Realizing Cybersecurity Value

The Business Benefits of Palo Alto Networks Platforms

For years, organizations have chased after new security threats and vulnerabilities as they occur, seeking out best-of-breed point products to address an ever-increasing range of specific problems. They've also had to cope with the reality that they continue to face daunting shortfalls in hiring experienced security professionals, making it far more difficult to keep up with the proliferation and potential magnitude of new threats and bad actors using traditional approaches. As a result, security teams have become overextended, the security cost center has gotten costlier, and cybersecurity value has become difficult to realize.

The years-long approach favoring adoption of disparate point products has bred inefficiency and complexity across three major categories of cybersecurity pain points: procurement, implementation, and operations of cybersecurity defenses. Relying on more and more threat-specific point products doesn't scale and clearly is not a viable strategy for 21st century cybersecurity.

As challenging as cybersecurity is for organizations today, it undoubtedly will become substantially more complex and more important in the future. Organizations simply need more from their cybersecurity solutions and frameworks—more visibility, more accurate parsing of alerts, faster identification of emerging threats, and better inventory of threat vectors from the data center to the edge to the cloud. It's time for a more strategic, modern approach that not only secures today's complex, dynamic enterprise but also drives real business value and operational efficiency to support their evolution.

Tackling the Point Product Problem in Cybersecurity

As enterprises encounter diversified new threats, cybersecurity product and services vendors have leaped into the breach to fill the gap. There are literally hundreds of different kinds of security tools available to choose from, and most vendors offer a wide array of hardware, software, and services—most of them designed to address a particular need. However, many of these tools aren't designed to work together seamlessly or even at all. Incompatibilities among different tools mean there are going to be visibility and coverage gaps that make it easier for hackers to get in and for enterprises to think they are truly secure at any point in time.

Simply having dozens or more firewalls, monitoring devices, management consoles, cloud security frameworks, and security operations center (SOC) tools isn't good enough for enterprises, and having a lot of products under one security vendor's roof doesn't mean they provide the kind of seamless, integrated, intelligent, and adaptable framework that breeds end-to-end security and cost-efficiency.

The importance of cybersecurity consolidation cannot be overstated when it comes to alleviating the challenges associated with unfilled cybersecurity positions. Research from ESG[1] indicates that an understaffed cybersecurity team is the single biggest challenge an organization faces when it comes to security.

The Era of Cybersecurity Consolidation

The new, better way forward centers on having a strategically designed portfolio of solutions built on a common platform that breeds integration, enterprise-wide visibility, and easy scalability as new threats emerge. Consolidated cybersecurity—especially platforms powered and enhanced by automation, artificial intelligence, and machine learning—helps alleviate personnel shortages. Intelligent platforms enable machines and bots to bridge the knowledge gap that often exists when myriad vendors with incompatible products are part of the equation. It also enables onsite security teams to focus more on high-value aspects of risk assessment and risk mitigation rather than on essential but lower-value tasks such as network monitoring and verifying credentials.

A platform mindset has proven to be a valuable and effective way for organizations in other industries to reap financial and operational benefits. For instance, Southwest Airlines flies a single type of aircraft because having a common fleet simplifies scheduling, maintenance, flight operations, and training activities.

To be effective, cybersecurity platforms must make it easy for enterprises to build rock-solid security from the data center to the edge to the cloud—and back. After all, enterprise data is constantly in motion, and the workloads built to serve mission-critical data are often migrating from on-premises to the cloud, from cloud to cloud, and from the cloud back to the on-premises environment. Without leveraging common platforms that integrate needed capabilities for critical areas of the business—such as network, cloud security, and SOC activities—coverage gaps will continue to exist.

1. *2022 Technology Spending Intentions Survey*, ESG Research, November 30, 2021, https://research.esg-global.com/reportaction/2022TechnologySpendingIntentionsSurveyRPT/Marketing.

Palo Alto Networks has architected its portfolio of security platforms on a next-generation approach that is consistent, flexible, and scalable to achieve heightened visibility, integration, and real-time monitoring to spot potential issues wherever and whenever they occur. As a result, Palo Alto Networks offers a wide range of benefits for customers in the procurement, implementation, and day-to-day operations of its solutions—including economic benefits, staff efficiencies, and heightened security readiness and responsiveness across the physical and virtual enterprise.

Studying Platform Business Efficiency Benefits

Easier to procure, manage, operate—and reduce risk

To understand if and how enterprises benefit from using Palo Alto Networks platforms to build and operate a modernized, future-proof security framework, we undertook an in-depth research study with a wide range of customers across different industries and geographies. (See "About the Research" at the end of this paper.) That questionnaire-based research was supplemented by several in-person interviews with those individuals either directly involved in security operations or responsible for evaluating and signing off on solutions expenditures.

The big-picture takeaway from the research is this: enterprise security decision-makers quantified and qualified 17 different benefits from using Palo Alto Networks security platforms, and those benefits spanned three major categories:

- Procurement and acquisition
- Implementation and deployment
- Security operations

Most importantly, customers said their quantifiable benefits yielded average improvements ranging from 21% to 24% compared with using a point product-based approach.

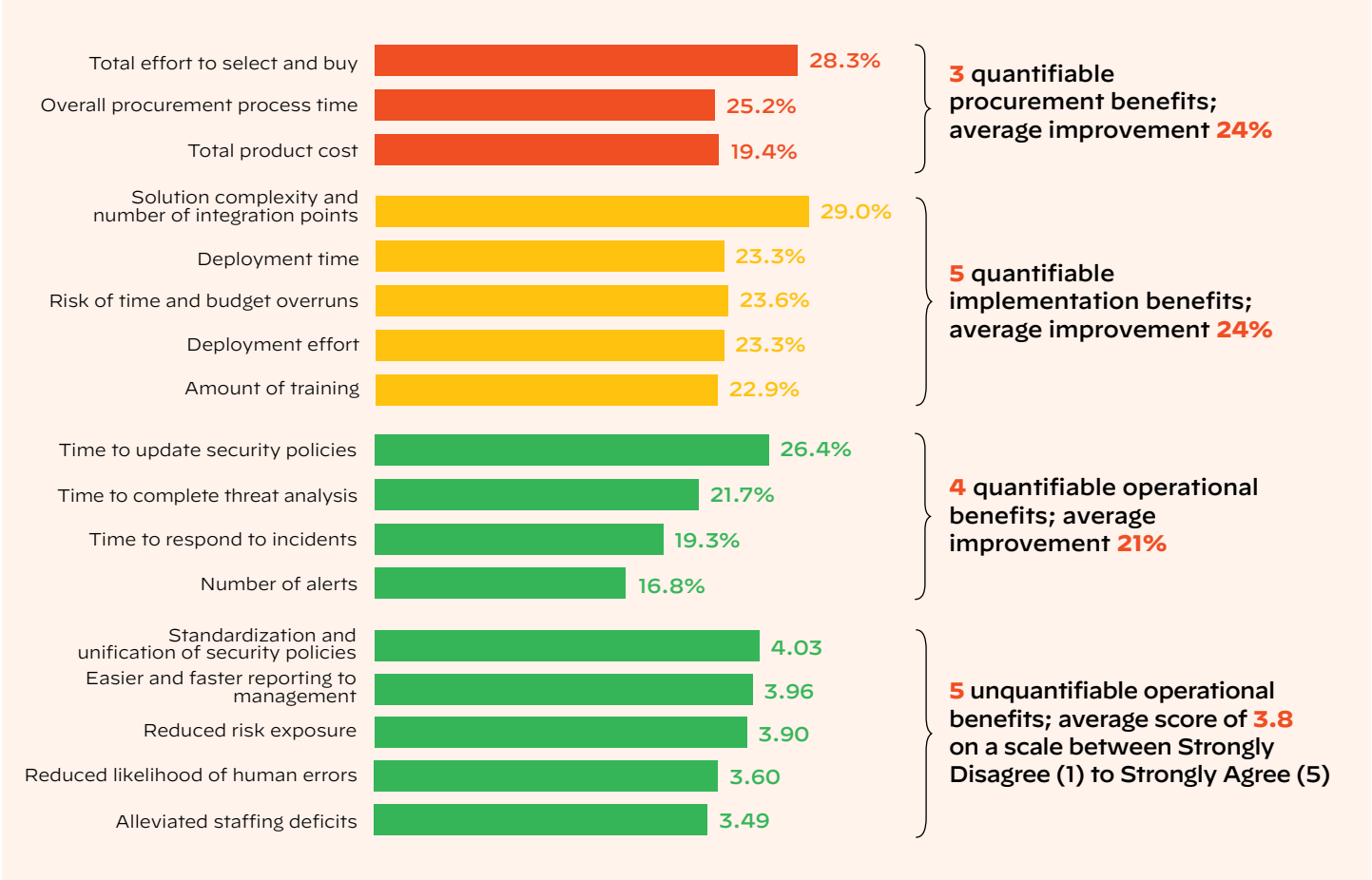

Figure 1: Benefits of using a platform approach over a point product-based approach

The quantifiable benefits across the three categories addressed a number of issues important to a wide range of decision-makers, including cost savings, time savings, reducing staff burdens, and improving time to value. Additionally, the quantifiable benefits indirectly reduced many of the same issues, such as reducing complexity and risk, better reporting, and consistent processes. In fact, respondents' answers to the survey and their follow-up comments made it clear that risk reduction is paramount to what they see as the benefits of a platform approach to cybersecurity.

Procurement Benefits

By reducing the use of dozens or more different vendors for security hardware, software, and services, survey respondents noted a substantial upside to utilizing the Palo Alto Networks platform methodology in procuring cybersecurity solutions. The top benefit—cited by more than 28% of the respondents—was reducing the total effort to select those products, while reducing the overall procurement process time and cutting total product expenditures were also widely cited.

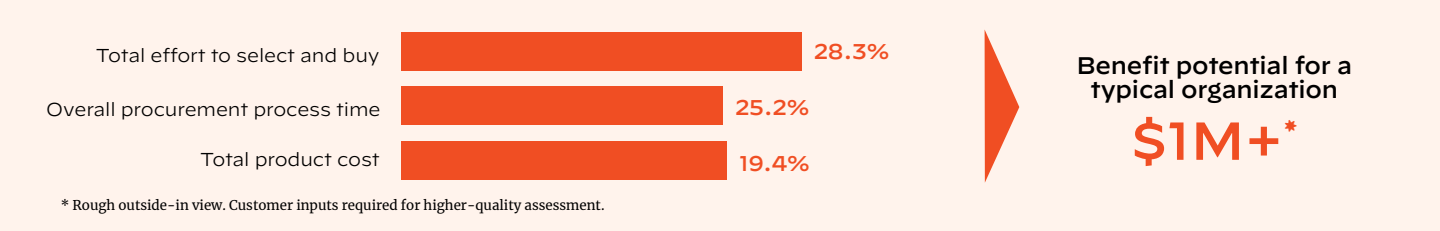

Figure 2: Potential savings based on reducing overall procurement process time and cutting product expenditures

Customers interviewed for follow-up commentary put the data into a real-world context. Typical comments included:

- "Without a platform approach, you might have two separate products—one doing A, B and C, and another doing B, C and D. Basically, you're paying double for B and C."
- "If you're going through one vendor, you can negotiate all products together. You have a higher bill with that one vendor, so it's a bigger discount."
- "We saved about 40–50% of the procurement time. The entire procurement process actually has to go through a bunch of different steps, so we saved at least two or three different steps."

Implementation Benefits

While procuring multiple cybersecurity products and services from different vendors is challenging, in many instances, the hurdles in actually implementing and deploying those products into a comprehensive, smoothly functioning system may be even more daunting.

Implementation takes time, staff, money, and expertise—all of which are badly stretched when implementation is done piecemeal through a patchwork of add-on solutions, replacements, and upgrades that take place over time. Legacy cybersecurity architecture is decidedly not "plug and play" because of the lack of a common cybersecurity platform and the absence of application programming interfaces to facilitate new functionality.

Deploying multiple products from multiple vendors often requires a level of experience rarely in place with already-stretched in-house security teams, necessitating the hiring of consultants and security service providers. This not only adds cost and time to the implementation process but often increases implementation complexity and risk because the outside partners must understand the vagaries of multiple vendors' products and how to get them to operate together seamlessly.

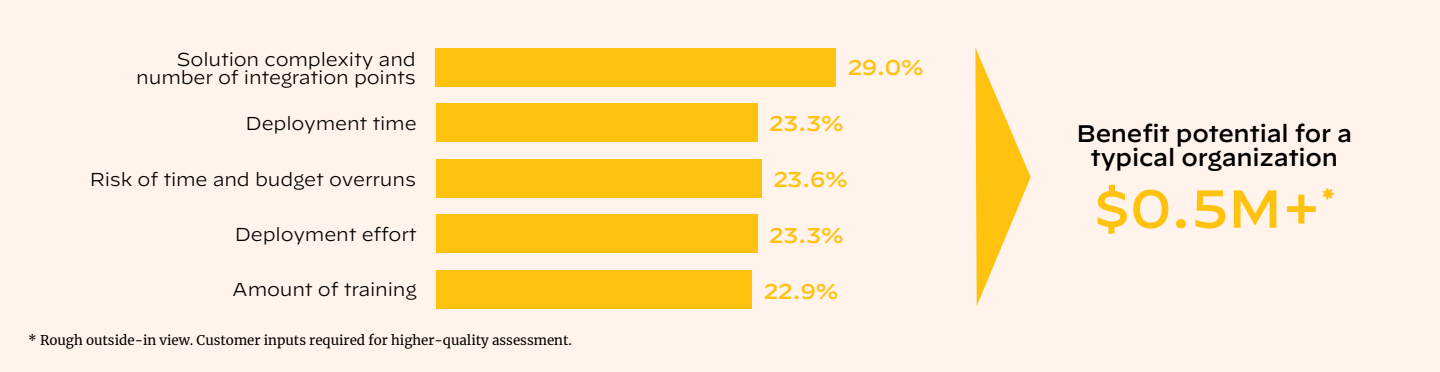

Figure 3: Potential implementation savings based on deploying multiple products from Palo Alto Networks vs. multiple products from multiple vendors

Reducing solution complexity and the number of integration points was cited as the top area where respondents saw their enterprises benefiting. On average, they believe they saw a 29% decrease in solution complexity and integration, followed by typical savings of 23% on such issues as deployment time, risks of time and budget overruns, deployment effort, and the amount of training.

Customers noted:

- "Earlier on, we had at least four to six different integration points just for firewalls and endpoint security before we went with Palo Alto."
- "Having one ecosystem really does get a lot of efficiencies with integrations being so seamless."
- "People already know how to do troubleshooting."

Operational Benefits

Once cybersecurity systems are procured and deployed, the focus shifts to actual security operations. This is another critical area where substantial benefits are being enjoyed by Palo Alto Networks customers, and those benefits are both quantifiable and qualifiable in nature.

Cybersecurity operations are, by definition, process- and policy-oriented and precise, yet must be adaptable to the inevitable threats and cyber challenges that arise, often without warning. As a result, security teams place a premium on flexibility, predictability, intelligence, and avoiding wasted energy and effort. That's undoubtedly why survey respondents said the security operations area with the greatest savings is the time necessary to update security policies; respondents said they saw an average of 26.4% reduction in the time required to update security policies with the Palo Alto Networks platform model, compared to legacy approaches.

Reducing the time to complete threat analyses, ensuring faster incident response, and reducing the number of false-positive alerts were other key areas of improvement, with reductions ranging from about 17% to nearly 22% using the Palo Alto Networks platform. The specific benefits respondents cited in working with the Palo Alto Networks cybersecurity platform architecture, as opposed to trying to manage a host of disparate products from multiple vendors, highlighted the ability to improve response time and to improve their ability to know if, when, and where to address problems.

These benefits included:

- Cutting the time to update security policies
- Trimming the time needed to complete a threat analysis
- Reducing incident response time
- Slashing the number of actionable security alerts

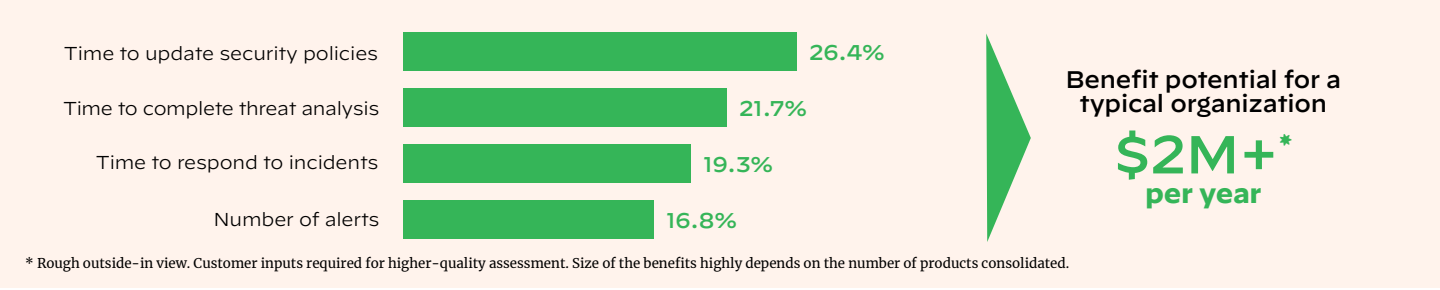

Figure 4: Potential savings based on security operations efficiencies realized through deployment of a platform approach

These quantifiable benefits were vitally important to the customers:

- "In a multi-vendor scenario, when you're trying to look at dashboards and figure out what to monitor, it just becomes a people nightmare."
- "You're not hunting for the login to the other system; you get right to it and drill down to what's going on. The platform approach definitely speeds things up."
- "Building security policy with fewer vendors is three or four times easier than upgrading a security policy for each different one."
- "Without a platform, we'd probably have to increase the SOC team by potentially 50–75%."

Of course, many benefits enterprises achieve from a platform-based cybersecurity approach are less tangible—but certainly no less important. For instance, respondents surveyed placed a high value on such benefits as standardization and unification of security policies. Anyone who works in information security understands how complex and frustrating it can be to juggle multiple security policies and rationalize a common policy management framework against multiple vendors and their myriad tools.

Respondents also cited the value of reduced risk exposure, fewer errors due to human intervention and faster, more comprehensive reporting to management on security events and unusual activity on the network and in the cloud.

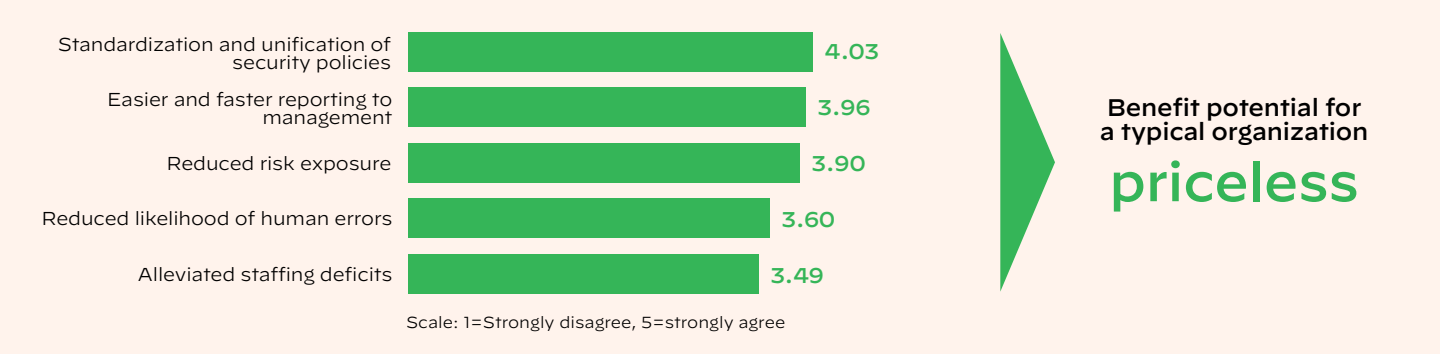

Figure 5: Intangible benefits realized with a platform approach

Customer feedback highlighted the many qualifiable benefits of using a platform approach to cybersecurity:

- "The less vendors you have, the less attack vectors you're exposing yourself to."
- "In six months to a year in a typical multi-vendor scenario, policies will be different because you forget that you have to get into two locations to update those policies."
- "Everyone is on the same page; there no longer are different skill sets, different platforms and different versions of the platforms. People know the same things and are able to back each other up."
- "We can generate reports that sum up all the changes that have happened, either to management or to security operations."

While all benefits—procurement, implementation, and operations—from a platform-based cybersecurity perspective are important, customers did point out that they place the highest importance on operational benefits. Specifically, customers termed "critical" the reduction of time to complete threat analysis, reducing the number of alerts and overall risk exposure.

Palo Alto Networks analysis of those critical benefits points to a five-year value of between $7 million and $8 million for a typical organization with 10,000 full-time equivalents. In this context, the value of a platform-based approach to cybersecurity can best be viewed as an opportunity for a higher return on investment rather than as another unavoidable combination of capex and opex costs.

Palo Alto Networks Platform Approach

Palo Alto Networks has assembled a portfolio of platforms with a best-in-class set of capabilities—leading in third-party evaluations and efficacy tests—under one umbrella. Our platform approach enables comprehensive Zero Trust, while tackling the most significant security challenges facing enterprises today:

- **Intelligent** to stay ahead of evolving threats
- **Integrated** to overcome security complexity
- **Automated** to accelerate response times and reduce human error

Our portfolio of platforms work better together to deliver the most comprehensive solutions for network, cloud, endpoint, and services. Leveraging the industry's largest footprint of intelligence, Palo Alto Networks unites products and services to enable a "network effect," and coordinated security enforcement across our customers.

Charting a Cybersecurity Consolidation Path

As organizations recognize the importance and benefit of developing and implementing a platform-based approach to cybersecurity, it's necessary to develop a strategic plan. That plan should be informed by answers to several key questions, with clearly understood next steps to progress along the path to a more comprehensive, flexible, and future-proofed cybersecurity platform.

Key Questions

- Can you identify the existence, status, and ownership of all digital assets—applications, data, cloud services, endpoints, servers, and networks—that could be targeted by hackers?
- How long does your procurement process usually take to evaluate and purchase a cybersecurity tool or service?
- What is the labor component of a typical cybersecurity deployment?
- How can you substantially mitigate the likelihood of human error in your cybersecurity processes?
- How many security alerts do you receive daily, and what percentage of those are determined to be actionable after triage?
- How often does the security team evaluate and adapt security privileges?
- What are the areas of biggest complexity in your cybersecurity architecture and processes, and what are the best ways to reduce them?

Next Steps

- Get a dialogue going among all key stakeholders—technical and non-technical, including the board—about the need to reduce complexity, cut costs, eliminate friction, and still improve the efficacy of enterprise cybersecurity.
- Adopt a Zero Trust approach to cybersecurity processes, privileges, and technology to ensure resilience, limit threat vectors, and build security operations standards.
- Agree upon the optimal ways to measure cybersecurity effectiveness and efficiency.
- Determine instances in cybersecurity infrastructure and processes that would benefit from a single-vendor platform approach.

- Do a full inventory of all cybersecurity vendor contracts, identify their internal owners, and determine how much could be saved with a vendor consolidation effort based on an open platform.
- Rethink your approach to cybersecurity training of your users and staff built upon having a single platform rather than a loosely knitted federation of point products.

For more information about this research or on Palo Alto Networks platform approach to cybersecurity, please visit www.paloaltonetworks.com.

About the Research

In late 2021, Palo Alto Networks undertook an extensive research study with its customers in order to identify the major business benefits of adopting a platform approach to cybersecurity. Palo Alto Networks customers were surveyed using the following criteria:

- Role in cybersecurity procurement either as an influencer, decision-maker, or final approver.
- Cybersecurity is managed internally or partially outsourced in collaboration with internal teams.
- Deployment of multiple Palo Alto Networks product pillars.

Research fieldwork was completed in early 2022, with 83 respondents completing an 18-question survey. Additionally, 10 customers were contacted directly for follow-up questioning. Anonymized excerpts of those interviews are included within this document.

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