The Business Value of Palo Alto Networks Cybersecurity Platforms

Frank Dickson
Vice President,
Cybersecurity Products, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary

Cybersecurity is more than detecting maliciousness. Frankly, the typical organization has a plethora of tools providing a number of alerts that exceed the organization's capability of assessing them, let alone respond to and subsequently remediate them. Surely, the threat landscape is an issue, but so too is the complexity presented by digitally transformed IT architectures and the almost unfair constraint levied on organizations by the cybersecurity talent shortage. Clearly, the point product cybersecurity tool approach is ineffective given the new reality.

Given the need to optimize the performance of security architectures rather than individual cybersecurity tools, security vendors are increasingly providing security platforms, owning the system integration responsibility of multiple security tools to improve time efficiency and increase the effectiveness of cybersecurity teams. Palo Alto Networks is one such vendor in the cybersecurity space that looks to lead with a platform approach. This Business Value Study looks to measure outcomes of the Palo Alto Networks cybersecurity platforms, using return on investment as our metric of choice.

IDC interviewed organizations using Palo Alto Networks cybersecurity platform solutions to understand the impact on their security capabilities, security operations, and business activities. Study participants reported achieving value by improving their ability to identify, assess, and respond to security threats, which results in tangible benefits in terms of business performance, security and IT staff time requirements, and security-related costs.

Based on these interviews, IDC calculates that study participants will realize an average of $22,300 per 100 users ($7.33 million per organization) by:

- **Enhancing security capabilities**, including robust threat detection, centralized management, and targeted security responses, resulting in faster identification and resolution of security events
- **Enabling more efficient and proactive business operations,** with fewer security-related interruptions, leading to improved customer experiences and business performance

Business Value Highlights

Click the highlights below to navigate to content within this document.

203%
three-year ROI

6 months
to payback

58%
faster to remediate security events

55%
faster to address cyberattacks

$27.75 million
higher revenue per organization

3.3%
higher productivity for 4,590 employees on average

34%
more efficient security teams

10%
lower annualized security-related platform costs

- **Gaining significant efficiencies for security and IT infrastructure teams,** with automation, advanced features, and standardization allowing for streamlined monitoring and management activities
- **Optimizing security-related costs** by consolidating their security environments

Situation Overview

Let's state the obvious: The threat landscape is the worst that it has ever been and is getting worse, but that has been the reality for more than a decade. Stuxnet, the Target Breach, WannaCry, and many other threats are part of our collective consciousness, each worse than the previous. Fortifying IT architectures to prevent attacks and detecting maliciousness before compromises turn into breaches is critical. Most organizations understand this. However, is that really a problem? Is there a detection problem, really?

A typical organization may have over 100 security products — security products that are continually detecting potential maliciousness. When Target got breached over a decade ago, the intrusion was in fact detected; the alert was just one of tens of thousands. So, it is not just good enough to detect; insights from multiple security products need to be combined and correlated to separate the signal from noise, as not all anomalies imply maliciousness. This effort is easier said than done, as the complexity of IT architecture is growing exponentially due to the proliferation of transformational technologies such as SaaS, PaaS, IaaS, and GenAI.

Not only is complexity aggravating the problem, but also, most organizations are likely challenged to find, hire, and retain qualified cybersecurity personnel. Finding more qualified people would dramatically help investigation abilities, but there are just not enough qualified people out there.

Even if organizations were perfect in identifying the malicious actions of cyber adversaries, only half of the problem would be addressed. Quickly responding to attacks to limit, manage, and subsequently remediate to eliminate the intrusion and prevent a repeat of the intrusion is the other half of the task. Complexity often makes response and remediation a Herculean task for even the most talented of cybersecurity professionals. Most organizations are essentially too understaffed to address cybersecurity challenges, and it is not going to get better. The result is that organizations are constantly making compromises to optimize their defenses within the constraints provided to them.

Perhaps the problem needs to be redefined. Instead of framing the issue as a detection problem, looking at this as a data problem would be more productive. If organizations can reduce the number of alerts to triage by correlating signals from multiple tools, then time is

created for analysts. If organizations can group alerts into incidents, they can address alerts with a force multiplier effect, creating time. If the investigation effort for security analysts is reduced, time is created. If the response can be automated, time is not only created for the analysts now, but remediation time is reduced by limiting the potential damage of cyber adversaries. Essentially, making security analysts more efficient and effective is built on a foundation of elegant security data management.

Reframing the problem reorients organizations' approaches to security. Many organizations select security tools individually, forcing organizations to be their own multivendor security systems integrators. In addition to the time tax that system integration will continually cost, independent tools from multiple vendors that are not designed to work together require extra effort to orchestrate. When an organization uses multiple vendors, the challenge of transforming and mapping the security data from multiple tools requires connectors to be built and rules and response playbooks to be written. Connectors and playbooks can be fragile, as they depend on stable security tools that do not change; changing tools is the rule in the new world of waterfall software updates. While all security tools have an API that can allow for integration, having an API available and actually getting it to work are very different stories. Thus, the optimization of individual tools creates a suboptimal security architecture.

Given the need to optimize the performance of security architectures, security vendors are increasingly providing security platforms. This streamlines the system integration responsibility of multiple security tools to create time efficiency and increased effectiveness for cybersecurity teams. Palo Alto Networks is one such vendor in the cybersecurity space that looks to lead with a platform approach.

This Business Value Study looks to use fewer words and more numbers. Instead of describing in prose the advantages of a platform to enable superior security, IDC looks to measure outcomes, using return on investment as our metric of choice.

Palo Alto Networks Cybersecurity Platform Approach Overview

Founded in 2005, Palo Alto Networks is a notable cybersecurity vendor, initially leading network security innovation with next-generation firewall platforms and currently providing cybersecurity platform solutions across on-premises, cloud, and hybrid work use cases.

Palo Alto Networks is working to solve three major problems impacting its customers today:

Managing risks in complex environments:
Navigating risks in complex environments with diverse infrastructure, including datacenters and hybrid locations, encompassing multiple clouds, and accommodating remote employees with both managed and unmanaged endpoints, necessitates the implementation of a zero trust strategy.

Enhancing security effectiveness while ensuring operational efficiency:
Many customers operate with a security stack comprising 30–50 vendors. They continually introduce more because start-ups are solving problems that other vendors ignore, however, the challenge lies in integrating these tools seamlessly to ensure the coherent functioning of the system.

Automating threat detection and response:
While preemptive threat prevention is the best defense, when it comes to detecting and mitigating threats, speed is crucial. Today's human-centered security operations center (SOC) is inundated by siloed data, causing analysts to be overwhelmed, reactive, and unable to keep up. To address these challenges effectively, the shift toward AI-driven cybersecurity becomes critical.

The Business Value of Palo Alto Networks Cybersecurity Platforms

Study Demographics

IDC conducted in-depth interviews to gain an understanding of the practical and real world impact for organizations using Palo Alto Networks cybersecurity platform approach. Interviews were designed to elicit feedback about both the quantitative and qualitative impact of these solutions from security and IT managers and executives. Study participants deployed Palo Alto Networks cybersecurity platform solutions both to supplement and replace their existing security environments, which included solutions from other networking and security vendors.

Table 1 provides an overview of the organizations interviewed for this study. As shown,

they are enterprise level, with an average of 41,750 employees and $5.63 billion in annual revenue (10,500 employees and $2.55 billion revenue, by median), and serve around 1.40 million customers on average. Interviewed Palo Alto Networks customers spoke to their experiences from a number of geographies, including North America, APAC, and EMEA, and an array of industry verticals, namely banking, education, financial services, government, healthcare, insurance, IT services, media, pharmaceutical, and professional services. For additional details about interviewed organizations, please see **Table 1.**

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	41,750	10,500
Number of IT staff	551	325
Number of customers	1.40M	15,000
Number of business applications	317	225
Annual revenue	$5.63B	$2.55B
Countries	United States (7), Canada, India, United Kingdom	
Industries	Banking, Education, Financial Services, Government, Healthcare, Insurance, IT Services, Media, Pharmaceutical, Professional Services	

n = 10; Source: IDC In-Depth Interviews, December 2023

Choice and Use of Palo Alto Networks Cybersecurity Platform Approach

Study participants spoke about the reasons that they decided to use security solutions across the Palo Alto Networks cybersecurity portfolio. The common thread across their investment decisions was the realization that they needed to establish more robust, integrated, and adaptable security environments. Numerous interviewed organizations cited the portfolio's strong underlying functionality, including advanced threat prevention,

next-generation firewalls (NGFW), and other technologies to defend against cyberattacks. They also noted that the portfolio's AI capabilities expedite threat detection and prevention. Further, they noted the value of standardization, both in terms of use across various device types and interfaces and in terms of management efficiencies.

Interviewed Palo Alto Networks customers detailed their selection criteria:

Strong security functionality of portfolio:

"We chose Palo Alto Networks cybersecurity solutions because they have advanced threat prevention and they use next-generation firewalls and sophisticated technology that help defend us against sophisticated cyberattacks such as malware, ransomware, zero-day threats, and Trojan horses."

Importance of having a common, standardized cybersecurity portfolio:

"We chose the Palo Alto Networks cybersecurity platform because we wanted to standardize upon one platform, one toolset, one methodology. The standardization was just a big piece of it and the ability to apply it across tens of thousands of devices."

Capabilities in the cloud:

"From the perspective of security coverage, the one specific reason for Palo Alto Networks is they were very good for coverage of cloud containers. Our previous solution still did not have a good enough solution for the security of containers in the cloud."

As shown in **Table 2** (next page), study participants secure most of their business operations with Palo Alto Networks cybersecurity platform solutions.

They reported using various Palo Alto Networks security solutions, including:

- NGFW and associated solutions, including for cloud environments
- Advanced Threat Protection
- Cortex XDR to run security operations
- Prisma Access
- SD-WAN

Interviewed Palo Alto Networks customers' use of solutions to cover tens of thousands of PCs and users (averages of 37,122 PCs and 32,950 users) across an average of 249 business locations speaks to the breadth and scale to which they rely on these security solutions. This extensive use is also reflected in terms of the business they support with Palo Alto Networks cybersecurity solutions, covering an average of 81% of revenue-generating services and applications (median of 100%). For additional details, please see **Table 2** (next page).

TABLE 2

Use of Palo Alto Networks Cybersecurity Platforms by Interviewed Organizations

	Average	Median
Number of sites/branches	249	93
Number of Palo Alto Networks firewalls	123	24
Number of PCs	37,122	5,000
Number of business applications	275	200
Number of users of applications	32,950	7,500
Percent of revenue supported	81%	100%

n = 10; Source: IDC In-Depth Interviews, December 2023

Business Value and Quantified Benefits of Palo Alto Cybersecurity Platforms

Study participants reported achieving significant value by consolidating on Palo Alto Networks cybersecurity platforms. They have not only realized important gains in their security capabilities, but they have also made their security operations more efficient and enabled their businesses by having the ability to scale their security with ease to match business needs. Interviewed Palo Alto Networks customers provided detailed explanations of what they view as most impactful for their organizations:

Threat detection and centralized management:

"The most important benefits of using Palo Alto Networks are threat detection and being able to assess the risk posed to our data … Palo Alto's cybersecurity solutions use ML/AI, which is important in protecting sensitive information. The other advantage is centralized management, which means fewer vulnerabilities for us to manage and monitor security policies across multiple branches and locations."

Ability to focus and target security response:

"The real benefit since we standardized on Palo Alto Networks is that if we see something, we can react to it almost immediately. Before, we didn't have that capability. It could have been hours, days, or weeks before we would've known that there was a potential issue … Right now, we get an alert, and we can respond to isolate that machine immediately."

Protect customers' data, avoid costs of security problems, and ensure credibility:
"With the Palo Alto Networks cybersecurity platform, we protect our customers' data and ensure that we do not breach any of the terms and conditions that we've agreed with a client. Any type of threat or breach in security can cost millions of dollars to remediate."

Scalability without compromising security:
"The number one benefit we get with Palo Alto Networks is the ability to scale into performance and do that in a secure manner without compromising security."

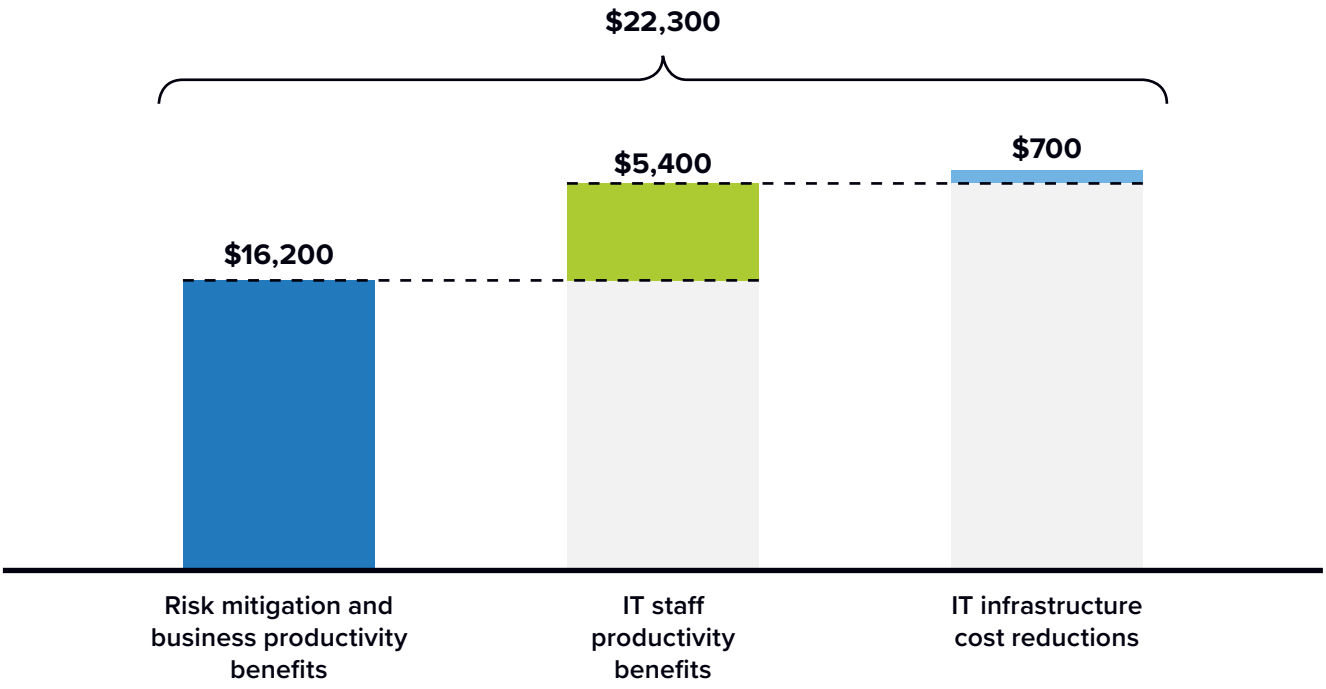
Based on interviews with Palo Alto Networks customers using their cybersecurity solutions, IDC calculates that they will capture benefits worth an annual average of $22,300 per 100 users ($7.33 million per organization) in the following areas of value (see **Figure 1**, next page):

- **Risk mitigation and business productivity benefits:**
  Study participants run their businesses more efficiently with hardened and more robust security environments, leading to higher net revenue and employee productivity. IDC puts the value of net revenue and productivity gains at an annual average of $16,200 per 100 users ($5.32 million per organization).
- **IT staff productivity benefits:**
  Study participants require less security and infrastructure team time for day-to-day responsibilities, such as monitoring and maintenance, enabling development teams to work with increased velocity. IDC calculates that these teams will realize efficiencies and productivity gains worth an annual average of $5,400 per 100 users ($1.78 million per organization).
- **IT infrastructure cost reductions:**
  Study participants optimize security-related costs by consolidating more of their security capabilities on a single platform. IDC estimates that they will save an average of $700 per 100 users per year ($221,400 per organization).

FIGURE 1

Average Annual Benefits per 100 Users

($ per year per 100 users)



n = 10; Source: IDC In-Depth Interviews, December 2023

For an accessible version of the data in this figure, see Figure 1 Supplemental Data in Appendix 3.

Enhanced Security Capabilities

Interviewed organizations cited their ability to improve their security capabilities and postures as a central benefit of using Palo Alto Networks cybersecurity solutions. They spoke to benefits that included more robust threat detection, centralized management, and the ability to focus and target security responses. Interviewed Palo Alto Networks customers linked gains in these areas to strong foundational security capabilities as well as newer functionalities driven by AI and other technology. They noted that Palo Alto Networks solutions help protect customer data, avoid the costs of security problems, and ensure their credibility from a security perspective.

Study participants provided details about security-related gains they have achieved with Palo Alto Networks cybersecurity platforms:

Much faster troubleshooting:

"We're able to troubleshoot much faster because having all that data in Palo Alto Networks makes it so much easier to go from one screen to the next without the burden of external integration and external API calls. We can do it within the Palo Alto ecosystem."

Strong protection against cyber threats and fraud:

"The Palo Alto Networks cybersecurity platform allows us to monitor and detect threats not only from cyber but also from fraudulent patterns. There are many fraudulent patterns where we have customers logging in and pretending to be somebody else, and they tend to do certain things on the account that are very slight."

Better correlation, faster time to respond:

"Our time to respond to incidents has improved with Palo Alto Networks because we can correlate things faster and be quicker to respond within minutes as opposed to hours … We've used Palo Alto to immediately isolate and block machines affected by possible malware and ransomware from our network until we were able to remediate."

Minimize false detection rate:

"After deploying Palo Alto Networks cybersecurity platforms, our false positive detection rate fell to 0.2% from higher than 2% earlier. That credit goes to the AI and ML features that are employed in the new NGFW solutions that Palo Alto provides."

Much-improved incident response capabilities:

"Our mean time for incident closure, what we would consider a high or a medium alert, is now 37 minutes. We were striving for under 3–4 hours with previous solutions, so this is a huge difference with Palo Alto Networks."

Figure 2 (next page) provides insight into the impact for study participants of using Palo Alto Networks cybersecurity platforms on important security-related KPIs. They reported that they can now work through the life cycle from threat detection to remediation much faster, which reduces their exposure to risk from security threats. On average, interviewed Palo Alto Networks customers reported remediating security events 58% faster, addressing cyberattacks 55% faster, and needing 43% less time to detect security events.

FIGURE 2

Impact on Security KPIs

(% benefit)

n = 10; Source: IDC Business Value In-Depth Interviews, December 2023

Beyond measurable security gains, study participants also linked their use of Palo Alto Networks cybersecurity solutions to changing how they conceptualize their security capabilities in the context of their business operations. One interviewed customer commented: *"Before Palo Alto, our cybersecurity efforts were based on customer requests … Now, with the Palo Alto Networks cybersecurity platform, it's the reverse, where we're telling customers that we do an exercise on a monthly basis. We prioritize any findings for them from critical to high to medium to low and then remediate them accordingly. So now the list has gotten longer in terms of the findings, but it's because the process is more stringent and rigorous."*

Business and Operational Enablement

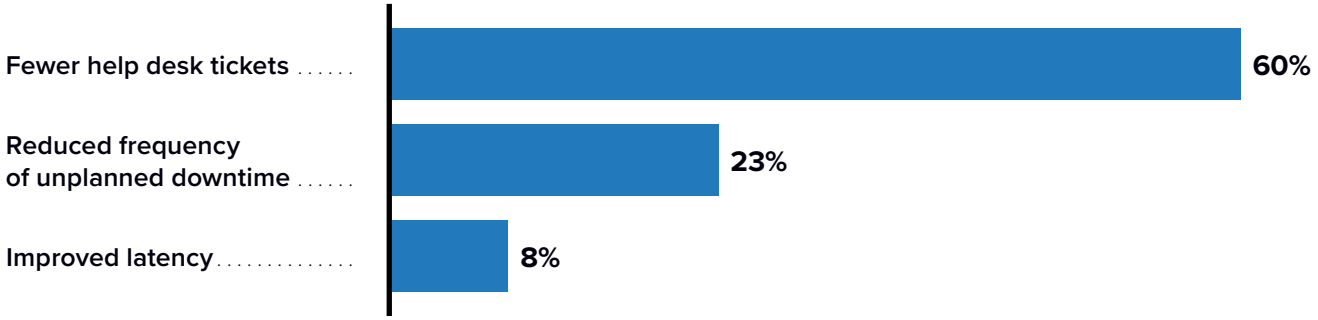
Interviewed organizations consistently reported that in addition to improving their security capabilities and results, their use of Palo Alto Networks cybersecurity platforms has also benefited their business operations. They explained that security-related concerns now exert less friction on their business activities and that they face less business interruption due to security issues. As a result, they can move proactively to address business opportunities and meet customer expectations while ensuring a better overall customer experience.

As shown in **Figure 3** (next page), study participants connected their use of Palo Alto Networks cybersecurity platforms to discrete improvements in IT and business performance. They reported not only handling fewer security-related help desk tickets (60% fewer on average) but also bringing down the frequency of impactful unplanned outages (23% fewer) while establishing the preconditions for better systems performance (8% lower latency).

FIGURE 3

Impact on Performance KPIs

(% benefit)



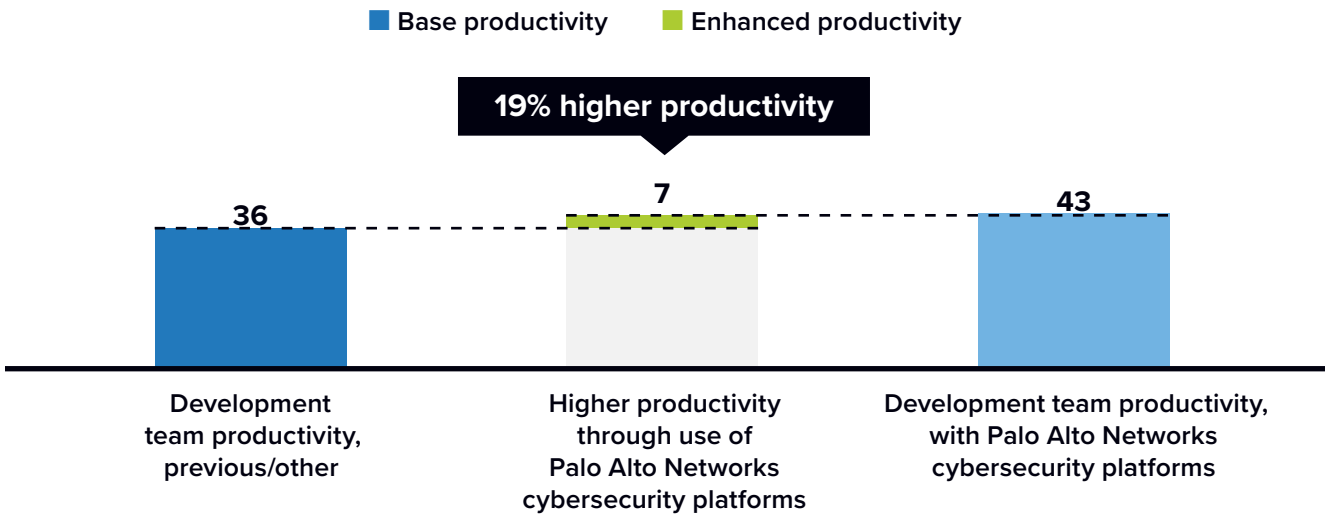
n = 10; Source: IDC Business Value In-Depth Interviews, December 2023

Importantly, even teams that would seem less directly impacted by security matters benefit from hardened security and increased agility with Palo Alto Networks cybersecurity platform solutions. For example, as shown in **Figure 4,** study participants reported that their development teams have benefited from average productivity gains of 19%, as they can work with more purpose and less friction in meeting business software-related needs.

FIGURE 4

Impact on Development Team Productivity

(Equivalent productivity, FTEs per organization)



n = 10; Source: IDC In-Depth Interviews, December 2023

For an accessible version of the data in this figure, see Figure 4 Supplemental Data in Appendix 3.

Interviewed Palo Alto Networks customers also provided numerous examples of how they have translated security and performance gains into business-focused benefits:

Significantly faster to integrate and get to market:

"Our revenue is positively impacted by the Palo Alto Networks cybersecurity platform because we can quickly integrate with new partners and deploy newer applications technologies. As a result, our go-to-market time is definitely reduced and probably results in a 15–20% improvement on the business side."

Proactive resolution of outages:

"The beauty of having Palo Alto Networks is that we're notified right away if there's downtime and we're able to bring it back up in minutes, and we have another backup that goes up right away. In the past, it took someone to manually figure out that something was down and what it would take to bring something back up. So, it's a dramatic impact."

Much faster time to market:

"Our time to market is very quick with Palo Alto Networks. We can spin up a new location 50% faster, and in acquisitions, we can drop in our equipment and have instant visibility into the entire estate … This has bettered our go-to-market time and confidence in leadership that we're able to stand up for our business side."

Table 3 shows the tangible benefits for study participants of improved security with Palo Alto Networks cybersecurity solutions, with average revenue gains of $27.75 million per organization. For the purposes of ROI calculation, IDC only considers 15% of this total revenue gain, leaving an average net revenue gain of $4.16 million per organization.

TABLE 3

Business Productivity Impact: Higher Revenue

	Average per Organization	Average per 100 Users
Higher revenue per year	$27.75M	$84,000
Assumed operating margin	15%	15%
Higher net revenue per year	$4.16M	$12,600

n = 10; Source: IDC In-Depth Interviews, December 2023

Study participants also reported becoming more operationally efficient with Palo Alto Networks cybersecurity platform solutions. This has allowed their employees to work more effectively and provided the foundation for establishing more efficient overall business operations:

Ability to extend secure, high-performing access to remote workers:

"We're using Palo Alto Networks for our core VPN connectivity, especially when we went remote with COVID-19, we expanded our VPN use 1,000–fold … We were able to stay in business because we had to rely on the VPN to extend our network to all our users that were working remote."

Foundation for use of new technologies and providing new services:

"The indirect benefit of Palo Alto Networks is that we can take a new networking approach that has improved our overall productivity as an organization by 20% easily with being able to expand offices, take advantage of faster connectivity at lower costs, and embrace new technologies and provide new services and all the things that we're now able to do."

As shown in **Table 4,** this has meant average productivity gains of 3.3% for 4,590 employees, creating significant value through operational enablement and increased organizational productivity.

TABLE 4

Business Productivity Impact: Higher User Productivity

Business Enablement — Higher User Productivity	Per Organization	Per 100 Users
Number of users, higher productivity	4,590	14
Percent productivity gain	3.3%	3.3%
Calculated FTE gain, higher productivity	152	0.50
Calculated FTE gain, higher net productivity	23	0.07
Hours per year, higher productivity	42,898	130
Calculated value of higher net productivity	$1.60M	$4,900

n = 10; Source: IDC In-Depth Interviews, December 2023

Security and IT Team Efficiencies

Interviewed organizations connected their use of Palo Alto Networks cybersecurity platform solutions to significant efficiencies for their security operations center and IT infrastructure teams. The Palo Alto Networks platforms enhance security functionality, automation, and the ability to leverage operational data, leading to an improved ability to identify and respond to security threats and events. The platforms also allow security teams to cover larger device environments more efficiently due to automation, standardization, greater visibility, and enhanced correlation capabilities. As a result, these teams spend significantly less time on a day-to-day basis on monitoring, management, and analysis activities, freeing them up to support growing environments or allowing them to support other business and IT initiatives.

Interviewed Palo Alto Networks customers provided specific examples of efficiencies for their SOC teams:

Foundation for efficient security team:

"With Palo Alto Networks, we're at about twice the efficiency of an equivalent-size Fortune 30 company … The Palo Alto toolset, by using automation, machine learning, a standardized set of tools, and standardized version deployment, has allowed us to work much greater numbers with the same staff all through automation, including playbooks."

Ability to refocus staff time on engineering:

"We're getting more efficient with Palo Alto Networks because less time is spent on troubleshooting, support, and wiring and more time on engineering and delivering applications. We're spending more on software and hardware but getting 30% of time back on our people to redirect them toward engineering."

Value of automation and templates:

"Because we have more capability and control in the Palo Alto Networks product, we have more opportunity to automate more than we do with [our other vendor solution] … Also, Palo Alto has a more structural approach with their device templates, which we can leverage to make changes."

As shown in **Table 5** (next page), study participants reported achieving strong efficiencies for their SOC teams with Palo Alto Networks cybersecurity platforms. On average, these teams are 34% more efficient, freeing up an average of almost 10 full-time equivalents to handle growing business activities or to concentrate on other business-enabling activities.

TABLE 5

Impact on Security Operations Team Efficiencies

	Previous/ Other Solutions	With Palo Alto Networks Cybersecurity Platforms	Difference	Benefit
FTEs required for same workloads	28.10	18.40	9.60	34%
Staff hours per 100 users	160	105	55	34%
Value of FTE time required ($ per organization per year)	$2.81M	$1.84M	$0.96M	34%

n = 10; Source: IDC Business Value In-Depth Interviews, December 2023

Interviewed Palo Alto Networks customers also reported that infrastructure team members benefit from having a more unified security platform, fewer issues to resolve, and platform functionalities such as automation and automated alerts. On average, IDC finds that these teams are 21% more efficient with Palo Alto Networks cybersecurity platforms, freeing up the time of an average of 4.0 FTEs per organization. (**Table 6**)

TABLE 6

Impact on IT Infrastructure Team Efficiencies

	Previous/ Other Solutions	With Palo Alto Networks Cybersecurity Platforms	Difference	Benefit
FTEs required for same workloads	18.50	14.50	4.00	21%
Staff hours per 100 users	105	83	23	21%
Value of FTE time required ($ per organization per year)	$1.85M	$1.45M	$0.40M	21%

n = 10; Source: IDC In-Depth Interviews, December 2023

Security Cost Efficiencies

Interviewed organizations also reported optimizing costs associated with securing their IT and business environments with Palo Alto Networks cybersecurity platforms. They attributed these cost efficiencies to consolidating the Palo Alto Networks portfolio of platforms and replacing less efficient security solutions and platforms. On average, IDC calculates that study participants will realize cost savings of 10%, saving $221,400 per organization per year.

ROI Summary

Table 7 provides IDC's analysis of the benefits and costs for study participants of using Palo Alto Networks cybersecurity platform solutions. On average, IDC calculates that study participants will achieve benefits in higher net revenue and productivity, staff efficiencies, and cost savings worth a discounted average of $52,500 per 100 users over three years ($17.31 million per organization). These benefits compare with average three-year discounted investment costs of $17,300 per 100 users ($5.70 million per organization). Based on these levels of benefits and investment costs, IDC projects that the average organization in this study will realize a three-year ROI of 203% and break even on their investment in an average of six months.

TABLE 7

ROI Analysis

	Three-Year Average per Organization	Three-Year Average per 100 Users
Benefit (discounted)	$17.31M	$52,500
Investment (discounted)	$5.70M	$17,300
Net present value (NPV)	$11.61M	$35,200
ROI (NPV/investment)	203%	203%
Payback	6 months	6 months
Discount rate	12%	12%

n = 10; Source: IDC Business Value In-Depth Interviews, December 2023

Challenges/Opportunities

Although Palo Alto Networks offers compelling cybersecurity platforms, it cannot be relied upon to be the sole provider of cybersecurity solutions. Frankly, no one vendor can.

IDC believes that digital trust will drive the success of digital transformation (DX) and that enterprise security strategies must adapt to the needs of digital transformation. Data, identities, and applications are increasing in importance while network and endpoint devices provide the infrastructure implementation points necessary to gain the required context to validate the integrity of transactions and establish trusted connections. Although Palo Alto Networks, as evidenced by the name, offers numerous security solutions, an organization will need to couple the platform offerings of Palo Alto Networks with those of other vendors to create a complete cybersecurity architecture.

Conclusion

The risk of business disruption and even organizational viability due to cyberattacks continues to grow. The continual escalation of threats coupled with complexity created by digitally transformed IT and business operations is problematic for organizations, given the worsening shortage of talent in the cybersecurity field. These factors tend to blunt the effectiveness of individual cybersecurity tools, especially over time, as the nature and scope of cybersecurity threats change. At a minimum, ensuring cybersecurity with individual tools often becomes inefficient and challenging to sustain over time, as security is a data problem requiring elegant data orchestration to solve. As a result, many organizations increasingly seek a platform-based approach to cybersecurity with strong integration that will allow for efficient and timely response to new and changing cyber threats.

Palo Alto Networks has established a compelling platform of cybersecurity solutions to meet this demand, and this study assessed the value for organizations of using Palo Alto Networks cybersecurity platform solutions. Interviewed Palo Alto Networks customers reported achieving significant value from cybersecurity vendor consolidation, most directly by improving their cybersecurity capabilities but also from efficiencies and increased business scalability and confidence. Thus, they have not only optimized direct cybersecurity costs and made their security operations center teams more effective, but they have also positioned their businesses to better serve customers and minimized the risk associated with cybersecurity threats and events. IDC's analysis shows that interviewed organizations using the Palo Alto Networks cybersecurity platforms will realize benefits worth more than three times investment costs over three years, resulting in an average three-year ROI of 203%, and break even on their investment in six months.

Appendix 1: Methodology

IDC's standard Business Value/ROI methodology was utilized for this project. This methodology is based on gathering data from organizations currently using Palo Alto Networks cybersecurity solutions.

Based on interviews with organizations using Palo Alto Networks cybersecurity platforms, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of using the Palo Alto Networks cybersecurity portfolio of platforms.** In this study, the benefits included security cost savings, IT staff efficiencies, user productivity gains, business gains, and security/risk benefits.

2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using Palo Alto Networks cybersecurity platforms and can include additional costs related to migrations, planning, consulting, and staff or user training.

3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use the Palo Alto Networks cybersecurity portfolio of platforms over a three-year period. ROI is the ratio of the net present value and the discounted investment. The payback period is the point at which the cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and manager productivity savings. For the purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of $100,000 per year for IT staff members and an average fully loaded salary of $70,000 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.

- Because IT solutions require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Appendix 2: Business Value Calculations

Table 8 provides a detailed view of the quantified benefits that study participants will achieve through their use of the Palo Alto Networks cybersecurity portfolio of platforms, which IDC puts at an annual average of $7.33 million per organization.

TABLE 8

Average Annual Benefits

Average Annual Benefits	Average Quantitative Benefit	Calculated Average Annual Value*
Infrastructure cost savings	Saving 10%, worth $221,400 per year	$221,400
Security team efficiencies	34% more efficient, worth 9.6 FTEs, $100,000 salary	$842,400
IT infrastructure team efficiencies	21% more efficient, worth 4.0 FTEs, $100,000 salary	$345,500
Application development team productivity gains	19% more productive, worth 7.0 FTEs, $100,000 salary	$593,800
Higher net revenue	$27.75M higher revenue per organization, 15% margin assumption	$3.64M
Higher net productivity, users	3.3% higher productivity, 4,590 users, 15% margin assumption	$1.40M
Total average annual benefits	**$7.33M per Organization**	

* Includes 4.6 average months deployment time in year 1

n = 10; Source: IDC Business Value In-Depth Interviews, December 2023

All dollar figures in this White Paper are in USD.

Note: All numbers in this document may not be exact due to rounding.

Appendix 3: Supplemental Data

This appendix provides an accessible version of the data for the complex figures in this document. Click "Return to original figure" below each table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

Average Annual Benefits per 100 Users

	Risk Mitigation and Business Productivity Benefits	IT Staff Productivity Benefits	IT infrastructure cost reductions
Per organization	$16,200	$5,400	$700
Average annual benefits per 100 users	**$22,300**		

n = 10; Source: IDC In-Depth Interviews, December 2023

Return to original figure

FIGURE 4 SUPPLEMENTAL DATA

Impact on Development Team Productivity

	Development team productivity, previous/other	Higher productivity through use of Palo Alto Networks cybersecurity platforms	Development team productivity, with Palo Alto Networks cybersecurity platforms
Equivalent productivity, FTEs per organization	36	7	43
Difference		**19% higher productivity**	

n = 10; Source: IDC In-Depth Interviews, December 2023

Return to original figure

About the IDC Analysts

Frank Dickson
Vice President, Cybersecurity Products, IDC

Frank leads the team that delivers compelling research in the areas of Network Security; Endpoint Security; Cybersecurity Analytics, Intelligence, Response, and Orchestration (AIRO); Identity & Digital Trust; Legal, Risk & Compliance; Data Security; IoT Security; and Cloud Security. Topically, he provides thought leadership and guidance for clients on a wide range of security products including endpoint security, identity and access management, authentication, threat analytics, and emerging products designed to protect transforming architectures and business models.

More about Frank dickson

Matthew Marden
Research Vice President, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

Message from the Sponsor

As a global cybersecurity leader, Palo Alto Networks continually delivers innovation to secure digital transformation.

With innovative solutions for network, cloud, and endpoints, Palo Alto Networks portfolio of platforms work together intelligently to strengthen security, simplify operations, and improve ROI. Let us show you how.

Click here to visit us

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com @idc @idc

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.