A Forrester Total Economic Impact™ Study Commissioned By Palo Alto Networks
March 2018

The Total Economic Impact™ Of Palo Alto Networks

Cost Savings And Business Benefits Enabled With Palo Alto Networks' Security Platform

FORRESTER®

Table Of Contents

Executive Summary **1**

Key Findings 1

TEI Framework And Methodology 4

The Palo Alto Networks Customer Journey **5**

Interviewed Organizations 5

Key Challenges 5

Key Results 6

Composite Organization 7

Financial Analysis **8**

Benefit 1: Security Management Savings From An Integrated Platform 8

Benefit 2: End User Productivity Recovery 9

Benefit 3: IT Help Desk Utilization Avoidance 10

Benefit 4: Alternative Capability Purchase Avoidance 11

Flexibility 12

Cost 1: Hardware And Related Support Costs 13

Cost 2: Software And Subscription Services 14

Financial Summary **15**

Palo Alto Networks: Overview **16**

Appendix A: Total Economic Impact **17**

Project Director:
Henry Huang

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

ROI
65%

Benefits PV
$9.9 million

NPV
$3.9 million

Payback
17 months

Executive Summary

Palo Alto Networks provides an enterprise security platform that help its customers protect and defend their data assets with highly effective tools at the network, data center, and endpoint levels. Palo Alto Networks commissioned Forrester Consulting to conduct this Total Economic Impact™ (TEI) study to examine the potential return on investment (ROI) enterprises may realize by deploying a spectrum of Palo Alto Networks products. This case study offers readers with a framework to evaluate the potential financial impact of the offering on their organizations.

To better understand the benefits, costs, and risks associated with the Palo Alto Networks investment, Forrester interviewed three customers with years of experience using the platform. These customers have implemented multiple products from the Palo Alto Networks portfolio. Forrester found that the offering delivers significant benefits in overall cyberdefense efficacy as well as security operations efficiency. While each product is effective as an individual, the integration between these security technologies truly drives success. Further, the visibility, flexibility, and automation created help organizations scale defenses using technology rather than a limited pool of available security professionals.

Prior to implementing Palo Alto Networks, the customers used a variety of disparate security products as independent cybersecurity defense measures, including those that protected network perimeters, endpoints, and internal private clouds. The combination of tools made for individually capable pieces, but was devoid of integration with other tools — ultimately requiring greater manual labor input from security operations. This lack of integration led to poor visibility across the enterprises on security posture and hampered the ability of security operators (SecOps) to keep the networks safe. Measurement on these devices and tools was difficult, and actionable insights were difficult to derive, leading to protracted periods for triage and analysis.

The salient point that interviewees conveyed was that undermanned security operations needed to pour through a deluge of unconnected data from different sources. This led to less than adequate reactionary actions. As cybersecurity incidents rose, these organizations asked themselves how they would scale their resources to be able to meet the increasing attack vectors and incidents that rose year over year. As it turns out, Palo Alto Networks was the answer.

Key Findings

Quantitative benefits. The following risk-adjusted quantified benefits are representative of those experienced by the companies interviewed:

FORRESTER®

Alternative capability purchase avoidance:
$3,480,956

Security management efficiency savings:
$4,754,618

IT help desk usage reduction:
$362,487

Palo Alto Networks three-year costs:
$6,000,352

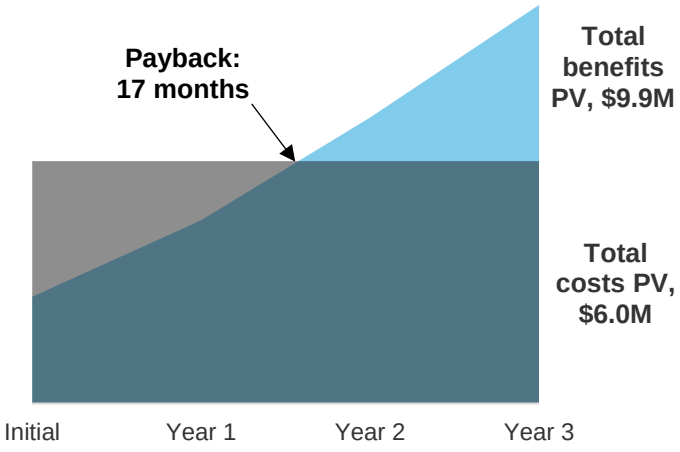
- **The integration of the Palo Alto Networks security products centralized security information and created meaningful visibility for SecOps.** Monitoring and analysis of security incidents became an easier exercise for SecOps that expedited the analysis and triage stages of security response. These resources were now able to perform deeper analysis and build advanced security policies and processes. Improved threat visibility, automated handling of incidents, and traceability reduced the time necessary to perform triage and analysis on cybersecurity threats by up to 1.25 hours per incident in the first year, growing to 1.52 hours per incident in the third year of operations. Total SecOps efficiencies realized amounted to $4,754,618 PV over three years.
- **Quicker triage and improved security workflows led to an improvement in end user uptime as the time to contain incidents was reduced.** By effectively improving the time to contain security incidents, end users realized a recovery in productivity that would have otherwise been lost to extenuated containment processes. Coupled with the avoidance of deep remediation or reimaging on a percentage of incidents, end users saw an improvement of $1,285,202 PV over three years.
- **IT help desk utilization was reduced.** Traps, WildFire, and AutoFocus quickly identified threats across the enterprise and deflected a number of help desk tickets and endpoint restoration. Three-year PV gains were $362,487.
- **To achieve similar levels of performance as the Palo Alto Networks, without the deep integration, would require a similar investment amount with disparate vendors.** Palo Alto Networks' next-generation firewalls (NGFWs), in conjunction with a broad set of cloud-based security services, work together, requiring a smaller overall stack of security tools with the added benefit of cost avoidance in the form of $3,480,956, present-value-adjusted.

Costs. The interviewed organizations experienced the following risk-adjusted costs:

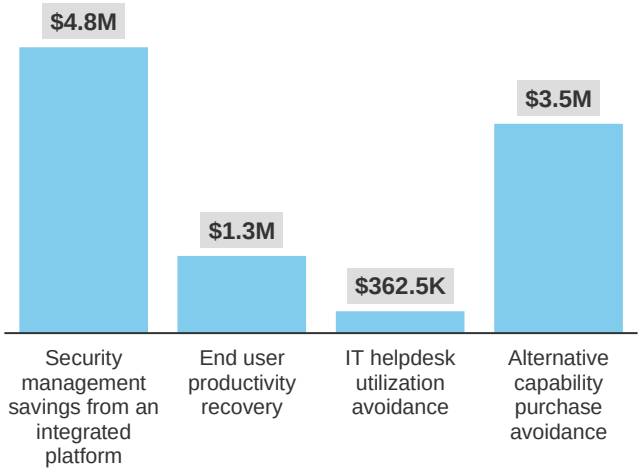
- **Palo Alto Networks hardware costs.** Costs in this category were capital purchases comprised largely of NGFWs and management consoles. Support licenses were purchased with a three-year agreement and were incurred in the initial purchase period. The purchased hardware pieces were sufficient to cover two large data centers handling enough throughput to drive large enterprises of more than 18,000 business users. The overall cost across three years was $2,787,152.
- **Software and subscriptions are also an integral part of the Palo Alto Networks overall platform.** Organizations used three-year prepaid licenses for subscriptions such as WildFire, URL Filtering, and Threat Prevention, which work in conjunction to prevent, protect, and contain threats. With Traps and AutoFocus, Palo Alto Networks also covered endpoints — minimizing malicious attack vectors. In all, three-year PV costs of the platform amounted to $3,213,200.

Forrester's interviews with three existing enterprise-level customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced benefits of $9.9 million over three years versus costs of $6.0 million, adding up to a net present value (NPV) of $3,882,912 and an ROI of 65%.

Financial Summary



Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Palo Alto Networks security appliances and tools as a comprehensive security offering.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the Palo Alto Networks platform can have on an organization:

The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

DUE DILIGENCE
Interviewed Palo Alto Networks stakeholders and Forrester analysts to gather data relative to the platform.

CUSTOMER INTERVIEWS
Interviewed three organizations using Palo Alto Networks products to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

CASE STUDY
Employed four fundamental elements of TEI in modeling Palo Alto Networks' impact: benefits, costs, flexibility, and risks. Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

FORRESTER®

The Palo Alto Networks Customer Journey

BEFORE AND AFTER THE PALO ALTO NETWORKS INVESTMENT

Interviewed Organizations

For this study, Forrester conducted multiple interviews with three Palo Alto Networks customers. Interviewed customers include the following:

INDUSTRY	HEADQUARTER	INTERVIEWEE	ENTERPRISE FOOTPRINT
Natural resources and energy	North America	Former CISO	Global with over 100,000 FTEs and 20 security operations FTEs
Healthcare	North America	Operations and infrastructure manager	Multiple sites with 1,400 FTEs and four security operations FTEs
Healthcare	North America	Security engineer lead	Multiple sites with over 300,000 FTEs and 1,300 security operations FTEs

Key Challenges

The organizations interviewed had all been long-time users of Palo Alto Networks. The conversations with these organizations revealed a few common issues prior to transitioning to Palo Alto Networks.

The first issue was significant performance degradation arising from the filtering bandwidth of network traffic to stay secure. Specifically, enabling intrusion prevention on the existing security platform reduced network throughput by a factor of half, with additional features like URL filtering further reducing performance by similar percentage levels. To produce acceptable levels of protection without performance degradation, these organizations required more hardware and software tools to simply establish a bare minimum level of security protection.

Beyond the performance degradation, these organizations employed disparate security products in their times prior to Palo Alto Networks. The aggregate of the legacy products created an enormous amount of security-related data that was difficult to disseminate and in turn to use for creating actionable insights. In a world where everyone was inundated with data, these organizations needed a platform that could communicate on the security level and bring to light the pieces that were pertinent in resolving security incidents.

One interviewee explained: “Our SecOps were running all over the place, glossing through miles of logs and wading through command line interfaces to find the root cause of issues. Now with Palo Alto Networks, everything is here in one spot — there is no need to grab things from the left and right.”

Their challenges boiled down to finding an offering that:

> “Our previous implementation just wasn’t fitting our needs, no matter how much we invested in it. There was no application layer firewall capability, and IPS/IDS were separate units all together. None of these pieces talked to one another.”
>
> *Manager of operations, healthcare provider*

- **Offered ample prevention of cybersecurity incidents by having the fastest and most advanced measures to detect intrusions.** Relying on traditional firewall rules and simple signature-based attacks was insufficient — interviewed organizations wanted to go deeper (at the layer 7 level) and understand the attack vectors so that they could produce policies to prevent situations from arising in the future. Just as high on the list of wants was the incorporation of an endpoint detection and response (EDR) platform into the security stack that protected against zero-day threats and automated with the rest of the security platform to limit east-west proliferation.
- **Supported business needs by keeping their data safe and the organization out of the news.** To protect the data, organizations needed a dependable platform that would leverage all data and highlight the important facts so that SecOps could identify issues and address them before them before they spread.
- **Leveraged integrated information flow from one end to the other within the security stack.** The organizations often found intrusions, but, due to the lack of integration between security tools, the malicious activity had transgressed further into the enterprise networks before SecOps could properly identify the issue.
- **Reduced the security stack, while growing and adding to security capabilities.** Gigabytes of logs did nothing for security professionals if they could not find the root cause of issues and stem it before proliferation.
- **Achieved better compliance by providing contextually relevant data when needed.** Without a centralized reporting function, organizations struggled when it came time to prove compliance. The need was there, but how would the documentation proving compliance be compiled efficiently?

"It's not really a matter of not enough data for our security managers, but really a matter of too much data that didn't correlate. Palo Alto Networks is a part of our incident response process — in gathering all the telemetry and pointing our managers to where they really needed to look."

Security engineer lead, healthcare organization

Key Results

The interviews revealed that key results from the Palo Alto Networks investment include:

- **Cost savings.** There are significant savings in a consolidated enterprise-class security platform when compared with legacy security hardware and platforms. While some competing platforms have recently begun offering layer 7-capable NGFWs, none of these platforms communicated with the rest of the security stack — making for laborious effort for SecOps to truly rein in the cause of attacks. Using tools such as AutoFocus and Panorama, SecOps reduced the time spent to triage and analyze incidents, making for an overall gain with the Palo Alto Networks platform. To further make the case, the organizations had been able to eliminate or avoid purchase of added capabilities to come near what Palo Alto Networks provides.

"The Palo Alto Networks platform has brought everything into one place for all our security needs. Because of what it can do and how it's helped our team, we can sleep better."

Manager of operations, healthcare provider

- **Labor savings.** IT help desk labor needs reduced with Traps when used in conjunction with WildFire, since the products could immediately stop malicious attacks. The composite organization was able to reduce its spending in IT help desk personnel and, instead, reallocate IT personnel to other value-add tasks. With nearly 16,500 help desk requests in the first year of implementation, the composite organization described below was able to reduce nearly 20% of these incidents — many of which would have resulted in analysis and remediation work.
- **Increased productivity.** The Palo Alto Networks Security Operating Platform is a business-enabling tool. The composite organization described Palo Alto Networks as an important component of end user enablement. With a lower amount of help desk tickets and self-resolved tickets from the Palo Alto Networks integrated platform, end users were able reap higher uptimes with their workstations, directly feeding into increased productivity.

"Our biggest gain wasn't in the next-generation firewalls; I mean, they're great, but where we really found value was in the automation in the single platform that Palo Alto Networks provides."

Former CISO, natural resources and energy company

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization is representative of the three companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization that Forrester synthesized from the customer interviews has the following characteristics:

Description of composite. This composite organization is a growing, technology-driven organization that previously operated with multivendor traditional stateful firewall appliances, intrusion prevention system (IPS), web security appliances, and a mixture of endpoint software with policy controls to achieve desired levels of protection and content filtering. As a large multinational enterprise, all aspects of cybersecurity are important, but the organization had been particularly interested in better intruder detection/prevention and reducing data breaches and account takeovers arising from malicious malware.

Deployment characteristics. To address the growing and constantly evolving security demands, the organization conducted an extensive request for proposals (RFP) and business case analysis, evaluating multiple vendors. The organization decided on Palo Alto Networks and procured the following hardware and software/subscriptions to replace its entire existing network security infrastructure over the course of three months, with redundant units for high availability:

- M-100 Panoramas for management.
- PA-5000 series firewalls for dual data centers and remote locations.
- VM-500 virtualized firewalls.
- Traps advanced endpoint protection.
- Subscriptions: WildFire, Threat Prevention, URL Filtering, and AutoFocus.

Key assumptions

-Multinational footprint
-18,000 office FTEs
-40 security analysts
-Two data centers
-350 cybersecurity related incidents weekly

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

REF.	BENEFIT	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Security management savings from an integrated platform	$0	$1,501,500	$1,906,278	$2,414,676	$5,822,454	$4,754,618
Btr	End user productivity recovery	$0	$450,450	$518,028	$595,728	$1,564,206	$1,285,202
Ctr	IT help desk utilization avoidance	$0	$127,050	$146,108	$168,022	$441,179	$362,487
Dtr	Alternative capability purchase avoidance	$2,642,733	$0	$518,918	$544,865	$3,706,516	$3,480,956
	Total benefits (risk-adjusted)	**$2,642,733**	**$2,079,000**	**$3,089,358**	**$3,723,266**	**$11,534,358**	**$9,883,263**

Benefit 1: Security Management Savings From An Integrated Platform

A key benefit from the Palo Alto Networks implementation was a greatly reduced amount of time to triage and analyze security events. With security events coming in as a constant barrage at the composite organization, the SecOps team was continuously digging in logs to find the truth behind these events. This triage and analysis process took the greatest time, primarily due to the need to determine relevant data. Palo Alto Networks systems (Panorama device and AutoFocus) reduced this via delivery of linked and contextually relevant data.

AutoFocus especially was able to help SecOps personnel dig through large data sets, bringing to the surface important data that helped SecOps and incident responders identify threats. In all, Forrester anticipates that the triage and analysis process was reduced by 1.25 hours per incident in the first year between the various SecOps professionals investigating the incident. With further efficiency and policy formation, the estimated savings from the existing state reached 1.52 hours by the third year.

Organizations that use virtualization to some degree often overlook east-west traffic in the security segment. One interviewee stated, “The virtual firewalls that we leverage from Palo Alto Networks has diminished the chances of malicious activity moving internally within our networks, and this has created a better and more secure environment overall.” While this benefit has not been quantified, SecOps should see an overall decrease to incidents as well as triage and analysis times.

The three-year PV benefit to SecOps efficiency equates to a value of $4,754,618.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of nearly $9.9 million.

Through automation and greater insight delivery, security incidents require 1.25 to 1.52 fewer hours of analyst involvement to resolve.

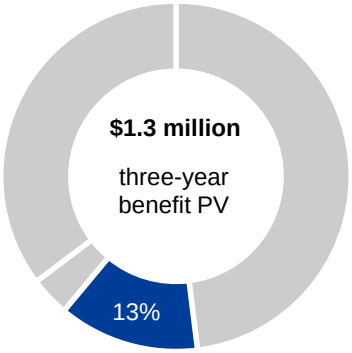
Security Management Savings From An Integrated Platform: Calculation Table					
REF.	**METRIC**	**`**	**YEAR 1**	**YEAR 2**	**YEAR 3**
A1	Cybersecurity incidents annually, endpoint and perimeter	350 incidents weekly in Year 1, growing at 15% yearly	18,200	20,930	24,070
A2	Triage and incident analysis effort reduced with automation, in hours per security incident	Assumption of multiple analysts allocated per incident	1.25	1.38	1.52
A3	Hours saved annually by security analysts with Palo Alto Networks automation	A1*A2	22,750	28,883	36,586
A4	Cybersecurity analyst hourly compensation, fully burdened	$110,000*1.2x benefits multiplier/2,000 hours	$66	$66	$66
At	Security management savings from an integrated platform	A3*A4	$1,501,500	$1,906,278	$2,414,676
	Risk adjustment	0%			
Atr	**Security management savings from an integrated platform (risk-adjusted)**		**$1,501,500**	**$1,906,278**	**$2,414,676**

Benefit 2: End User Productivity Recovery

While the delivery of a secure network environment was pivotal to all of the interviewed organizations, business end user productivity was equally as important to those interviewed. The composite organization benefited greatly from security incidents that were either deflected due to the Palo Alto Networks platform or mitigated before causing extensive damage to workstations. Due to the speed of threat neutralization on endpoints, end users were able to save on average half an hour per incident on their endpoint.

More serious exploits that had previously passed through but were now neutralized with Palo Alto Networks averted deeper level remediation or complete reflashes of the system — equal to 1.5 hour on these types of incidents. Ultimately, these users are saving over 10,000 hours per year because of the efficiency of the Palo Alto Networks platform.

Using a figure of $42/hour (or $70,000 annually plus benefits) for a fully burdened average business user, the total time saved by this group amounts to roughly half a million dollars annually. The three-year value of end user productivity reclaimed is $1,285,202 PV.



End user productivity recovery: **13%** of total benefits

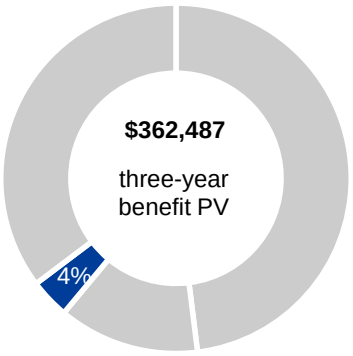
FORRESTER®

End User Productivity Recovery: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
B1	Annual endpoint incidents requiring IT help desk remediation due to malicious activity		16,500	18,975	21,821
B2	End user uptime improvement from automation and quicker containment process, in hours per incident		0.5	0.5	0.5
B3	Hours saved annually by end users	B1*B2	8,250	9,488	10,911
B4	End user hourly compensation, fully burdened	$70,000*1.2x benefits multiplier/ 2,000 hours	$42	$42	$42
B5	Reimage/full scale remediation situations avoided, measured in hours	B1*10% of incidents*1.5 hours per incident	2,475	2,846	3,273
Bt	End user productivity recovery	B3*B4+B4*B5	$450,450	$518,028	$595,728
	Risk adjustment	0%			
Btr	**End user productivity recovery (risk-adjusted)**		**$450,450**	**$518,028**	**$595,728**

Benefit 3: IT Help Desk Utilization Avoidance

IT help desk tickets were often the first line of support for end users at interviewed organizations. With WildFire and Traps, these organizations were able to demarcate issues that could easily be resolved or nullify the incidents altogether with a higher success rate than previous antivirus (AV) platforms. As these cases were deflected, the IT help desk spent less time to identify and remediate these situations, allowing for more complex incidents to be passed through to the SecOps team. At 10 minutes for identification and 45 minutes of remediation per help desk request, multiplied by the 20% reduction in such incidents made possible by Palo Alto Networks, the savings amounted to roughly $127,050 in the first year alone. The newly freed time allowed IT help desk personnel to concentrate on other tasks such as user support.

The total value of IT help desk time reclaimed is valued at $362,487 PV over a period of three years.



IT help desk utilization avoidance: 4% of total benefits

FORRESTER®

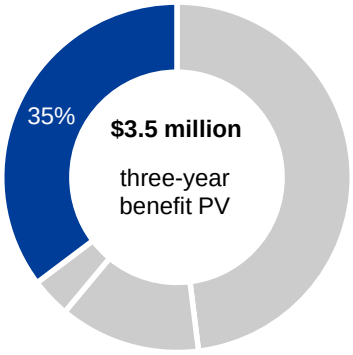
IT Help Desk Utilization Avoidance: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
C1	Annual endpoint incidents requiring IT help desk assistance due to malicious activity		16,500	18,975	21,821
C2	Time required of technician per incident for remediation, in minutes		45	45	45
C3	Time required of technician per incident for preliminary assessment, in minutes		10	10	10
C4	Reduction in malicious endpoint incidents requiring IT help desk		20%	20%	20%
C5	IT help desk hourly compensation, fully burdened	$70,000*1.2X benefits multiplier/ 2,000 hours	$42	$42	$42
Ct	IT help desk utilization avoidance	C1*(C2+C3)/60* C4*C5	$127,050	$146,108	$168,022
	Risk adjustment	0%			
Ctr	**IT help desk utilization avoidance (risk-adjusted)**		**$127,050**	**$146,108**	**$168,022**

Benefit 4: Alternative Capability Purchase Avoidance

The composite organization indicated that a key benefit from the Palo Alto Networks implementation was a reduction in capital and operating expenditure. Prior to deploying the comprehensive Palo Alto Networks platform, the composite organization utilized stateful firewalls implemented with various hardware- and software-based technologies deployed around the firewall to run intrusion detection and web security capabilities. As a result, the composite organization still relied largely on network policies and previous-generation hardware, introducing the potential for significant slowdowns in network bandwidth when software tools were enabled to attain the desired levels of security.

Newer technologies that produced these capabilities with better throughput of these features required multiple subscription licenses from many different vendors that lacked integration. With the lack of integration, several of the organizations spent an incredible amount of time to resolve incidents — pushing the overall operation expense higher, while spending just as much or more on software and subscriptions.

Following the Palo Alto Networks implementation, the composite organization avoided the hardware and software expenses as would be required from other offerings. By procuring one consolidated platform that handled the capabilities of what typically would require four vendors, the composite organization was able to save on long-term support costs that stretched further into the horizon than that of Palo Alto Networks. The avoided cost of procuring an alternate offering is $3,480,956 (PV-adjusted). Readers should also note that Traps and AutoFocus do not incur additional support cost following the initial purchase.



Alternative capability purchase avoidance: **35%** of total benefits

Impact risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

FORRESTER®

Alternative Capability Purchase Avoidance: Calculation Table						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Alternate offering hardware cost		$1,595,250			
D2	Alternate offering subscription/software/ support costs		$549,120		$576,576	$605,405
D3	Endpoint software replacement, three-year term		$792,000			
Dt	Alternative capability purchase avoidance	D1+D2+D3	$2,936,370	$0	$576,576	$605,405
	Risk adjustment	↓10%				
Dtr	**Alternative capability purchase avoidance (risk-adjusted)**		**$2,642,733**	**$0**	**$518,918**	**$544,865**

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Palo Alto Networks and later realize additional uses and business opportunities, including:

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

- **The enablement of application- and user-level blocking.** In organizations that depended on OS-level policies and other legacy modes of regulating network traffic, network administrators found themselves in a constant battle to manage end users who sought to circumvent policies to use unauthorized and questionable applications. According to a separate study conducted by Salary.com in 2014, “69% of all respondents said they waste at least some time at work on a daily basis.” Additional research conducted in a US survey of computer-using workers who used their computers for more than 5 hours per day found that 80% of employees regularly used the network for purposes such as sending personal emails and doing nonproductive web browsing.

  The visibility created by Palo Alto Networks provides an easily definable network usage policy that is aligned with organizational goals. Security professionals are empowered to identify the specific end users who violate the policy and stem the problem directly rather than wait for the nonauthorized usage to proliferate threats within the network.
- **The ability to partition off internal network threats.** Organizations traditionally have maintained hardened perimeter and endpoint controls, but what if the threat starts internally from a home-brought malware or virus exploiting unpatched software? With virtual firewalls controlling east-west traffic, organizations can more easily achieve a zero-trust policy — segmenting and curtailing malicious code even inside the network.

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	Hardware and related support costs	$2,787,152	$0	$0	$0	$2,787,152	$2,787,152
Ftr	Software and subscription services	$3,213,200	$0	$0	$0	$3,213,200	$3,213,200
	Total costs (risk-adjusted)	**$6,000,352**	**$0**	**$0**	**$0**	**$6,000,352**	**$6,000,352**

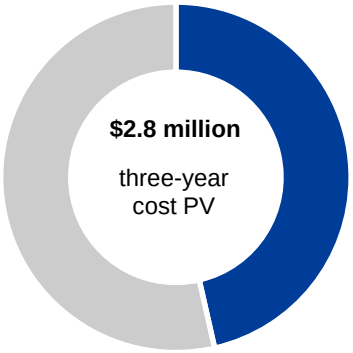
The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $6 million.

Cost 1: Hardware And Related Support Costs

The organization incurred hardware appliance fixed costs during the initial implementation period. As a capital expenditure, this cost encapsulated the cost of various firewalls to support the security needs of the composite organization's architecture. In addition to the NGFWs it deployed, the composite organization required a management console, in the form of a pair of redundant M-100 Panorama devices, to manage and log the distributed network of firewalls and subscription services. This cost analysis also includes virtual firewalls.

Beyond capital expenses, the composite organization incurred premium support fees, which are represented separately in the table below. The support fee included 24x7 support and software firmware upgrades developed by Palo Alto Networks that enhance core functionalities and expand the range of industry-specific features. In the interest of business continuity, the premium support selected by the composite organization includes next-business-day parts shipping and hardware replacement with the option of upgrading to a 4-hour advanced shipment.

On a present value basis, Forrester estimates the composite organization incurred a cost of $2,654,430 for the hardware appliances and related support over three years. Recognizing that various organizations have differing needs — such as high availability (HA), multiple data centers, and bandwidth needs — Forrester has risk-adjusted this cost up by 5% to account for some variability in demands. The total cost following the upward risk adjustment comes to $2,787,152 PV.



Hardware and related support costs: **46%** of total costs

Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

FORRESTER®

Hardware And Related Support Costs: Calculation Table						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Hardware costs — inclusive of next-generation firewalls and management consoles		$1,772,500			
E2	Three-year support costs		$881,930			
Et	Hardware and related support costs	E1+E2	$2,654,430	$0	$0	$0
	Risk adjustment	↑5%				
Etr	**Hardware and related support costs (risk-adjusted)**		**$2,787,152**	**$0**	**$0**	**$0**

Cost 2: Software And Subscription Services

Software license and subscriptions are a large factor in the cost equation and contribute to providing organizations value beyond firewall technologies. With the various attack vectors and new malicious code sprouting daily, an always-on and near instantly updating threat recognition engine is the main piece that solidifies an organization's defenses. As previously mentioned, the speed of threat identification and mitigation are key to product benefits on the organizational level. Preventing data breaches is equally if not more valuable. These key software and subscription components are crucial to complete the security stack.

Software and subscription services had a cost of $3,213,200 in PV figures over the three-year study.

- It is possible to purchase portions of the Palo Alto Networks platform, but this defeats the point of a well-integrated system and compromises the efficiency of SecOps groups.
- For organizations that had taken a more engaged approach, the platform can be further integrated into a security information and event management (SIEM) or incident response platform for even greater automation and orchestration.

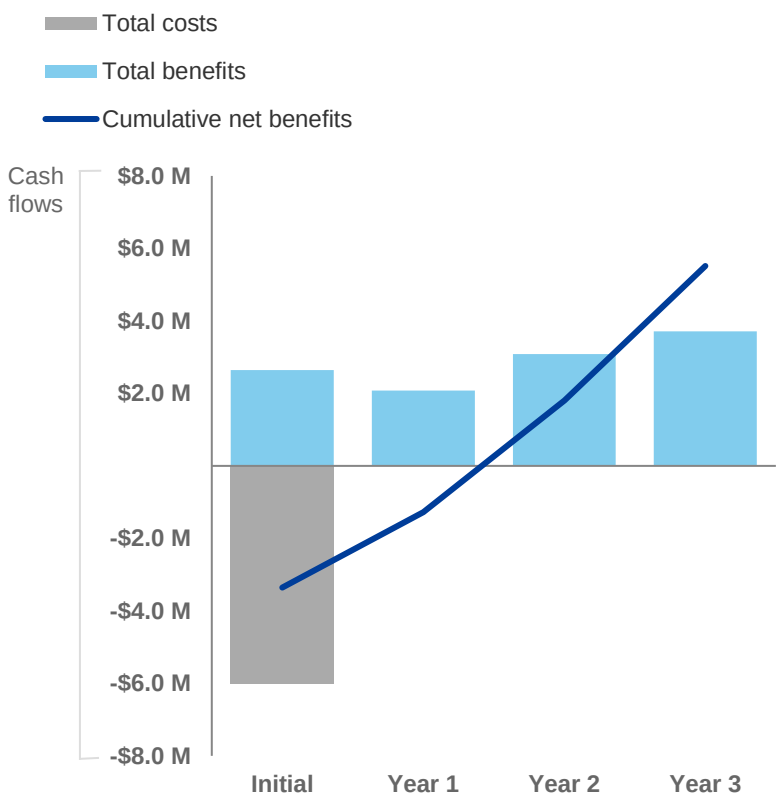
Customers state that Palo Alto Networks devices seem to be priced high upfront on a per-device level. However, when operational costs are accounted for, Palo Alto Networks comes out significantly ahead on ROI.

Software And Subscription Services: Calculation Table						
REF.	**METRIC**	**CALC.**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Subscription costs — inclusive of Threat Prevention, Wildfire, and URL Filtering		$1,715,600			
F2	Endpoint protection software — Traps and AutoFocus, perpetuity license		$1,497,600			
Ft	Software and subscription services	F1+F2	$3,213,200	$0	$0	$0
	Risk adjustment	0%				
Ftr	**Software and subscription services (risk-adjusted)**		**$3,213,200**	**$0**	**$0**	**$0**

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($6,000,352)	$0	$0	$0	($6,000,352)	($6,000,352)
Total benefits	$2,642,733	$2,079,000	$3,089,358	$3,723,266	$11,534,358	$9,883,267
Net benefits	($3,357,619)	$2,079,000	$3,089,358	$3,723,266	$5,534,006	$3,882,915
ROI						65%
Payback period						17 months

FORRESTER®

Palo Alto Networks: Overview

The following information is provided by Palo Alto Networks. Forrester has not validated any claims and does not endorse Palo Alto Networks or its offerings.

The Palo Alto Networks Security Operating Platform allows you to prevent successful cyberattacks. Teams gain visibility into all activity across cloud, data center, and mobile with consistent enforcement of application, user, and content-based policies. The platform makes it easy to implement security best practices without operational burden, reducing opportunities for attack. Threats are automatically blocked, with continual updates to intelligence as new threats are identified. Comprehensive, consistent protections extend across all major cloud providers, traditional networks, and the endpoint.

Routine security tasks are automated with analytics, allowing analysts to focus on hunting threats. Natively integrated innovations, including malware analysis and behavior analytics, continue to learn, making it easy identify and stop new attacks. New enhancements are continually delivered and build on your existing investment. Third-party security apps take advantage of an open framework, using existing sensors and enforcement points to integrate into your environment.

FORRESTER®

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.