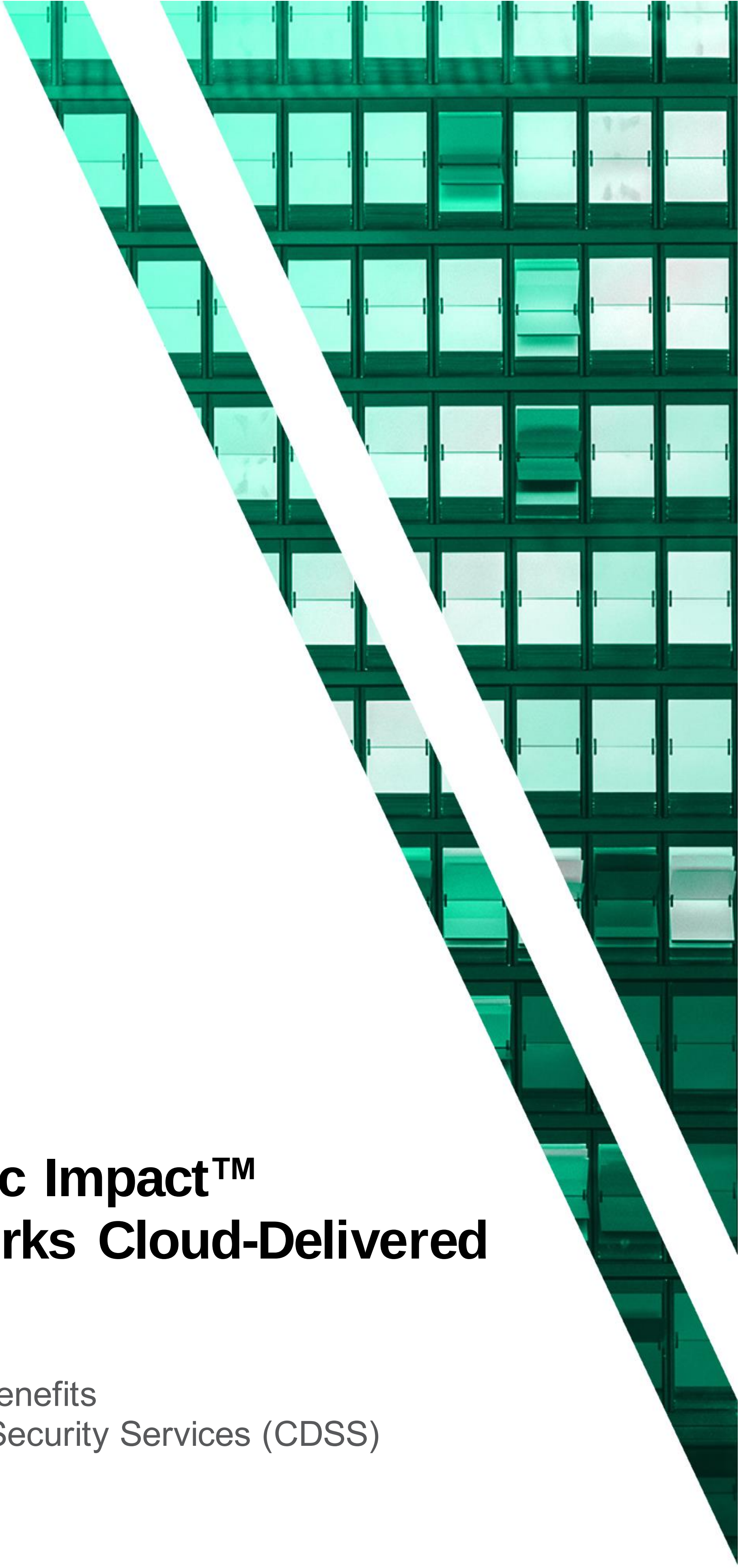
FORRESTER®



The Total Economic Impact™ Of Palo Alto Networks Cloud-Delivered Security Services

Cost Savings And Business Benefits Enabled By Cloud-Delivered Security Services (CDSS)

NOVEMBER 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY PALO ALTO NETWORKS

Table Of Contents

Executive Summary..1

The Palo Alto Networks Cloud-Delivered Security Services Customer Journey..............................7

Key Challenges...7

Investment Objectives....................................8

Composite Organization.................................9

Analysis Of Benefits 11

Security And IT Operations Efficiency...............11

End-User Productivity Gain............................14

Data Breach Risk Reduction 16

Security Infrastructure Cost Reduction And Avoidance..18

Security Stack Management Efficiency From Common Platform 19

Unquantified Benefits...................................21

Flexibility..21

Analysis Of Costs...23

Installation And Deployment Costs..................23

Internal Time Investment For User Training And Ongoing Management 25

CDSS Subscription And Services Costs............27

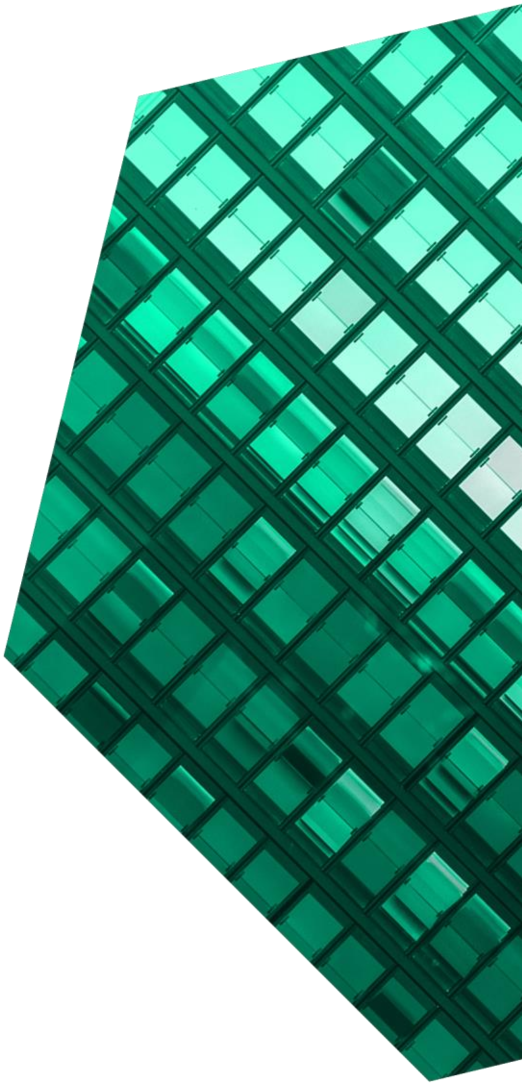
Financial Summary.......................................28

Appendix A: Total Economic Impact 29

Appendix B: Supplemental Material 30

Appendix C: Endnotes 30

Consulting Team: Adi Sarosa
Isabel Carey



Executive Summary

As network architecture becomes more complex, security teams increasingly struggle to adapt and provide consistent security to all devices, data, users and applications traversing their networks and clouds. Forrester research found IoT devices to be the most common target of external attacks[1]. Subscription-based security services are a growing piece of most organizations' security strategies, enabling rapid scalability of protection with up-to-the-minute updates and simplifying the deployment and management of security.

Palo Alto Networks Cloud-Delivered Security Services (CDSS) are a set of solutions that offer specialized security depending on different use cases and are designed to defend against known, unknown, and evasive threats. The different solutions include Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, DNS Security, Enterprise, Medical, and Industrial IoT Security, SaaS Security, and Enterprise DLP.

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 its CDSS.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of its CDSS on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Palo Alto Networks CDSS. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a distributed enterprise with 50,000 employees and $7 billion in annual revenue.

KEY STATISTICS

Return on investment (ROI)
357%

Net present value (NPV)
$10.04M

Prior to deploying Palo Alto Networks for network security needs, the customers leveraged various point solutions to secure their environments. The organizations lacked modern security technology as security and IT teams tried to keep up with evolving business needs. Digital transformation initiatives pushed more data, applications, and processes to the cloud, while other core business functions remained on-premises. Adding to the complexity was the need for the organizations to support more flexible and remote work options for their employees as employee expectations and other environmental factors drove up demand for remote access to critical applications and data. This piecemeal approach left organizations with many different vendors in their security stacks, making it challenging for security operations (SecOps) teams to integrate technologies, benefit from analytics, apply consistent policies, and deliver a consistent experience to end users.

Additionally, the lack of a unified platform and next-generation firewall capabilities left the organizations stuck in a cycle of devoting valuable resources to management, operations, and maintenance activities while work on new initiatives and enhancements fell by the wayside.

After the investment in Palo Alto Networks CDSS, the customer~~s~~ were able to realize various operational efficiencies across different activities, which significantly reduced investigational effort and freed up valuable resources to focus on enhancements and securing the entire network.

Key results from the investment are highlighted by efficiency gains for IT, security, and networks operations teams; business end users; and in-store workers. Further, interviewees' organizations benefited from a reduced likelihood of a data breach, as well as reduced costs associated with licensing and managing legacy point-solution infrastructure.

KEY FINDINGS

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

- **Reduced number of security incidents requiring manual investigation by 25% to 60%, decreased mean time to resolution (MTTR) by 20%, and reduced number of endpoint devices requiring reimaging, all resulting in $1.1 million saved over three years.** By using Palo Alto Networks CDSS in combination with the other solutions implemented in its security environment, the composite organization is able to reduce the number of security incidents requiring manual investigation, the time to respond and resolve incidents, and the number of endpoint devices requiring reimaging. This is a result of being able to track the performance and usage of the different implemented solutions across the organization in one place, giving the SecOps and IT ops teams the ability to quickly identify and respond to potential threats. Over three years, this time savings totals $1.1 million to the composite organization.
- **Improved end-user productivity with better system availability and less intrusion to the network, totaling $5.2 million in business value over three years.** The composite organization also realizes end-user productivity gains by minimizing disruption caused by its security investigations, as well as just overall better system availability of the environment. This is a product of the better integration and compatibility of the different Palo Alto Networks solutions, as well as overall performance. Over three years, this end-user productivity increase is worth nearly $5.2 million to the composite organization.

Annual tech stack spend savings from vendor consolidation

20%

- **Decreased likelihood of a data breach by 50% after three years.** The different subscriptions that fall under CDSS provide a more secure environment for various activities and use cases across the composite organization. As a result, CDSS decreases the likelihood of a significant data breach. Over three years, this reduced risk from a data breach is worth close to $2.8 million to the composite organization.
- **Avoided and rationalized security infrastructure, saving $3.4 million over three years.** Using CDSS also allows the composite organization to consolidate its spending on security tech stack vendors. Over three years, this cost savings from vendor consolidation totals $3.4 million to the composite organization.
- **Reallocated roughly 50% full-time security professionals to higher-value initiatives due to management efficiencies from a common**

platform, saving $378,000 over three years. Related to the vendor consolidation benefit, the composite organization also realizes efficiencies for its employees who manage the different tools. By using the Panorama management tool to manage all Palo Alto Networks solutions, the composite organization can potentially repurpose certain employee time or even entire team members to other prioritized or higher-value work. Over three years, this efficiency generates $378,000 in value to the composite organization.

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

- **Improved visibility in the security environment.** With Palo Alto Networks CDSS monitoring and tracking various security activities and use cases across the organization, the composite organization realizes improved visibility to its security environment. In addition to the time savings and efficiencies related to this visibility, the composite organization also now has more robust information to act on or react to, which allows it to further improve its situation, if needed.

- **Better integration with tools and platforms in the security tech stack.** The composite organization also benefits from the fact that CDSS solutions integrate better with one another and with the other Palo Alto Networks solutions such as firewalls in both hardware and software form factors in the environment.

- **Better employee experience.** The combination of the increased visibility and better integration means that the composite organization also improves the employee experience. All employees, whether part of the security organization or general end users, realize some sort of ease, comfort, and confidence that they are well protected from potential attacks and threats. In addition to the productivity boost quantified above, this can also potentially improve their attachment to the organization and the brand from the perspective of both internal and external stakeholders.

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

- **Installation and deployment costs totaling $843,000 over three years.** Time and labor are required to deploy and install the various components of the Palo Alto Networks solution throughout the composite organization. Deployment of CDSS solution relative to other Palo Alto Networks solutions (i.e., NGFWs and Prisma SASE) is assumed to require 25% of the implementing staff’s time.

- **Training costs and ongoing management time investment totaling $63,000 over three years.** Palo Alto Networks required less training than legacy solutions and interviewees and respondents reported that the provided training was more effective and efficient, allowing employees to get up to speed faster and expand their skill sets. Once trained, the team spends some time maintaining and managing the system on an ongoing basis.

- **Palo Alto Networks CDSS annual licensing costs totaling $1.9 million over three years.** The composite organization is able to purchase hardware upfront and leverage three-year contract terms to add the CDSS, helping reduce the overall costs of Next-Generation Firewalls (NGFWs); IPS/IDS; web security; web proxy; VPN; Advanced URL Filtering; malware analysis (e.g., sandboxing); and DNS security, SaaS security applications, data loss prevention, and Enterprise IoT/OT Security solutions. Combining this with services like Prisma SASE allows the CDSS solutions to be extended for branch offices or remote workers, and organizations can scale up and down based on usage and needs.

The representative interviews and financial analysis found that a composite organization experiences benefits of $12.85 million over three years versus costs of $2.81 million, adding up to a net present value (NPV) of $10.04 million, an ROI of 357%, and a payback period of less than six months.

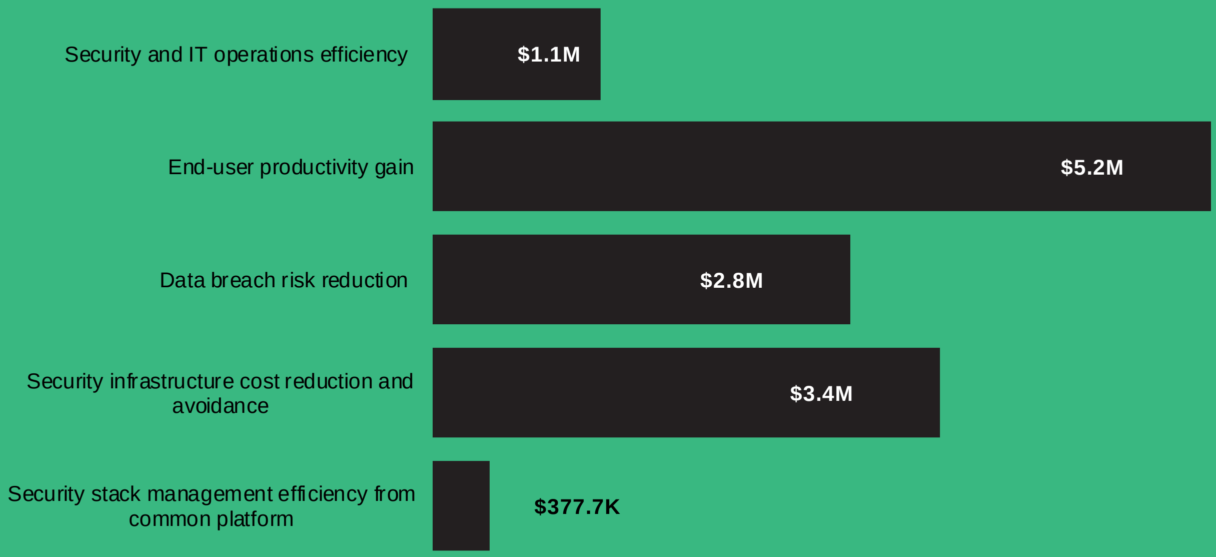
ROI
357%

BENEFITS PV
$12.85M

NPV
$10.04M

PAYBACK
<6 months

Benefits (Three-Year)



> **“The main value of CDSS is having a better understanding of our assets in the potential deficiencies those assets may have from a security perspective, the vulnerabilities and exposure that we could have, from the biases that govern the network access into the organization.”**
>
> — Information security architect and CISO, healthcare

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 Palo Alto Networks CDSS.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Palo Alto Networks CDSS 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.

DUE DILIGENCE

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

INTERVIEWS

Interviewed four representatives at organizations using Palo Alto Networks CDSS to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

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 PANW CDSS.

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.

The Palo Alto Networks CDSS Customer Journey

🟩 Drivers leading to the CDSS investment

Interviews

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

KEY CHALLENGES

Prior to using Palo Alto Networks, interviewees shared that they used a myriad of security point solutions and services designed to address specific needs. They would often work with different vendors for different solutions. They would have to spend time and resources of their SecOps and IT ops teams to manage the different platforms, which created a significant technical burden and operational inefficiencies.

The interviewees noted how their organizations struggled with common challenges related to their overall network security, including:

- **The need to update security for modern work environments.** Interviewees shared that with the growth of remote and hybrid work, the adoption of cloud technologies, and increasingly more sophisticated cybersecurity attacks, having the most updated, modern, and comprehensive security system for their work environment was paramount. The SVP in IT at a financial services firm noted: "Before Palo Alto Networks, we had a traditional network infrastructure with a hardened firewall perimeter and a soft-squishy inside. We recognized we needed to move security services closer to the users/resources. I have around 250,000+ users on the network who I don't trust any more than the internet, so I had to move to an environment where all traffic was vetted."

> **"One of the biggest risks that we have today is the speed that technology causes for companies. More and more people are working out of the office. The old-fashioned way of doing security is that you had everyone connected over to the same network, in closed locations. That no longer works."**
>
> *Director, security architecture and engineering, manufacturing*

- **Suboptimal business user experience with legacy security environment.** Interviewees also noted that they experienced a lot of disruption with their previous environments, either caused by a cybersecurity threat or by a security measure responding to a potential threat that ended up being invasive to the overall system. As a result, a lot of business and end users would see their work disrupted for periods of time, which could get frustrating very fast. The director of security architecture and engineering at a manufacturing company said: "Security measures started to become a blocking point to user experience. We had people complaining that their work is becoming too slow. We wanted to bring a good quality of experience for the end user while keeping security at max."

- **Security gaps from disparate solutions that did not integrate and work well together.** Interviewees also noted that by using disparate solutions, they had security gaps in their environment. Either their legacy solutions were not comprehensive enough to provide full coverage to an ever-evolving cybersecurity threat, or the different point solutions would neither integrate nor work well with one another. The enterprise network architect in government said, "We realized we had gaps in our security maintaining so many disparate solutions."

Additionally, interviewees also noted some pain points specifically related to their need for Palo Alto Networks CDSS, such as:

- **Lack of visibility into IoT devices, resulting in operational inefficiencies to the IT organization.** Interviewees noted that as their IoT device footprint grew within their organizations, they did not have any visibility or process to understand how the IoT devices were used or if any of the devices were becoming a security concern. The information security architect and CISO in healthcare told Forrester: "Prior to using Palo Alto Networks IoT, our inventory was dependent on devices identified by our legacy vendor. We would then have to manually convert that information to and from different platforms and correlate that information together. It wasn't an easy process, and the IoT solution helped obtain that visibility in a central repository for us."

- **Operational inefficiency from having to manage multiple vendors.** Interviewees also noted that by using different point solutions in their previous environments, they had many operational inefficiencies because employees were overextended trying to manage multiple vendors. This was especially true when thinking about the activities and use cases that are now covered by CDSS. The enterprise network architect at a government agency shared: "In the past, I still had a legacy URL filtering solution that was serving for all of our URL filtering for K-12, higher ed, state government — it does everything that we need for the basic URL level. We had a very large, expensive contract for URL filtering that is now included as part of our firewall spend."

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- **Reduce risk by creating a less-complex and better-integrated security environment.**

> **"We chose Palo Alto Networks because integration was easy. Our team was already knowledgeable about Palo Alto Networks solutions. Also, we could integrate Prisma SASE into the same central management, making it a centralized effort to configure everything."**
>
> *Information security architect and CISO, healthcare*

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

Whether it's an A/B test or a large-scale demographic analysis, businesses base critical decisions on the results of data and AI models

Data that's been altered, whether intentionally or accidentally, will reduce the efficacy of marketing campaigns, lead to negative customer sentiment, or reduce customer engagement overall for a business.

This will give attackers ample incentive to tamper with a business's existing data.

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

Interviewees shared with Forrester that with ever-growing external cybersecurity threats, what they could control was eliminating the inefficiencies in their security operation. They looked for a solution that could help them create a simpler security environment where the different elements and tools integrate well with one another. The director of security architecture and engineering at a manufacturing company said, "The consolidation and the integration with the other tools is key to reducing the complexity of the architectures and to be able to mitigate risk easily or more effectively."

- **Be a partner with extensive industry knowledge.** Interviewees also noted that they were looking for a partner that could help them navigate the ever-changing security landscape. The information security architect and CISO in healthcare shared: "For IoT, I was impressed by Palo Alto Networks' knowledge of networks and how network systems work. That was their native bread and butter. I knew that our network security would continue to evolve, so I had a lot of confidence that Palo Alto Networks would stay current with those changes."

COMPOSITE ORGANIZATION

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

Description of composite. The composite organization is a distributed enterprise with 50,000 employees and $7 billion in annual revenue. It has 400 sites, including its headquarters, data center, cloud, branch office, and retail and manufacturing locations. On average, the composite's security team responds to 1,200 incidents per week, or 62,400 in the first year, with each incident taking an average of 2 hours to resolve.

Key Assumptions

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

Deployment characteristics. The organization uses Palo Alto Networks Cloud-Delivered Security Services to supplement each NGFWs deployment (physical, virtual, cloud-delivered) with 24/7 monitoring of all vulnerabilities (Advanced Threat Prevention), all web-borne threats (Advanced URL Filtering, DNS Security, and Prisma SASE), and all file-based threats (Advanced WildFire), providing protection against zero-day threats for all threat vectors with inline machine learning (ML) and updates delivered in seconds or less. The organization deploys Enterprise IoT Security to monitor and secure expanding device risk from IoT.

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Security and IT operations efficiency	$311,666	$488,555	$580,617	$1,380,838	$1,123,323
Btr	End-user productivity gain	$2,084,940	$2,084,940	$2,084,940	$6,254,820	$5,184,937
Ctr	Data breach risk reduction	$1,119,360	$1,119,360	$1,119,360	$3,358,080	$2,783,683
Dtr	Security infrastructure cost reduction and avoidance	$1,360,000	$1,360,000	$1,360,000	$4,080,000	$3,382,119
Etr	Security stack management efficiency from common platform	$151,875	$151,875	$151,875	$455,625	$377,691
	Total benefits (risk-adjusted)	$5,027,841	$5,204,730	$5,296,792	$15,529,363	$12,851,753

SECURITY AND IT OPERATIONS EFFICIENCY

Evidence and data. Interviewees shared with Forrester that by moving to Palo Alto Networks CDSS, they were able to realize time savings and efficiencies among their security and IT operations teams. Through the different Palo Alto Networks solutions, interviewees noted that their organizations were able to introduce automation and repeatable templates in their process, which saved time in doing certain activities.

> **"[Palo Alto Networks] helps us rate the risk severity and understand which remediation we should focus on for the various network-connected devices out there."**
>
> *Information security architect and CISO, healthcare*

- The enterprise network architect in government said: "For [Advanced] URL Filtering, the vast majority of automation is on detecting and managing email phishing. We can now look at logs and see if a user actually clicked on a phishing link and remediate down through that. The whole process is automated, whereas before, it was manual."
- The same interviewee also shared, "We've seen a 60% decrease in time needed to deal with threats because of automation."
- The director of security architecture and engineering at a manufacturing company told Forrester, "[With Palo Alto Networks], we have reduced our incident response time from 4 hours to a little over 60 minutes."
- The SVP of IT in financial services said, "SecOps efficiency increased by roughly 25% for time to resolution for IT tickets and overall resourcing."

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

- With the previous solution, 1,200 security incidents per week required multitouch, advanced investigation work from the SecOps team, increasing by 5% annually.

- The composite sees an initial reduction in the number of incidents requiring action by 25% in Year 1, and this increases to 50% and 60% in Years 2 and 3, respectively, by shifting left enabled by Palo Alto Networks solutions on the core network and cloud perspectives.
- Prior to using Palo Alto Networks, MTTR was 120 minutes. With the new capabilities and automation, this improves by 20%.
- The average fully burdened salary for members of the SecOps team is $121,500 annually or $58 per hour.
- With the legacy solution, 50 endpoint devices per week required reimaging or other services from the IT operations (IT ops) team with the legacy solution.
- The average fully burdened salary for the IT ops team is $81,000 annually or $39 per hour.
- Taking into account that part of the efficiency is gained from using the different Palo Alto Networks tools together (Prisma SASE, Next-Generation Firewalls, and CDSS), a 25% attribution to CDSS is assumed.

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

- The number of security incidents that require manual intervention before implementing Palo Alto Networks.
- The other tools and solutions implemented to support the work of the SecOps and IT ops teams.
- The number of devices requiring service and labor associated with servicing those devices.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.1 million.

Security And IT Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Security incidents requiring manual investigation/remediation using legacy security solution	Composite	62,400	65,520	68,796
A2	Reduction in security incidents requiring manual investigation/remediation with Palo Alto Networks	Interviews	25%	50%	60%
A3	Manual multitouch security incidents avoided	A1*A2	15,600	32,760	41,278
A4	MTTR with prior solution (minutes)	Composite	120	120	120
A5	Subtotal: Time savings due to avoided investigations with Palo Alto Networks	A3*A4/60*A8	$1,809,600	$3,800,160	$4,788,248
A6	MTTR improvement with PANW	Interviews	20%	20%	20%
A7	Minutes saved per incident	A4*A6	24	24	24
A8	Average fully burdened hourly salary of involved employee	TEI standard	$58	$58	$58
A9	Subtotal: SecOps efficiency related to critical alerts due to Palo Alto Networks	((A1-A3)*A7/60)*A8*A15)	$1,085,760	$760,032	$638,418
A10	Endpoint devices requiring reimaging or other services (annually)	Composite	2,600	2,600	2,600
A11	Time spent per device with legacy solution (minutes)	Composite	45	45	45
A12	Reduction in number of endpoint devices requiring reimaging with Palo Alto Networks	Interviews	50%	50%	50%
A13	Average fully burdened hourly salary of involved employee	TEI standard	$39	$39	$39
A14	Subtotal: Reduced IT effort — reimaging	((A10*A11)/60)*A12*A13	$37,969	$37,969	$37,969
A15	Attribution to CDSS	Composite	25%	25%	25%
A16	Productivity recapture for security FTE	TEI standard	50%	50%	50%
At	Security and IT operations efficiency	(A5+A9+A14)*A15*A16	$366,666	$574,770	$683,079
	Risk adjustment	↓15%			
Atr	Security and IT operations efficiency (risk-adjusted)		$311,666	$488,555	$580,617
	Three-year total: $1,380,838		**Three-year present value: $1,123,323**		

END-USER PRODUCTIVITY GAIN

Evidence and data. Interviewees noted that prior to using Palo Alto Networks, their previous security environment sometimes disrupted work done by business and end users. This could be through investigation procedures that were too disruptive; other times, security gaps that existed in their legacy environment caused cybersecurity attacks that could significantly disrupt employee productivity.

By moving to Palo Alto Networks, specifically certain Cloud-Delivered Security Solutions such as Enterprise IoT Security or Advanced Threat Prevention, interviewees shared that activities such as vulnerability scanning are no longer too invasive. For tools that protect remote workers, they could now ensure that all end users have the same experience regardless of their location. As a result of all the prevented disruption, end users realized improved productivity.

- The information security architect and CISO in healthcare shared: "Our previous vulnerability scanning solution was invasive. The aggressiveness of the scanning can sometimes trigger a negative consequence to a device and take it down."
- The SVP of IT in financial services noted: "We want to give end users the same experience and performance regardless of how they are accessing the network. With Palo Alto Networks, we have 99.99% performance at or above expectation. We can run encryption without sacrificing performance."
- The director of security architecture and engineering at a manufacturing company told Forrester: "We are able to increase the quality of the experience of the end users yet at the same time also reduce the risk of internal malware that may exist with the new feature that we have put in place, such as DNS Security or Advanced Threat Protection. We can block any kind of malicious activity from going outside of our network."

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

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

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

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

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $5.2 million.

End-User Productivity Gain

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

DATA BREACH RISK REDUCTION

Evidence and data. Interviewees shared that their organizations previously relied on point solutions that did not necessarily integrate well as an overall environment. This left potential security coverage gaps, even more so if their organization had a mix of on-premises and cloud environments.

With Palo Alto Networks, organizations had the visibility to easily identify and close these gaps. 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 director of security architecture and engineering at a manufacturing company noted, "We have reduced the risk by 100% because today we are doing device posture and identity check properly."
- The enterprise network architect in government said: "We have not seen a significant breach since 2021. On average, we would have one every six to nine months before Palo Alto Networks. That is due to the threat engine on the firewall."
- The information security architect and CISO in healthcare shared: "Our IoT Security subscription helps us get visibility on our medical device inventory. Where do they reside, how often are they used, are there any FDA recalls, etc. That helps us reduce risk related to our devices."

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

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

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

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

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

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

Data Breach Risk Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average data breaches per year	Composite	3.2	3.2	3.2
C2	Employees	B1	50,000	50,000	50,000
C3	Average potential cost of a data breach per employee, exclusive of internal user downtime	Composite	$53	$53	$53
C4	Average total potential cost of a data breach	C2*C3	$2,650,000	$2,650,000	$2,650,000
C5	Reduced likelihood of a breach	Interviews	50%	50%	50%
C6	Attribution to CDSS	Composite	33%	33%	33%
Ct	Data breach risk reduction	C1*C4*C5*C6	$1,399,200	$1,399,200	$1,399,200
	Risk adjustment	↓20%			
Ctr	Data breach risk reduction (risk-adjusted)		$1,119,360	$1,119,360	$1,119,360
	Three-year total: $3,358,080		**Three-year present value: $2,783,683**		

SECURITY INFRASTRUCTURE COST REDUCTION AND AVOIDANCE

Evidence and data. Interviewees shared that by using different CDSS solutions, they were able to realize cost savings by retiring or discontinuing parts of their security tech stack spending. Palo Alto Networks CDSS subscriptions supplanted most of the legacy services that interviewees relied on, allowing them to end those contracts and reduce the number of vendors and disparate systems in their environments.

- The SVP of IT in financial services noted: “[We saw a] 30% to 35% reduction across all vendors. CDSS was where the majority of the cost savings were.”

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

- The annual security tech spending of the organization is $8 million.
- The vendor consolidation enabled by using Palo Alto Networks CDSS represents 20% of the annual security tech spend.

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

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

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $3.4 million.

Security Infrastructure Cost Reduction And Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Annual security tech stack spend	Composite	$8,000,000	$8,000,000	$8,000,000
D2	Percentage of savings from vendor consolidation related to CDSS	Interviews	20%	20%	20%
Dt	Security infrastructure cost reduction and avoidance	D1*D2	$1,600,000	$1,600,000	$1,600,000
	Risk adjustment	↓15%			
Dtr	Security infrastructure cost reduction and avoidance (risk-adjusted)		$1,360,000	$1,360,000	$1,360,000
	Three-year total: $4,080,000		**Three-year present value: $3,382,119**		

SECURITY STACK MANAGEMENT EFFICIENCY FROM COMMON PLATFORM

Evidence and data. Interviewees shared a number of efficiencies they were able to realize related to managing Palo Alto Networks CDSS. For example, being able to reduce the number of vendors in their environments, in addition to realizing cost savings related to the vendor licensing cost described before, resulted in less-complex vendor and platform management work on the part of the IT organization staff. Added to the fact that all Palo Alto Networks' solutions can be managed from a unified management tool resulted in significant time savings and efficiency gains that could be repurposed for other work across the organization.

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

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

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

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

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $378,000.

> **"With Panorama, we manage our entire firewall fleet as a single group. We have hundreds of policy changes that happen per month. In the past, most of our time was spent searching on where to put a policy, not even looking [to see] if the policy should be there or if it is working. With [a unified management tool], we get all of that time back."**
>
> *Enterprise network architect, government*

Security Stack Management Efficiency From Common Platform

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Team responsible for platform management	Composite	15	15	15
E2	Percentage of time savings due to common platform efficiency	Interviews	50%	50%	50%
E3	Attribution to CDSS	Composite	20%	20%	20%
E4	Average fully burdened annual salary for IT organization (NetOps, SecOps, and IT ops)	TEI standard	$112,500	$112,500	$112,500
Et	Security stack management efficiency from common platform	E1*E2*E3*E4	$168,750	$168,750	$168,750
	Risk adjustment	↓10%			
Etr	Security stack management efficiency from common platform (risk-adjusted)		$151,875	$151,875	$151,875
	Three-year total: $455,625		**Three-year present value: $377,691**		

UNQUANTIFIED BENEFITS

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

- **Increased visibility for security environment.** Interviewees noted that the one of the main sources of value from having Palo Alto Networks is the enhanced visibility they now have on the condition, performance, and usage of different parts of its security organization. CDSS specifically gives them the ability to deploy specific tools for specific use cases and situations in their organization. The SVP of IT in financial services said: "The other very attractive thing about Palo [Alto Networks] was the interface and visibility. Their reporting was the best for us in terms of UI. It instantly performed better than our purpose-built reporting software that we had struggled to maintain."

  The information security architect and CISO in healthcare added, "The visibility of the IoT tool in terms of usage helps the purchasing and supply organization when they would get requests from the clinical engineering team about needing new equipment"

- **Better integration with other parts of their security tech stack.** As mentioned previously, interviewees sought a simpler security environment, and part of that equation was a security tech stack whose components integrated well with one another, as well as with other Palo Alto Networks solutions implemented in the environment. The director of security architecture and engineering at a manufacturing company said: "Palo Alto Networks gives you the path to integrate more things and continue to optimize your environment easily. It's integrated and optimized to be easy to use and secure."

- **Better employee experience, both in using the different solutions and in benefitting from the more robust, less intrusive security environment at their organization.** The interviewees noted that the combination of all the benefits above created a better employee experience at their organization. The same director in manufacturing noted: "Palo Alto Networks came and worked perfectly. We had great feedback from people in terms of quality of experience."

> **"We are able to easily monitor traffic and see what is actually happening on the network."**
>
> *SVP of IT, financial services*

> **"Having Palo Alto Networks prepares you for the rest of the path, which is to integrate more things such as remote networks, branch offices, and CASB."**
>
> *Director of security architecture and engineering, manufacturing*

FLEXIBILITY

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

- **The long-term virtuous impact of having a complete security solution in the environment.** In the long run, having an efficient and comprehensive security environment can have far-reaching impact on company

> performance, its brand, and how it copes with new and emerging threats. The enterprise network architect in government said: “With Palo Alto [Networks], we’ve ended up deploying a lot more of the Palo Alto [Networks] suite. I definitely see a lot of benefit from looking at a suite of products that play together. Everything is integrated. It’s allowed us to optimize and make our security better, faster, and cheaper.”

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

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

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

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

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

Analysis Of Costs

🟩 Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Ftr	Installation and deployment costs	$558,900	$163,013	$100,913	$69,863	$892,688	$842,981
Gtr	Internal time investment for user training and ongoing management	$950	$24,948	$24,948	$24,948	$75,794	$62,992
Htr	CDSS subscription and services costs	$0	$766,570	$766,570	$766,570	$2,299,710	$1,906,346
	Total costs (risk-adjusted)	$559,850	$954,531	$892,431	$861,381	$3,268,192	$2,812,319

INSTALLATION AND DEPLOYMENT COSTS

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

- The information security architect and CISO in healthcare noted: “To get IoT up and running, we had to figure out how we capture data from different locations. We started by deploying small firewall network sensors in those locations. There’s somewhat of a limitation to how many devices we could deploy given our licenses. We had weekly calls with the development team.”

- The director of security architecture and engineering at a manufacturing company added: “My team and people from networking were involved in installation. There was also one person from Palo Alto Networks. The first three to four days required about 50% of my team’s time, because that was mostly done by the Palo Alto Networks folks. As soon as the tenant on the cloud was ready to use, that became 100% from my team. The networking person on the other side spent 50% of their time.”

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

- For the NGFWs and CDSS deployment, 10 network operations employees spend a total of nine months upgrading firewalls and aligning policies in the initial period, and they spend almost five months fine-tuning in Year 1. The organization leverages end-of-life cycles and invests time to test the deployment, extending the timeline but also ensuring a smooth transition away from its legacy solution.

- The involved employees initially spend 80% of their time on deployment, which gradually reduces in the subsequent years.

- The average fully burdened annual salary for a network operations employee is $135,000.

- Since organizations typically deploy NGFWs and CDSS together, the model assumes that the composite spends 20% of the total installation and deployment time for CDSS.

- For the Enterprise IoT Security deployment, a team of eight network operations employees spends three months connecting and testing all

IoT devices. A team of two network operations employees spends roughly six weeks per year managing and maintaining the IoT deployment.

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

- The amount of time and effort needed to deploy the NGFWs and CDSS.
- The particular CDSS being implemented and the coverage of its implementation.
- The average salary for deployment team members.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $843,000.

Installation And Deployment Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Network team members working on PANW installation	Composite	10	10	10	10
F2	Time spent per staff member	Interviews	80%	40%	20%	10%
F3	Annual salary: NetOps employee	TEI standard	$135,000	$135,000	$135,000	$135,000
F4	Percentage of work time necessary to deploy CDSS	Interviews	20%	20%	20%	20%
F5	Subtotal: Implementation labor for CDSS software and subscriptions	F1*F2*F3*F4	$216,000	$108,000	$54,000	$27,000
F6	IoT deployment team members	Composite	8	2	2	2
F7	Time spent per staff member	Interviews	25%	12.5%	12.5%	12.5%
F8	Annual salary: NetOps employee	Forrester standard	$135,000	$135,000	$135,000	$135,000
F9	Implementation and fine-tuning labor for IoT security deployment	F6*F7*F8	$270,000	$33,750	$33,750	$33,750
Ft	Installation and deployment costs	F5+F8	$486,000	$141,750	$87,750	$60,750
	Risk adjustment	↑15%				
Ftr	Installation and deployment costs (risk-adjusted)		$558,900	$163,013	$100,913	$69,863
	Three-year total: $892,688			**Three-year present value: $842,981**		

INTERNAL TIME INVESTMENT FOR USER TRAINING AND ONGOING MANAGEMENT

Evidence and data. Interviewees noted that ongoing management was relatively easy for their team. Additionally, the training resources that Palo Alto Networks provided were effective and gave employees the tools and knowledge they needed to be successful working across the various products and solutions.

- The director of security architecture and engineering at a manufacturing firm said: "Ongoing management is 10% of our time. It's really easy to operate. It's just people on my team involved."

- The enterprise network architect in government added: "On the security side, CDSS is all automated. We've done full automation throughout. We never push manual patches on that side of it. We really don't touch it. It takes care of itself, which is really nice."

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

- A total of 20 hours of training is required for the NGFWs and CDSS training for employees new to Palo Alto Networks. In subsequent years, 8 hours of training is required to share any new features, updates, and enhancements.

- For Enterprise IoT Security, 8 hours of training is required to initially familiarize employees with the new platform and capabilities. Two hours of training on new features and updates is required in subsequent years.

- The average fully burdened salary across IT is $54 per hour.

- Once training is completed, ongoing management is assumed to involve the 10 people trained yearly. They spend 10% of their time managing NGFWs and CDSS.

- Since organizations manage NGFWs and CDSS together, the model assumes that 20% of the total time spent for ongoing management is for CDSS.

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

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

- The average salary of IT employees.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $63,000.

Internal Time Investment For User Training And Ongoing Management

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	FTEs receiving training for ongoing management	Composite	10	10	10	10
G2	Hours per training session	Interviews	8	2	2	2
G3	Average fully burdened annual salary for IT organization (NetOps, SecOps, and IT ops)	TEI standard	$54	$54	$54	$54
G4	Internal time investment for user training	G1*G2*G3	$4,320	$1,080	$1,080	$1,080
G5	Percentage of time spent for ongoing management	Interviews		10%	10%	10%
G6	Value of internal time investment for ongoing management	G1*G4*2,080*G5		$112,320	$112,320	$112,320
G7	Attribution to CDSS	Composite	20%	20%	20%	20%
Gt	Internal time investment for user training and ongoing management	(G4+G6)*G7	$864	$22,680	$22,680	$22,680
	Risk adjustment	↑10%				
Gtr	Internal time investment for user training and ongoing management (risk-adjusted)		$950	$24,948	$24,948	$24,948
	Three-year total: $75,794		**Three-year present value: $62,992**			

CDSS SUBSCRIPTION AND SERVICES COSTS

Evidence and data. CDSS cost and structure vary by type and usage and are often connected to the NGFWs deployment. Interviewees shared that their Palo Alto Networks solution could also be purchased with credits that could be used on different solutions.

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

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

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

- The number of CDSS offerings implemented in the organization, which can be impacted by the size of the NGFWs deployment.
- The number of IoT devices and remote sites included in the deployment.

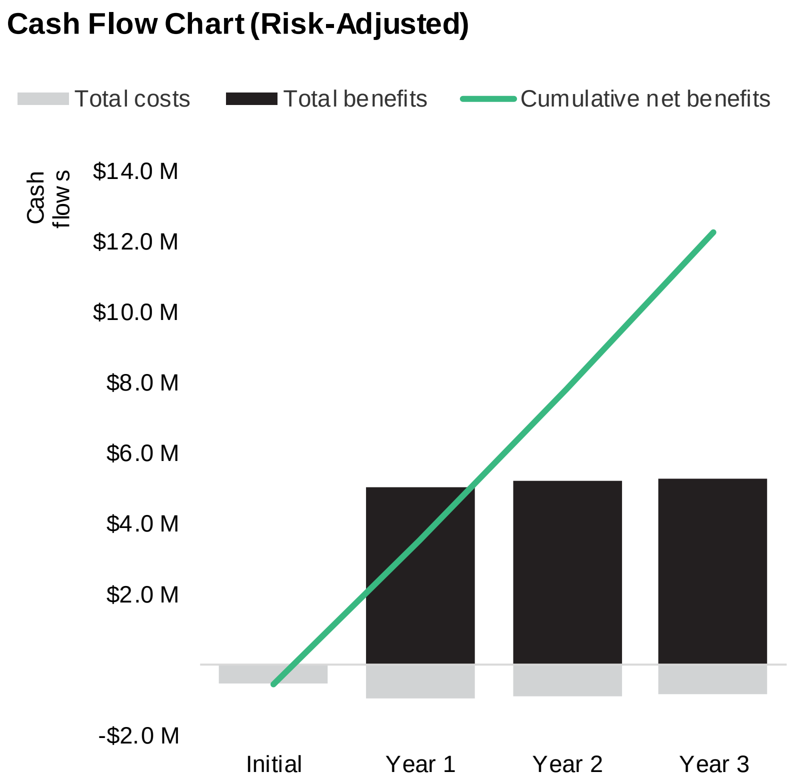
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $1.9 million.

CDSS Subscription And Services Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	CDSS subscription and services costs	Palo Alto Networks	0	$730,067	$730,067	$730,067
Ht	CDSS subscription and services costs	H1	$0	$730,067	$730,067	$730,067
	Risk adjustment	↑5%				
Htr	CDSS subscription and services costs (risk-adjusted)		$0	$766,570	$766,570	$766,570
	Three-year total: $2,299,710		**Three-year present value: $1,906,346**			

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



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	($559,850)	($954,531)	($892,431)	($861,381)	($3,268,192)	($2,812,319)
Total benefits	$0	$5,027,841	$5,204,730	$5,296,792	$15,529,363	$12,851,753
Net benefits	($559,850)	$4,073,311	$4,312,299	$4,435,412	$12,261,171	$10,039,434
ROI						357%
Payback						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Supplemental Material

Related Forrester Research

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

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

Appendix C: Endnotes

[1] Source: "The State Of IoT Security, 2023," Forrester Research, Inc., May 18, 2023.

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

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020.

FORRESTER®