape.

The approach that worked in the past is no longer suitable to meet today's needs. In fact, this combination of the older or "legacy" approach to security, combined with the increasing sophistication of threats, creates a set of technology risks that translate very directly to business risk. As we have seen in highly publicized examples across industries, cyber risks can penetrate to the revenue-generating core of any business. Security breaches can lead to an inability to service customers, damage to brand image, and legal liability.

In order to properly mitigate such risks to the company's ability to generate revenue, companies need to run their business on highly resilient platforms that have the ability to automatically protect themselves from advanced cyberthreats. This new approach leads to a reduction in operational complexity and cost and, most importantly, reduces risk to the company's ability to reliably serve customers and generate revenue.

As a senior leader, executive or corporate board member, you should understand the difference between the old paradigm and the new and how it impacts the risk to your business. This will allow you to engage with your technical teams to understand where you are today and lead them toward securely enabling your business with the automated, resilient and integrated security platforms needed to reduce business risk well into the future.

Legacy Security Architecture

In this new age of next-generation security platforms, we often refer to "legacy" security architectures that represent the old paradigm and mindset. It is worthwhile to define this architectural mindset and why it made sense at one point. This understanding is key to uncovering the reasons why next-generation security platforms have become the new standard for preventing and responding to modern cyberthreats.

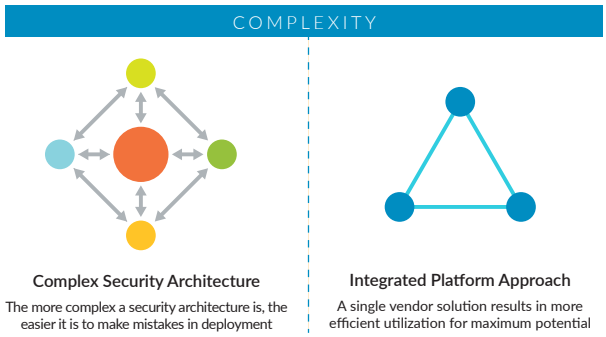

Figure 1: Legacy approach vs. integrated platform approach

Legacy Architecture Defined

Security tools have traditionally been only moderately effective at detecting threats. This fact gave rise to the legacy architectures that comprise multiple redundant security tools. There are certain advantages to having multiple layers of protection and the "defense-in-depth" concept is rooted in that logic. However, there is a line between smart, multilayered security architecture and the

highly redundant architecture with which most organizations ended up. These wasteful models often include some or all of the following:

- Network firewalls or UTM blades
- Web application firewalls
- Web proxies
- Intrusion Detection or Intrusion Prevention Systems (IDS/IPS)
- Anti-advanced persistent threat (APT) appliances (sometimes one for each protocol to cover HTTP, SMTP, etc.)
- Email antivirus
- Endpoint antivirus
- … and the list goes on

The strategy was to choose the best product in each category and layer them. This led to a cumbersome mix of appliances and software that needed to be managed and maintained and, more importantly, an unmanageable volume of alerts being generated by all of these tools. According to one survey, organizations spend over $1.27 million in wasted effort each year chasing down alerts that are largely false positives.[1] Because of the operational overhead, many of the tools were deployed with less than optimal configuration. It simply took too much administrative overhead to fine-tune each tool and turn on all of its capabilities. New features and software versions would come out, and they would largely be ignored because security teams were so busy trying to keep up with the deluge of alerts. The potential value that these solutions offered was never realized because 1) they weren't finely tuned or optimized at initial deployment, and 2) they were neglected and allowed to go out of date shortly after deployment.

The deluge of alerts led to the adoption of new tools that attempted to stitch together the disparate systems and make some sense out of the logs and alerts. With so many different vendors involved, it was difficult to correlate events or take any automated actions. Security operations teams had to manually view alerts from multiple systems in order to investigate an incident. Even with the adoption of security information event management (SIEM) tools, it was an uphill battle.

The traditional architectural model also suffered from another key limitation: lack of visibility. With the volume of encrypted traffic steadily on the rise, it became increasingly difficult to monitor that traffic. According to some reports, approximately 70 percent of internet traffic will be encrypted by the end of 2016.[2] With appliances often attached to network taps and span ports, in-line decryption was typically not within reach. Many organizations simply chose to turn a blind eye to encrypted traffic.

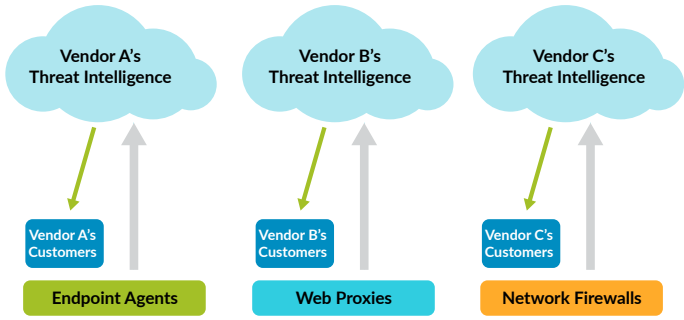

Figure 2: Legacy architecture defined

Over time, the effectiveness of such tools as antivirus software declined to severely insufficient levels as threats evolved from standard off-the-shelf malware to more advanced and targeted threats. As this saga unfolded, mega-breaches were on the rise. Some security vendors saw this rise in breaches, declining effectiveness of security tools, and increasingly overwhelmed security operations teams as an opportunity to sell more incident response services and remediation tools; in some cases, even moving from the products business to the services business to capitalize on that pain. Others tried to determine why we reached this place and how to best create tools that would turn the tables back in favor of the good guys.

Reasons Legacy Architecture Made Sense

One of the main reasons this sort of legacy architecture made sense at the time was the simple fact that true security platforms did not yet exist. Each security tool was designed to address a separate problem; one tool for web security, another for email security, another for network intrusion detection, others for antivirus, and the list goes on. These tools usually did not integrate with each other. So it made sense to simply choose the best tool for each job and use them all.

To make matters worse, each security vendor collected valuable threat intelligence from its customers and kept that threat intel private in order to provide value to its own customers, but not the broader community. Threat intelligence was thought of as a competitive advantage, thus shielding the big incumbent players from competition by smaller innovative players who did not yet benefit from a large customer base. Because each vendor had its own proprietary threat intelligence, it made sense as a security architect to diversify security vendors. With a vendor diversification strategy, an organization could benefit from the knowledge of multiple proprietary repositories of threat intelligence.

These unfortunate technical limitations and business practices necessitated an architectural approach that resulted in numerous appliances, agents and tools layered on top of each other. It's no wonder that security operations teams have been overwhelmed with alerts and administrative overhead, turning the economics in favor of the adversary.

Next-Generation Security Architecture

We now live in an age of next-generation security platforms. It is no longer necessary to deploy dozens of tools from tens of security vendors. Integrated and automated platforms are available to prevent the most advanced threats, reduce the clutter, and relieve the burden on security operations teams.

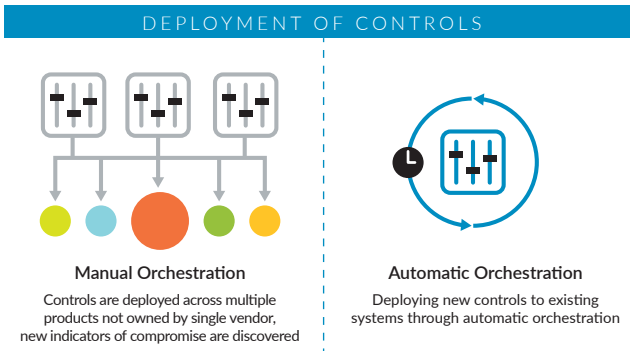

Figure 3: Deployment of controls

Next-Generation Architecture Defined

There are four core capabilities that comprise a next-generation security architecture:

1. Provide complete visibility.
2. Reduce the attack surface.
3. Prevent known threats.
4. Prevent unknown threats.

Complete visibility is a fundamental requirement because you cannot protect what you cannot see. In order to gain complete visibility, you need to have both the right vantage point and the right capabilities. This means the security device needs to be placed at the right point in the network to see all traffic. The firewall is the logical place for this inspection because it is the one security device through which all traffic should flow. Add-on devices are less likely to be so well-positioned. In addition to position, the device must understand what it can see. This means it needs the ability to decrypt traffic, and it must have a deep understanding of each application protocol.

Many approaches to security have stopped at trying to prevent or detect known threats. Next-generation security involves preventing the unknown. The most advanced attacks will not rely on recycled methods. They will be specifically crafted with one target in mind, using completely new techniques that have never been used before. Preventing these types of threats is imperative if we are to turn the tables back in favor of the good guys and thwart today's adversaries. In order to prevent unknown threats, it is necessary to rapidly turn unknown objects into known objects by leveraging rapid dynamic analysis, static analysis, and machine learning at scale.

Rise of the Next-Generation Security Platform

A next-generation security platform provides all of the capabilities defined above in a single integrated and automated platform comprised of devices, software and cloud-based services working in concert.

You may recall that one of the reasons used to legitimize the legacy architectural models of the past was the need to diversify security vendors in order to gain the benefit of each vendor's unique threat intelligence. That need no longer exists. Today's next-generation vendors are putting their customers' best interests first by sharing threat intelligence. The Cyber Threat Alliance (CTA) is a group of leading cybersecurity solution providers that have come together to share threat intelligence on advanced attacks, their motivations, and the tactics of the malicious actors behind them.

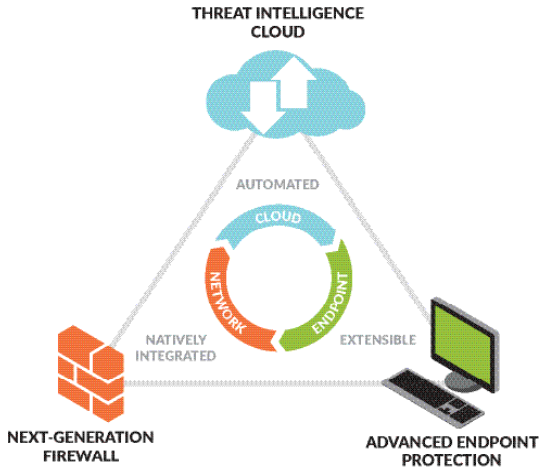

Figure 4: Palo Alto Networks Next-Generation Security Platform

Now organizations can focus on deploying and maintaining one automated and integrated security platform that streamlines the architectural clutter and administrative overhead while preventing the most advanced cyberthreats.

How to Make the Move

Next-generation security architecture and the consolidation of legacy architecture is a paradigm shift in the industry. Many organizations have already made the transition, but most are still in the process or contemplating how to get started. The transition is usually done in phases, but the improved security outcomes and operational benefits are realized fairly quickly.

The phases typically include:

1. **Identify the platform of choice.** Evaluate vendors who can provide the best capabilities in all of the areas identified above. The right vendor will have the most innovative capabilities available covering network, cloud, endpoint

and data center with world-class support to back it up. You should also look for a vast customer base feeding the threat intelligence services and participation in the Cyber Threat Alliance.

2. **Identify the first component to implement.** Many organizations will implement a platform over time rather than purchase and deploy all components at once. One organization may have a need to replace firewalls this year, while another is coming up on the renewal of an antivirus tool that has grown obsolete. Perhaps cloud is the priority of the year. Identify the priority that has budget and commitment and pursue that.
3. **Try it in your environment.** Everything looks great on paper. Try the solution in your environment to see how it works for your specific use cases.
4. **Deploy.** Train your staff on the new solution and make sure you have a plan for full and successful deployment. Replacing old tools with new ones is only the first step. It is important to use those new tools in a way that they provide the intended value and security protection. This means understanding, turning on and tuning the advanced capabilities. Professional services from the vendor or a value-added reseller may help to secure success in this stage.

Business Impacts of Smarter Security Investments

Optimizing your company's cybersecurity investments by consolidating onto a next-generation platform and eliminating complexity and redundancy will not only improve security, it will have positive impacts to the success of the business. The reduction in the number of security devices, along with reduced administrative overhead and manual interventions, will result in lower operating costs for the security infrastructure. But organizations are not rapidly adopting this approach just to reduce costs. Companies need to protect the resiliency and integrity of their business operations.

Beyond simple cost reduction, the ability to automatically prevent the most advanced cyberthreats means the preservation of your company's ability to reliably generate revenue. Cyberthreats pose a direct risk to the revenue-generating core of the business. It is essential for senior leaders to understand this and guide their organizations toward the reduction of such risks.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

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

www.paloaltonetworks.com