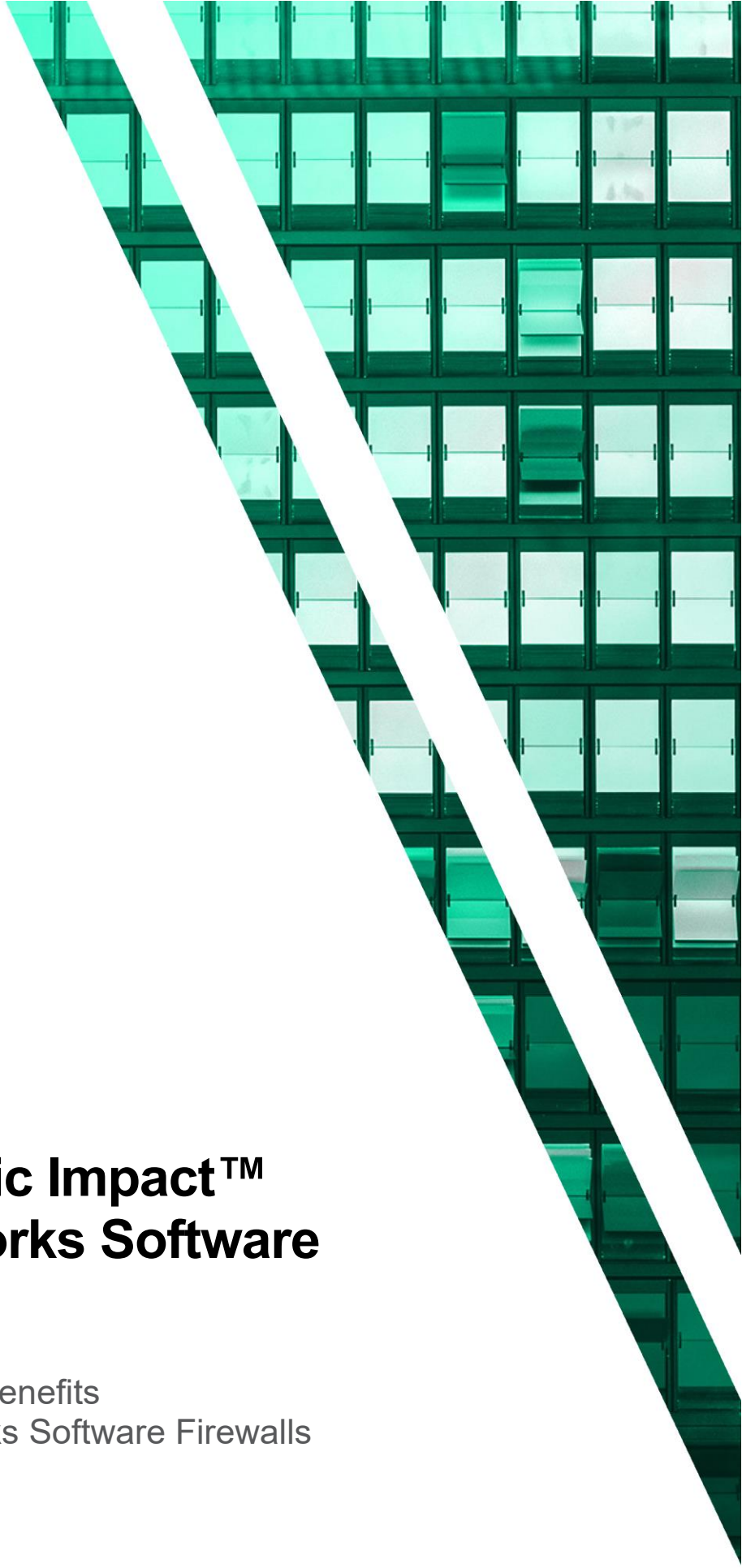
FORRESTER®



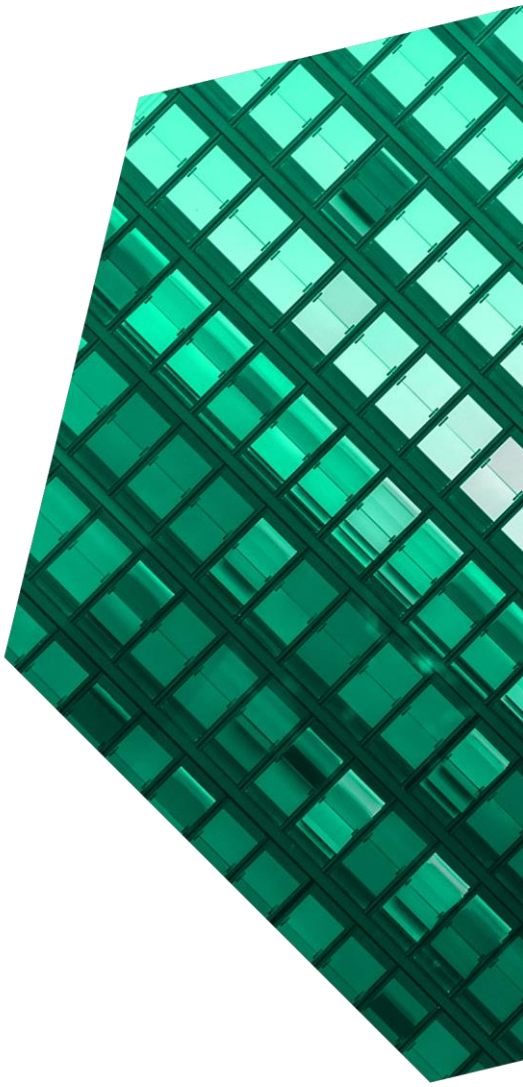
The Total Economic Impact™ Of Palo Alto Networks Software Firewalls

Cost Savings And Business Benefits Enabled By Palo Alto Networks Software Firewalls

OCTOBER 2023

Table Of Contents

Consulting Team: Sam Sexton
Matt Dunham



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

It is paramount for organizations to maintain adequate security postures in cloud and virtualized environments and to do so without wasting time and effort on troubleshooting when they could be improving security. Right now, organizations struggle with both: They juggle legacy physical firewalls that require more time and effort for worse security visibility and overall posture. Moving to a centralized software platform with powerful capabilities and centralized management is one way to square the circle.

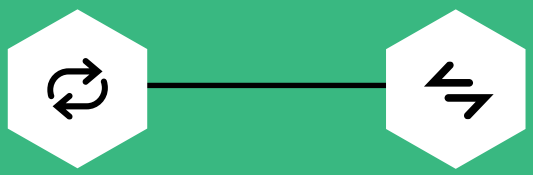
As the name suggests, Palo Alto Networks Software Firewalls are firewalls in software form rather than physical. These firewalls can be deployed for cloud platforms like AWS or Azure and virtual machines or containers, and they are governed by Panorama, Palo Alto Networks' centralized firewall management platform that provides unified rulemaking and visibility.

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 Palo Alto Networks Software Firewalls.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Software Firewalls on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives of five organizations and surveyed 158 additional respondents with experience using Palo Alto Networks Software Firewalls. For the purposes of this study, Forrester aggregated the experiences of the interviewees and survey respondents and combined the results into a single composite organization.

The interviewees noted that prior to using Software Firewalls, their organizations had myriad physical firewalls deployed in their legacy environments for east-west security. In many instances, these firewalls were siloed, unreliable, and required excessive labor to manage and update. This left the organizations short on labor and still without adequate risk management.

KEY STATISTICS



Return on investment (ROI)
163%

Payback period
0 months

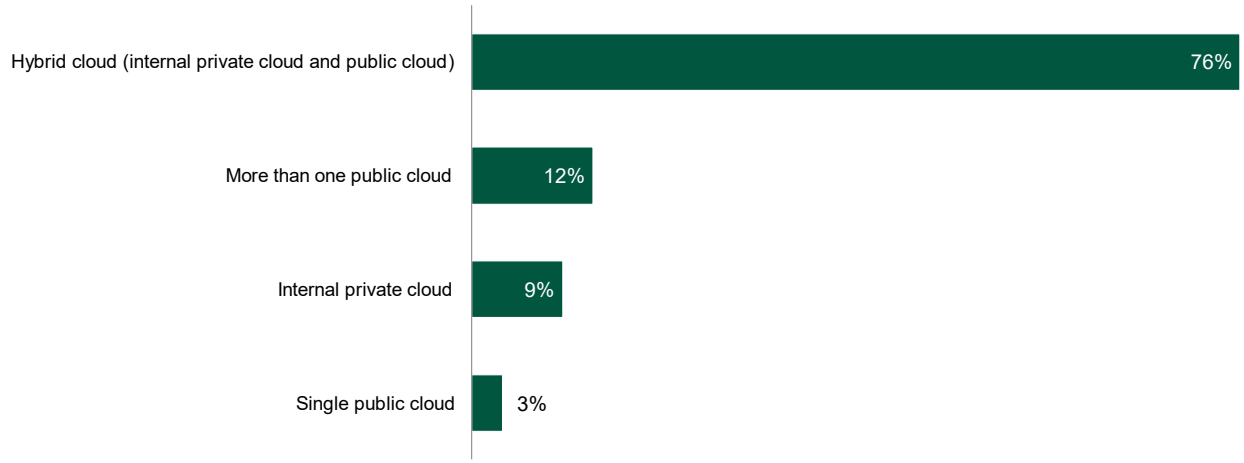
After the investment in Software Firewalls, the organizations were able to replace their legacy firewalls quickly and spend less effort maintaining them. Improved, centralized governance and additional capabilities enabled them to reduce their reliance on other security tools while significantly improving reliability and security.

KEY FINDINGS

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

- **25% savings in firewall deployment and 35% savings in time dedicated to firewall security and network management.** The composite organization requires significantly less effort to deploy Software Firewalls than it did for its legacy

"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

firewalls, and Palo Alto Networks Software Firewalls also require less active effort to manage. With Software Firewalls, the composite organization saves more than 12,000 hours of effort per year on deployment and management, resulting in a three-year, risk-adjusted present value (PV) of $1.8 million.

- **50% reduction in time required to attain security posture.** In addition to having teams for basic deployment and maintenance, the composite organization requires security and network operations teams to adjust and fine-tune security devices to ensure they meet security standards. With Software Firewalls, the composite organization reduces the amount of time spent on these tasks by 50%, which contributes to three-year, risk-adjusted savings of more than $145,300.
- **Automatic filtration of security incidents and a 50% reduction in remediation labor.** The centralized visibility and governance of Palo Alto Networks Software Firewalls enable the composite organization to completely avoid remediation effort for certain events via automatic filtration, and it reduces the remediation time for other incidents flagged by the firewalls by 50%. This leads to a three-year, risk-adjusted PV of nearly $238,800 for the composite organization.
- **67% reduction in end-user downtime and a 50% reduction in overall downtime length.** The virtual nature of Palo Alto Networks Software Firewalls and centralized governance of all types of firewalls via Panorama makes it significantly less likely that the composite will see outages for reasons like hardware failure or making updates. The firewalls also improve the composite's visibility, which significantly reduces the time required for updating or bringing firewalls back online. This contributes to a risk-adjusted, three-year PV of nearly $682,900 for the composite organization.
- **More than $700,000 in avoided hardware spend per year.** Palo Alto Networks Software Firewalls don't just replace the composite organization's existing physical firewalls, they also provide additional capabilities that allow it to replace devices. These include Domain Name System (DNS) security, advanced threat protection, and more. Paired with avoiding the overprovisioning of physical firewalls, the composite organization saves a risk-adjusted total of nearly $1.6 million over three years.

- **Reduced risk and impact of a security breach.** The composite organization reduces the likelihood of a security breach by 15% with easier management and consistent rules, visibility, and governance provided by Palo Alto Networks Software Firewalls. This also reduces the amount of internal productivity impacted by each incident. With Software Firewalls, the composite organization saves a three-year, risk-adjusted total of $1.6 million.

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

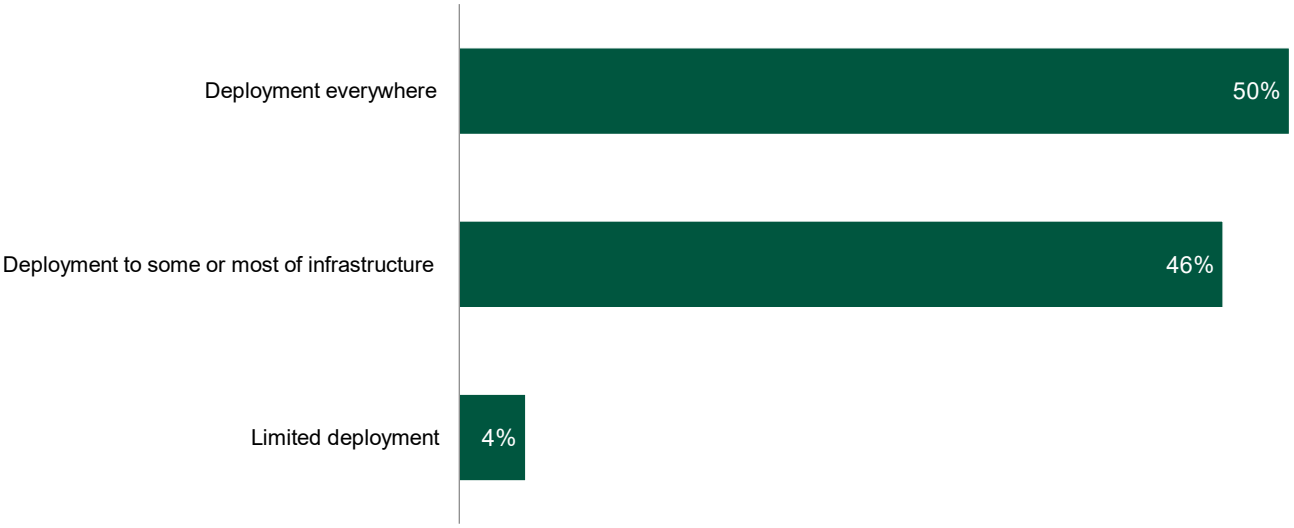
- **Faster, more secure migrations.** Organizations can move faster and with more confidence during cloud and digital migrations because they know they have consistent security solutions.
- **Additional capabilities and compatibility with other Palo Alto Networks solutions.** Organizations can expect to see additional capabilities and functionality from their Palo Alto Networks Software Firewalls, especially when working with other Palo Alto Networks solutions.

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

- **Annual usage fees for Palo Alto Networks Software Firewalls.** The composite organization pays an annual fee for each of its firewalls based on the type of firewall and usage that totals a three-year, risk-adjusted cost of $1.2 million.
- **$40,000 in total deployment costs.** Each of the composite's Palo Alto Networks Software Firewall deployments takes an average of 3.75 hours. Over three years, this costs the composite a risk-adjusted total of $40,000.
- **$396,000 in annual ongoing management costs.** The composite uses a team of 20 FTEs to manage its Software Firewalls, and the team spends 20% of its time on this task. This leads to a risk-adjusted total cost of $986,000 over three years.

The financial analysis which is based on the interviews and survey found that a composite organization experiences benefits of $5.98 million over three years versus costs of $2.28 million, adding up to a net present value (NPV) of $3.70 million and an ROI of 163%. The payback period is immediate, which means the composite organization begins to recoup its initial investment immediately upon implementation.

“To what degree are you currently using a cloud security solution at your organization?”



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

ROI
163%

BENEFITS PV
$5.98M

NPV
$3.70M

PAYBACK
0 months

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Palo Alto Network Software Firewalls.

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 Palo Alto Networks Software Firewalls can have on an organization.

Forrester Consulting conducted an online survey of 158 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in August 2023.

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 Software Firewalls.

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.

Forrester fielded the double-blind survey using a third-party survey partner.

DUE DILIGENCE

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

INTERVIEWS AND SURVEY

Interviewed six representatives of five organizations and surveyed 158 respondents at organizations using Palo Alto Networks Software Firewalls to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees and survey respondents.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews and survey using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees and survey respondents.

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 Software Firewalls Customer Journey

Drivers leading to the Palo Alto Networks Software Firewalls investment

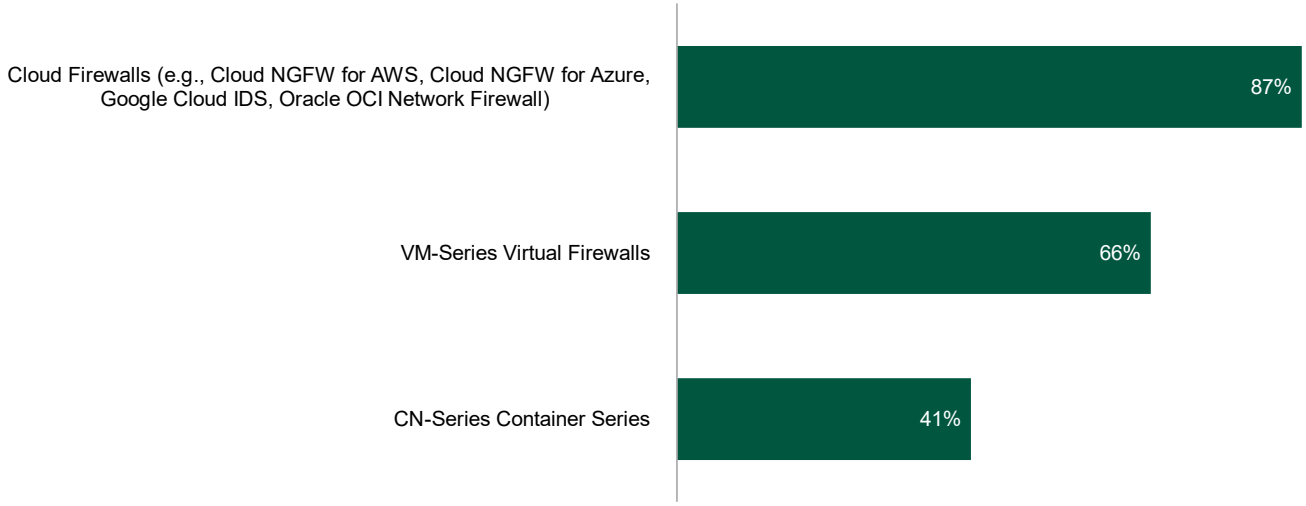
KEY CHALLENGES

Forrester interviewed six representatives of five organizations with experience using Palo Alto Networks Software Firewalls at their organizations and surveyed an additional 158 respondents. For more details on these individuals and the organizations they represent, see Appendix B.

Both interviewees and survey respondents noted how their organizations struggled with common challenges, including:

- **Costly and difficult governance and management.** Several interviewees explained that their organization's disparate legacy firewalls and security solutions were siloed and generally difficult to manage or update. The AVP of a financial services organization told Forrester: "When each vendor is different with different patch levels and end-of-life dates, keeping up becomes nearly impossible."
- **Downtime due to unreliable devices.** Interviewees said that in addition to requiring more time to manage and standardize, the myriad legacy devices their organizations relied upon before using Palo Alto software firewalls were generally unreliable and downtime was a semi-frequent occurrence. The AVP of a financial services organization said: "We used to have outages all the time because all these different devices had different software versions and different bugs."
- **Increased risk of attack due to inconsistent security posture.** The overall difficulty in managing these disparate devices coupled with frequent downtime left the interviewees' and survey respondents' organizations vulnerable to attacks. The enterprise infrastructure architect at a government agency told Forrester: "Prior to having Palo Alto Networks Software Firewalls, we really had no visibility. We didn't know how bad our network actually was [or] where the blind spots and threats were."

"Which software firewalls do you have?"



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

SOLUTION REQUIREMENTS

The interviewees and survey respondents searched for a solution that could:

- Provide centralized, easy-to-manage governance and maintenance for their organization's environment.
- Improve security posture through increased capabilities and reliability.

"There was no central framework or standard governance."

Associate director, IT services

COMPOSITE ORGANIZATION

Based on the interviews and survey, 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 five interviewed organizations and 158 survey respondents, 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 global, industry-agnostic company that generates $15 billion annually and has 20,000 employees.

Deployment characteristics. The composite organization deploys 50 Palo Alto Networks Software Firewalls in Year 1, 70 in Year 2, and 90 in Year 3 for a total of 210 firewalls by the third year of the investment. Specifically, the composite organization deploys 40 VM-100 VM-Series virtual firewalls and two CN-Series container firewalls in Year 1, 60 VM-100 virtual firewalls and four CN-Series container firewalls in Year 2, and an additional 60 VM-100 and four VM-Series firewalls in Year 3. It deploys the remaining Cloud Next-Generation Firewalls (Cloud NGFW) on Azure and AWS as needed.

Key Assumptions

- **$15B in revenue**
- **20,000 employees**
- **210 total Palo Alto Networks Software Firewalls by Year 3**

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	Firewall deployment and maintenance savings	$708,460	$709,671	$710,883	$2,129,014	$1,764,657
Btr	Security-posture attainment savings	$58,438	$58,438	$58,438	$175,313	$145,325
Ctr	Improved security and IT operations remediation efficiency	$96,023	$96,023	$96,023	$288,068	$238,794
Dtr	Reduced end-user downtime due to improved reliability	$274,587	$274,587	$274,587	$823,760	$682,856
Etr	Security infrastructure cost reduction and avoidance	$626,823	$631,073	$635,323	$1,893,219	$1,568,715
Ftr	Data breach reduction savings	$634,338	$634,338	$634,338	$1,903,015	$1,577,506
	Total benefits (risk-adjusted)	$2,398,668	$2,404,130	$2,409,591	$7,212,389	$5,977,853

FIREWALL DEPLOYMENT AND MAINTENANCE SAVINGS

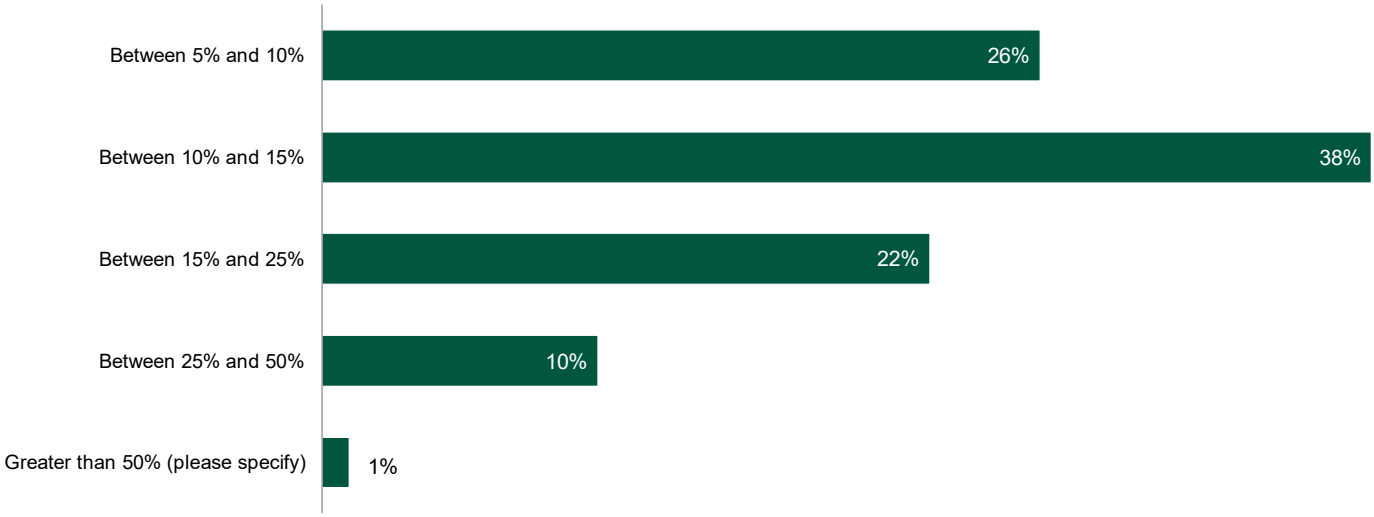
Evidence and data. Survey respondents and interviewees described Palo Alto Networks Software Firewalls as much faster to deploy and perform routine maintenance on than their prior solutions, partially due to the digital nature of the software firewalls and partially due to the ease of maintenance with centralized visibility and control through Panorama. They said Palo Alto Networks cloud firewalls offered as managed services such as Cloud NGFW for AWS and Cloud NGFW for Azure in particular are extremely simple to deploy.

- The principal security engineer at a financial services organization explained to Forrester: "[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."

"In the past, we would have to buy physical firewalls to put in front of a new environment. We'd have to possibly stand up a new [VMware] EXSi environment. All of that takes time and money. … Nowadays, we just build it on a [virtual machine] with the regular NSX environment and firewall it using the VM-Series."

Principal security engineer, financial services

"You noted faster time to deploy Palo Alto Networks security solutions. Can you estimate the percentage improvement compared to your previous environment?"



Base: 89 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

- The enterprise infrastructure architect at a government agency spoke about how Panorama simplified management of their organization's solutions: "We manage the entire fleet as a single group. We can deploy the same policy set to all of our internet-facing firewalls."
- The senior VP 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."
- 94% of the survey respondents told Forrester that Palo Alto Networks Software Firewalls improved their organization's management, administration, and operations efforts.

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

- The composite organization deploys 50 new Palo Alto Networks Software Firewalls in Year 1, 70 in Year 2, and 90 in Year 3.
- Before using Palo Alto Networks, deploying a firewall required 5 hours. With Palo Alto Networks, the organization realizes time savings of 25% on each deployment.
- Previously, a team of 20 IT maintenance FTEs spent 50% of their time managing the composite's firewall security and network settings. With Palo Alto Networks Software Firewalls, this time is reduced by 35%.

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

- The amount of time the organization spends on deployment and maintenance before deploying Palo Alto Networks Software Firewalls.
- The size of the team the organization has 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 $1.8 million.

Firewall Deployment And Maintenance Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Net new Palo Alto Networks Software Firewalls deployed	Composite	50	70	90
A2	Time required to deploy legacy firewalls (hours)	Interviews	5	5	5
A3	Reduction in time required to deploy Palo Alto Networks Software Firewalls	Interviews	25%	25%	25%
A4	Subtotal: Total reduction in annual deployment time (hours)	A1*A2*A3	63	88	113
A5	IT firewall maintenance team members	Composite	20	20	20
A6	Percent of time dedicated to firewall security and network management before using Palo Alto Networks Software Firewalls	Interviews	50%	50%	50%
A7	Percentage of time dedicated to firewall security and network management with Palo Alto Networks Software Firewalls	Interviews	15%	15%	15%
A8	**Management time saved (hours)**	**(A5*2,080 hours per year*A6-(A5*2,080 hours per year*A7)**	**14,560**	**14,560**	**14,560**
A9	Average hourly salary of an IT deployment and maintenance employee	TEI standard	$57	$57	$57
At	Firewall deployment and maintenance savings	(A4+A8)*A9	$833,483	$833,483	$833,483
	Risk adjustment	↓15%			
Atr	Firewall deployment and maintenance savings (risk-adjusted)		$708,460	$708,460	$708,460
	Three-year total: $2,129,014			**Three-year present value: $1,764,657**	

SECURITY-POSTURE ATTAINMENT SAVINGS

Evidence and data. Interviewees told Forrester that in addition to helping with initial deployment and routine maintenance, Palo Alto Networks Software Firewalls saved the time of their organizations' higher-level security and network operations employees while ensuring new additions to their networks met security standards.

- The senior VP of IT for a financial services organization told Forrester: "[With Palo Alto Networks Software Firewalls,] we have standardization [and] higher efficacy. … It's a significant improvement."
- The enterprise infrastructure architect at a government agency said Palo Alto Networks Software Firewalls provided their organization with much more visibility than it had in its prior state. They said: "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 director of network security engineering at a financial services organization told Forrester: "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."
- 94% of survey respondents told Forrester that Palo Alto Networks Software Firewalls increased efficiencies for their organizations' security teams.

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

- The composite organization has a team of four SecOps FTEs and two NetOps FTEs.
- Before deploying Palo Alto Networks Software Firewalls, the team spent 50% of its time attaining security posture on firewalls.
- Palo Alto Networks Software Firewalls reduces this time spend to 25%.

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

- The size of the security team that manages the organization's security posture on firewalls.
- The amount of time saved by moving to Palo Alto Networks Software Firewalls.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $145,300.

Security-Posture Attainment Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Fully loaded annual salary of a SecOps FTE	TEI standard	$125,000	$125,000	$125,000
B2	Fully loaded annual salary of a NetOps FTE	TEI standard	$135,000	$135,000	$135,000
B3	SecOps FTEs required to attain security posture after deployment of firewalls	Composite	4	4	4
B4	NetOps FTEs required to attain security posture after deployment of firewalls	Composite	2	2	2
B5	Percentage of time spent on security attainment tasks in prior state	Survey	50%	50%	50%
B6	Percentage of time spent on security attainment tasks with Palo Alto Networks Software Firewalls	Survey	25%	25%	25%
B7	Cost to achieve security with legacy system	(B1*B3*B5)+(B2*B4*B5)	$261,250	$261,250	$261,250
B8	Cost to achieve security with Palo Alto Networks Software Firewalls	(B1*B3*B6)+(B2*B4*B6)	$192,500	$192,500	$192,500
Bt	Security-posture attainment savings	B7-B8	$68,750	$68,750	$68,750
	Risk adjustment	↓15%			
Btr	Security-posture attainment savings (risk-adjusted)		$58,438	$58,438	$58,438
	Three-year total: $175,313			**Three-year present value: $145,325**	

IMPROVED SECURITY AND IT OPERATIONS REMEDIATION EFFICIENCY

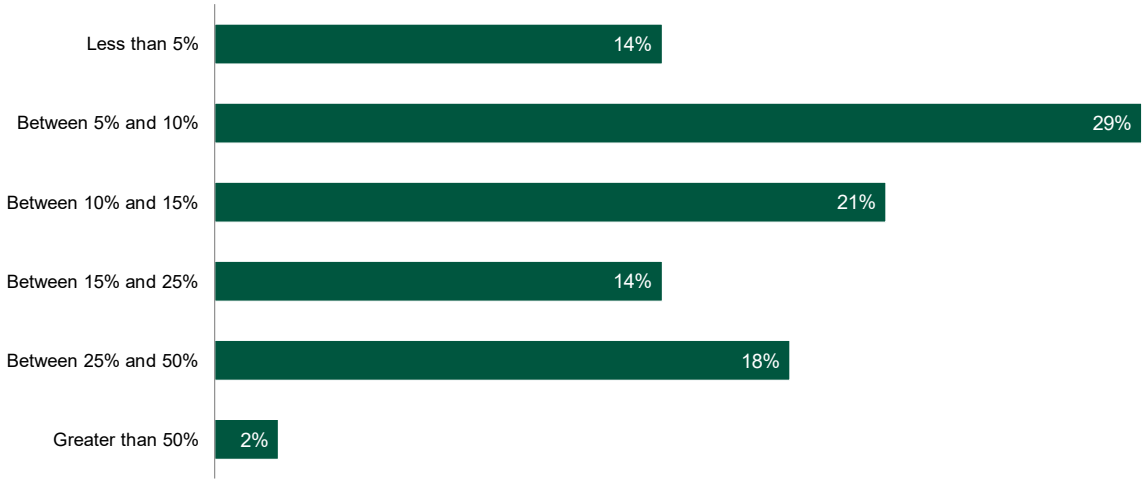
Evidence and data. Interviewees and survey respondents said they are impressed with the ability of Palo Alto Networks Software Firewalls to filter out false-positive incidents and reduce the time required to remediate other incidents via more consistent governance, automation, and more visibility.

- The principal security engineer at a financial services organizations told Forrester, "The great visibility that Palo Alto Networks logs give us has helped [us] resolve issues a lot faster than we would if we had no visibility."
- The AVP at another financial services organization told Forrester, "We found that the ability that Palo Alto Networks Software Firewalls had to see our traffic and filter against it was simply far superior [to what we had]."
- The enterprise infrastructure architect for a government agency explained how their organization was able to automate certain security responses to reduce remediation effort and time: "We automate the vast majority of our phishing responses. We can automatically verify if an incident was phishing [and] look at firewall logs. … That would have been a manual process prior."

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

- Before engaging with Palo Alto Networks, the composite organization had 5,824 annual incidents that required some form of response.
- Palo Alto Networks Software Firewalls filter 18% of these incidents.
- Before deploying Palo Alto Networks Software Firewalls, each incident required 31 minutes of active labor time to resolve.
- With Palo Alto Networks Software Firewalls, this time is reduced by 50%.

"You noted a lower false-positive detection rate due to Palo Alto Networks Software Firewalls (including use with any security service). Can you estimate the percentage improvement compared to your previous environment?"



Base: 66 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

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

- The number of incidents that require investigation per year.
- Whether or not east-west firewall filtration filters false positives.
- Whether or not additional capabilities improve remediation efficiency.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $238,800.

Improved Security And IT Operations Remediation Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Security incidents that require manual investigation/remediation flagged by legacy firewalls	Survey	5,824	5,824	5,824
C2	Percentage of security incidents filtered by better screening and cohesive standards with Palo Alto Networks Software Firewalls	Interviews	18.0%	18.0%	18.0%
C3	Reduction in security incidents that require manual investigation/remediation with Palo Alto Networks Software Firewalls	C1*C2	1,048	1,048	1,048
C4	Remediation labor with prior solution (minutes)	Survey	31	31	31
C5	Subtotal: Avoided investigations with Palo Alto Networks Software Firewalls	C3*C4/60*C8	$32,550	$32,550	$32,550
C6	Remediation labor improvement with Palo Alto Networks software firewalls	Interviews	50%	50%	50%
C7	Time saved per incident (minutes)	C4*C6	15.5	15.5	15.5
C8	Average fully burdened hourly salary of a SecOps FTE (rounded)	TEI standard	$60	$60	$60
C9	Subtotal: SecOps efficiency related to critical alerts (rounded)	((C1-C3)*C7/60) *C8	$74,142	$74,142	$74,142
Ct	Improved security and IT operations remediation efficiency	C5+C9	$106,692	$106,692	$106,692
	Risk adjustment	↓5%			
Ctr	Improved security and IT operations remediation efficiency (risk-adjusted)		$96,023	$96,023	$96,023
	Three-year total: $288,068			**Three-year present value: $238,794**	

REDUCED END-USER DOWNTIME DUE TO IMPROVED RELIABILITY

Evidence and data. Interviewees said that by introducing centralized governance and improved visibility with Panorama, their organizations significantly reduced downtime for end users.

- The AVP in financial services explained how better updating and visibility meant less downtime for their organization: “If we find out about a bug, we can just plan on how to deal with it, find the data center, and go in. … With our homogenous environment, we were able to minimize our downtime.”
- The senior VP of IT at a financial services organization said reducing downtime played a large role in creating an excellent end-user experience: “Having the same experience [end users] expect on what they can access on the internet is huge.”
- Survey respondents also said they are impressed with the ability of Palo Alto Networks Software Firewalls to reduce downtime.
    - Half of the respondents said that before their organization deployed Palo Alto Networks Software Firewalls, 10% to 25% of its users were impacted by firewall downtime. The same respondents said that with Palo Alto Networks Software Firewalls, less than 10% of users are impacted.
    - 38% of respondents told Forrester that before deploying Palo Alto Networks Software Firewalls, each downtime incident at their organization lasted between 2 and 4 hours, but that with Palo Alto Networks Software Firewalls, this downtime fell to less than 2 hours.

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

- The composite organization has 20,000 employees and 10% are impacted by downtime each year.
- Palo Alto Networks Software Firewalls reduces the number of users who experience downtime by 67% and the length of downtime for users who still experience it by 50%.

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

- The number of users subjected to downtime.
- The average length of downtime.
- Whether or not Palo Alto Networks Software Firewalls impact reliability and downtime.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $682,900.

Reduced End-User Downtime Due To Improved Reliability

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Users	Composite	20,000	20,000	20,000
D2	Percentage of users affected by downtime in prior state	Assumption	10%	10%	10%
D3	Reduction in employees affected by downtime with Palo Alto Networks Software Firewalls	Interviews	67%	67%	67%
D4	Users who avoid downtime with Palo Alto Networks Software Firewalls	D1*D2*D3	1,340	1,340	1,340
D5	Average length of downtime in prior state (hours)	Interviews	4.0	4.0	4.0
D6	Subtotal: End-user time saved from avoided downtime (hours)	D4*D5	5,360	5,360	5,360
D7	End users who still experience downtime events with Palo Alto Networks Software Firewalls	(D1*D2)-D4	660	660	660
D8	Reduction in downtime length with Palo Alto Networks Software Firewalls	Survey	50%	50%	50%
D9	Average downtime avoided per affected user with Palo Alto Networks Software Firewalls	D5*D8	2	2	2
D10	Subtotal: End-user time saved for existing events	D7*D9	1,320	1,320	1,320
D11	Average hourly salary of a business user (rounded)	TEI standard	$46	$46	$46
Dt	Reduced end-user downtime due to improved reliability	(D6+D10)*D11	$305,096	$305,096	$305,096
	Risk adjustment	↓10%			
Dtr	Reduced end-user downtime due to improved reliability (risk-adjusted)		$274,587	$274,587	$274,587
	Three-year total: $823,760		**Three-year present value: $682,856**		

SECURITY INFRASTRUCTURE COST REDUCTION AND AVOIDANCE

Evidence and data. Many interviewees and survey respondents said Palo Alto Networks Software Firewalls have expanded capabilities that allowed their organizations to retire multiple security solutions and avoid overprovisioning their firewalls.

- The principal security engineer for a financial services organization told Forrester: “Every team I can think of benefits because we don’t have to do all this extra spend. We have one resilient environment, and it covers all our needs.”
- 34% of survey respondents said their organization saw a total reduction of 10% to 15% in network security asset management costs, and another 28% said their organization saw reductions between 15% and 30%.
- Survey respondents reported a wide array of licenses and services their organizations were able to reduce or eliminate spend for by using Palo Alto Networks Software Firewalls. These include but are not limited to mobile protection license costs (34% of respondents), retired security firewalls (35%), threat intelligence services (38%), security or unmanaged network device protection (46%), malware analysis (50%), and identity access management (52%).

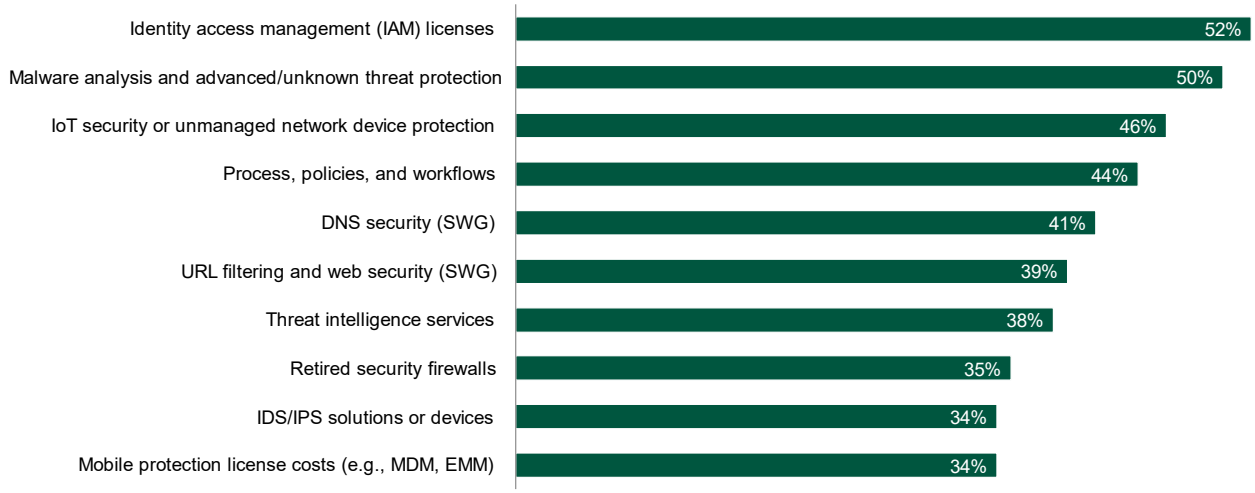
Modeling and assumptions. For the composite organization, Forrester assumes the following:

- The composite organization realizes savings in the following areas:
  - Threat intelligence services.
  - Security firewalls.
  - Intrusion detection system (IDS)/intrusion prevention system (IPS) devices.
  - DNS security (e.g., secure web gateway [SWG]).
  - Malware analysis and advanced/unknown threat protection (ATP).
  - Internet-of-things (IoT) security or unmanaged network device protection.
- The composite organization avoids overprovisioning its physical firewalls.

“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

"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

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

- The degree to which Palo Alto Networks Software Firewalls can replace or augment existing security solutions.
- The degree to which overprovisioning can be eased by Palo Alto Networks Software Firewalls.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.6 million.

Security Infrastructure Cost Reduction And Avoidance					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
E1	Retired threat intelligence services costs	Composite	$86,160	$86,160	$86,160
E2	Retired security firewalls costs	Composite	$130,380	$130,380	$130,380
E3	Retired IDS/IPS devices costs	Composite	$178,713	$178,713	$178,713
E4	Retired DNS security (SWG) costs	Composite	$84,100	$84,100	$84,100
E5	Retired malware analysis and advanced/unknown threat protection (ATP) costs	Composite	$122,457	$122,457	$122,457
E6	Retired IoT security or unmanaged network device protection costs	Composite	$123,129	$123,129	$123,129
E7	Avoided overprovisioning of physical firewalls	A1*25%*1,000	$12,500	$17,500	$22,500
Et	Security infrastructure cost reduction and avoidance	E1+E2+E3+E4+E5+ E6+E7	$737,439	$742,439	$747,439
	Risk adjustment	↓10%			
Etr	Security infrastructure cost reduction and avoidance (risk-adjusted)		$626,823	$631,073	$635,323
	Three-year total: $1,893,219		**Three-year present value: $1,568,715**		

DATA BREACH REDUCTION SAVINGS

Evidence and data. Many of the interviewees and survey respondents expressed increased confidence in their organizations' security postures due to better management, vendor consolidation, and faster responses to incidents. They provided the following examples:

- Palo Alto Network Software Firewalls provided better filtration and remediation capabilities to help prevent potential breaches.
- Their organizations also avoided breaches due to reduced firewall downtime.
- Increased visibility, centralized governance, and more consistent updates allowed their organizations to limit the potential damage from incidents before they became worse.

"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."

Director of network security engineering, financial services

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

- The composite organization has an average of 3.2 data breaches per year and stands to lose $1.06 million per breach.[2]
- Palo Alto Networks Software Firewalls improve the composite's security posture and reduce the likelihood of a breach by 15%.
- Internal business users lose an average of 3.6 hours in productivity per breach per employee impacted.[3]
- Palo Alto Networks Software Firewalls eliminates this lost productivity for 18% of the composite's employees.

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

- The frequency and cost of breaches at the organization.
- The number of employees impacted by breaches.
- The degree to which Palo Alto Networks Software Firewalls mitigate breaches.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $1.6 million.

Data Breach Reduction Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Data breaches per year	Forrester research	3.2	3.2	3.2
F2	Cost of a data breach exclusive of internal user downtime	Forrester research	$1,060,000	$1,060,000	$1,060,000
F3	Reduced likelihood of a data breach	Composite	15%	15%	15%
F4	Subtotal: Avoided costs of remediation post-breach	F1*F2*F3	$508,800	$508,800	$508,800
F5	Internal employees	Composite	20,000	20,000	20,000
F6	Average hourly salary of a business user	TEI standard	$46	$46	$46
F7	Diminished/eliminated internal user productivity time per breach (hours)	Forrester research	3.6	3.6	3.6
F8	Percentage of employees affected per breach	Composite	18%	18%	18%
F9	Subtotal: Avoided productivity losses	F1*F3*F5*F6*F7* F8	$284,123	$284,123	$284,123
Ft	Data breach reduction savings	F4+F9	$792,923	$792,923	$792,923
	Risk adjustment	↓20%			
Ftr	Data breach reduction savings (risk-adjusted)		$634,338	$634,338	$634,338
	Three-year total: $1,903,015			**Three-year present value: $1,577,506**	

UNQUANTIFIED BENEFITS

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

- **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 AVP 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."
- **Additional capabilities and compatibility with other Palo Alto Networks solutions.** Interviewees told Forrester their organizations gained more capabilities over time with Software Firewalls, and that these capabilities were expanded for organizations using other Palo Alto Networks security solutions. The senior VP of IT for a financial services organization told Forrester, "We can figure out how to manage and convert policy across an entire ecosystem for one use case."

FLEXIBILITY

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

- **Having the ability to switch firewall types as needed.** While many of the interviewees said their organization uses Palo Alto Network's enterprise license agreement (ELA)-based pricing model, 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**
Gtr	Firewall subscription costs	$0	$312,028	$514,891	$717,755	$1,544,674	$1,248,451
Htr	Internal deployment effort costs	$0	$11,756	$16,459	$21,161	$49,376	$40,189
Itr	Ongoing management costs	$0	$396,750	$396,750	$396,750	$1,190,250	$986,659
	Total costs (risk-adjusted)	$0	$720,534	$928,100	$1,135,666	$2,784,300	$2,275,299

FIREWALL SUBSCRIPTION COSTS

Evidence and data. Interviewees told Forrester their organizations paid consumption-based rates for their Palo Alto Networks Software Firewalls.

- These rates varied based on the types of firewalls and total usage. The rates for VM-Series virtual firewalls and CN-Series container firewalls is based on the number of firewalls, and the rates for Cloud NGFW firewalls are based on usage.
- Organizations pay in credits, which enables them to reallocate their firewalls without changing their annual costs.
- The fees also include additional the cost of features and services (e.g., Panorama).

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

- In Year 1, the composite organization pays usage fees for 40 VM-Series Software Firewalls. It pays for 100 firewalls in Year 2 and 160 in Year 3.
- The composite organization pays a consistent usage-based fee for its cloud firewalls.
- In Year 1, the composite organization pays usage fees for two CN-Series container Software Firewalls. It pays fees for six in Year 2 and 10 in Year 3.
- Pricing may vary. Contact Palo Alto Networks for additional details.

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

- The size of negotiated discounts.
- The number of firewalls the organization deploys.
- The organization's usage of each firewall.

Results. To account for these risks, Forrester adjusted this cost upward by 0%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.2 million.

Firewall Subscription Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	VM-Series Software Firewalls deployed	Composite		40	100	160
G2	Credits required for VM-Series Software Firewalls	Composite		637.56	1,593.90	2,550.24
G3	**Cost of VM-Series Software Firewalls**	**Composite**		**$123,368**	**$308,420**	**$493,471**
G4	CN-Series Software Firewalls deployed	Composite		2	6	10
G5	Credits required for CN-Series Software Firewalls	Composite		46.02	138.07	230.12
G6	**Cost of CN-Series Software Firewalls**	**Composite**		**$8,905**	**$26,717**	**$44,528**
G7	**Usage-based costs of Cloud NGFW Software Firewalls**	**Composite**		**$179,755**	**$179,755**	**$179,755**
Gt	Firewall subscription costs	G3+G6+G7		$312,028	$514,891	$717,755
	Risk adjustment	0%				
Gtr	Firewall subscription costs (risk-adjusted)		$0	$312,028	$514,891	$717,755
	Three-year total: $1,544,674			**Three-year present value: $1,248,451**		

INTERNAL DEPLOYMENT EFFORT COSTS

Evidence and data. 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.

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

- In its legacy environment, the composite would have required 5 hours to deploy a firewall.
- With Palo Alto Networks Software Firewalls, this time is reduced to 3.75 hours per firewall.

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

- The number and types of Palo Alto Networks Software Firewalls the organization deploys.
- The time required to deploy each Palo Alto Networks Software Firewall.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $40,200.

Internal Deployment Effort Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Time required for deployment (hours)	A1*3.75 hours		188	263	338
H2	Average hourly salary of a deployment team member	Assumption		$57	$57	$57
Ht	Internal deployment effort costs	H1*H2	$0	$10,688	$14,963	$19,238
	Risk adjustment	↑10%				
Htr	Internal deployment effort costs (risk-adjusted)		$0	$11,756	$16,459	$21,161
	Three-year total: $49,376			**Three-year present value: $40,189**		

ONGOING MANAGEMENT COSTS

Evidence and data. Interviewees said that to reap the full benefits of Palo Alto Networks Software Firewalls, their organizations need teams of managers to maintain, update, and configure the firewalls as necessary.

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

- A total of 20 FTEs are involved in ongoing management of the composite's security configurations and updates.
- This team spends 15% of its time managing Palo Alto Networks Software Firewalls.

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

- The size of the organization's security maintenance and management teams.
- The percentage of time spent these teams spend managing Palo Alto Networks Software Firewalls.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $987,000.

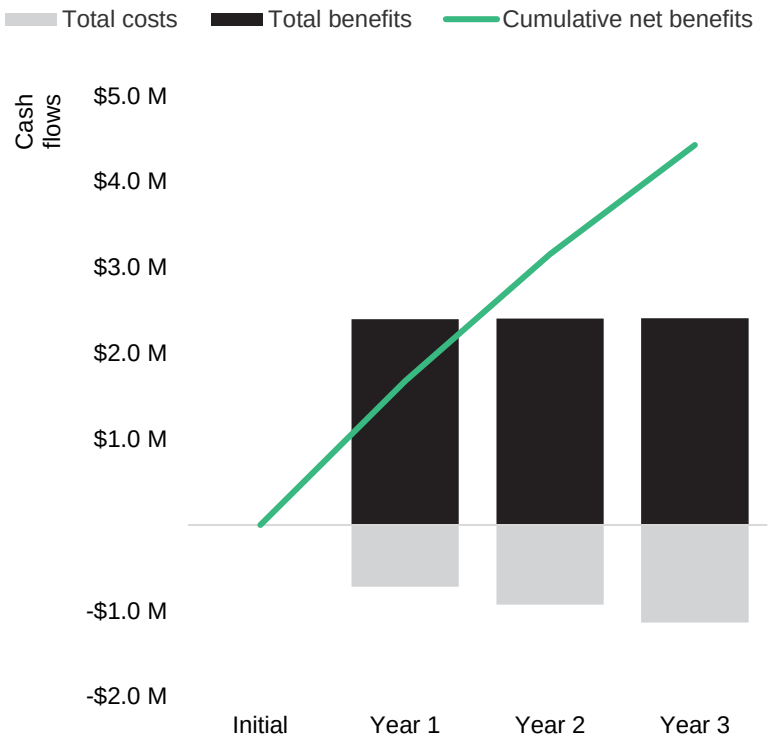
Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	FTEs involved in ongoing management	Composite		20	20	20
I2	Percentage of time FTEs spend solely on Palo Alto Networks Software Firewalls management	A7		15%	15%	15%
I3	Average annual compensation rate of an FTE involved in ongoing management	TEI standard		$115,000	$115,000	$115,000
It	Ongoing management costs	I1*I2*I3	$0	$345,000	$345,000	$345,000
	Risk adjustment	↑15%				
Itr	Ongoing management costs (risk-adjusted)		$0	$396,750	$396,750	$396,750
	Three-year total: $1,190,250			**Three-year present value: $986,659**		

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	$0	($720,534)	($928,100)	($1,135,666)	($2,784,300)	($2,275,299)
Total benefits	$0	$2,398,668	$2,404,130	$2,409,591	$7,212,389	$5,977,853
Net benefits	$0	$1,678,134	$1,476,030	$1,273,925	$4,428,089	$3,702,554
ROI						163%
Payback						0 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 consider 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.

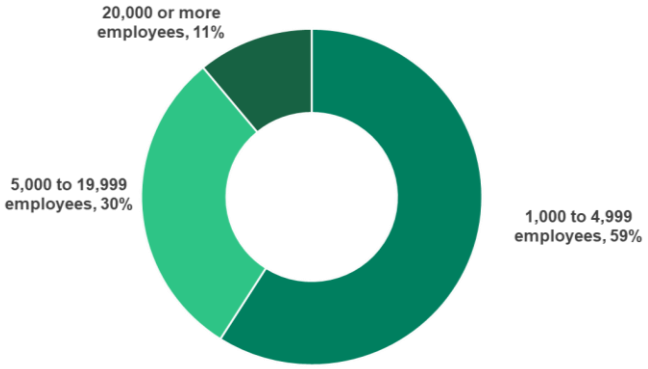
Appendix B: Interview And Survey Demographics

Interviews

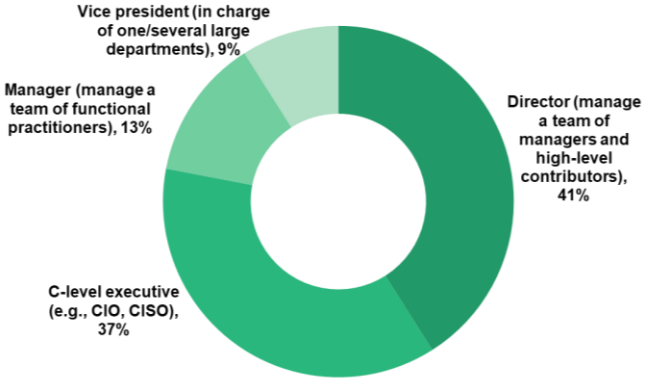
Role	Industry	Firewalls	Employees
Director of network security engineering Principal security engineer	Financial services	VM series with limited use of Azure/AWS	2,500
Senior VP of IT	Financial services	VM series	3,000
Enterprise infrastructure architect	Government	VM series	10,000
AVP	Financial services	VM series	60,000
Associate director	IT services	VM series	87,000

Survey Demographics

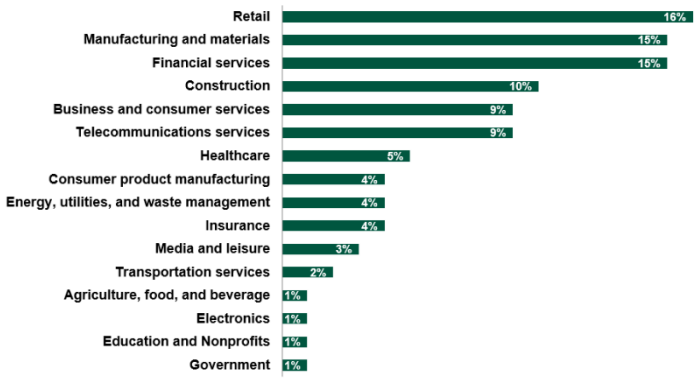
"Using your best estimate, how many employees work for your organization/firm worldwide?"



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

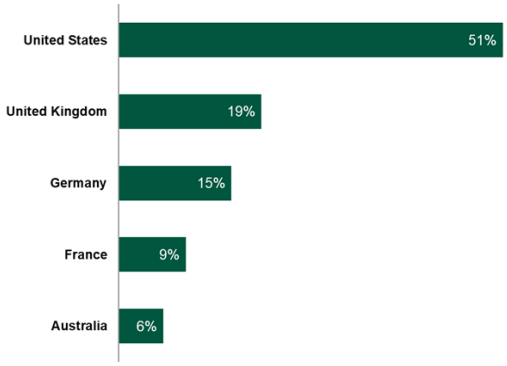


"Which of the following best describes the industry to which your organization belongs?"



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

"In which country are you located?"



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®