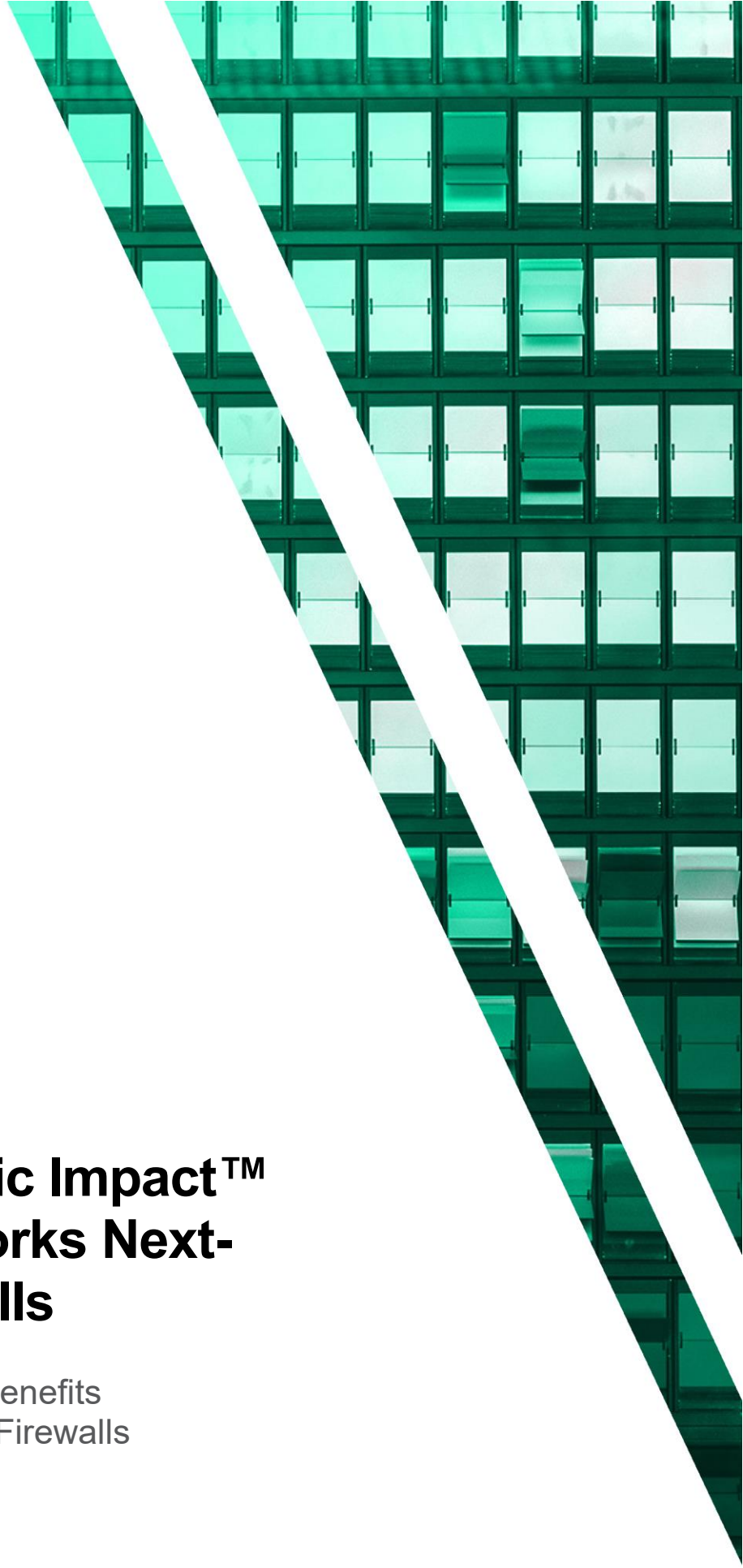
FORRESTER®



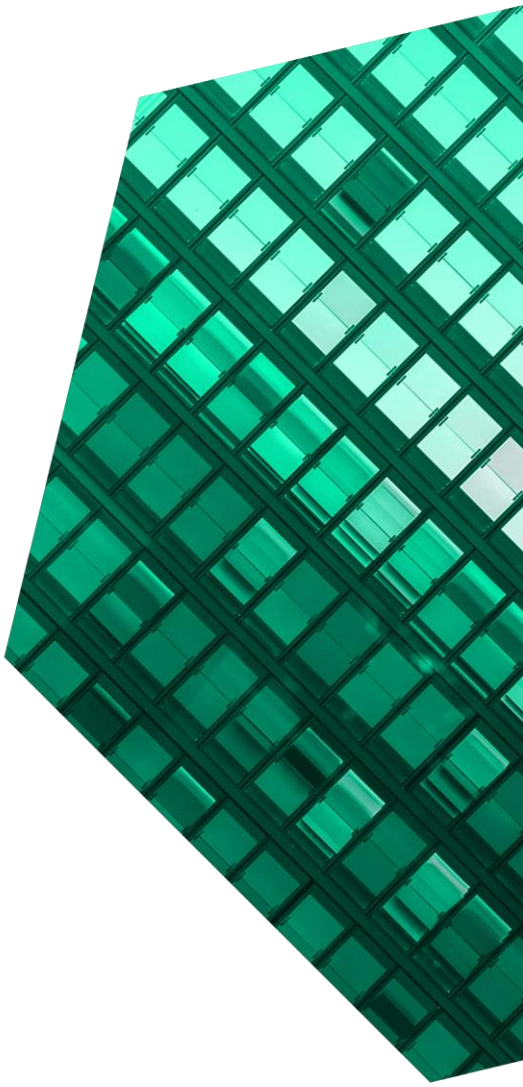
The Total Economic Impact™ Of Palo Alto Networks Next-Generation Firewalls

Cost Savings And Business Benefits Enabled By Next-Generation Firewalls

JANUARY 2024

Table Of Contents

Consulting Team: Isabel Carey
Adi Sarosa



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.

Executive Summary

Firewalls are one of the main and most effective protections against cybersecurity threats. However, traditional hardware firewalls struggle to keep pace with evolving workplace trends, such as the shift to remote work and the increasing volume and sophistication of security threats. Organizations must elevate their existing firewall infrastructure and re-envision their security strategies to provide seamless and scalable protection that goes beyond traditional firewalls of the past.

Palo Alto Networks' machine learning (ML)-powered Next-Generation Firewalls (NGFWs) includes a variety of both hardware and software firewall solutions that provide a Zero Trust experience monitoring both north-south and east-west traffic. The breadth of Palo Alto Networks' firewall offerings can fit a variety of needs to provide both effective protection with ease of use and can build impenetrable protections for the entirety of an organization's network architecture when combined with other Palo Alto Networks security products.

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 cybersecurity company's NGFWs.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of NGFWs on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives from five organizations with experience using NGFWs. 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.

Prior to using Palo Alto Networks NGFWs, these interviewees noted their organizations' security environments were monitored by a variety of point solutions. Though individually effective, many of the point solutions did not integrate well and failed to provide complete and cohesive coverage across the tech stack, leaving significant gaps and vulnerabilities. In addition, security teams lacked visibility across their full ecosystems and were often playing catch-up when dealing with threats and security breaches. Without a unified way to deal with threats, teams struggled with the time-consuming and inefficient management required to work across different vendors.

KEY STATISTICS

Return on investment (ROI)
229%

Net present value (NPV)
$9.82M

KEY FINDINGS

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

- **Increased security and IT operations efficiency totaling savings of $2.5 million.** With Palo Alto Networks NGFWs, the composite organization automates previously manual processes, define better rules for alerts, and improve visibility into network traffic. Security and IT operations teams quickly identify and respond to potential threats, leading to a reduction in the number of incidents requiring manual investigation by 25% to 60%, decreased mean-time-to-resolution (MTTR) by 20%, and a reduction of the number of devices requiring reimaging. Over a three-year period, these time savings totaled $2.5 million for the composite organization.
- **Improved end-user productivity by reducing disruption and system downtime, totaling $5.1 million in business value over three years.** When working with other Palo Alto Networks solutions, NGFWs delivers a seamless working experience for end users, regardless of location. End users saw time savings in remote logins, a reduction in security incidents causing business disruptions and downtime, and increased network availability and performance. Over three years, end users saw a productivity increase that translates to almost $5.2 million in business value.
- **Decreased likelihood of a data breach by 50% after three years.** The comprehensive and seamless support provided by NGFWs and other Palo Alto Networks solutions delivered comprehensive Zero Trust security for the entire organization. As a result, 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 $2.8 million.
- **Provided cost savings in retired and avoided security infrastructure, saving $2.5 million over the modeled period.** The composite organization retires and replaces legacy firewall solutions, as well as consolidates its security vendor tech stack to reduce unnecessary redundancy in its environment. Over three years, the cost savings from vendor consolidation provides $2.5 million in savings for the composite.
- **Reallocated 50% of full-time security professionals to higher-value initiatives due to management efficiencies from vendor consolidation and using a common platform.** By using an increasing network of Palo Alto Networks solutions including NGFWs, the composite organization streamlines management and frees up employee time to focus on higher-value and more strategic initiatives. Over the three-year modeled period, the composite recognizes $1.1 million in benefit.

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

- **Increased visibility across security environments.** Leveraging NGFWs allows the composite to easily visualize both north-south

Time savings in time required to handle security incidents

60%

and east-west traffic across its network. Instead of needing to consult multiple vendor dashboards to get a full sense of traffic and security, security and IT operations staff can consult and make changes with just the centralized management feature that Palo Alto Networks solutions come with. Beyond the time savings and efficiencies discussed in the quantified benefit, this visibility provides ease of use and strategic visibility to leadership as they continue to optimize their security stack.

- **Improved integration between tools and across the platform.** NGFWs work seamlessly with each other, but also integrate easily with the rest of the Palo Alto Networks security ecosystem. Better 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.** The composite organization also sees improvements in the employee experience, not only for security and IT operations staff, but also for end users. Security and IT staff experience efficiencies across their jobs, allowing them to focus on higher-value work and approach problems proactively instead of constantly playing catch-up. End users see reduced downtime and network processing speeds and availability not encumbered by security incidents.

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

- **Installation and deployment costs totaling $2.1 million over three years.** As with any technology deployment, the composite requires time and labor to set up and install the various components of Palo Alto Networks security solutions. It is assumed that installation and deployment of NGFWs in particular takes 55% of the set-up time and effort. The bulk of this effort is focused on Year 1; subsequent years see a decrease in time needed as the security environment is completed.
- **Time investments for user training and ongoing management totaling $315,000 over three years.** Additional resources are also required to train users on the Palo Alto Networks solutions and for ongoing management. Management includes policy updates, upgrades, and other activities related to the health and success of the NGFWs.
- **Firewall subscription and services costs totaling $1.9 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.

The representative interviews and financial analysis found that a composite organization experiences benefits of $14.11 million over three years versus costs of $4.29 million, adding up to a net present value (NPV) of $9.82 million and an ROI of 229%.

ROI	BENEFITS PV	NPV	PAYBACK
229%	**$14.11M**	**$9.82M**	**7 months**

Benefits (Three-Year)

“[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

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 NGFWs.

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 NGFWs 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 NGFWs.

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.

DUE DILIGENCE

Interviewed Palo Alto Networks stakeholders and Forrester analysts to gather data relative to NGFWs.

INTERVIEWS

Interviewed six representatives at five organizations using NGFWs to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

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.

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 NGFWs Customer Journey

Drivers leading to the NGFWs investment

Interviews

Role	Industry	Annual Revenue	Number Of Employees
Director, security architecture and engineering	Manufacturing	$17 billion	160,000
SVP, IT	Financial services	$3.2 billion	3,000
Enterprise network architect	Government	$16 billion	400,000
• Information security architect • CISO	Healthcare	$2.2 billion	11,000
Director of network security engineering	Financial services	$1.9 billion	2,500

KEY CHALLENGES

Prior to investing in Palo Alto Networks NGFWs, interviewees noted their organizations used a disparate collection of competitor security solutions. For some organizations, this culminated in a best-of-breed approach that led to them to pursue a multitude of providers across their security infrastructures. The more common story, however, was of organizations adding solutions as needed to provide patchwork coverage to support their growing and changing businesses.

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

- **The need to update security for modern work environments.** Interviewees emphasized the changing requirements and challenges of modern work as a main driver towards a new security paradigm. Modern work realities, such as the rise of hybrid and remote work, the increasing adoption of cloud technologies, and the rising sophistication and prevalence of cybersecurity attacks, meant 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 measures started to become a blocking point to user experience. … We had people complaining that their work is becoming too slow. We wanted to bring a good quality of experience for the end user while keeping security at max."

Director of security architecture and engineering, manufacturing

The SVP in IT at a financial services firm further explained: "Before Palo Alto Networks, we had a traditional network infrastructure with a hardened firewall perimeter and a soft-squishy inside. We recognizes we needed to move security services closer to the users/resources. I have around

250,000-plus users on the network that I don't trust any more than the internet, so I had to move to an environment where all traffic was vetted."

- **Suboptimal business user experience with legacy security environment.** In their prior environments, interviewees also reported problems with end-user experiences that impacted productivity and disrupted core business functions. Especially in a remote environment, workers reported slow processing speeds and lengthy, multistep login processes. End users were also impacted by downtime and security events, causing work disruptions. IT security leadership struggled with balancing worker productivity and experience with maintaining a secure environment. The enterprise network architect at a government organization described: "We had a different competing VPN solution that was failing miserably, and users didn't like it. Just to log in, users would have to juggle a different authenticator app, a different application on their desktop … It was not working at all."
- **Security gaps from disparate solutions that did not integrate and work well together.** Lastly — and for many, most importantly — interviewees also recognized gaps in the security of their organizations' environments. While using a variety of often overlapping and unconnected systems, not all point solutions integrated or worked well with each other. Struggling to manage and have visibility across the breadth of their solutions often meant security concerns and weaknesses were often not recognized until a breach or security incident occurred. The enterprise network architect in government said, "We realized we had gaps in our security maintaining so many disparate solutions." The information security architect at a healthcare company shared their experience, "To be completely honest, we had a ransomware scare that convinced us we needed to upgrade our security."

"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

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 more comprehensive and easier-to-manage security 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. Interviewees noted that Palo Alto Networks solutions 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 this, saying, "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."
- **Find a partner with extensive industry knowledge.** Interviewees also emphasized their intent to partner with a well-established vendor in the security space. As security concerns and

threats rapidly evolve, interviewees needed a partner they could rely on to know their space and provide solutions and support in rapidly changing environments. The information security architect at a healthcare company shared their 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 their initial firewall investment, this interviewee's organization has expanded their use of Palo Alto Networks security solutions.

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 four interviewees, 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. It has 400 sites including headquarters, data centers, the 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 Year 1, with each incident taking an average of 2 hours to resolve.

Deployment characteristics. The composite organization deploys both physical and software (virtual, container, managed service) firewalls to cover north-south and east-west traffic in its data centers and clouds. Firewall management is centralized using Palo Alto Networks Panorama. In addition to its firewalls deployment, the organization also leverages other Palo Alto Networks solutions, including Prisma SASE, Cloud-Delivered Security Services (specifically Advanced Threat Prevention, Advanced URL Filtering, DNS Security, and Advanced Wildfire), and IoT Security.

Key Assumptions

- **$7 billion annual revenue**
- **50,000 employees**
- **400 sites**
- **Four data centers**

Forrester Perspective: Poisoning Data Will Become A Primary Motivation Of Threat Actors

From A/B testing to large-scale demographic analyses, the results of data and AI models are often used when businesses make critical decisions.

Because of this, altered data — whether it's been altered intentionally or accidentally — reduces the efficacy of marketing campaigns. This can lead to negative customer sentiment and reduce customer engagement, giving attackers incentive to tamper with a business's existing data.

Source: "The Future Of Cybersecurity And Privacy," Forrester Research, Inc., August 3, 2023.

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	Security and IT operations efficiency	$685,679	$1,074,834	$1,277,372	$3,037,884	$2,471,345
Btr	End-user productivity gain	$2,084,940	$2,084,940	$2,084,940	$6,254,820	$5,184,937
Ctr	Data breach risk reduction	$1,119,360	$1,119,360	$1,119,360	$3,358,080	$2,783,683
Dtr	Security infrastructure cost reduction and avoidance	$1,020,000	$1,020,000	$1,020,000	$3,060,000	$2,536,589
Etr	Security stack management efficiency from common platform	$455,625	$455,625	$455,625	$1,366,875	$1,133,072
	Total benefits (risk-adjusted)	$5,365,604	$5,754,759	$5,957,297	$17,077,659	$14,109,626

SECURITY AND IT OPERATIONS EFFICIENCY

Evidence and data. By deploying Palo Alto Networks NGFWs, interviewees reported time savings and efficiencies for both their security and IT operations teams. With Palo Alto Networks, interviewees automated previously manual processes, defined better rules for alerts, and improved visibility into network traffic. With these efficiencies, the interviewees' teams no longer ran from emergency to emergency, and instead focused on other high-value work, such as future-proofing efforts, expanding use cases, and supporting teams.

- The enterprise network architect in government said: "We have extended our automation greatly. We are automating a vast majority of our [threat detection] and automating our responses that feed into our firewalls. We want to keep our analysts out of the loop. We don't want them to manually intervene unless absolutely necessary."
- The director of security architecture and engineering at a manufacturing company told Forrester, "[With Palo Alto Networks], we have reduced our incident response time from 4 hours to a little over 60 minutes."

"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

- The SVP of IT in financial services said, "SecOps' [security and operations'] efficiency increased by roughly 25% for time to resolution for IT tickets and overall resourcing."
- The same interviewee discussed what they do with these time savings: "With their time, the network security team can progress to the next thing. … There are so many things we didn't have time to do in the past like expanding our use cases. … Now we can support more use cases, more compute-based workloads, be able to expand into the cloud more easily, and actually support our teams."

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

- With the previous solutions, 1,200 security incidents per week required multitouch, advanced investigation work from the SecOps team, increasing by 5% annually.
- There is an initial reduction in the number of incidents requiring action by 25% in Year 1. This increases to 50% and 60% in Years 2 and 3 as more security workloads are shifted to Palo Alto Networks solutions.
- Prior to using Palo Alto Networks, MTTR was 120 minutes. With the new capabilities and automation, this improves by 20%.
- The average fully burdened salary for the SecOps team is $121,500 annually or $58 per hour.
- With the legacy solutions, 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 outlined.
- Considering that part of the efficiency is gained from using the different Palo Alto Networks' tools together (Prisma SASE, hardware and software ML-Powered NGFWs, and Cloud-Delivered Security Services [CDSS]), a 55% attribution to NGFWs is assumed.

Risks. The exact benefit realized by an organization may depend on:

- The number of security incidents that require manual intervention before implementing Palo Alto Networks NGFWs and other security solutions.
- The other tools and solutions implemented to support the work of the SecOps and IT Ops team.
- The 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 of $2.5 million.

Security And IT Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of security incidents requiring manual investigation/remediation before Palo Alto Networks NGFWs	Composite	62,400	65,520	68,796
A2	Reduction in security incidents requiring manual investigation/remediation with Palo Alto Networks NGFWs	Interviews	25%	50%	60%
A3	Manual multitouch security incidents avoided with NGFWs	A1*A2	15,600	32,760	41,278
A4	MTTR before Palo Alto Networks NGFWs (minutes)	Composite	120	120	120
A5	Subtotal: Time savings due to avoided investigations with Palo Alto Networks NGFWs	A3*A4/60*A8	$1,809,600	$3,800,160	$4,788,248
A6	MTTR improvement with Palo Alto Networks NGFWs	Composite	20%	20%	20%
A7	Minutes saved per incident	A4*A6	24	24	24
A8	Average fully burdened hourly salary for SecOps	TEI standard	$58	$58	$58
A9	Subtotal: SecOps efficiency related to critical alerts due to Palo Alto Networks NGFWs	((A1-A3)*A7/60) *A8)	$1,085,760	$760,032	$638,418
A10	Number of endpoint devices requiring reimaging 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 the number of endpoint devices requiring reimaging with Palo Alto Networks	Composite	50%	50%	50%
A13	Average fully burdened hourly salary for IT Ops	Forrester standard	$39	$39	$39
A14	Subtotal: Reduced IT effort — reimaging	((A10*A11)/60)*A12*A13	$38,025	$38,025	$38,025
A15	Productivity recapture of security FTE	Composite	50%	50%	50%
A16	Attribution to NGFWs	Composite	55%	55%	55%
At	Security and IT operations efficiency	(A5+A9+A14)*A15*A16	$806,681	$1,264,510	$1,502,790
	Risk adjustment	↓15%			
Atr	Security and IT operations efficiency (risk-adjusted)		$685,679	$1,074,834	$1,277,372
	Three-year total: $3,037,884			**Three-year present value: $2,471,345**	

END-USER PRODUCTIVITY GAIN

Evidence and data. Interviewees described a prior environment where end users were consistently impacted by security-related slowdowns. This involved downtime due to both security breaches or disruptive investigative procedures. End users also found previous 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.

Palo Alto Networks NGFWs in concert with other Palo Alto Networks security products reduced downtime associated with security issues by reducing the number of security incidents, decreasing the mean-time-to-resolution (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 running on the hardware firewalls with great success.”
- The 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”
- SVP 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.”

> **“We are able to provide the scale, the speed of access, no matter where the local user is.”**
>
> *SVP of IT, financial services*

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

- There are 50,000 employees.
- Of these employees, 45% work directly with cloud products, which are the most affected by Palo Alto Networks solutions.
- During any system downtime, 10% of the employees working directly with cloud products have their productivity impacted by the downtime event.
- Using Palo Alto Networks solutions, 8% of the lost time and productivity due to system downtime is recouped.
- The average fully burdened annual salary of an end user is $87,750.
- The composite organization recaptures 50% of the efficiency gains outlined.
- An equal attribution between NGFWs, CDSS, and Prisma SASE is applied at 33% each.

Risks. The exact benefit realized by an organization may depend on:

- 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, 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 of $5.2 million.

End-User Productivity Gain

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of employees	Composite	50,000	50,000	50,000
B2	Percentage of work done in the cloud	Composite	45%	45%	45%
B3	Percentage of end users impacted by system downtime	Composite	10%	10%	10%
B4	Percentage of time recapture due to better availability/less downtime	Interviews	8%	8%	8%
B5	Average annual salary for business user	TEI standard	$87,750	$87,750	$87,750
B6	Productivity recapture	Composite	50%	50%	50%
B7	Attribution to NGFWs	Composite	33%	33%	33%
Bt	End-user productivity gain	B1*B2*B3*B4*B5*B6*B7	$2,606,175	$2,606,175	$2,606,175
	Risk adjustment	↓20%			
Btr	End-user productivity gain (risk-adjusted)		$2,084,940	$2,084,940	$2,084,940
	Three-year total: $6,254,820			**Three-year present value: $5,184,937**	

DATA BREACH RISK REDUCTION

Evidence and data. With Palo Alto Networks Firewalls and other Palo Alto Networks solutions, interviewees noted that their organizations reduced organizational security risk, even in an increasingly hostile cybersecurity environment. Interviewees shared that they lacked complete coverage with their previous conglomerate of security point solutions. Often, gaps were not discovered until a security incident or breach. Palo Alto Networks delivered full visibility across their environment to identify and close gaps, as well as providing seamless and easy-to-integrate coverage to reduce the number of vulnerabilities in the first place.

- 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."
- The SVP of IT at a financial services organization shared, "The consolidation and the integration, it's key to reducing the complexity of the architectures and mitigating risk more easily and more effectively."

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

- According to Forrester data, organizations that are the size of the composite organization experience an average of 3.2 breaches per year relying on point solutions.[2]
- Forrester models the cost of a breach by employee count at organizations. For the composite, this is $53 per employee, not counting loss of worker productivity.[3] The costs include:
  - Fines to regulatory bodies.
  - Customer reimbursement/lawsuits.
  - Incident response and remediation.
  - Lost revenues.
  - Brand equity rebuild costs.
  - Cost of customer reacquisition.
- With Palo Alto Networks, the composite organization reduces the likelihood of a data breach by up to 50% after three years.
- An equal attribution between NGFWs, CDSS, and Prisma SASE is applied at 33% each.

Risks. The exact benefit realized by an organization may depend on:

- The impact that Palo Alto Networks has on the organization's overall security posture compared to its previous solution.
- The percentage of employees impacted by a breach and the duration of the associated downtime.
- The average salary for business users.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2.8 million.

Data Breach Risk Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average number of data breaches per year	Forrester research	3.2	3.2	3.2
C2	Average potential cost of data-breach (exclusive of internal user downtime)	Forrester research	$2,650,000	$2,650,000	$2,650,000
C3	Reduced likelihood of a breach	Interviews	50%	50%	50%
C4	Attribution to NGFWs	Composite	33%	33%	33%
Ct	Data breach risk reduction	C1*C2*C3*C4	$1,399,200	$1,399,200	$1,399,200
	Risk adjustment	↓20%			
Ctr	Data breach risk reduction (risk-adjusted)		$1,119,360	$1,119,360	$1,119,360
	Three-year total: $3,358,080			**Three-year present value: $2,783,683**	

SECURITY INFRASTRUCTURE COST REDUCTION AND AVOIDANCE

Evidence and data. By using Palo Alto Networks NGFWs, interviewees experienced cost savings by retiring legacy solutions and services they no longer needed. For the most part, this involved retiring legacy firewall solutions and replacing them with Palo Alto Networks hardware and software firewalls. Interviewees using multiple Palo Alto Networks solutions to form a more complete security solution typically saw these savings amplified, as they were also able to reduce the tooling required for other key vendors, and often found Palo Alto Networks products in concert outperformed and made other security solutions redundant.

- The director of security architecture and engineering at a manufacturing organization shared: "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 SVP of IT at a financial services organization described, "There's a big benefit of having a single vendor. … We made the decision to try to consolidate tooling to a key vendor as much as possible."

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

> **"[Every] team I can think of benefits. … Everybody benefits because we don't have to do all this extra spend. We can have one resilient environment that covers all our needs."**
>
> *Director of network security engineering, financial services*

- The annual security tech spending of the organization is $8 million.
- The vendor consolidation enabled by using Palo Alto Networks NGFWs represents 15% of the annual security tech spend.

Risks. The exact benefit realized by an organization may depend on:

- The annual cost associated with each technology being replaced.
- The speed at which an organization can replace these technologies due to license agreements/terms and network configurations.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $2.5 million.

Security Infrastructure Cost Reduction And Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Annual security tech stack spend	Composite	$8,000,000	$8,000,000	$8,000,000
D2	Percentage of savings from retiring legacy firewall solutions	Interviews	15%	15%	15%
Dt	Security infrastructure cost reduction and avoidance	D1*D2	$1,200,000	$1,200,000	$1,200,000
	Risk adjustment	↓15%			
Dtr	Security infrastructure cost reduction and avoidance (risk-adjusted)		$1,020,000	$1,020,000	$1,020,000
	Three-year total: $3,060,000			**Three-year present value: $2,536,589**	

SECURITY STACK MANAGEMENT EFFICIENCY FROM COMMON PLATFORM

Evidence and data. Interviewees expressed frustration with the time-consuming management required for their prior firewall solutions. Previously, firewalls were handled mostly individually. With the Palo Alto Networks Panorama, their common management solution, all NGFWs could be easily updated or changed in groups at the touch of a button. Process speeds were further reduced with the introduction of automation to decrease manual effort and increase efficiency.

- The SVP of IT at a financial services firm shared, "Previously, a firewall change would take three to four business days. We have reduced that down to 10 minutes with automation."
- The enterprise network architect in government described: "Today with Panorama, we manage the entire fleet [of firewalls] as a single group. I can easily deploy policy sets to all of them at once."
- The same interviewee also described the update process: "Replacing firewalls used to be a time-consuming effort. It meant exporting the configuration, putting it back on the device, making sure it's working, etc. That's at least several hours of work every time. Now that everything is Panorama-centric, we drop a new firewall into the right device group, we get it online and it's good to go in half an hour."

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

- There are 15 employees responsible for platform management.
- By managing all Palo Alto Networks tools from a common platform, 50% of the employees' time is recaptured.
- Managing CDSS takes about 20% of the platform management teams' time.
- The average fully burdened annual salary of an employee within the IT organization is $112,500.

Risks. The exact benefit realized by an organization may depend on:

- The size and skill set of an organization's security management team.
- The capabilities and systems that are in place before deploying Palo Alto Networks.
- The average salary of the network, security, and IT operations teams

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1.1 million.

> **"In the past, most of our time was spent searching on where to put a policy, not even looking if the policy should be there or if it's working. With Panorama, we get all of that time back."**
>
> *Enterprise network architect, government*

Security Stack Management Efficiency From Common Platform					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Team responsible for platform management	Composite	15	15	15
E2	Percentage of time savings due to common platform efficiency and Panorama	Interviews	50%	50%	50%
E3	Attribution to Panorama	Composite	60%	60%	60%
E4	Average annual salary for the IT organization	TEI standard	$112,500	$112,500	$112,500
Et	Security stack management efficiency from common platform	E1*E2*E3*E4	$506,250	$506,250	$506,250
	Risk adjustment	↓10%			
Etr	Security stack management efficiency from common platform (risk-adjusted)		$455,625	$455,625	$455,625
	Three-year total: $1,366,875			**Three-year present value: $1,133,072**	

UNQUANTIFIED BENEFITS

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

- **Increased visibility across security environments.** Interviewees consistently mentioned that there was no single source of truth from a security perspective in their prior environments, which was a pain point. With Palo Alto Networks, they gained enhanced visibility into condition, performance, and usage data for their entire security organization. Instead of wasting time patchworking together a state of affairs from multiple vendor solutions, security teams could easily get the complete picture with Palo Alto Networks' interface. The enterprise network architect in government shared: "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. It instantly performed better than our purpose-built reporting software that we had struggled to maintain."
- **Improved integration with other parts of the security tech stack.** Because Palo Alto Networks solutions integrate easily with each other, it was easy for security teams to optimize their environments for visibility, usage, and efficiency. 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."
- **Improved employee experience.** The interviewees noted that the combination of all the

"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."

Enterprise network architect, government

benefits above created a better employee experience at their organizations — both in using the different solutions and in benefitting from the more robust, less intrusive security environment at their organizations. The director of security architecture and engineering in manufacturing noted: "Palo Alto Networks came and worked perfectly. We had great feedback from people in terms of quality of experience."

FLEXIBILITY

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

- **The long-term, virtuous impact of having a complete security solution in their environment.** In the long run, having an efficient and comprehensive security environment allowed for future growth and the ability to easily scale or be flexible to meet the changing needs of the business. The director of security architecture and engineering at a manufacturing firm shared, "Having Palo Alto Networks prepares you for the rest of the path, which is to integrate more things, such as remote networks, branch offices, and CASB."

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

Forrester Perspective: Top Cybersecurity Threats In 2023 Are A Combination Of Established And Emerging Threats

Defending against attacks on machine learning and artificial intelligence was a niche discipline until recently. Use cases for adversaries to use AI have emerged. AI will help adversaries scale and wreak havoc in ways they simply could not do prior to the emergence of these technologies.

Cloud computing presents security challenges due to the footprint of the cloud and the complexity of cloud environments. Security threats will be exacerbated by the growth in flavors of cloud compute and storage infrastructure, and the inability of information-as-a-service (IaaS) providers to cover these new compute and storage infrastructure flavors.

Source: "The Future Of Cybersecurity And Privacy," Forrester Research, Inc., August 3, 2023.

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	$1,188,000	$594,000	$297,000	$148,500	$2,227,500	$2,085,025
Gtr	Internal time investment for user training and ongoing management	$4,752	$124,740	$124,740	$124,740	$378,972	$314,962
Htr	NGFW subscription and service costs	$1,353,555	$217,070	$217,070	$217,070	$2,004,765	$1,893,376
	Total costs (risk-adjusted)	$2,546,307	$935,810	$638,810	$490,310	$4,611,237	$4,293,363

INSTALLATION AND DEPLOYMENT COSTS

Evidence and data. Interviewees described a straightforward process to install and deploy Palo Alto Networks NGFWs. 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 remote, 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.

- The director in manufacturing noted: “I deployed it in less than two weeks for 35,000 employees that were being pushed to remote. Less than two weeks to deploy, and everyone was happy.”
- The SVP of IT at the financial services firm added: “The actual replacement time was probably eight months, with the rest being dragged out because of lack of available FTEs.”

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

- For the deployment of NGFWs and CDSS, 10 network operations employees spend a total of nine months upgrading firewalls and aligning policies in the initial period, and they spend almost five months fine-tuning in Year 1. The composite organization leverages end-of-life cycles and invests time to test the deployment, extending the timeline, but also ensuring a smooth transition away from its legacy solution.
- The involved employees spend 80% of their time for deployment initially, which gradually reduces in the subsequent years.
- The average fully loaded annual salary for a network operations employee is $135,000.
- Since organizations typically deploy NGFWs and CDSS together, the model assumes that the composite spends 55% of the total installation and deployment time for NGFWs.

Risks. The exact cost incurred by an organization may depend on:

- The amount of time and effort needed to deploy the NGFWs and CDSS.

- The average salary for deployment team members.

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 $2.1 million.

Installation And Deployment Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Network team working on firewall installation	Composite	10	10	10	10
F2	Time spent per staff	Interviews	80%	40%	20%	10%
F3	Average fully burdened annual salary for a network operations employee	TEI standard	$135,000	$135,000	$135,000	$135,000
F4	Percentage work allocated to firewall management	A16	55%	55%	55%	55%
Ft	Installation and deployment costs	F1*F2*F3	$1,080,000	$540,000	$270,000	$135,000
	Risk adjustment	↑10%				
Ftr	Installation and deployment costs (risk-adjusted) (risk-adjusted)		$1,188,000	$594,000	$297,000	$148,500
	Three-year total: $2,227,500			**Three-year present value: $2,085,025**		

INTERNAL TIME INVESTMENT FOR USER TRAINING AND ONGOING MANAGEMENT

Evidence and data. 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. With the Palo Alto Networks centralized management tool, this work was streamlined and simplified. User training was also reported to be effective and simple, allowing employees to easily transition from working with legacy solutions to Palo Alto Networks.

- An enterprise network architect at a government agency described: “We have a firewall team that handles our fleet. Compared to [their previous solution], they are able to keep up and are less behind on projects.”
- The same interviewee went on to describe the benefit of centralized management with Panorama: “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.”
- The director of security architecture and engineering at a manufacturing firm said: “For ongoing management, that is 10% of our time. It’s really easy to operate. It’s just people on my team involved.”

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

- A total of 8 hours of training is required for the NGFWs and CDSS training for employees new to Palo Alto Networks. In subsequent years, 2 hours of training is required to share any new features, updates, and enhancements.
- The average fully loaded salary across IT is $54 per hour.
- Once training is completed, ongoing management is assumed to involve the 10 people trained yearly. They spend 10% of their time managing NGFWs and CDSS.
- Since organizations manage NGFWs and CDSS together, the model assumes that 10% of the total time spent for ongoing management is for NGFWs.

Risks. The exact cost incurred by an organization may depend on:

- The size and experience level of the IT organization with Palo Alto Networks solutions.
- The average salary of IT employees.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $315,000.

Internal Time Investment For User Training And Ongoing Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Number of FTEs receiving training for ongoing management	Composite	10	10	10	10
G2	Number of hours per training session	Interviews	8	2	2	2
G3	Average fully burdened hourly salary for the IT organization	TEI standard	$54	$54	$54	$54
G4	Internal time investment for user training	G1*G2*G3	$4,320	$1,080	$1,080	$1,080
G5	Percentage of time spent for ongoing management of NGFWs	Interviews		10%	10%	10%
G6	Internal time investment for ongoing management	G1*G3*2,080 hours*G5	$0	$112,320	$112,320	$112,320
Gt	Internal time investment for user training and ongoing management	G4+G6	$4,320	$113,400	$113,400	$113,400
	Risk adjustment	↑10%				
Gtr	Internal time investment for user training and ongoing management (risk-adjusted)		$4,752	$124,740	$124,740	$124,740
	Three-year total: $378,972			**Three-year present value: $314,962**		

NGFW SUBSCRIPTION AND SERVICE COSTS

Evidence and data. 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 their software firewalls were often purchased through credits with Palo Alto Networks that could also be used for Palo Alto Networks CDSS software solutions.

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

- Subscription contracts are amortized over the three-year term.
- Pricing may vary. Contact the Palo Alto Networks for additional details.

Risks. The exact cost incurred by an organization may depend on:

- The quantity and types of NGFWs implemented across the organization.
- Usage of software firewalls and Panorama.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $1.9 million.

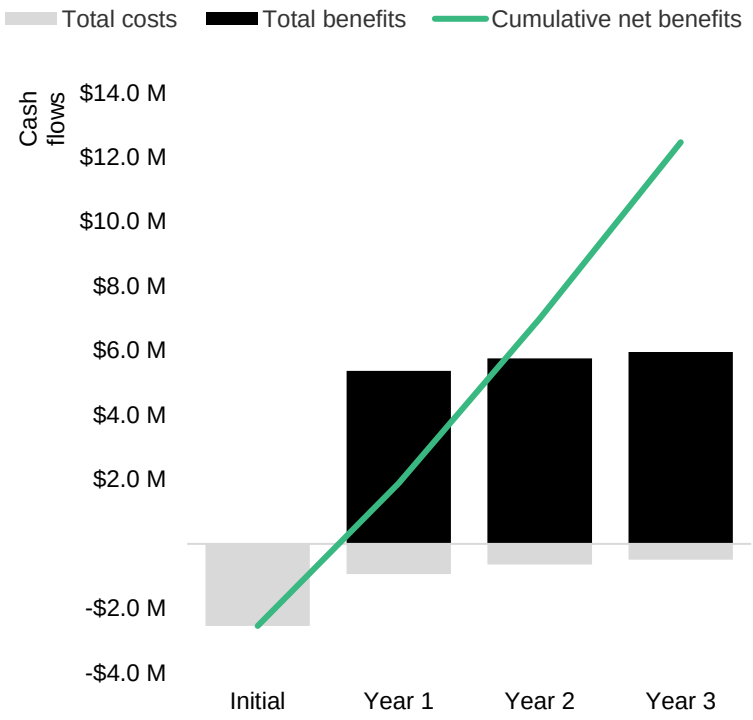
NGFW Subscription And Service Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Hardware costs	Composite	$1,289,100			
H2	NGFW subscription and services cost	Composite		$206,733	$206,733	$206,733
Ht	NGFW subscription and service costs	H1+H2	$1,289,100	$206,733	$206,733	$206,733
	Risk adjustment	↑5%				
Htr	NGFW subscription and service costs (risk-adjusted)		$1,353,555	$217,070	$217,070	$217,070
	Three-year total: $2,004,765			**Three-year present value: $1,893,376**		

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	($2,546,307)	($935,810)	($638,810)	($490,310)	($4,611,237)	($4,293,363)
Total benefits	$0	$5,365,604	$5,754,759	$5,957,297	$17,077,659	$14,109,626
Net benefits	($2,546,307)	$4,429,794	$5,115,949	$5,466,987	$12,466,422	$9,816,263
ROI						229%
Payback						7 months

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."

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.

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.

Appendix B: Supplemental Material

Related Forrester Research
"The Future Of Cybersecurity And Privacy," Forrester Research, Inc., August 3, 2023.

"Top Cybersecurity Threats In 2023," Forrester Research, Inc., April 17, 2023.

Appendix C: Endnotes

[1] 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.

[2] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[3] Ibid.


FORRESTER®