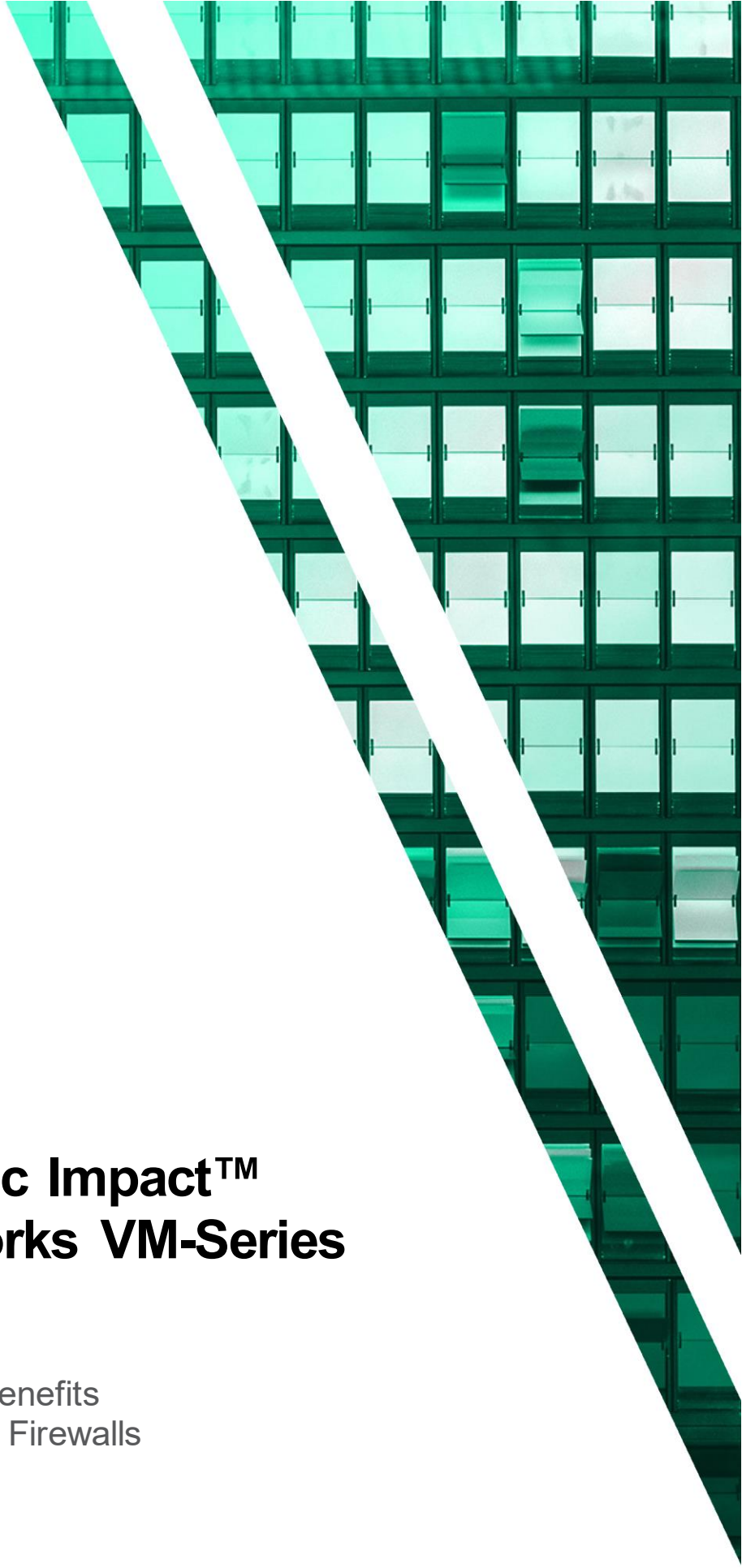
FORRESTER®



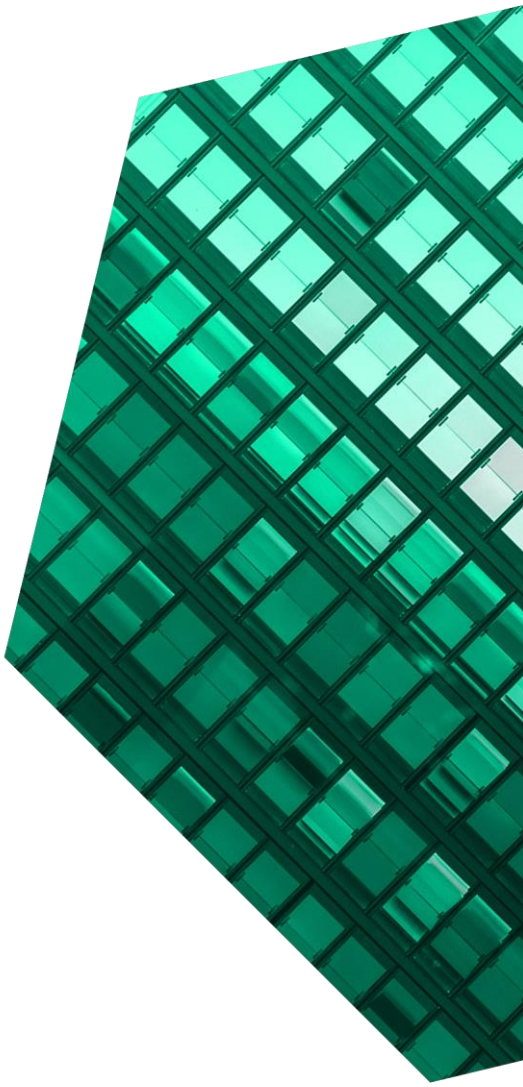
The Total Economic Impact™ Of Palo Alto Networks VM-Series Virtual Firewalls

Cost Savings And Business Benefits Enabled By VM-Series Virtual Firewalls

SEPTEMBER 2021

Table Of Contents

Consulting Team: Sam Conway
Isabel Carey



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

Executive Summary

As enterprises migrate to the cloud and explore the benefits of hybrid cloud and multicloud deployments, their security teams must contend with a new breed of vulnerabilities and networking demands. Firewalls remain one of the most dependable tools for security professionals providing on-premises security while next-generation firewalls have emerged as a control plane to secure data paths to multiple clouds. Palo Alto Networks VM-Series firewalls provide flexible security solutions for agile enterprises.

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 VM-Series virtual firewalls.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Palo Alto Networks VM-Series virtual firewalls on their organizations.

Palo Alto Networks' VM-Series firewalls provide all the capabilities of the Palo Alto Networks hardware next-generation firewalls (NGFWs) in a virtual machine (VM) form factor. VM-Series firewalls offer a broad range of capabilities to meet today's network security challenges across public and private clouds, virtualized data centers, and software-defined branch locations. Organizations can leverage their existing hardware infrastructures to cohost firewalls with other virtualized networks, security services, or even applications.

Payback period:

<6 months

KEY STATISTICS

Return on investment (ROI)
115%

Net present value (NPV)
$1.83M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed eight decision-makers and surveyed 132 who have experience using VM-Series virtual firewalls. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization.

Prior to using VM-Series virtual firewalls, the interviewees' organizations primarily relied on hardware firewalls with point solutions. However, as they took on larger digital transformation projects and moved toward virtualizing across the enterprises to consolidate network and security infrastructures and public clouds, they found that legacy firewalls lacked the flexibility teams required. The organizations investigated relying on the native security capabilities of cloud service providers, but they found them lacking the proficiency that a mature security provider like Palo Alto Networks can provide. Furthermore, the organizations used an average of four public clouds,

and they did not want to introduce more complexity to their security stacks.

After investing in VM-Series virtual firewalls, the interviewees' organizations addressed the security challenges of their hybrid-cloud and multicloud environments. Their security teams could easily deploy advanced security controls and define, enforce, and manage consistent security policies from a single console. With improved visibility, they gained precise control of inbound, outbound, and east-west traffic, which ensured that attack surfaces were greatly reduced. The form factor of the VM-Series also afforded the organizations the flexibility to automate firewall deployment and provisioning and to scale with demand. This reduced deployment times and eliminated overprovisioning costs.

Reduction in firewall deployment time

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Reduced the time required to deploy firewalls by 90% and improved network and security team efficiencies by 80%, saving $1.3 million over three years.** It takes significantly less time to deploy VM-Series firewalls than traditional legacy firewalls, where hardware would be shipped, installed, and tuned. Additionally, the interviewees' organizations recognized efficiencies from consolidating firewall management in Palo Alto Networks Panorama (which provides centralized network security management), maintaining a single set of policies across clouds, centralizing patching, and making upgrades.
- **Reduced time to achieve proper security posture by 30%, saving $436,800 over three years.** By leveraging Palo Alto Networks' NGFWs and cloud-delivered security services, the interviewees' organizations were able to stand up their security solutions faster and reach steady states more quickly. This gave security teams a head start on optimizing the solution to the Zero Trust standards compared to using point solutions.

> **[Palo Alto Networks] enabled us to move away from different security and networking components and look at security more as a platform play. It helped us simplify the environment and enabled us to move to the cloud. That was the reason we brought in [Palo Alto Networks]. Otherwise you'd have to bring in different vendors and different tools, and then you would have to stitch them together.**
>
> — Global head of IT engineering, beverage

- **Reduced the number of security incidents requiring manual investigation by 18% and decreased mean-time-to-resolution (MTTR) by 25%, resulting in $240,100 saved over three years.** Deploying the centrally managed VM-Series firewalls helped network security, IT, and security operations (SecOps) professionals automate previously manual processes and improve visibility into network traffic. With better visibility and data, teams were able to resolve issues faster.
- **Reduced incidents and improved end-user efficiency, valued at $493,400 over three years.** With stronger threat protection and fewer incidents, end users endured less downtime and could focus on their primary roles. This drove additional value for the interviewees' organizations.
- **Reduced the total cost of security stacks by eliminating point solutions and avoiding overprovisioning, which saved nearly $573,800 over three years.** Interviewees said VM-Series firewalls allowed their organizations to use one consistent toolset across multicloud deployments and to utilize cloud-delivered security services. This helped them to confidently secure all traffic that traversed any network or clouds and eliminate point solutions. Additionally, the ease of deploying VM-Series firewalls provided the organizations with a level of scalability not available with traditional appliances and eliminated the need to overprovision in anticipation of increased use.

"If you have two different firewall technologies you are maintaining, you almost double the effort."
CISO, medical devices

- **Decreased the likelihood of a data breach by 20% after three years.** With Palo Alto Networks, the organizations were able to enact Zero Trust security models and apply consistent security policies. They used VM-Series to reduce attack surfaces with segmentation and microsegmentation, advanced threat prevention, and application-level firewalls.

We came at [our decision to invest in Palo Alto Networks] from a financial perspective, a security perspective, and operational overhead efficiency savings perspective, and from a feature-set [perspective] too.. When you put [Palo Alto Networks] side-by-side with a lot of other vendors, there was really no comparison dollar per dollar.

— EVP of engineering, IT services

Unquantified benefits. Benefits that are not quantified for this study include:

- **Being able to use existing skills to avoid training and recruitment.** Organizations were able to deploy and manage Palo Alto Networks VM-Series firewalls using existing resources. As an industry leader in firewalls, Palo Alto Networks firewall skills are widely available, eliminating the need to recruit and train additional resources.
- **Increasing scalability and flexibility.** In their virtual form factor, VM-Series firewalls can be quickly deployed or removed as needed. This capability ensures that organizations can quickly adapt to changing needs while controlling costs.
- **Improving competitiveness.** Some interviewed organizations used Palo Alto Networks as a competitive advantage when providing technology services. These organizations provided cloud-hosted services, and used the security provided by VM-Series as a differentiator to win and retain customers.
- **Ensuring that security is not a barrier to digital transformation efforts.** Security teams have a mandate to ensure that operations are as secure as possible, but do not want to be a hindrance to digital transformation efforts of their business. With VM-Series, teams could quickly deploy firewalls and attain the required level of security posture so their organizations could recognize the benefits of public and hybrid cloud migrations. Additionally, the teams could quickly react to new threat vectors created by digital transformation and secure assets at the very edge of their network – such as retail kiosks.

Costs. Risk-adjusted PV costs include:

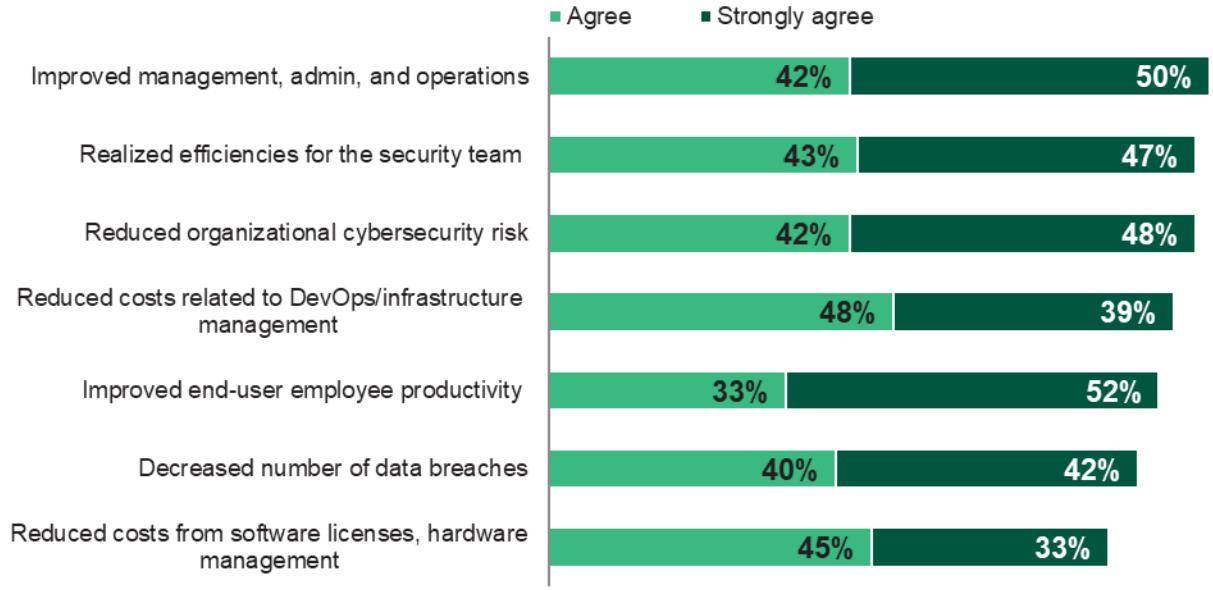
- **Firewall licensing totaling $1 million over three years.** Organizations traditionally paid annual licensing fees for the use of VM-Series firewalls and cloud-delivered security services, but Palo Alto Networks recently introduced a flexible-consumption model that allows them to dynamically adjust the size of their firewalls based on need and change or add new cloud-delivered subscription services (CDSS) options. This flexible pricing model (which is meant to allow customers to adjust security to fit rapidly changing environments) is designed to provide even more cost efficiencies than the annual licensing fees Forrester modeled for the composite organization.
- **Internal deployment effort totaling $4,900 over three years.** Interviewees said it required time and labor to deploy VM-Series firewalls and as additional firewalls were installed in subsequent years.
- **Ongoing management totaling nearly $441,000 over three years.** Interviewees said their organizations incurred internal labor costs for ongoing management of their organizations' VM-Series deployments. This included tuning, updating, and pushing new policies.
- **White-box appliance costs of $151,000 over three years.** The organizations deployed their VM-Series firewalls using commodity hardware, and they incurred some additional costs for new appliances.

Reduced likelihood of a data breach

20% reduction by Year 3

The customer interviews and financial analysis found that a composite organization experiences benefits of $3.43 million over three years versus costs of $1.6 million, adding up to a net present value (NPV) of $1.83 million and an ROI of 115%.

Figure 1. "On a scale of 1 to 5 where 1 means 'strongly disagree' and 5 means 'strongly agree,' how much do you agree that Palo Alto Networks VM-Series virtual firewalls (including use with any security service) have the following?"



Base: 132 cloud-security decision makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

ROI
115%

BENEFITS PV
$3.43M

NPV
$1.83M

PAYBACK
<6 months

Benefits (Three-Year)

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in VM-Series virtual 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 VM-Series virtual firewalls can have on an organization.

Forrester Consulting conducted an online survey of 351 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 November 2020.

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 VM-Series virtual 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.

DUE DILIGENCE

Interviewed Palo Alto Networks stakeholders and Forrester analysts to gather data relative to VM-Series virtual firewalls.

CUSTOMER INTERVIEWS

Interviewed eight decision-makers and surveyed 132 decision-makers at organizations using VM-Series virtual firewalls 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 decision-makers.

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 VM-Series Virtual Firewalls Customer Journey

Drivers leading to the VM-Series virtual firewalls investment

Interviewed Decision-Makers			
Interviewee	**Industry**	**Region**	**Revenue**
Lead architect	IT services	Europe	$80 million
Senior expert in networking	IT services	Europe	$80 million
Network engineer	Communications infrastructure	United States	$6 billion
EVP of engineering	IT services	United States	N/A
Global head of IT engineering	Beverage	Global	$37 billion
Information security engineer	Business services	North America	$3 billion
Senior security engineer	Business services	North America	$3 billion
CISO	Medical devices	North America	$800 million

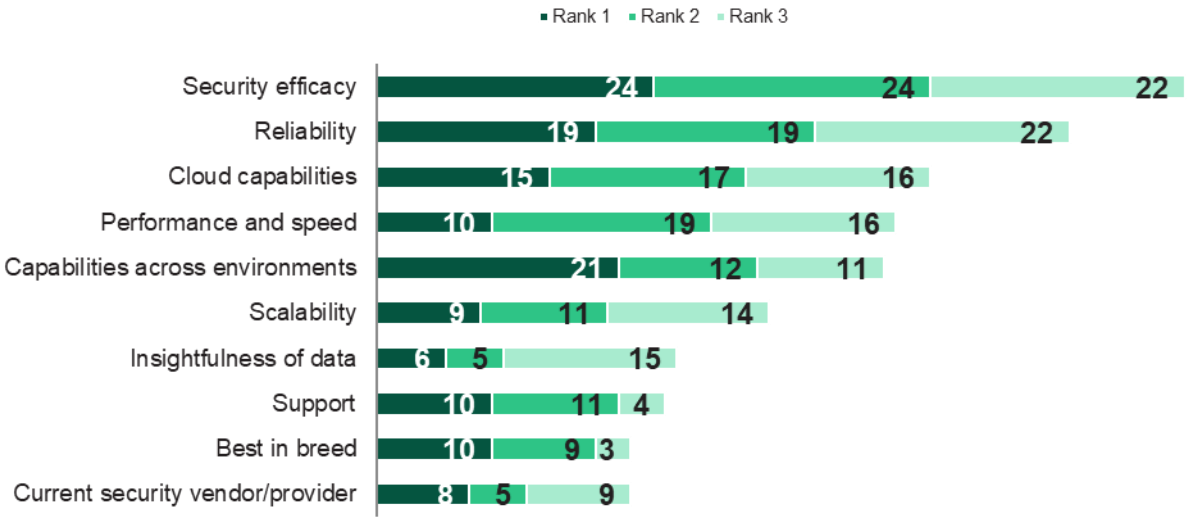
KEY CHALLENGES

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

- **Underperforming legacy point solutions.** The interviewees said prior legacy point solutions failed to meet expectations around speed, performance, and customer support from vendors. Previously deployed products were slow to upgrade and required significant internal effort to deploy and to maintain.
- **Decentralized security platforms and capabilities.** Prior to using VM-Series firewalls, the interviewees' organizations struggled to manage decentralized security tools, and that led to gaps in visibility and redundant work. For example, organizations that used multiple clouds would have to write and push multiple versions of the same policies when using native tools.
- **Organizational cloud migration mandates.** Many of the organizations operated in environments with strict timelines to achieve cloud migrations. These organizations needed security solutions that could be quickly deployed and that ensured they had proper visibility to adequately protect their new cloud deployments.

> **"When we separated from the mother company, we had a four day weekend to separate locally. So, we built everything in parallel – new firewalls X, Y, and Z systems to make a cut in such a short timeframe. For us, it was a priority to progress on the transformational efforts."**
> *CISO, medical devices*

Figure 2. "From the list below, select the three most important criteria when choosing a network security vendor and rank from them from 1 to 3 in order of importance where 1 is most important."



Base: Variable cloud security decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

WHY PALO ALTO NETWORKS

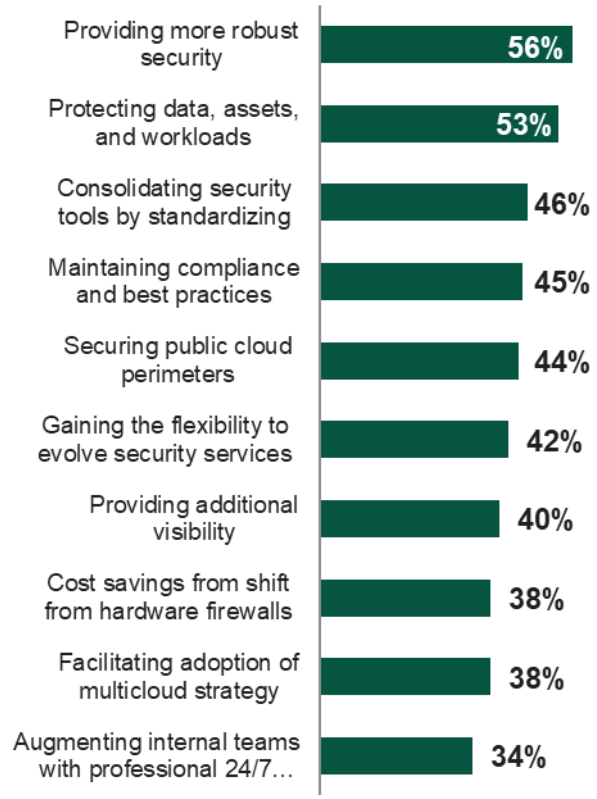
The interviewees' organizations evaluated multiple solutions before eventually deciding to invest in VM-Series virtual firewalls. Key capabilities that factored into the investments included:

- **Layer 7 visibility.** VM-Series firewalls offer application visibility across all ports and provide pertinent data for making policy decisions.
- **Application segmentation.** Organizations can use VM-Series firewalls to segment and control application communication. This is bolstered by advanced threat prevention to identify and block lateral network threats.
- **Advanced security with CDSS.** Palo Alto Networks security subscriptions can be enabled on the VM-Series without requiring the installation or deployment of additional sensors or appliances. This allows organizations to recognize the additional protection benefits of services such as advanced intrusion prevention systems (IPS), domain name system (DNS) security, URL filtering, and zero-day threat prevention and sandboxing without additional overhead.
- **User-based policies.** VM-Series firewalls natively provide user-based policies, and they are integrated with a wide range of user repositories. This enables dynamic, user-based access control policies in addition to application-based policies.

> **"One of the things that Palo Alto brings to the table from a security standpoint is that it is more focused, and the DNA is around identity and being able to refresh security in real time."**
> *Global head of IT engineering, beverage*

- **Centralized management for consistent policies and simplified management.** VM-Series firewalls can be managed centrally through Panorama, which ensures policy consistency across multiple cloud and on-premises deployments. Panorama also alleviates the need for operators to manage their network security postures from multiple, disparate consoles.
- **Automated deployment and policy updates.** Organizations can leverage VM-Series capabilities to integrate security into application development workflows including automatic provisioning, automated policy updates, use of native cloud provider templates, and cloud-native scalability.

Figure 3. "What were some of the key factors that drove the decision to invest in Palo Alto Networks VM-series virtual firewalls?"



Base: 132 cloud security decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

Key assumptions

- **$3B revenue**
- **Based in the US**
- **100 initial VM-Series firewalls**
- **7,500 employees**
- **12 SecOps FTEs**
- **8 NetOps FTEs**

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 eight decision-makers that Forrester interviewed and the 132 companies that Forrester surveyed, 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 $3 billion in annual revenue and 7,500 employees. The organization is headquartered in the United States, and it has global teams. The organization's security team handles 154 incidents per week.

Deployment characteristics. The composite organization uses VM-Series firewalls to secure both north-south and east-west traffic across multiple cloud deployments. The organization maintains 156 virtual firewalls that are deployed on commodity appliances by Year 3. It manages its VM-Series firewalls with Panorama. Palo Alto Networks CDSS enhance each NGFW deployment with in-line prevention of known and unknown threats (with Palo Alto Networks Threat Prevention and WildFire malware analysis) and all web-borne threats (with

Palo Alto Networks URL Filtering and DNS Security). This includes command-and-control mitigation and data loss prevention (DLP).

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	$531,498	$517,624	$518,780	$1,567,902	$1,300,736
Btr	Security posture attainment	$381,758	$56,858	$56,858	$495,473	$436,760
Ctr	Security Ops and IT operations efficiency	$96,562	$96,562	$96,562	$289,686	$240,136
Dtr	Reduced end-user downtime	$198,398	$198,398	$198,398	$595,195	$493,387
Etr	Security infrastructure cost reduction and avoidance	$240,996	$224,121	$225,527	$690,645	$573,754
Ftr	Data breach risk reduction	$105,083	$157,624	$210,166	$472,873	$383,699
	Total benefits (risk-adjusted)	$1,554,294	$1,251,188	$1,306,291	$4,111,774	$3,428,472

FIREWALL DEPLOYMENT AND MAINTENANCE

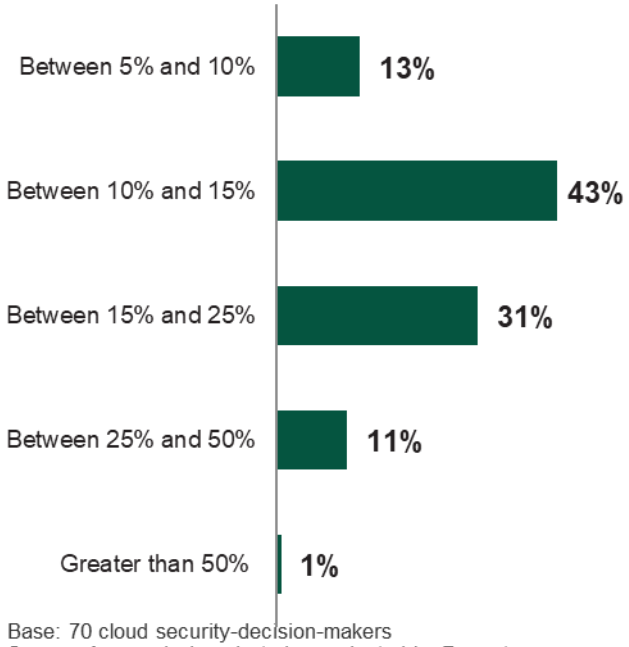
Evidence and data. Interviewees said that in a virtual form factor, VM-Series firewalls require far less time for deployment and maintenance than legacy solutions. Previously, their organizations primarily used traditional physical appliances that required manual labor to install and tune as well as long shipping periods. Interviewees from organizations that had used native cloud service provider solutions said having the ability to manage VM-Series deployments through Panorama was a key time saver and created a single policy model across on-premises and cloud deployments.

- A network engineer at a communications infrastructure firm said: "After we got rid of all the appliances, the support costs were much lower. There's also the time to spin up these devices and get them out in the field and the time involved in configuring all this equipment, so we're definitely saving that way. For example, with our old firewall, if you didn't size it correctly with an appliance, you would have to go out and purchase another appliance that was bigger. With [VM-Series virtual firewalls], you just put a different license in, and now you've got a firewall that's the right size."
- An EVP of engineering for an IT services firm said: "When you're deploying security services and running a firewall, security is the top priority. Right? So, the amount of man hours required to update individual firewalls is just untenable with multiple solutions. In the past, when we would deploy something, we would spend 2 to 3 hours per firewall, and that was just to get it going and get it deployed to get all the networks and everything set up. That did not include any rule sets, any refinements of the rules, or any of that. Now, we've got that [timeframe] down to less than 10 minutes, and our provisioning team can do multiple at a time. So, we've not only gone from [needing] 2 to 3 hours per firewall down to about 10 minutes or less, but [our provisioning team] can do more than one at a time. So, that's massively scaled our ability to deploy these."
- A global head of engineering at a beverage organization stated: "With the [VM-Series virtual

firewalls], it's templatized and cookie cutter. Once you've got that done, you can automate a lot. For us, I would say the cost and effort of deployment and configuration has been cut down by at least 90%."

- The same interviewee also described the arduous experience of deploying a legacy solution. They said: "When you include the cost of shipping the physical components, the delays in getting that equipment shipped out there, and then racking, that is a pretty large amount of time wasted before you can bring the firewall up and running."
- Among survey respondents, 92% said VM-Series virtual firewalls (and security services) improved their organization's management, admin, and operation efforts on cybersecurity (see Figure 1). Fifty-eight percent of these respondents said their organization experienced faster time-to-deploy Palo Alto Networks security solutions that are not the physical firewall, and 57% said their organization experienced faster deployment and configuration of security policies (see Figure 4).

Figure 4. "You noted faster deployment of security policies due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). How do you estimate the percentage improvement compared to with your previous environment?"



Base: 70 cloud security-decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

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

- The organization deploys 100 VM-Series firewalls in Year 1.
- The organization's deployment grows 25% annually with organizational need.
- Legacy solutions required 5 hours to fully deploy and tune.
- A team of 10 employees was responsible for managing the legacy solution, which consisted of installing the solution, managing security policies, and applying updates and infrastructure patches. These resources dedicated 75% of their time solely to firewalls.
- The average fully burdened annual salary for members of the team responsible for managing the legacy solution is $112,500.
- VM-Series firewalls require 90% less effort to deploy virtually, and the firewall team is 80% more efficient with centralized policy control, automated updating, patching, and elimination of racking.
- Eighty percent of the time saved is redeployed to productive work.

Risks. Risks that could impact the realization of this benefit include:

- The size and skill set of the organization's security management team.
- The capabilities and systems that are in place before deploying VM-Series virtual firewalls.
- The average salaries of network, security, and IT operations team members.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.3 million.

Firewall Deployment And Maintenance

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Net new firewalls deployed	Composite	100	25	31
A2	Time required to deploy legacy firewalls (hours)	Interviews	5	5	5
A3	Reduction in time required to deploy VM-Series firewall	Interviews	90%	90%	90%
A4	Total reduction in annual deployment time (hours)	A1*A2*A3	450	113	141
A5	Firewall team FTEs required	Composite	10	10	10
A6	Percent of time dedicated to firewall work	Assumption	75%	75%	75%
A7	Improvement in firewall security and network management (e.g., centralized control, single set of policies, racking, routing, and patching)	Interviews	80%	80%	80%
A8	Management time saved (hours)	A5*2,080 hours*A6*A7	12,480	12,480	12,480
A9	Productivity recapture	Assumption	80%	80%	80%
A10	Average hourly salary of IT employee (e.g., NetOps, SecOps, IT operations)	Assumption	$54	$54	$54
At	Firewall deployment and maintenance	(A4+A8)*A9*A10	$559,471	$544,868	$546,085
	Risk adjustment	↓5%			
Atr	Firewall deployment and maintenance (risk-adjusted)		$538,498	$517,624	$518,780
	Three-year total: $1,567,902	**Three-year present value: $1,300,736**			

SECURITY POSTURE ATTAINMENT

Evidence and data. Interviewees said Palo Alto Networks' consistent technology, unified platform, and advanced management capabilities allowed their organizations to get to steady state more quickly. They could stand up their security stacks faster, reduce their implementation efforts, and allow security teams to start fine-tuning sooner than if the organizations leveraged point solutions.

With Palo Alto Networks, the organizations were able to integrate all components on a common platform and give them each a similar look and feel. This made deployments faster and freed up resources to fine-tune the solution, implement automated workflows, and find ways to improve efficiency for security, IT, and business users.

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

- The organization uses the same deployment team in both scenarios. The team includes 12 SecOps employees and eight NetOps employees in the initial year of the deployment.
- The average fully burdened annual salary of a SecOps employee is $121,500.

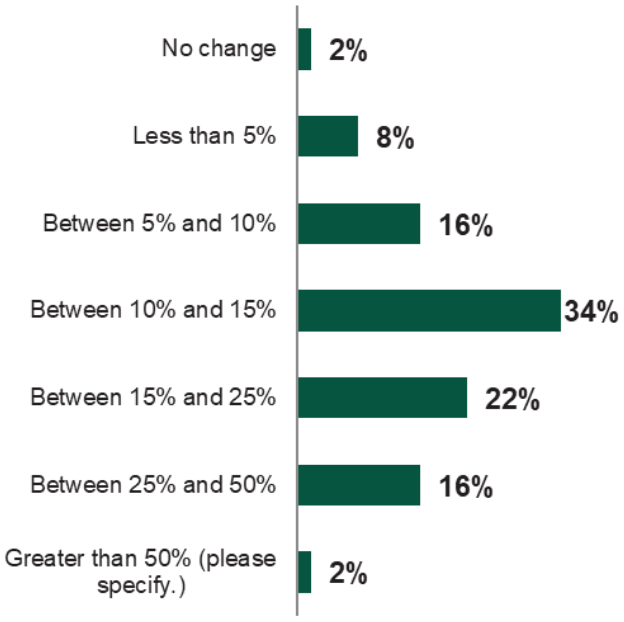
- The average fully burdened annual salary of a NetOps employee is $135,000.
- With Palo Alto Networks, the organization reaches a steady state 30% faster than with point solutions, reducing the time to steady state from 6.3 months to 4.4 months.

Risks. Risks that could impact the realization of this benefit include:

- The size of the deployment team and relative salaries.
- The specific components being deployed and the time it takes to reach steady state.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $436,800.

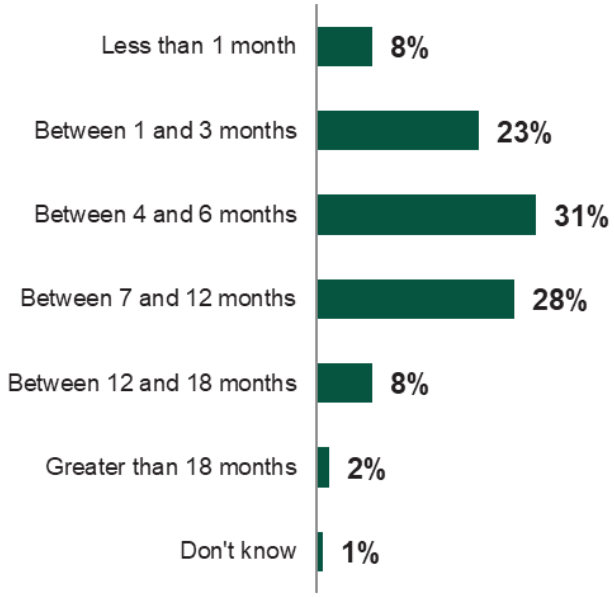
Figure 5. You noted faster time to produce information during audits due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service)? Can you estimate the percentage improvement compared to your previous environment?



Base: 50 cloud security decision makers

Source: "PAN Virtual Firewalls TEI", a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

Figure 6. You noted reduced organizational cybersecurity risk due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service)? Can you estimate the time it took your organization to achieve 'steady state' security posture with prior point solutions?



Base: 119 cloud security decision makers

Source: "PAN Virtual Firewalls TEI", a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

Security Posture Attainment					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	SecOps FTE annual salary with benefits	Assumption	$121,500	$121,500	$121,500
B2	NetOps FTE annual salary with benefits	Assumption	$135,000	$135,000	$135,000
B3	SecOps FTEs required	Composite	12	2	2
B4	NetOps FTEs required	Composite	8	1	1
B5	Time required to achieve proper security posture with point solutions (months)	Survey results	6.3	6.3	6.3
B6	Time required to achieve proper security posture with Palo Alto Networks (months)	Survey results	4.4	4.4	4.4
B7	Initial and ongoing time difference between point solutions and VM-Series virtual firewalls (rounded)	1-(B6/B5)	30%	30%	30%
B8	Cost to steady state point solutions	(B1*B3/12*B5)+(B2*B4/12*B5)	$1,332,450	$198,450	$198,450
B9	Cost to attain with VM-Series virtual firewalls	(B1*B3/12*B6)+(B2*B4/12*B6)	$930,600	$138,600	$138,600
Bt	Security posture attainment	B8-B9	$401,850	$59,850	$59,850
	Risk adjustment	↓5%			
Btr	Security posture attainment (risk-adjusted)		$381,758	$56,858	$56,858
	Three-year total: $495,473		**Three-year present value: $436,760**		

SECURITY OPERATIONS AND IT OPERATIONS EFFICIENCY

Evidence and data. Interviewees said SecOps and IT teams benefited from their organization's VM-Series deployment through a reduced number of investigations, faster MTTR, and fewer security issues that impacted devices. SecOps and IT operations teams automated previously manual processes, and they improved visibility into network traffic, which allowed for a faster response to issues. Additionally, the interviewees' organizations took advantage of log tracing and analysis in Prisma Cloud to further reduce MTTR.

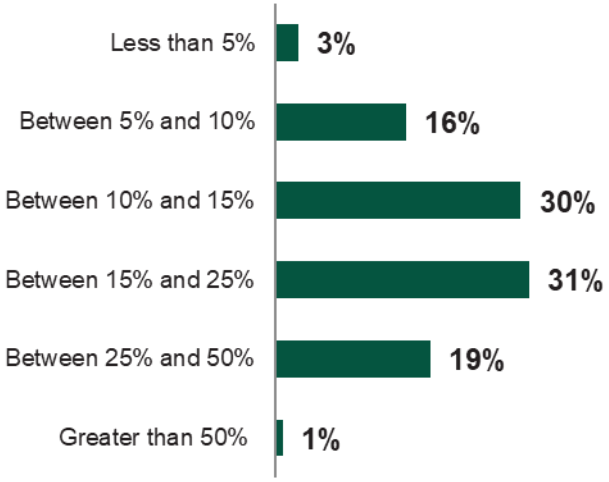
MTTR reduced by

25%

- The global head of engineering at a beverage firm said: "The efficacy rate is really high with Palo Alto Networks and having the ability to update the content and policies on a daily basis helps. With the VM-Series, we enabled application-driven user policies from the get go. We've reduced the number of false positives requiring human intervention by 40% to 50%, and we've reduced our tickets by at least 40% just

from the network threat modeling capability. [My organization's support team] is getting a lower volume of tickets, and when they do get a ticket, then we know it's something they need to look into versus doubting it."

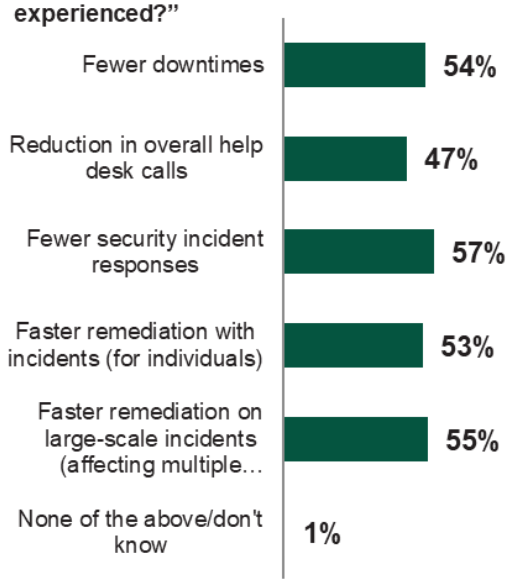
Figure 7. "You noted faster mean-time-to-know on security incidents due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Can you estimate the percentage improvement compared to your previous environment?"



Base: 70 cloud security-decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

- The network engineer for a communications infrastructure firm said: "It's easier to manage. The logging from the cloud coming through the network to [Palo Alto Networks'] logging servers just gives it so much visibility into what's happening in the cloud. We go into Panorama, enter the configuration that they need, and then we push it out. So, the time savings on that versus somebody going to each firewall and actually having to enter that information is tremendous. And the time that it takes to do that is minutes to do something like that. So, there's definite time savings for security to be able to act on something we are seeing from the logging information."

Figure 8. "You noted improved end-user employee productivity due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Which of the following have you experienced?"

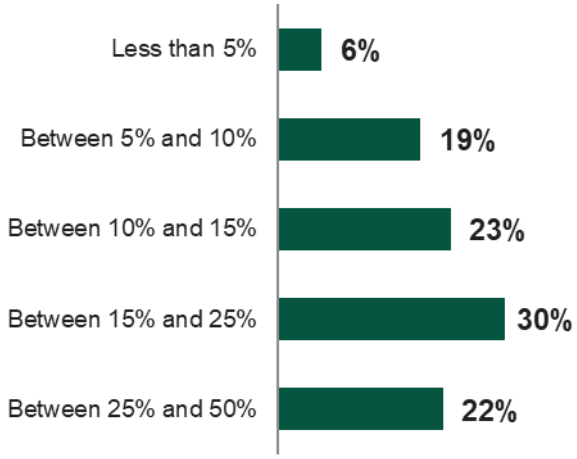


Base: 113 cloud security decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

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

- With its previous solution, 154 security incidents per week required multi-touch, advanced investigation work from the SecOps team. With quickly adaptable policies consistently deployed on-premises and across clouds, the composite organization improves visibility and threat prevention, and it reduces the number of incidents by 18%.
- In its prior state, the composite's average MTTR was 45 minutes. With better contextual data and fewer false positives, the composite organization reduces MTTR by 25%.
- The average fully annual burdened salary for a SecOps team member is $121,500. The hourly rate is $58 per hour.
- Eighty percent of the time saved is redeployed to productive activities.

Figure 9. "You noted lower false positive detection rate due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Can you estimate the percentage improvement compared to your previous environment?"



Source: "PAN Virtual Firewalls TEI", a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

Risks. Risks that could impact the realization of this benefit include:

- The number of security incidents that require manual intervention before implementing VM-Series virtual firewalls.
- The overall impact to MTTR.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $240,100.

Security Operations And IT Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of security incidents requiring manual investigation/remediation with legacy security solution	Composite	8,008	8,008	8,008
C2	Reduction in security incidents requiring manual investigation/remediation with VM-Series virtual firewalls	Survey results	18%	18%	18%
C3	Manual multi-touch security incidents avoided (rounded)	C1*C2	1,441	1,441	1,441
C4	MTTR with prior solution (minutes)	Survey results	45	45	45
C5	Subtotal: Avoided investigations and remediation with VM-Series firewalls	C3*C4/60*C8	$62,703	$62,703	$62,703
C6	MTTR improvement with VM-Series firewalls	Survey results	25.0%	25.0%	25.0%
C7	Time saved per incident (minutes)	C4*C6	11	11	11
C8	Average fully burdened hourly salary of SecOps employee (rounded)	Assumption	$58	$58	$58
C9	Subtotal: Security operations efficiency related to critical alerts (rounded)	((C1-C3)*C7/60)*C8	$71,411	$71,411	$71,411
C10	Productivity capture of security FTE	Assumption	80%	80%	80%
Ct	Security operations and IT operations efficiency	(C5+C9)*C10	$107,291	$107,291	$107,291
	Risk adjustment	↓10%			
Ctr	Security operations and IT operations efficiency (risk-adjusted)		$96,562	$96,562	$96,562
	Three-year total: $289,686		**Three-year present value: $240,136**		

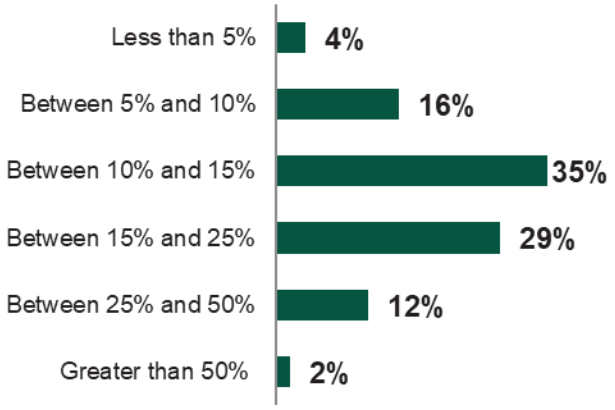
REDUCED END-USER DOWNTIME

Evidence and data. Interviewees said VM-Series made it is easy to ensure consistent policies are deployed across myriad environments (e.g., on-premises, public cloud, etc.). Consistent enforcement ensured that fewer threats caused downtime incidents and having centralized management of the VM-Series firewalls facilitated faster response times.

- Surveyed respondents said an average of 18.1% of end users were impacted by downtime events prior to deploying VM-Series firewalls. After deployment, this fell to 5.6% of users.
- An IT services organization that provides B2B cloud services used VM-Series firewalls to segment customer environments. In the past, hardware failure caused outages for groups of customers. But if a VM-Series firewall failed, the outage would be limited to one customer. The organization's lead architect said: "If we pushed an update and caused an hour of downtime, that would be felt by all our customers who were on the appliance. With the [VM-Series firewalls], each customer has their own. We've experienced no downtime, but if we did, it would be a limited impact."
- Interviewees said having NGFW capabilities like being able to offload traffic reduced the likelihood that firewalls would impede users. The global head of IT engineering with a beverage organization said: "With policy-based management, we were very easily able to offload traffic that is not required to be monitored like white-listed websites and all our audio and video. People are using more and more, and I can offload the traffic at a local point with a click of a button, compared to other tools that don't do that. So, we were able to provide a good user experience by offloading those and providing a better throughput for the network."

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

Figure 10. "You noted reduction in average triage time due to Palo Alto Networks Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Can you estimate the percentage improvement compared to your previous environment?"

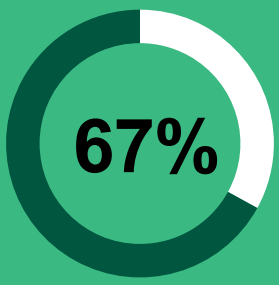


Base: 49 cloud security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

- In its legacy state, 18% of its 7,500 employees were impacted by downtime events each year. With VM-Series firewalls, this declines by 67% and only 6% of the employees experience a downtime event.
- Historically, downtime events lasted an average of 4.5 hours. After deploying VM-Series firewalls, this declines by 45% (by 2 hours) for users still impacted by downtime.

Reduction in user downtime



- The average fully burdened annual salary for an end user is $87,750. The hourly rate is $42.

Risks. Risks that could impact the realization of this benefit include.

- The percentage of security incidents that impact end users
- The amount of downtime experienced due to investigations.
- The average fully burdened salaries of end users.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $493,400.

Reduced End-User Downtime

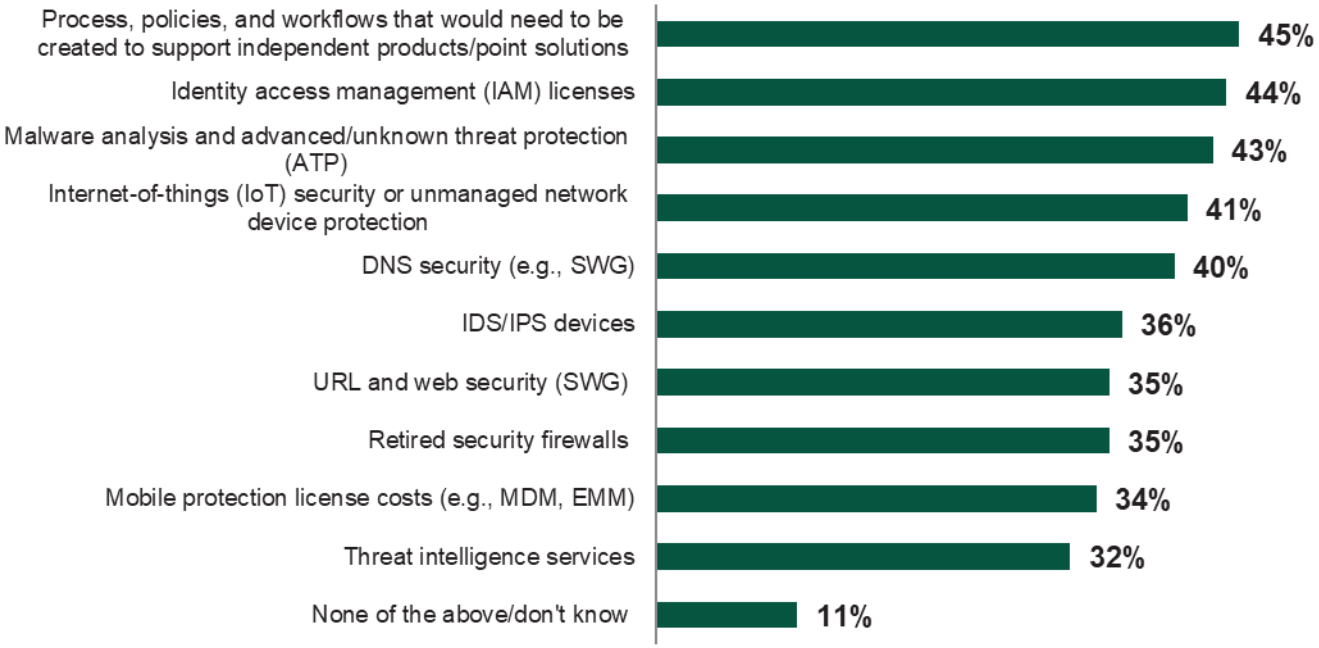
Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of users	Composite	7,500	7,500	7,500
D2	Percent of users affected by downtime in prior state	Interviews	18%	18%	18%
D3	Reduction in downtime with VM-Series firewalls	Interviews	67%	67%	67%
D4	Users avoiding downtime with VM-Series firewalls	D1*D2*D3	904.5	904.5	904.5
D5	Average time of downtime in prior state (hours)	Composite	4.5	4.5	4.5
D6	End-user time saved from avoided events	D4*D5	4,070	4,070	4,070
D7	End users still experiencing downtime events with VM-Series firewalls	(D1*D2)-D6	445.5	445.5	445.5
D8	Reduction in downtime length with VM-Series firewalls	Interviews	45%	45%	45%
D9	Average downtime avoided per affected user with VM-Series firewalls (hours)	D5*D8	2.0	2.0	2.0
D10	End-user time saved for existing events	D7*D9	902.1	902.1	902.1
D11	Average hourly salary of business user (rounded)	Assumption	$42	$42	$42
Dt	Reduced end-user downtime	(D6+D10)*D11	$208,840	$208,840	$208,840
	Risk adjustment	↓5%			
Dtr	Reduced end-user downtime (risk-adjusted)		$198,398	$198,398	$198,398
	Three-year total: $595,195			**Three-year present value: $493,387**	

SECURITY INFRASTRUCTURE COST REDUCTION AND AVOIDANCE

Evidence and data. VM-Series firewalls can be paired with Palo Alto Networks CDSS to deliver additional threat protection to organizations. By leveraging these solutions, the interviewees' organizations were able to eliminate spend on existing point solutions within their security stacks.

- Organizations took advantage of deploying Palo Alto Networks Threat Prevention, DNS Security, GlobalProtect, WildFire, and URL Filtering with their VM-Series firewalls. A senior security engineer at a business services firm said, "Basically, [we decided] to switch from the legacy infrastructure to a next-gen firewall in the first place so that we could integrate a lot of these solutions and manage them through a single platform."
- Organizations recognized additional benefits due to the scalability of VM-Series firewalls. They were able to quickly deploy new firewalls as needed instead of provisioning appliances in advance, which often leads to unnecessary spend. A CISO at a medical devices firm stated: "You have an ability to really start small, and if you have the need, you can go up. Or I can also kind of just blow it away if I no longer need it. If I have an internal on-prem system, I always have to buy hardware, I always have to kind of have the right capacity available, and so on. That's not really a headache here. I can turn it on and, if I need to [turn it off] in four months, I can and it's gone."

Figure 11. "You noted reduced costs from software licenses, hardware, and/or maintenance and support management due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Which of the following has your organization realized costs savings compared to your previous environment?"



Base: 103 cloud security decision-makers
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

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

- The composite takes full advantage of Palo Alto Networks' CDSS product suite.
- In its legacy state, the organization overprovisioned firewall resources by 25% (which the recently announced flexible consumption model may address).

Risks. Risks that could impact the realization of this benefit include:

- The prior state of security solutions and the ability to discontinue contracts.
- Current security needs and usage of Palo Alto Networks CDSS products.
- Typical growth and overprovisioning practices.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $573,800.

Security Infrastructure Cost Reduction And Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Cost of threat intelligence services	Survey results	$71,037	$71,037	$71,037
E2	Cost of retired security firewalls	Survey results	$63,665	$63,665	$63,665
E3	Cost of IDS/IPS devices	Survey results	$55,590	$55,590	$55,590
E4	Cost of DNS security (e.g., secure web gateway)	Survey results	$21,704	$21,704	$21,704
E5	Cost of malware analysis and advanced/unknown threat protection (e.g., advanced threat protection)	Survey results	$18,390	$18,390	$18,390
E6	Cost of IoT security or unmanaged network device protection	Survey results	$12,389	$12,389	$12,389
E7	Avoided overprovisioning of physical firewalls	A1*25%*1000	$25,000	$6,250	$7,813
Et	Security infrastructure cost reduction and avoidance	E1+E2+E3+E4+E5+E6+E7	$267,774	$249,024	$250,586
	Risk adjustment	↓10%			
Etr	Security infrastructure cost reduction and avoidance (risk-adjusted)		$240,996	$224,121	$225,527
	Three-year total: $690,645		**Three-year present value: $573,754**		

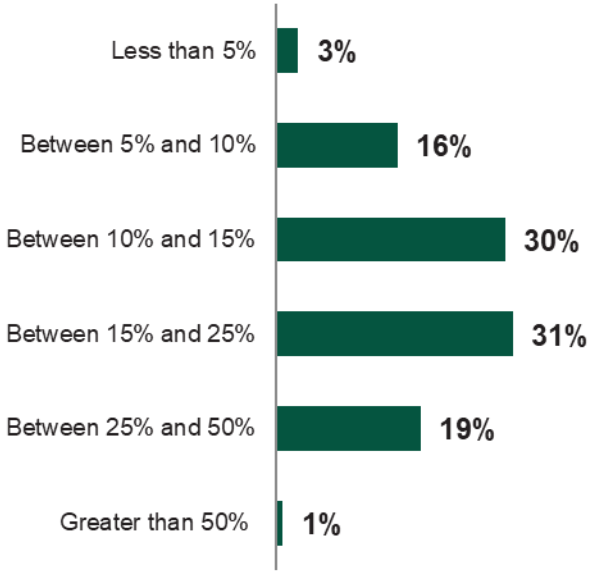
DATA BREACH RISK REDUCTION

Evidence and data. Interviewees said their organizations were able to improve their overall security postures, reduce attack surfaces, and move to Zero Trust models for network security**.** With a centralized and unified solution, the organizations could implement the Zero Trust model that Palo Alto Networks technology supports.

"We did an evaluation of the native [CSP] firewall and saw that they didn't do the deep packet inspection. There was no threat protection that we could tie to it. The logs were not as convenient. We didn't have a central source of management like we do with Panorama. So, it was kind of just those sorts of things that added more security, more visibility for us to be able to do our jobs more efficiently." *Information security engineer, business services*

- Interviewees from organizations that previously relied on point solutions said the solutions did not necessarily complement or communicate with each another. Having multiple firewalls and advanced network security solutions also led to inconsistent policies and gaps in coverage, especially between on-premises and cloud.
- By using VM-Series firewalls, the interviewees' organizations gained unified solutions they could manage from central locations, and this allowed security teams to easily identify and close any gaps. The fidelity of the information being shared between the security systems is key in effective automated prevention of breaches. Palo Alto Networks CDSS further enhanced network security by providing 24/7 coverage and support, including automated updates to all NGFWs to protect against the latest threats.
- The global head of IT engineering in the beverage industry said: "We do yearly internal audits, and the number of findings around the networking and the firewall-specific space has declined by 40% from where we were year-over-year because of some of the governance and policies that are in place and how the rules are being created. We can easily find and fix stale policies based on IP addresses or those that were not written based on applications."

Figure 12. "You noted faster mean-time-to-know on security incidents due to Palo Alto Networks VM-Series virtual firewalls (including use with any security service). Can you estimate the percentage improvement compared to your previous environment?"



Base: 70 cloud security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, June 2021

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

- According to Forrester data, the composite organization would experience an average of 3.2 breaches per year if it relied on point solutions.[2]
- The cost of a breach is $53 per employee, not counting the loss of worker productivity. The costs include the following:
    - Fines to regulatory bodies
    - Customer reimbursement/lawsuits
    - Incident response and remediation
    - Lost revenue
    - Repairing brand equity
    - Cost of customer reacquisition
- With VM-Series firewalls, the organization reduces the likelihood of a data breach by up to 20% after three years.
- Each breach impacts 18% of all employees and leads to an average of 3.6 hours lost per employee per breach. This is an addition to the individual costs highlighted above.

Risks. Risks that could impact the realization of this benefit include:

- The impact that VM-Series firewalls have on the organization's overall security posture compared to its previous solution.
- The percentage of employees impacted by a breach and the associated duration of downtime.
- The average salaries of business users.

Results. To account for these risks, Forrester adjusted this benefit downward by 30%, yielding a three-year, risk-adjusted total PV of $383,700.

Data Breach Risk Reduction					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
F1	Average number of data breaches	Forrester research	3.2	3.2	3.2
F2	Average potential cost of a data-breach exclusive of internal user downtime	Forrester research	$265,000	$265,000	$265,000
F3	Reduced likelihood of a breach	Composite	10%	15%	20%
F4	**Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs**	**F1*F2*F3**	**$84,800**	**$127,200**	**$169,600**
F5	Number of internal employees	Composite	7,500	7,500	7,500
F6	Average hourly salary of business user	D8	$42	$42	$42
F7	Diminished/eliminated internal user productivity time per breach (hours)	Forrester research	3.6	3.6	3.6
F8	Average percent of employees affected per breach	Composite	18%	18%	18%
F9	**Cost of reduced internal productivity**	**F1*F3*F5*F6*F7*F8**	**$65,318**	**$97,978**	**$130,637**
Ft	Data breach risk reduction	F4+F9	$150,118	$225,178	$300,237
	Risk adjustment	↓30%			
Ftr	Data breach risk reduction (risk-adjusted)		$105,083	$157,624	$210,166
	Three-year total: $472,873		**Three-year present value: $383,699**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Being able to use existing skills to avoid training and recruitment.** Most of the interviewees' organizations had readily available internal resources to deploy VM-Series firewalls. However, interviewees from those that did not said it was relatively easy to externally attain the necessary skills due to the prevalence of Palo Alto Networks use. The CISO at a medical devices firm said, "Palo Alto [Networks products] are widely used enough to easily get the [necessary] skill sets and people who are already trained."
- **Increasing scalability and flexibility.** Interviewees said VM-Series firewalls could be quickly deployed or removed as needed because of their virtual form factor. This capability ensured that the organizations could quickly adapt to changing needs while controlling costs. The CISO in the medical devices industry stated: "Last year, with our response to the COVID-19 pandemic, we had a 20-times ramp-up that we needed to go through in terms of output. And this required further scaling up systems that weren't necessarily scalable. We couldn't have done that as fast with hardware."

- **Improving competitiveness.** Some interviewees said their organization leveraged their use of Palo Alto Networks products as a competitive advantage when providing technology services. A senior expert in networking in the IT services industry said: "I think [my organization] used this to attract our customers to not only look at the public cloud, but also to look at private clouds. If there are some other regulations like GDPR [the General Data Protection Regulation] or something, then we could offer [the customer] a secure solution in the private cloud. So, I think it could benefit us."
- **Exploring new use cases and reducing costs and new threat vectors.** Some of the organizations used VM-Series firewalls to secure assets at the very edge of their networks, like at retail kiosks. The global head of IT engineering for a beverage firm said: "We were running [our in-store kiosks] on a private 5G network, and [employees] used to have 5G cards. But once [the program] was growing, we said, 'Okay, we need a different way of doing that.' People were stealing those 5G cards. So, we partnered with Palo Alto Networks, and it was able to write a special package for us that would allow those machines to communicate with our VM-Series firewalls or VPN. Now, we could put those machines in the customer environment, or we don't have to go and buy cards from 5G network companies. That was with the partnership with Palo Alto Networks. It wrote a special endpoint client for us that those machines can use, which gave us drastic savings in cost around that area."
- **Ensuring that security is not a barrier to digital transformation efforts.** Security teams have a mandate to ensure that operations are as secure as possible, but they don't want to hinder digital transformation efforts. With VM-Series firewalls, teams could quickly deploy firewalls and attain the required level of security posture so their organizations could recognize the benefits of public and hybrid cloud migrations.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Palo Alto Networks VM-Series firewalls and later realize additional uses and business opportunities.

Palo Alto Networks recently adopted a flexible consumption model in lieu of the traditional industry-standard of perpetual licensing and enterprise license agreement (ELA) models that interviewees said their organizations were previously on. With a flexible consumption model, organizations pay only for the firewalls and security services they need at any given time, which allows them to scale up and down as usage requires. This additional flexibility enabled the interviewees' organizations to recognize extra savings in firewall costs.

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 licensing	$0	$321,300	$401,625	$502,031	$1,224,956	$1,001,196
Htr	Internal deployment effort	$3,407	$0	$852	$1,065	$5,324	$4,911
Itr	Ongoing management	$0	$177,188	$177,188	$177,188	$531,563	$440,639
Jtr	White-box appliances	$105,000	$0	$26,250	$32,813	$164,063	$151,347
	Total costs (risk-adjusted)	$108,407	$498,488	$605,914	$713,096	$1,925,905	$1,598,093

FIREWALL LICENSING

Evidence and data. Interviewees said Palo Alto Networks offers competitive pricing with various VM-Series firewall sizes and subscription levels to meet customer needs.

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

- The composite organization deploys 100 VM-Series firewalls in Year 1, and the deployment and subscription base grows by 25% annually.
- To model this cost for the composite organization, Forrester used the ELA models that the interviewees' organizations were on prior to using VM-Series firewalls, but Palo Alto Networks has moved to a consumption-based pricing model.

Risks. Risks that could impact these costs include:

- The size of the firewall deployment.
- The number of cloud-delivered security services and level of support needed.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1 million.

Firewall Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Cost per license per VM-series firewall	Interviews		$3,060	$3,060	$3,060
G2	Total number of VM-Series deployed	Composite		100	125	156
Gt	Firewall licensing	F1*F2		$306,000	$382,500	$478,125
	Risk adjustment	↑5%				
Gtr	Firewall licensing (risk-adjusted)		$0	$321,300	$401,625	$502,031
	Three-year total: $1,224,956		**Three-year present value: $1,001,196**			

INTERNAL DEPLOYMENT EFFORT

Evidence and data. Interviewees said that while there was some time and effort involved with deploying Palo Alto Network products, their organizations' deployments ran smoothly and they did not experience any significant delays or roadblocks due to Palo Alto Network's consistent technology and the ability to automatically update policies across the network.

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

- The organization is an existing Palo Alto Networks user.
- Deployment costs do not factor into the time required for implementation of ancillary products (e.g., Palo Alto Networks SD-WAN, Prisma Cloud, Panorama, etc.).
- New VM-Series firewalls take 30 minutes to deploy.
- The average fully loaded annual salary for a network operations employee is $135,000.

Risks. Risks that could impact these costs include:

- The organization's existing usage and familiarity with Palo Alto Networks products.
- Average salaries of deployment team members.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $4,900.

Internal Deployment Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Time to deploy (hours) (rounded)	A1*0.5	50		13	16
H2	Average hourly salary of deployment team member	Assumption	$65		$65	$65
Ht	Cost of internal deployment effort	H1*H2	$3,245	$0	$811	$1,014
	Risk adjustment	↑5%				
Htr	Internal deployment effort (risk-adjusted)		$3,407	$0	$852	$1,065
	Three-year total: $5,324			**Three-year present value: $4,911**		

ONGOING MANAGEMENT

Evidence and data. Interviewees noted that VM-Series firewalls requires significantly less ongoing management than legacy solutions. While their organizations automated or consolidated many previously manual tasks, they did require a small amount of effort from internal teams for managing firewalls and policies, troubleshooting, making updates, and performing other administrative tasks.

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

- The composite organization has 10 FTEs involved in the ongoing management of its VM-Series deployment.
- Internal resources dedicate 15% of their time solely on firewall management.
- The average annual salary of involved FTEs is $112,500.

Risks. Risks that could impact this cost include:

- The size and scope of the deployment.
- The organization's internal skill sets and ability to automate tasks.
- Average annual salaries.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $440,600.

Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
I1	FTEs involved in ongoing management	Composite		10	10	10
I2	Percent of time spent on firewall management	Interviews		15%	15%	15%
I3	Average annual compensation rate of FTEs	Assumption		$112,500	$112,500	$112,500
It	Cost of ongoing management	I1*I2*I3		$168,750	$168,750	$168,750
	Risk adjustment	↑5%				
Itr	Ongoing management (risk-adjusted)		$0	$177,188	$177,188	$177,188
	Three-year total: $531,563		**Three-year present value: $440,639**			

WHITE-BOX APPLIANCES

Evidence and data. Many of the interviewees' organizations that operated multiple data centers or branch locations chose to deploy their firewalls on cost-effective commodity hardware. Interviewees from organizations that chose this route said installation was easy and that branch employees with no IT experience could install the hardware.

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

- The composite organization deploys its VM-Series firewalls using new white-box appliances.
- As the deployment grows by 25% annually, the organization purchases new appliances.
- The average cost of commodity hardware required to deploy a VM-Series firewall is $1,000.

Risks. Risks that could impact these costs include:

- The size of the deployment.
- The prices of commodity hardware.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $151,300.

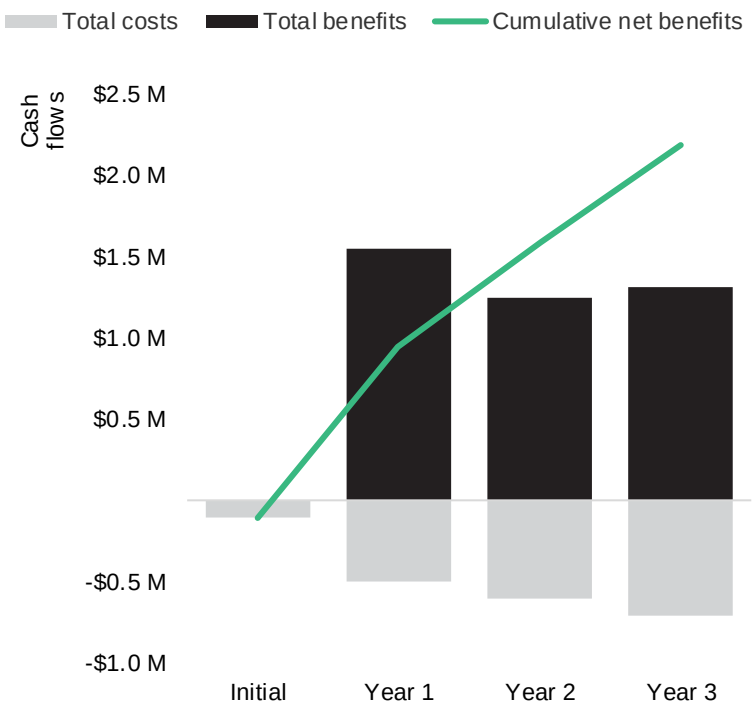
White-Box Appliances

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
J1	White-box appliances	Composite	100	0	25	31
J2	Price per appliance	Interviews	$1,000	$1,000	$1,000	$1,000
Jt	Cost of white-box appliances	J1*J2	$100,000	$0	$25,000	$31,250
	Risk adjustment	↑5%				
Jtr	White-box appliances (risk-adjusted)		$105,000	$0	$26,250	$32,813
	Three-year total: $164,063			**Three-year present value: $151,347**		

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	($108,407)	($498,488)	($605,914)	($713,096)	($1,925,905)	($1,598,093)
Total benefits	$0	$1,554,294	$1,251,188	$1,306,291	$4,111,774	$3,428,472
Net benefits	($108,407)	$1,055,807	$645,273	$593,195	$2,185,868	$1,830,379
ROI						115%
Payback period (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

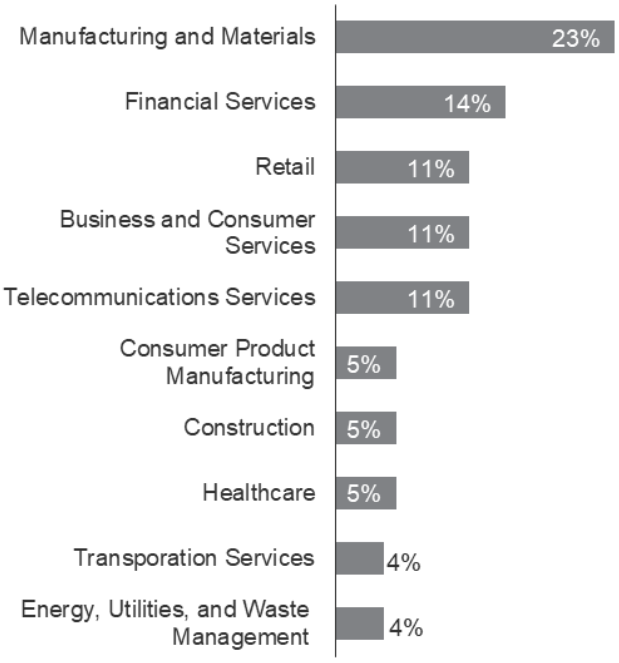
The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

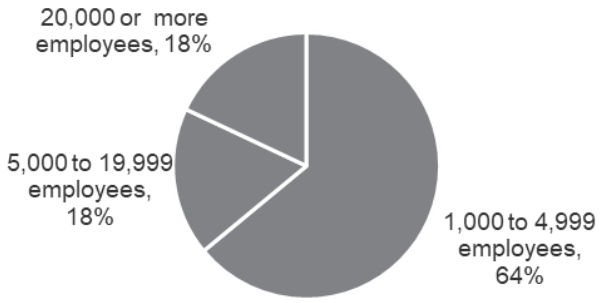
The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Survey Demographics

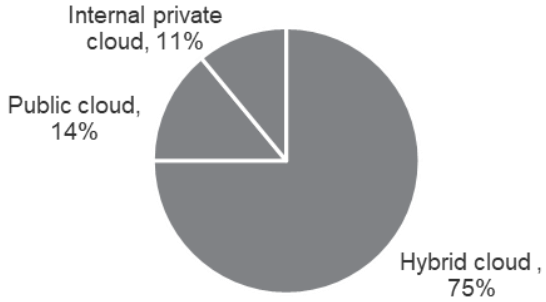
"Which of the following best describes the industry to which your company belongs?"



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



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



"In which country are you located?"

53%	United States
19%	Germany
17%	United Kingdom
6%	France
5%	Australia

Base: 132 cloud security decision makers (percentages may not add to 100% due to rounding)
Source: "PAN Virtual Firewalls TEI," a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, October 2021

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, Q4 2020."


FORRESTER®