FORRESTER®

The Total Economic Impact™ Of The Strata Network Security Platform From Palo Alto Networks

Cost Savings And Business Benefits Enabled By The Strata Network Security Platform

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY PALO ALTO NETWORKS, AUGUST 2024

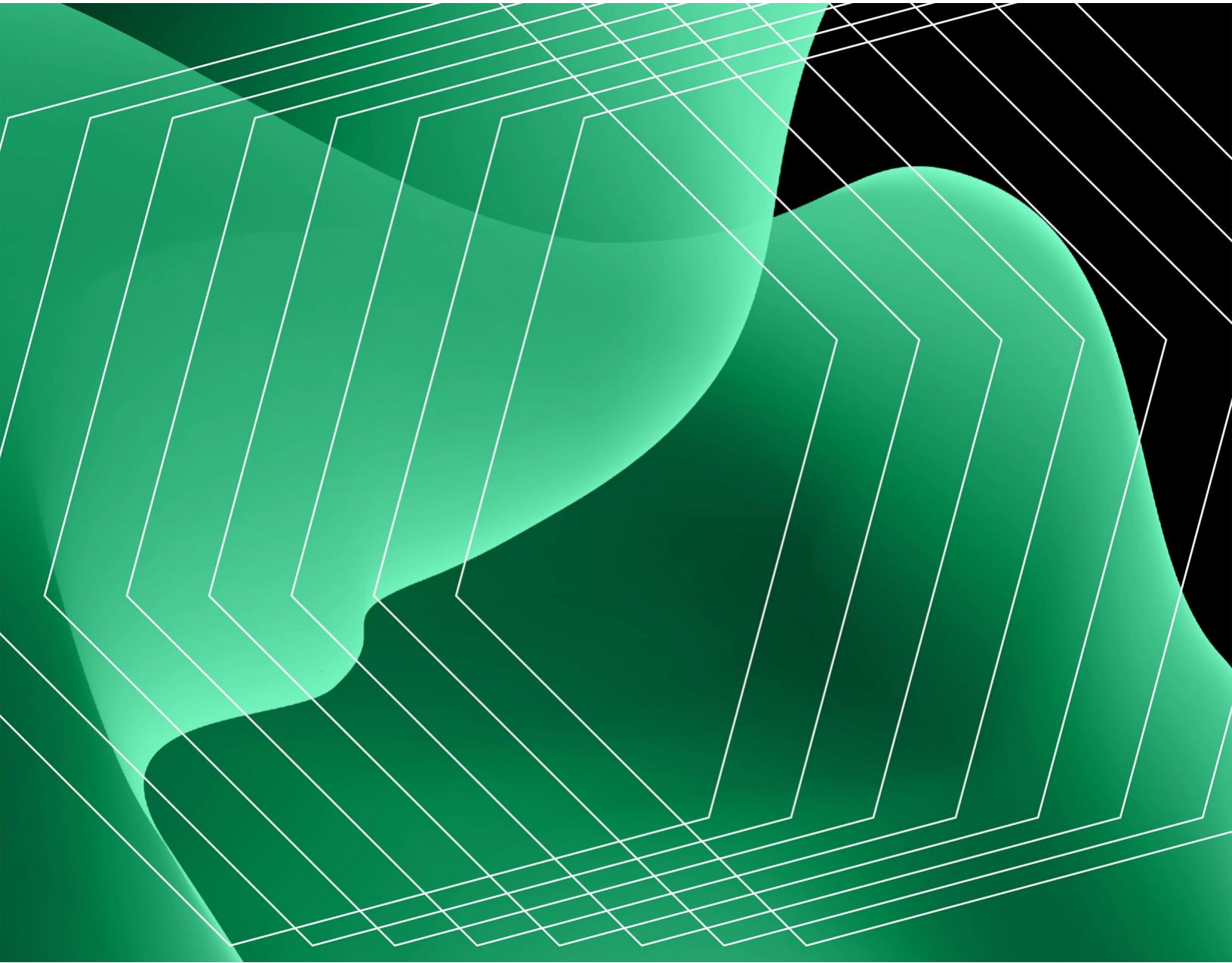


Table Of Contents

Executive Summary	3
The Palo Alto Networks Strata Network Security Platform Customer Journey	12
Analysis Of Benefits	18
Analysis Of Costs	38
Financial Summary	45

Consulting Team:

Adi Sarosa

Sam Sexton

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Cybersecurity breaches offer teachable moments about network security defenses. These issues often arise from incomplete toolsets, limited understanding of network topology, and a lack of visibility.[1] As the threat landscape continues to evolve, organizations aim to elevate their existing security infrastructure and re-envision their security strategies — to provide seamless and scalable protection that goes beyond what disparate, disconnected infrastructure of the past can offer.

The Strata Network Security Platform from Palo Alto Networks provides protection to different IT infrastructure assets including network, endpoint, data center, private and public cloud, as well as software-as-a-service (SaaS) solutions.

Palo Alto Networks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Strata Network Security Platform.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Network Security Platform on their organizations. These products include Next-Generation Firewalls (NGFWs), Cloud-Delivered Security Services (CDSS), and Prisma SASE. Palo Alto Networks' machine learning-powered NGFWs include a both hardware and software firewall solutions that provide a Zero Trust experience monitoring both north-south and east-west traffic.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed nine representatives with experience using the Strata Network Security Platform, and conducted a survey of 158 additional respondents with experience using Palo Alto Networks software firewalls. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a distributed enterprise with 50,000 employees and $7 billion in annual revenue.

Return on investment (ROI)
174%

Net present value
$26.2M

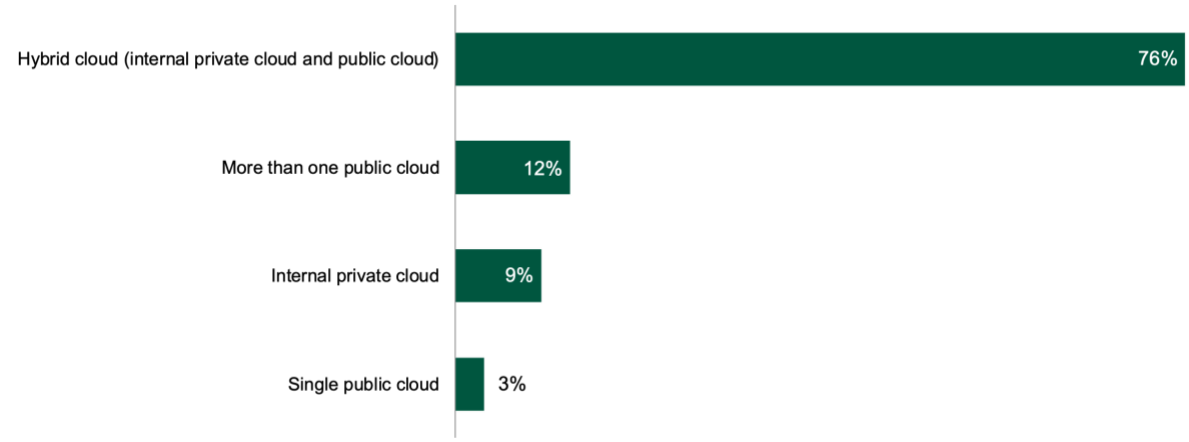
Interviewees said that prior to using the Strata Network Security Platform, their organizations leveraged traditional firewalls with point solutions to secure their environments. They noted that their organizations lacked interconnected security technology and security and their IT teams tried to keep up with evolving business needs. Digital transformation initiatives pushed more data, applications, and processes to the cloud while other core business functions remained on-premises. Adding to the complexity was the need to support more flexible and remote work options for employees as employee expectations and other environmental factors drove demand for remote access to critical applications and data. However, this piecemeal security approach left organizations with as many as 17 different vendors in their security stacks. This made it challenging for security operations (SecOps) teams to integrate technologies, benefit from analytics, apply consistent policies, and provide end users with uninterrupted access to data and applications.

Additionally, the lack of a unified platform and NGFW capabilities left the organizations stuck in a cycle of devoting valuable resources to security management, operations, and maintenance activities while their work on new initiatives and enhancements — both within security and for general development — fell to the wayside.

After the investment in Palo Alto Networks' Strata Network Security Platform, the interviewees gained access to the Panorama security management solution, a centralized visibility tool. Panorama significantly reduced investigational effort and freed up valuable resources to focus on enhancing, rather than maintaining, security. The interviewees' organizations deployed some or all of these network security components and SD-WAN solutions from Palo Alto Networks.

Key results from the investment in the platform include efficiency gains for IT, security, and networks operations teams, business end users, and in-store workers; a reduced likelihood of a data breach with the enablement of Zero Trust; reduced costs associated with licensing and managing legacy point-solution infrastructure due to vendor consolidation to achieve Zero Trust; and improvements to both IoT Security and SD-WAN capabilities.

"Where is your organization currently hosting its data, applications, and workloads?"



Base: 158 IT security decision-makers with experience using Palo Alto Networks Software Firewalls at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, August 2023

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Improved security and IT operational efficiency totaling savings of $2.9 million.** Strata Network Security Platform enables the composite organization to automate previously manual processes to better define rules for alerts and ultimately improve visibility into network traffic. Security and IT operations teams quickly identify and respond to potential threats, reducing the number of incidents requiring manual investigation by 65%, decreasing mean-time-to-resolution (MTTR) by 25%, and reducing the number of devices requiring reimaging. Over a three-year period, these time savings total $2.9 million for the composite organization.
- **Efficiency gain of 80% in firewall deployment, policy changes, and new site setups.** The composite organization requires significantly less effort to deploy NGFWs than it did for its legacy firewalls, and Palo Alto Networks software firewalls also require less active effort to manage. Beyond having teams for basic deployment and maintenance, the composite organization also requires security and network operations teams to adjust and fine-tune security devices to ensure

they meet security standards. This efficiency gain is worth a three-year, risk-adjusted savings of close to $2.2 million.

- **Improved end-user productivity by reducing disruption and system downtime, totaling $26.5 million in business value.** The Strata Network Security Platform delivers a seamless working experience for end users, regardless of the location they work from. The different Palo Alto Networks solutions in the platform offer better integration and compatibility, as well as better overall performance. For end users, the Strata Network Security Platform offers time savings with remote logins, reduces the number of security incidents causing business disruptions and downtime, and increases network availability and performance. Over three years, this translates to a productivity increase for end users that is worth almost $26.5 million in business value.
- **Cost savings from retiring and avoiding security infrastructure, worth $8.3 million.** Strata Network Security Platform enables the composite organization to retire and replace legacy firewall solutions, as well as consolidate its security tech stack to reduce unnecessary redundancy in its environment. Using CDSS also allows the composite organization to consolidate its spending on security. Additionally, Prisma SASE can enable further savings by reducing the number and complexity of vendor relationships. The cost savings from all the vendor consolidation provides a three-year, risk-adjusted savings of $8.3 million for the composite organization.
- **Cost savings from decreased likelihood of a data breach by 15%.** The Palo Alto Networks NGFWs and other Network Security Platform solutions deliver comprehensive Zero Trust security for the entire composite organization. The different CDSS subscriptions provide a more secure environment for various activities and use cases across the organization, including preventing malware, securing IoT devices from AI-powered threats, and AI-driven URL filtration. These different subscriptions also mean Prisma SASE better fills security gaps that previously existed. As a result of all these vectors, the composite organization carries less risk and is less likely to experience a costly breach even as the volume and sophistication of threats continues to rise. Over three years, this benefit amounts to $1.4 million.

"[Palo Alto Networks] is a cornerstone of our security program. If we didn't have it, we would probably be in trouble managing different consoles and having feature limitations as certain models of firewall have certain capabilities. Without it, I think we would have a lot less certainty about performance."

DIRECTOR OF NETWORK SECURITY ENGINEERING, FINANCIAL SERVICES

Time savings in handling security incidents

60%

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Increased visibility across security environments.** Leveraging the different components of the Strata Network Security Platform allows the composite to easily visualize both north-south and east-west traffic across its network. Instead of needing to consult multiple vendor dashboards to get a full sense of security and traffic, security and IT operations staff can consult and make changes with just the centralized management capabilities. Beyond quantified time savings and efficiencies, this visibility provides leadership teams with ease of use as organizations continue to optimize their security stack.
- **Improved integration between tools and across the platform.** Palo Alto Networks' network solutions work seamlessly with each other. Optimized integration provides a seamless experience from start to finish — including set up, deployment, and management. It also means security teams can be

confident there are no gaps or potential vulnerabilities that often pop up when integrating a patchwork of multivendor security solutions.

- **Improved employee experience (EX).** The composite organization also sees improvements in EX for security and IT operations staff and also for end users. End users enjoy reduced downtime and network processing speeds and availability that is not encumbered by security incidents. Security and IT staff experience efficiencies across their jobs, allowing them to focus on higher-value work and be able to proactively approach problems instead of constantly playing catch-up.

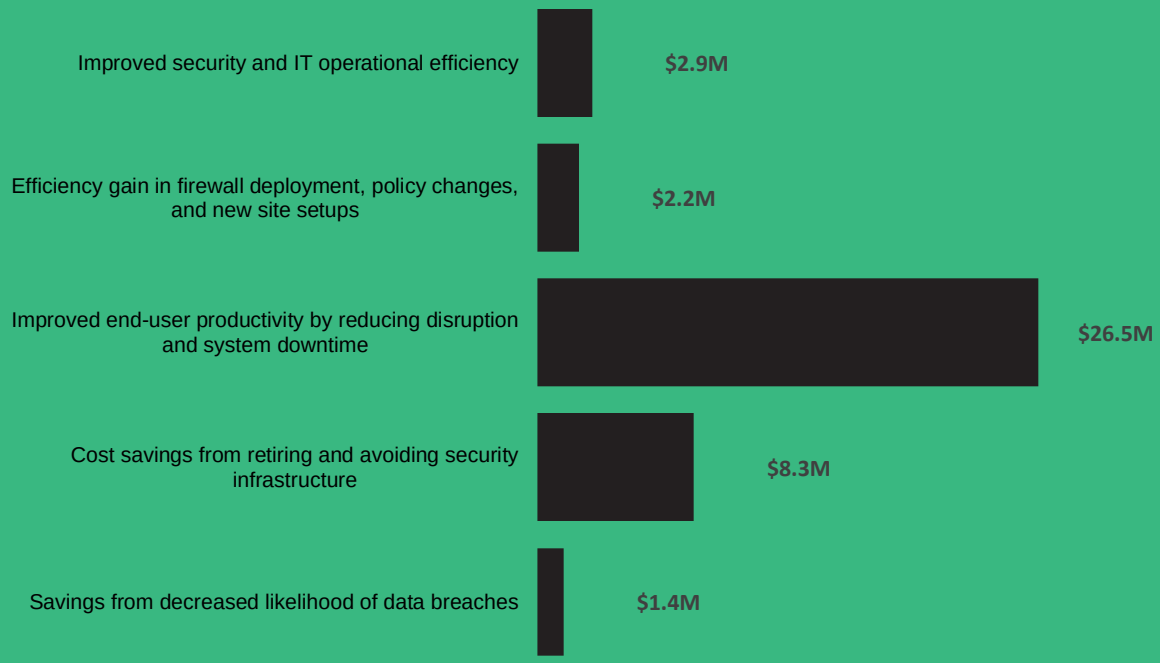
Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Installation and deployment costs totaling $2.6 million over three years.** As with any technology deployment, the composite requires time and labor to set up and install the various components of the Strata Network Security Platform. Most of this effort is focused on Year 1, as less effort and time is needed in subsequent years as the network security environment is completed.
- **Time investments for user training and ongoing management totaling $330,000 over three years.** Additional resources are also required to train users on the Palo Alto Networks solutions and for ongoing management. The Strata Network Security Platform requires less training than legacy solutions and provides more effective and efficient training, thus allowing employees to get up to speed faster and expand their skill sets. Once trained, the team spends some time maintaining and managing the system on an ongoing basis.
- **Subscription and services costs totaling $12.1 million over three years.** Firewall costs include both initial hardware costs, as well as ongoing subscription and services costs required for both NGFWs along with the Panorama management system. Software firewalls are billed by usage in a credits system. CDSS subscription costs include: intrusion detection and prevention systems (IPS/IDS), web security, web proxy, VPN, advanced URL filtering, malware analysis (e.g., sandboxing), and domain name system (DNS) security, SaaS security applications, data loss prevention, and enterprise IoT/OT security solutions. Prisma SASE includes payment for Prisma Access, Prisma SD-WAN hardware appliance, and the subscription, all of which are impacted by the number of branches where it is installed.

The representative interviews and financial analysis found that a composite organization experiences benefits of $41.3 million over three years versus costs of $15.1 million, adding up to a net present value (NPV) of $26.2 million and an ROI of 174%.

ROI	BENEFITS PV	NPV	PAYBACK
174%	$41.3M	$26.2M	<6 months

Benefits (Three-Year)



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in the Strata Network Security Platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the Strata Network Security Platform can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Palo Alto Networks and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in the Strata Network Security Platform.

Palo Alto Networks reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Palo Alto Networks provided the customer names for the interviews but did not participate in the interviews.

1. **Due Diligence**
   Interviewed Palo Alto Networks stakeholders and Forrester analysts to gather data relative to the Strata Network Security Platform
2. **Interviews**
   Interviewed nine representatives at organizations using the Strata Network Security Platform to obtain data about costs, benefits, and risks.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.
5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

The Palo Alto Networks' Strata Network Security Platform Customer Journey

Drivers leading to the Strata Network Security Platform investment

Interviews			
Role	**Industry**	**Region**	**Total Employees**
Principal architect	Healthcare	$30 billion	15,000
Director of security architecture and engineering	Manufacturing	$17 billion	160,000
Senior vice president of IT	Financial services	$3 billion	3,000
Senior director	Hospitality	$20 billion	380,000
Enterprise network architect	Government	$16 billion	400,000
Information security architect and CISO	Healthcare	$2.2 billion	11,000
Director of network security engineering	Financial services	$1.9 billion	2,500
Associate vice president	Financial services	$50 billion	60,000
Associate director	IT services	$16 billion	87,000

KEY CHALLENGES

Forrester interviewed nine representatives from organizations with experience using Palo Alto Networks' Strata Network Security Platform, and surveyed an additional 158 respondents on their usage of Software Firewalls. For more details about these individuals and the organizations they represent, see Appendix B. Prior to using the Strata Network Security Platform, the interviewees told Forrester they typically worked in environments with inconsistent and incomplete security. They used a disparate

collection of competitor security solutions that culminated in a hodgepodge approach where they pursued a multitude of providers across their security infrastructures. More commonly, organizations would add solutions as needed to provide patchwork coverage to support their growing and changing businesses. They often had to backhaul their network traffic to data centers for security policy enforcement, which resulted in negative end-user experience. Additionally, scaling into new offices or providing hybrid and remote workers with security was incredibly challenging.

The interviewees noted how their organizations struggled with common challenges, including:

- **The need to update security for a modern work environment.** Interviewees emphasized the changing requirements and challenges of modern work as a main driver toward a new security paradigm. Modern work realities (e.g., the rise of hybrid and remote work, increased adoption of cloud technologies, and enhanced sophistication and prevalence of cybersecurity attacks) meant that legacy security solutions could not meet organizations' evolving security needs. The director of security architecture and engineering at a manufacturing organization described: "One of the biggest risks that we have today is the speed that technology causes change to companies. More and more people are working out of the office. The old-fashioned way of doing security is you had everyone connected over to the same network, in closed locations. That no longer works."
- **Security gaps from disparate solutions that did not integrate and work well together.** Interviewees noted that using disparate solutions caused security gaps in their environment. Interviewees faced one of two problems: Either their legacy solutions were not comprehensive enough to provide full coverage for an ever-evolving cybersecurity threat, or the different point solutions would neither integrate nor work well with one another. The enterprise network architect in government said, "We realized we had gaps in our security maintaining so many disparate solutions."
- **Inconsistency in user experience impact productivity.** Interviewees also noted that they experienced much disruption with their previous environments which were either caused by cybersecurity threats, or by a security measure responding to a potential threat that ended up being invasive to the overall

system. As a result, many business and end users faced disruptions to their work for periods of time, which could quickly become frustrating. The senior vice president of IT at a financial services company said: “For a user, using their laptop at home vs. in the office the next day are two totally different experiences, [with] different technologies on the back end. This can cause disruption in their workflow, such as needing to raise tickets or asking our operations team to investigate what’s happening. If there’s a policy mismatch or a vendor not supporting something the user is trying to do, there is a lot of productivity cost from that standpoint.”

- **Challenges in scaling their existing security environment.** Finally, interviewees noted how their existing security solutions were unable to match their business growth. The senior director in hospitality said: “Our organization has grown so much. Having individually-managed routers has become a nightmare to manage. Particularly when wanting to make changes to policy — historically, we have to touch every single router in the environment.”

INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- **Reduce risk by creating a less complex and more integrated security environment.** Interviewees sought to gain security that is more comprehensive and easier to manage with Palo Alto Networks. Instead of managing multiple security point solutions with limited visibility across their security infrastructure, interviewees turned to Palo Alto Networks to eliminate inefficiencies and shore up their environments from cybersecurity threats. They also noted that Strata Network Security Platform’s components integrated seamlessly with each other to provide easy-to-manage and comprehensive security. The director of security architecture and engineering at a manufacturing company emphasized that, “The consolidation and integration with the other tools is key to reducing the complexity of the architectures and being able to mitigate risk easily or more effectively.”
- **Offer extensive industry knowledge.** As security concerns and threats rapidly evolve, interviewees needed a well-established partner they could rely on to know their space, as well as provide solutions and support in rapidly-changing

environments. The information security architect and CISO at a healthcare company shared their organization's journey: "We started with Palo Alto Networks' firewalls as they are the leaders in the space. … We had a great experience with their expertise and capabilities." Since its initial firewall investment, this interviewee's organization has expanded its use of Palo Alto Networks security solutions.

> "We chose Palo Alto Networks because integration was easy. Our team was already knowledgeable about their solutions. Also, we could integrate [the different solutions] into the same central management, making it a centralized effort to configure everything."
>
> **INFORMATION SECURITY ARCHITECT AND CISO, HEALTHCARE**

> "Palo Alto Networks is best of the breed in terms of the technology around firewalling. It's easy to use and integrate and delivers maximum security."
>
> **DIRECTOR OF SECURITY ARCHITECTURE AND ENGINEERING, MANUFACTURING**

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the nine interviewees and the 158 surveyed decision-makers, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The composite organization is a distributed enterprise with 50,000 employees and $7 billion in annual revenue. Thirty-three percent of its workforce work remotely or are hybrid workers. It has 400 sites including its headquarters, data center, cloud, branch offices, and retail and manufacturing locations. On average, the composite's security team responds to 1,200 incidents a week, or 62,400 in the first year, with each incident taking an average of two hours to resolve.

Deployment characteristics. The composite organization deploys both physical and software firewalls (i.e., virtual, container, managed service) to cover north-south and east-west traffic in its data centers and clouds. Firewall management is centralized using Palo Alto Networks Panorama. The organization also uses Palo Alto Networks CDSS to supplement each NGFWs deployment (i.e., physical, virtual, cloud-delivered) with 24/7 monitoring of all vulnerabilities. Advanced Threat Prevention, Advanced URL Filtering, DNS Security, and Prisma SASE handles all web-borne threats, and Advanced WildFire tackles all file-based threats. This provides protection against zero-day threats for all threat vectors with inline machine learning and updates delivered in seconds or less. The organization deploys Palo Alto Networks' Enterprise IoT Security to monitor and secure expanding device risk from IoT.

Finally, the organization uses Palo Alto Networks Prisma SASE to securely connect remote networks at its retail locations and branch offices, as well as to connect its remote and hybrid workers. The organization leverages end-of-life cycles with legacy solutions and then invests time to test the deployment of the Strata Network Security Platform to ensure a smooth transition away from its legacy solution. The network security team is involved in deployment.

KEY ASSUMPTIONS

$7 billion revenue

50,000 employees

33% of employees are remote or hybrid

400 sites

Four data centers

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Improved security and IT operational efficiency	$819,170	$1,222,937	$1,512,437	$3,554,544	$2,891,708
Btr	Efficiency gain in firewall deployment, policy changes, and site setups	$876,017	$884,623	$893,229	$2,653,869	$2,198,569
Ctr	Improved end-user productivity by reducing disruption and system downtime	$10,661,625	$10,661,625	$10,661,625	$31,984,875	$26,513,883
Dtr	Cost savings from retiring and avoiding security infrastructure	$3,332,000	$3,332,000	$3,332,000	$9,996,000	$8,286,191
Etr	Savings from decreased likelihood of data breaches	$1,542,480	$0	$0	$1,542,480	$1,402,255
	Total benefits (risk-adjusted)	$17,231,291	$16,101,185	$16,399,292	$49,731,768	$41,292,606

IMPROVED SECURITY AND IT OPERATIONAL EFFICIENCY

Evidence and data. Interviewees noted that moving to Prisma SASE reduced SecOps and network operations (NetOps) team workloads. This is a result of the managed service aspect of the solution, as well as various automation of activities that can be implemented in the process.

- The principal architect in healthcare noted: “Previously, we would have multiple teams involved in SecOps. There was a software layer, a hardware layer, and an application layer. Today, those three formations have been removed. We only have application SME people. So, we can rely on one or two people vs. five to 10.”

- The same interviewee further highlighted the ease of scaling with Prisma SASE: “Scaling is a lot easier. The same policies apply. Scaling is done automatically. Without PANW, we would have to add additional gateways ourselves. We would have to increase back-end systems that deal with databases and all the back-office processing that comes with that.”
- The director of security architecture and engineering in manufacturing shared: “In terms of making policy changes with SASE, we went from four business days to less than one hour. We make around 120 changes per day [e.g., 80% of time].”
- The same director also specifically noted the value their organization received from using Autonomous Digital Experience Management (ADEM): “My networking team uses ADEM for each time they receive a ticket from the help desk or the service desk around network latency. They use ADEM to understand where the problem is.”
- The senior director at a hospitality organization said: “With SD-WAN, setting up is a single push. That’s minutes or hours vs. weeks of multiple people’s time. Previously, it was easily five or six people working through changes like that over a two-week period. We do two to three change cycles per quarter.”

Modeling and assumptions. For the purpose of the composite organization, Forrester assumes:

- With the legacy solution, 1,200 security incidents per week required multitouch, advanced investigation work from the SecOps team, and these incidents increased by 5% annually.
- The number of incidents that require action initially reduces by 25% in Year 1. This reduction increases to 50% in Year 2, and 65% in Year 3 as Palo Alto Networks solutions enable security testing to be conducted sooner on the core network and cloud perspectives.
- Prior to using Palo Alto Networks, MTTR was 120 minutes. The new capabilities and automation improves MTTR by 25% to 90 minutes.
- The average fully-burdened salary for the SecOps team is $121,500 annually or $58 per hour.

- With the legacy solution, 50 endpoint devices per week required reimaging or other services from the IT operations (IT Ops) team.
- The average fully-burdened salary for the IT Ops team is $81,000 annually or $39 per hour.
- The composite organization recaptures 50% of the efficiency gains.

Risks. Factors that could impact the size of this benefit for organizations include:

- Number of security incidents that require manual intervention before implementing the Strata Network Security Platform.
- Other tools and solutions implemented to support the work of the SecOps and IT Ops team.
- Number of devices requiring service and labor associated with servicing those devices.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.9 million.

Reduction in endpoint devices requiring reimaging with Palo Alto Networks' solutions

60%

"With Palo Alto Networks, we've seen a 60% decrease in the time needed to deal with threats because of automation."

ENTERPRISE NETWORK ARCHITECT, GOVERNMENT

Improved Security And IT Operational Efficiency					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Security incidents requiring manual investigation/remediation with legacy security solution	Composite	62,400	65,520	68,796
A2	Reduction in security incidents requiring manual investigation/remediation with Palo Alto Networks	Interviews	25%	50%	65%
A3	Avoided manual multitouch security incidents	A1*A2	15,600	32,760	44,717
A4	MTTR with legacy solution	Composite	120	120	120
A5	**Subtotal: Time savings due to avoided investigations with Palo Alto Networks**	**A3*A4/60*A8**	**$1,809,600**	**$3,800,160**	**$5,187,218**
A6	MTTR improvement with Palo Alto Networks	Composite	25%	25%	25%
A7	Minutes saved per incident	A4*A6	30	30	30
A8	Average fully-burdened SecOps hourly salary (rounded)	Composite	$58	$58	$58
A9	**Subtotal: SecOps efficiency related to critical alerts due to Palo Alto Networks**	**((A1-A3)*A7/60) *A8**	**$1,357,200**	**$950,040**	**$698,279**
A10	Endpoint devices requiring re-imaging or other services annually	Composite	2,600	2,600	2,600
A11	Time spent per device with legacy solution (minutes)	Composite	45	45	45
A12	Reduction in number of endpoint devices requiring re-imaging with Palo Alto Networks	Composite	60%	60%	60%
A13	Average fully-burdened hourly salary of an IT Ops FTE	TEI standard	$39	$39	$39
A14	**Subtotal: Reduced IT effort for re-imaging**	**((A10*A11)/60)* A12*A13**	**$45,630**	**$45,630**	**$45,630**
A15	Productivity recapture of a security FTE	Composite	50%	50%	50%
A16	Attribution to Palo Alto Networks	Composite	60%	60%	60%
At	Improved security and IT efficiency for operations	(A5+A9+A14)*A15 *A16	$963,729	$1,438,749	$1,779,338
	Risk adjustment	↓15%			
Atr	Improved security and IT efficiency for operations (risk-adjusted)		$819,170	$1,222,937	$1,512,437
	Three-year total: $3,554,544			**Three-year present value: $2,891,708**	

EFFICIENCY GAIN IN FIREWALL DEPLOYMENT, POLICY CHANGES, AND NEW SITE SETUPS

Evidence and data. Survey respondents and interviewees described Palo Alto Networks' Software Firewall components to be much easier to deploy and maintain than their prior solutions, partially due to their digital nature and also the ease of maintenance with centralized visibility and control offered by Panorama. The survey respondents and interviewees said Palo Alto Networks' cloud firewalls offered as managed services are extremely simple to deploy.

Interviewees noted that in addition to helping with initial deployment and routine maintenance, Palo Alto Networks' Software Firewalls saved time for their organizations' higher-level security and network operations employees while ensuring that new endpoint additions to their networks due to remote work or increasing office footprint meet security standards.

- The director of security architecture and engineering at a financial services organization explained: "[With virtual machines,] you don't have to manually go and deploy on each hypervisor. You just have to build out your templates and create a service account that Palo Alto Networks can use. Once the firewalls are deployed, then you just build out your policies."
- The enterprise infrastructure architect at a government agency spoke about how Panorama simplified their organization's management of its network security solutions: "We manage the entire fleet as a single group. We can deploy the same policy set to all of our internet-facing firewalls. Now we've got this huge amount of data that we can see actual results on. We can absolutely be more agile, more dynamic, and more secure because we actually know what we have."
- The senior vice president of IT for a financial services organizations stated: "[With Palo Alto Networks Software Firewalls,] what it boils down to is not having to deal with reengineering everything to implement our policies. We have standardization [and] higher efficacy. … It's a significant improvement."
- The director of network security engineering at a financial services organization shared: "We're able to just go with it. We haven't had a security issue or challenge or ask that we haven't been able to meet."

- Ninety-four percent of the survey respondents told Forrester that Palo Alto Networks' Software Firewalls improved their organizations' management, administration, and operations efforts, while also increasing efficiencies for their organizations' security teams.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The SecOps organization includes 20 FTEs, who spend 90% of their time managing tools, deploying firewalls, and making policy changes.
- Software Firewalls and Strata Network Security Platform enables this work to be done 80% faster each year.
- There are also 12 FTEs in the NetOps organization who spend 25% of their time scaling and setting up new sites.
- Software Firewalls and Strata Network Security Platform enables this work to be done 80% faster in Year 1, 85% faster in Year 2, and 90% faster in Year 3.
- The average annual fully-burdened salary of a NetOps member is $135,000.
- The composite organization recaptures 50% of the efficiency gains.

Risks. Factors that could impact the size of this benefit for organizations include:

- The amount of time the organization spends on deployment and maintenance before deploying Palo Alto Networks' Software Firewalls.
- The size of the team in place to adjust and configure Palo Alto Networks' Software Firewalls for maximum efficiency.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.2 million.

Efficiency gain related to managing tools, deploying firewalls, and managing policy changes

80%

"[By using Palo Alto Networks firewalls as a managed service], we don't have to keep our eyes on it everyday. We don't have to worry about the system, the gateways, or network latency. All that is no longer our concern."

PRINCIPAL ARCHITECT, HEALTHCARE

Efficiency Gain In Firewall Deployment, Policy Changes, And New Site Setups

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	FTEs in the SecOps team	Composite	20	20	20
B2	Percentage of time managing tools, deploying firewalls, and making policy changes	TEI standard	90%	90%	90%
B3	Percentage of efficiency gain due to Palo Alto Networks	Interviews	80%	80%	80%
B4	Total time savings in managing tools, deploying firewalls, and making policy changes	B1*B2*B3*A8*2080 hours per year	$1,737,216	$1,737,216	$1,737,216
B5	FTEs in the NetOps team	Composite	12	12	12
B6	Percentage of time spent scaling and setting up new sites	Composite	25%	25%	25%

B7	Percentage of efficiency gain due to Palo Alto Networks	Interviews	80%	85%	90%
B8	Average annual fully-burdened salary of a NetOps FTE	TEI standard	$135,000	$135,000	$135,000
B9	Total value of efficiency gain for NetOps team	B5*B6*B7*B8	$324,000	$344,250	$364,500
B10	Productivity recapture	TEI standard	50%	50%	50%
Bt	Efficiency gain in firewall deployment, policy changes, and new site setups	(B4+B9)*B10	$1,030,608	$1,040,733	$1,050,858
	Risk adjustment	↓15%			
Btr	Efficiency gain in firewall deployment, policy changes, and new site setups (risk-adjusted)		$876,017	$884,623	$893,229
	Three-year total: $2,653,869			**Three-year present value: $2,198,569**	

IMPROVED END-USER PRODUCTIVITY BY REDUCING DISRUPTION AND SYSTEM DOWNTIME

Evidence and data. Interviewees described a prior environment where end users were consistently impacted by security-related slowdowns. This included downtime due to security breaches or disruptive investigative procedures. End users also found their organization's prior security infrastructure made the move to remote work difficult and time-consuming. Previous solutions centralized around being in-office and connected to one network. During the COVID-19 pandemic and after — as remote and hybrid-work policies persisted — users experienced slowdowns to processing speeds, lengthy and unwieldy login processes, and other inefficiencies that hampered worker productivity.

The Strata Network Security Platform reduced downtime associated with security issues by reducing the number of security incidents, decreasing the MTTR on incidents, and providing a seamless and flexible solution that allowed workers to be productive regardless of their location.

- The enterprise network architect at a government organization shared: "Everyone went home for COVID-19… we had a different competing VPN solution that was failing miserably. We upgraded to Palo Alto Networks' GlobalProtect that run on the hardware firewalls with great success."

- The information security architect and CISO in healthcare shared: “Our previous vulnerability scanning solution was invasive. The aggressiveness of the scanning can sometimes trigger a negative consequence to a device and take it down”
- The senior vice president of IT in financial services noted: “We want to give end users the same experience and performance regardless of how they are accessing the network. With Palo Alto Networks, we have 99.99% performance at or above expectation. [We] can run encryption without sacrificing performance.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- There are 50,000 employees. Of these employees, 45% work directly with cloud products, which are the most affected by Palo Alto Networks’ solutions.
- Any system downtime impacts the productivity of 10% of the employees working directly with cloud products.
- Strata Network Security Platform recoups 30% of the lost time and productivity due to system downtime.
- The average fully-burdened annual salary of a business end user is $87,750.
- The composite organization recaptures 50% of the efficiency gains from reduced system downtime.
- There is a 45% attribution to Strata Network Security Platform.

Risks. Factors that could impact the size of this benefit for organizations include:

- The size of the organization and the percentage of end users whose productivity may be impacted by security solution downtime.
- The complexity of the IT environment, which can impact the amount and significance of downtime experienced due to investigations and device reimaging.
- The geography and industry where the organization operates in, which can impact the average fully-burdened salary for end users.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $26.5 million.

Percentage of time recaptured due to better availability and less downtime

30%

"If we find out about a bug, we can plan on how to deal with it, find the data center, and go on. With our homogenous environment, we were able to minimize our downtime."

ASSOCIATE VICE PRESIDENT, FINANCIAL SERVICES

Improved End-User Productivity By Reducing Disruption And System Downtime					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Employees	Composite	50,000	50,000	50,000
C2	Percentage of work done in the cloud	Composite	45%	45%	45%
C3	Percentage of end users impacted by system downtime	TEI standard	10%	10%	10%
C4	Percentage of time recaptured due to better availability/less downtime with Palo Alto Networks	Composite	30%	30%	30%
C5	Average fully-burdened salary of a business end user	TEI standard	$87,750	$87,750	$87,750

C6	Productivity recapture	TEI standard	50%	50%	50%
C7	Attribution to Palo Alto Networks	Interviews	45%	45%	45%
Ct	Improved end-user productivity by reducing disruption and system downtime	C1*C2*C3*C4*C5*C6*C7	$13,327,031	$13,327,031	$13,327,031
	Risk adjustment	↓20%			
Ctr	Improved end-user productivity by reducing disruption and system downtime (risk-adjusted)		$10,661,625	$10,661,625	$10,661,625
	Three-year total: $31,984,875			**Three-year present value: $26,513,883**	

COST SAVINGS FROM RETIRING AND AVOIDING SECURITY INFRASTRUCTURE

Evidence and data. Interviewees told Forrester that investing in the Strata Network Security Platform enabled a variety of total-cost-of-ownership savings, both from retiring existing solutions and tools and avoiding expenditures for additional capabilities.

- Palo Alto Networks' CDSS subscriptions enabled several interviewees' organizations to replace disparate legacy services, enabling both a reduction in license expenses and consolidation of vendors. The senior vice president of IT for the financial services organization told Forrester: "[We saw a] 30% to 35% reduction across all vendors. CDSS was where the majority of the cost savings were."
- Prisma SASE enabled the interviewees' organizations to retire additional licensing around networking technology. The principal architect for the healthcare organization gave Forrester a few examples: "We had a specific product for remote access. Then, we had what we call our H-security, or the secure gateway. That's the security for remote users. Then, data loss prevention was a separate system. These were three distinct things, separate solutions, that required different expertise and different teams. Now, it's all blended."
- These savings also applied to organizations using Software Firewalls and NGFW.

- Interviewees said the benefits of vendor consolidation were particularly notable by replacing the previous hodge-podge of firewall solutions with Palo Alto Networks. The director of security architecture and engineering at the manufacturing organization explained: “The architecture of our cybersecurity environment is less complex. We are taking out vendors that we don’t need. We are also reducing the number of services that are needed to be provided.”
- The survey of Software Firewall users confirmed this impression: 34% of survey respondents said their organization saw a total reduction of between 10% to 15% in network security asset management costs, and another 28% said their organization saw reductions between 15% and 30%.

Modeling and assumptions. For the composite organization, Forrester assumes the following:

- It spends $8 million per year on its security tech stack.
- It can avoid 20% of this spend due to vendor consolidation via CDSS.
- It can avoid 5% of this spend due to vendor consolidation from Prisma SASE and SD WAN.
- It can avoid 15% of this spend from retiring legacy firewall solutions.
- It can avoid 9% of this spend from implementing additional capabilities related to Software Firewalls.

Risks. Factors that could impact the size of this benefit for organizations include:

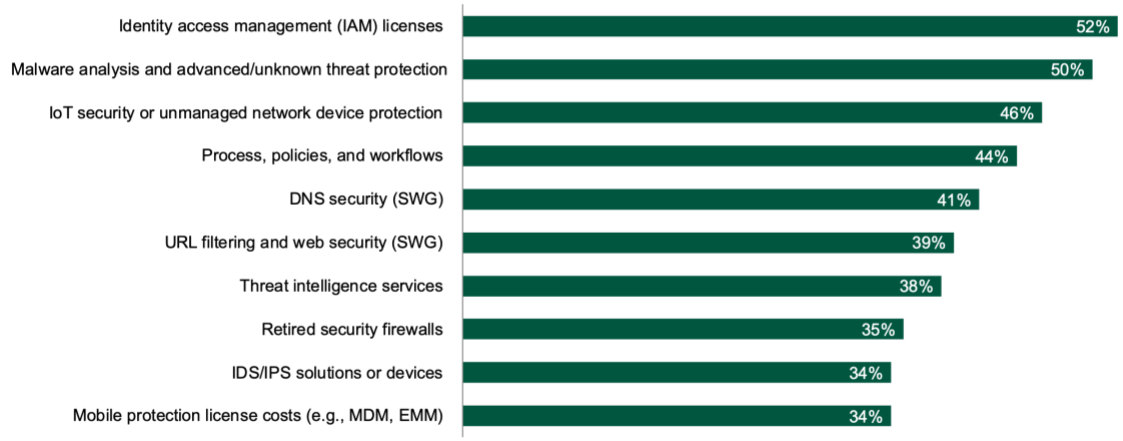
- Size and nature of annual security tech stack.
- Degree to which vendor consolidation, time savings, and additional features and capabilities can reduce spend.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $8.3 million.

Total savings on annual security tech stack spending:

49%

"You noted reduced costs from software licenses, hardware, and/or maintenance and support management due to Palo Alto Networks Software Firewalls (including use with any security service). Which of the following has your organized realized cost savings compared to your previous environment?"



Base: 137 IT security decision-makers with experience using Palo Alto Networks Software Firewalls at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, August 2023

"We had significant cost savings. … Moving to Palo Alto Networks [Software Firewalls] means we're not wasting tons of procurement time on firewall purchases."

ENTERPRISE INFRASTRUCTURE ARCHITECT, GOVERNMENT

Cost Savings From Retiring And Avoiding Security Infrastructure					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Annual security tech stack spending	Composite	$8,000,000	$8,000,000	$8,000,000
D2	Percentage of savings from vendor consolidation related to CDSS	Interviews	20%	20%	20%
D3	Percentage of savings from vendor consolidation related to Prisma SASE and SD WAN	Interviews	5%	5%	5%
D4	Percentage of savings from retiring legacy firewall solutions	Interviews	15%	15%	15%
D5	Percentage of savings from implementing additional Software Firewall capabilities	Interviews	9%	9%	9%
Dt	Cost savings from retiring and avoiding security infrastructure	D1*(D2+D3+D4+D5)	$3,920,000	$3,920,000	$3,920,000
	Risk adjustment	↓15%			
Dtr	Cost savings from retiring and avoiding security infrastructure (risk-adjusted)		$3,332,000	$3,332,000	$3,332,000
	Three-year total: $9,996,000			**Three-year present value: $8,286,191**	

SAVINGS FROM DECREASED LIKELIHOOD OF DATA BREACHES

Evidence and data. Interviewees told Forrester that they were able to reduce security risk by reducing the complexity of their security environments, enabling new security capabilities, and improving security employee productivity.

- Prisma SASE helped interviewees' organizations improve visibility by ensuring that all point solutions were integrated and communicated with each other. The director in manufacturing noted, "Having the security perimeter be around the user instead of a closed location reduces the risk."
- Software firewalls provided better filtration and remediation capabilities to prevent potential breaches, and reduced firewall downtime. The director of network security engineering for the financial services organization shared: "Palo Alto

Networks' Software Firewalls [are] a cornerstone of our security program. ... If we didn't have them, I think we'd be in trouble."

- Palo Alto Networks' NGFWs delivered full environmental visibility and closed gaps to reduce vulnerabilities. The director of security architecture and engineering at a manufacturing company noted, "We have reduced the risk by 100% because today we are doing device posture and identity check properly."
- Palo Alto Networks CDSS provided organizations with 24/7 coverage and support, including automated updates to all NGFWs to protect against the latest threats. The enterprise network architect in the government agency said: "We have not seen a significant breach since 2021. On average, we would have one every six to nine months before Palo Alto Networks. That is due to the threat engine on the firewall."

Modeling and assumptions. For the composite organization, Forrester assumes the following:

- It experiences 3.2 data breaches per year.
- Each data breach costs the organization $2.65 million, or $53 per employee.
- Each data breach also impacts 18% of the organization's 50,000 employees productivity, causing 3.6 lost hours per employee impacted.
- Palo Alto Networks' solutions reduce the likelihood of a data breach by 15%.

Risks. Factors that could impact the size of this benefit for organizations include:

- Number and cost of breaches experienced per year.
- Degree to which breaches can be avoided by improved visibility, vendor consolidation, and improved support.
- Degree to which breaches impact employee productivity.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.4 million.

Reduced likelihood of a data breach

15%

"When we see something coming, that will trigger our signal to light up. That could be from Advanced WildFire, DNS, or any other tool. That will then trigger our playbook on how we respond. We are now more aware of potential threats."

ENTERPRISE INFRASTRUCTURE ARCHITECT, GOVERNMENT

Savings From Decreased Likelihood Of Data Breaches					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Average number of data breaches per year	Forrester research	3.2	3.2	3.2
E2	Average potential cost of a data breach, exclusive of internal user downtime	Forrester research	$2,650,000	$2,650,000	$2,650,000
E3	Reduced likelihood of a breach	Composite	15%	15%	15%
E4	**Subtotal: Avoided costs of remediation post-breach**	**E1*E2*E3**	**$1,272,000**	**$1,272,000**	**$1,272,000**
E5	Internal employees	C1	50,000	50,000	50,000
E6	Average fully-burdened salary of a business user (hourly)	C5/2080 hours	$42	$42	$42
E7	Diminished/eliminated internal user productivity hours per breach	Forrester research	3.6	3.6	3.6

E8	Average percentage of employees affected per breach	Composite	18%	18%	18%
E9	**Subtotal: Cost of reduced internal productivity**	**E1*E3*E5*E6*E7*E8**	**$656,100**	**$656,100**	**$656,100**
Et	Savings from decreased likelihood of data breaches	E4+E9	$1,928,100	$0	$0
	Risk adjustment	↓20%			
Etr	Savings from decreased likelihood of data breaches (risk-adjusted)		$1,542,480	$0	$0
	Three-year total: $1,542,480			**Three-year present value: $1,402,255**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Increased visibility across security environments.** Interviewees noted that one of the main sources of value from implementing Palo Alto Networks' solutions is the enhanced visibility they now have on the condition, performance, and usage of different parts of its security organization.
    - The senior vice president of IT in financial services said: "The other very attractive thing about Palo [Alto Networks] was the interface and visibility. Their reporting was the best for us in terms of UI [user interface]. It instantly performed better than our purpose-built reporting software that we had struggled to maintain."
    - The principal architect in healthcare shared, "We're able to easily monitor traffic and see what is actually happening on the network."
- **Improved integration with the broader security tech stack.** As mentioned previously, interviewees sought a simpler security environment, and part of that equation was a security tech stack whose components integrated well with one another, as well as with other Palo Alto Networks solutions implemented in the environment.

  - The director of security architecture and engineering at a manufacturing company said: “Palo Alto Networks gives you the path to integrate more things and continue to optimize your environment easily. It’s integrated and optimized to be easy to use and secure.”
  - The enterprise network architect for the government organization explained: “I definitely see a lot of benefit from working with a suite of products that play together. Everything is integrated. It’s allowed us to optimize and make our security better, faster, and cheaper.”

- **Improved EX.** Interviewees noted that the cumulative effect of the above benefits was to improve ease of use for employees, and reduce troubleshooting. The director in manufacturing noted: “Palo Alto Networks came and worked perfectly. We had great feedback from people in terms of quality of experience.”
- **Faster, more secure migrations.** Interviewees said that with their organizations’ networks more thoroughly secured, they feel more confident proceeding quickly and confidently with larger migrations. The associate vice president at a financial services organization told Forrester: “Having that ability to be nimble has let us turn things around faster. … We’re not a roadblock in teams getting what they want to get done in a secure way.”

> “Having PANW prepares you for the rest of the path, which is to integrate more things such as remote networks, branch offices, and CASB.”
>
> **DIRECTOR OF SECURITY ARCHITECTURE AND ENGINEERING, MANUFACTURING**

> "We are able to easily monitor traffic and see what is actually happening on the network."
>
> SENIOR VICE PRESIDENT OF IT, FINANCIAL SERVICES

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement the Strata Network Security Platform and later realize additional uses and business opportunities, including:

- **Long-term, virtuous impact.** In the long run, having a complete security solution in the composite organization's environment can enable future growth and the ability to easily scale or adapt to meet the business' changing needs.
- **Consistent security and enforcement.** With a uniform operating system across all form factors (e.g., hardware, software, SASE) and security services that can be applied universally, organizations will find onboarding and operations to be much more streamlined while ensuring consistent security everywhere.
- **Attack prevention from new threats.** Palo Alto Networks leverages threat intelligence from its Unit 42 team and extensive data from its vast customer network to deliver robust security outcomes in real time. Their AI continually evolves to stay ahead of adversaries who exploit AI and cloud computing for evasive threats, providing next-generation AI/ML, Deep Learning, and Gen AI specifically built for cybersecurity.
- **Flexibility to allocate resources.** While many of the interviewees said their organization uses Palo Alto Network's enterprise license agreement (ELA)-based pricing model for Software Firewall, associate director at an IT services firm described how using Palo Alto Network's credit-based pricing model gave their

organization significantly more flexibility in deploying its firewalls than it had before: “We can spin a firewall down [and] send the credits to another team in the world that may need some. … We can quickly spin up and spin down based on the projects we’re working on. … We’re not locked in. We have this flexibility.”

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Ftr	Installation and deployment costs	$1,552,500	$659,813	$349,313	$194,063	$2,755,688	$2,586,820
Gtr	Time investment for user training and ongoing management	$14,256	$127,116	$127,116	$127,116	$395,604	$330,375
Htr	PANW subscription and services costs	$1,515,623	$4,275,390	$4,275,390	$4,275,390	$14,341,793	$12,147,885
	Total costs (risk-adjusted)	$3,082,379	$5,062,319	$4,751,819	$4,596,569	$17,493,084	$15,065,080

INSTALLATION AND DEPLOYMENT COSTS

Evidence and data. Interviewees described various processes for deploying different parts of the Strata Network Security Platform from Palo Alto Networks.

- Interviewees noted that deploying Prisma SASE was an involved process that required collaboration from different teams at their organizations (e.g., IT, SecOps, and NetOps) with the Palo Alto Networks team.
- Interviewees and survey respondents said their organizations could deploy Palo Alto Networks Software Firewalls — especially Cloud NGFW Software Firewalls — much more quickly than their legacy firewalls.
    - The length of implementation varied based on resources available and organizational appetite for speed. Some interviewees got their firewalls up and running in a matter of weeks due to external pressure when the COVID-19 pandemic forced the workforce to work remotely, while others shared that their organization took over a year to slowly migrate existing firewalls over to Palo Alto Networks due to lack of internal focus. Processes were consistent across organizations, with typical steps

including analyzing current environment, setting up the solution, and making adjustments as needed once deployed.

- Interviewees noted that the installation and deployment process of Palo Alto Networks CDSS depended on the exact solution implemented, by largely including analyzing the current environment where the solution will be implemented, setting up the solution, and making adjustments, especially if there were specific needs or use cases at the organization.

Modeling and assumptions. For the composite organization, Forrester assumes the following:

- It has a network team of 10 FTEs installing PANW.
- This network team spends 80% of their time on these tasks for initial implementation, 40% in Year 1, 20% in Year 2, and 10% in Year 3.
- An IoT deployment team of NetOps employees works on deployment and installation. This team consists of eight members upon initial implementation, and two members from Year 1 to Year 3 of the investment.
- The IoT team spends 25% of its time on implementation tasks, and 12.5% of its time on tasks from Year 1 to Year 3 of the investment.

Risks. Factors that could impact the size of this cost for organizations include the following:

- Size and salaries of the network and IoT teams.
- Amount of time required for implementation and deployment tasks.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.6 million.

> "I deployed [NGFW] in less than two weeks for 35,000 employees who were being pushed to remote. Less than two weeks to deploy, and everyone was happy."
>
> DIRECTOR OF SECURITY ARCHITECTURE AND ENGINEERING, MANUFACTURING

Installation And Deployment Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Network team members working on PANW installation	Composite	10	10	10	10
F2	Time spent per staff member	Interviews	80%	40%	20%	10%
F3	Annual fully-burdened salary of a NetOps FTE	TEI standard	$135,000	$135,000	$135,000	$135,000
F4	**Subtotal: Implementation labor for PANW network security (excluding IoT)**	**F1*F2*F3**	**$1,080,000**	**$540,000**	**$270,000**	**$135,000**
F5	IoT deployment team members	Composite	8	2	2	2
F6	Time spent per staff member	Interviews	25.0%	12.5%	12.5%	12.5%
F7	**Subtotal: Implementation and fine-tuning labor for IoT security deployment**	**F3*F5*F6**	**$270,000**	**$33,750**	**$33,750**	**$33,750**
Ft	Installation and deployment costs	F4+F7	$1,350,000	$573,750	$303,750	$168,750
	Risk adjustment	↑15%				
Ftr	Installation and deployment costs (risk-adjusted)		$1,552,500	$659,813	$349,313	$194,063
	Three-year total: $2,755,688			**Three-year present value: $2,586,820**		

TIME INVESTMENT FOR USER TRAINING AND ONGOING MANAGEMENT

Evidence and data. The amount of internal effort to train users and manage the Strata Network Security Platform from Palo Alto Networks varied based on which parts of the platform organizations chose to implement.

- Once set up, interviewees noted varying degrees of what ongoing management would look like for Prisma SASE. For some, it was an easy platform to monitor, while others spent additional time and investment to ensure that they fully maximized the potential of the solution for their organizations.
- Interviewees noted that ongoing management of CDSS was relatively easy for their team. Additionally, the training resources that Palo Alto Networks provided were effective and gave employees the tools and knowledge they needed to be successful working across the various products and solutions.
- Interviewees noted easy and straightforward ongoing management of NGFWs, especially when leveraging Panorama. Their security teams typically transitioned from managing firewalls from multiple vendors; where making updates and policy changes was time-consuming and tedious. The Palo Alto Networks centralized management tool streamlined and simplified the process of making these updates and policy changes. User training was also reported to be effective and simple, allowing employees to easily transition from working with legacy solutions to Palo Alto Networks.
- Interviewees said that to reap the full benefits of Palo Alto Networks Software Firewalls, their organizations needed teams of managers to maintain, update, and configure the firewalls as necessary.

Modeling and assumptions. For the composite organization, Forrester assumes the following:

- Ten FTEs are trained for ongoing management of the platform.
- These FTEs are trained for 24 hours over the course of the initial implementation, and for six hours each year after the initial implementation.
- These 10 FTEs spend 10% of their time on ongoing management tasks.

Risks. Factors that could impact the size of this cost for organizations include the following:

- Size and salaries of management team.
- Amount of time required for ongoing management.
- Amount of time required for initial and ongoing training.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $330,000.

> "Everything is 100% Panorama-managed and now, instead of managing 104 disparate firewalls, I'm managing firewalls easily by group. Our team spends their day in a single pane of glass in Panorama."
>
> ENTERPRISE NETWORK ARCHITECT, GOVERNMENT

Time Investment For User Training And Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	FTEs receiving training for ongoing management	Composite	10	10	10	10
G2	Hours per training session	Interviews	24	6	6	6
G3	Average fully-burdened hourly salary of a SecOps, NetOps, IT Ops FTE	TEI standard	$54	$54	$54	$54
G4	Internal time investment for user training	G1*G2*G3	$12,960	$3,240	$3,240	$3,240
G5	Percentage of time spent for ongoing management of PANW network security	Interviews		10%	10%	10%
G6	Internal time investment for ongoing management	G1*G3*2,080*G5	$0	$112,320	$112,320	$112,320
Gt	Time investment for user training and ongoing management	G3+G6	$12,960	$115,560	$115,560	$115,560
	Risk adjustment	↑10%				
Gtr	Time investment for user training and ongoing management (risk-adjusted)		$14,256	$127,116	$127,116	$127,116
	Three-year total: $395,604			**Three-year present value: $330,375**		

PANW SUBSCRIPTION AND SERVICES COSTS

Evidence and data. Each component of the Palo Alto Networks Strata Network Security Platform required its own subscription and service costs for the interviewees.

- Interviewees noted that the NGFWs' cost and structure varied by type and usage. Hardware firewalls required an initial hardware purchase followed by annual subscription costs. Software firewalls were priced based on consumption. This varied based on the type of firewall, total usage, and any additional features added, such as the usage of Panorama. Interviewees shared that their software firewalls were often purchased through credits with Palo Alto Networks that could also be used for Palo Alto Networks CDSS software solutions.
- CDSS cost and structure vary by type and usage and are often connected to the NGFWs deployment. Interviewees shared that their Palo Alto Networks solution could also be purchased with credits that could be used on different solutions.
- For PRISMA SASE, interviewees purchased hardware upfront and were able to amortize the subscription costs over the three-year contract term, providing predictable annual costs.

Modeling and assumptions. For the composite organization, Forrester assumes the following:

- It pays an initial cost of $154,350 for Prisma SASE, and $3.135 million each year onwards.
- It pays an initial cost of $1.289 million for costs related to software and NGFWs, and annual costs of $206,733.
- The composite organization pays annual costs of $730,067 for CDSS.
- Pricing may vary. Contact Palo Alto Networks for additional details.

Risks. Factors that could impact the size of this cost for organizations include:

- Total number of users and sites where Palo Alto Networks solutions will be implemented.
- Specific add-ons implemented to further strengthen performance.
- Total consumption of Palo Alto Networks services.

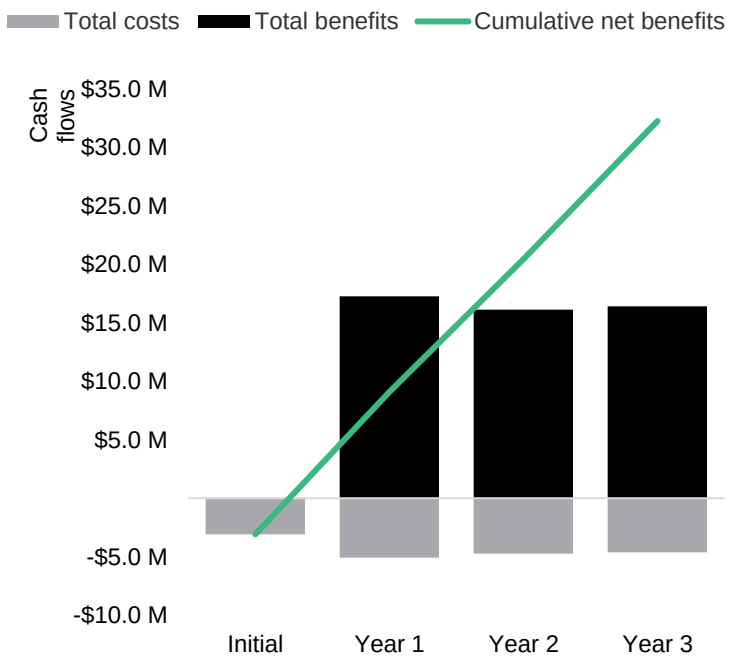
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $12.1 million.

PANW Subscription And Services Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Prisma SASE-related costs	PANW	$154,350	$3,135,000	$3,135,000	$3,135,000
H2	NGFW-related costs	PANW	$1,289,100	$206,733	$206,733	$206,733
H3	CDSS-related costs	PANW	$0	$730,067	$730,067	$730,067
Ht	PANW subscription and service costs	H1+H2+H3	$1,443,450	$4,071,800	$4,071,800	$4,071,800
	Risk adjustment	↑5%				
Htr	PANW subscription and service costs (risk-adjusted)		$1,515,623	$4,275,390	$4,275,390	$4,275,390
	Three-year total: $14,341,793			**Three-year present value: $12,147,885**		

Financial Summary

Consolidated Three-Year Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($3,082,379)	($5,062,319)	($4,751,819)	($4,596,569)	($17,493,084)	($15,065,080)
Total benefits	$0	$17,231,291	$16,101,185	$16,399,292	$49,731,768	$41,292,606
Net benefits	($3,082,379)	$12,168,973	$11,349,366	$11,802,723	$32,238,684	$26,227,526
ROI						174%
Payback period (months)						Less than 6

APPENDIX A: TOTAL ECONOMIC IMPACT

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

Total Economic Impact Approach

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

Present Value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Net Present Value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

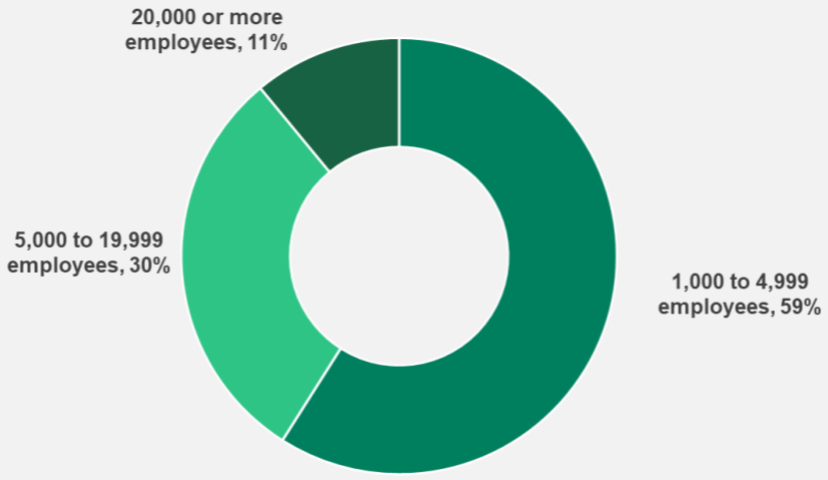
Payback period

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

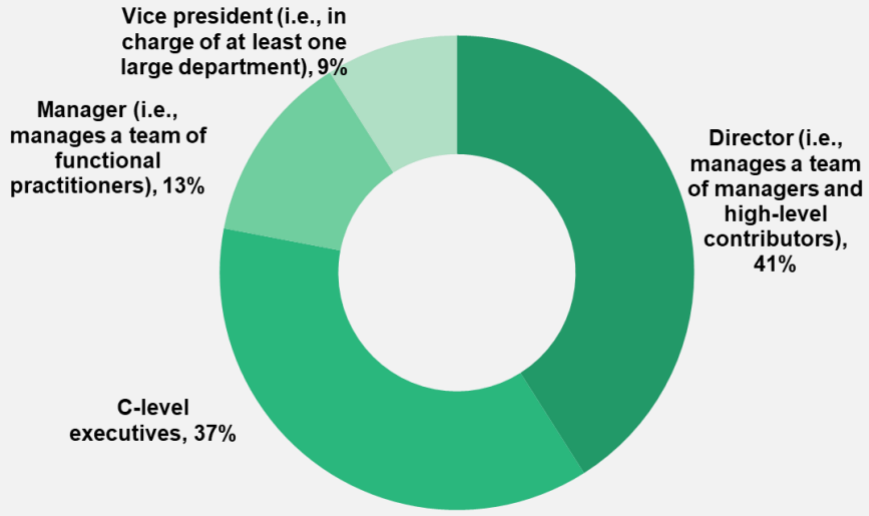
The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

APPENDIX B: INTERVIEW AND SURVEY DEMOGRAPHICS

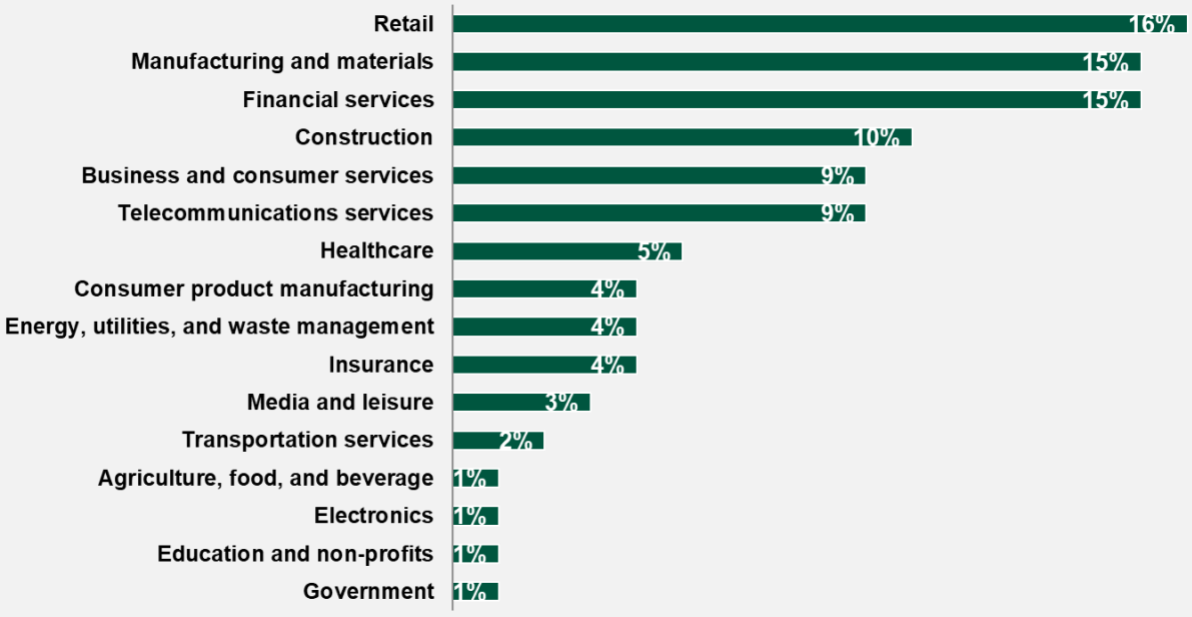
"Using your best estimate, how many employees work for your organization/firm worldwide?"



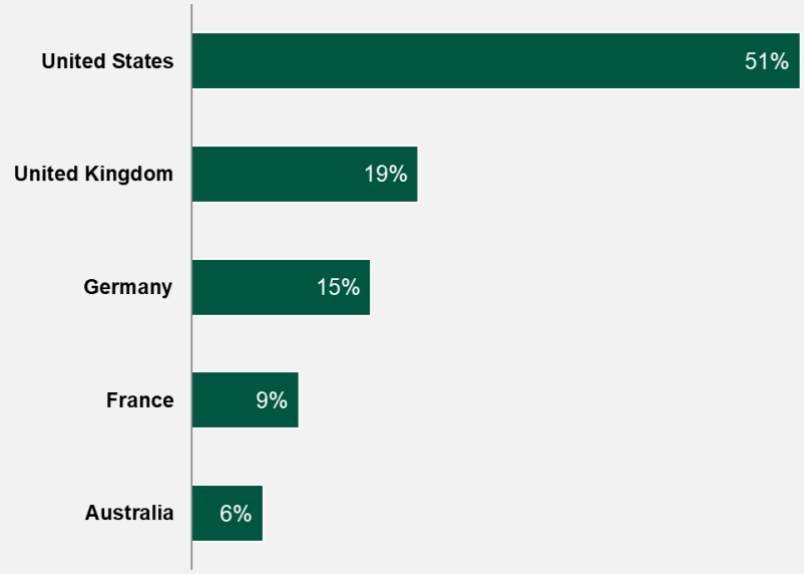
"Which title best describes your position at your organization?"



"Which of the following best describes the industry to which your organization belongs?"



"In which country are you located?"



Base: 158 IT security decision-makers with experience using Palo Alto Networks Software Firewalls at their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, August 2023

APPENDIX C: ENDNOTES

[1] Source: The Modern Definition of NAV, Forrester Research, Inc., April 23, 2024.

[2] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

{/Endnotes}
{/SectionCollapsedAppendix}

{SectionFooter}
{Footer}

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

{/Footer}
{/SectionFooter}

FORRESTER®