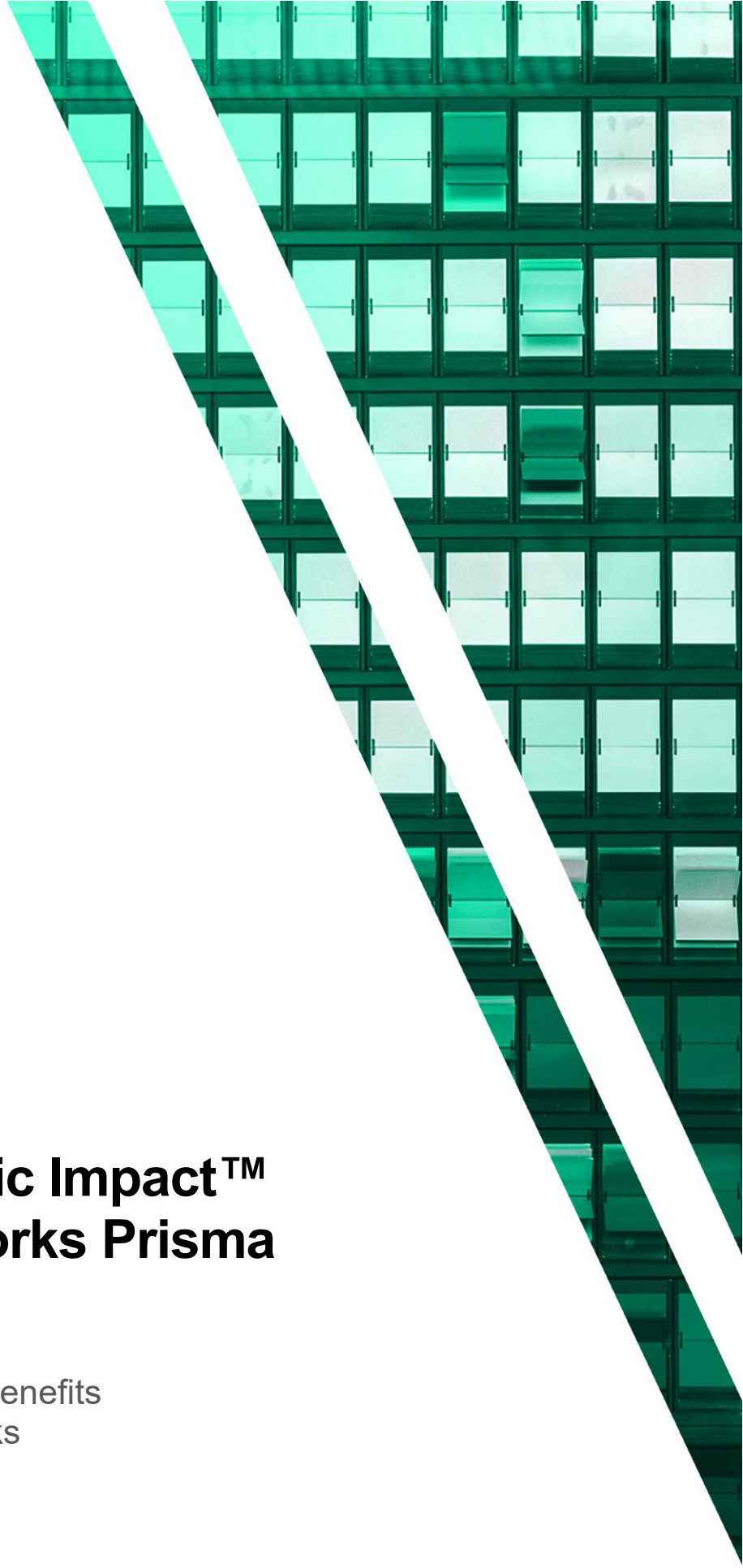
FORRESTER®



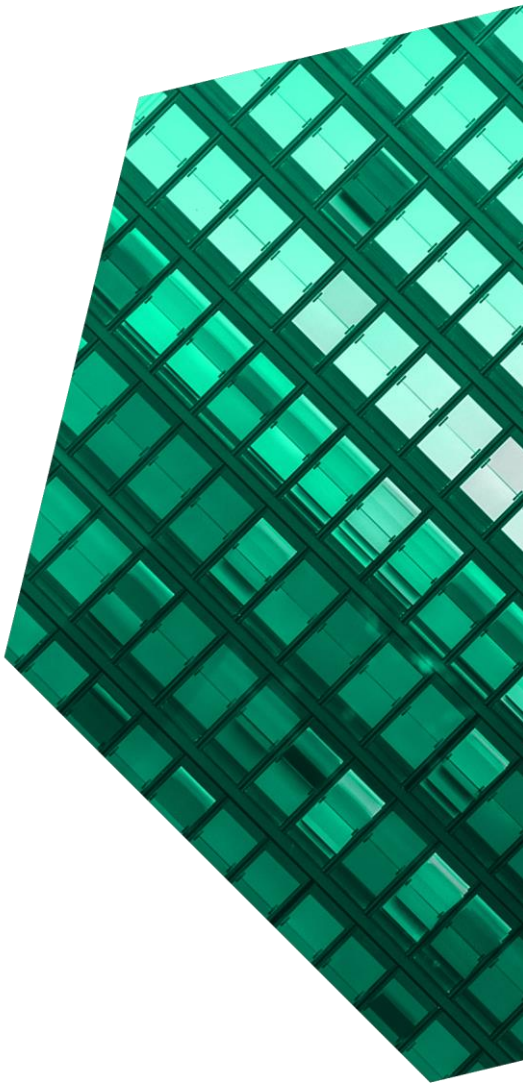
The Total Economic Impact™ Of Palo Alto Networks Prisma SASE

Cost Savings And Business Benefits Enabled By Palo Alto Networks

DECEMBER 2023

Table Of Contents

Consulting Team: Adi Sarosa
Isabel Carey



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Highly distributed organizations — those with many sites or a large percentage of remote workers — often look for secure access service edge (SASE) architecture mainly because of its ability to authenticate and authorize users who connect to and through their platform. However, SASE is a transformative technology, centralizing multiple networking and security capabilities into a unified solution with a single interface and data lake. Selecting the right solution provider can be a high-risk, high-reward decision.

Prisma SASE converges network security, SD-WAN, and autonomous digital experience management (ADEM) in the cloud. This provides security for all applications used by an organization, regardless of the location of the user.

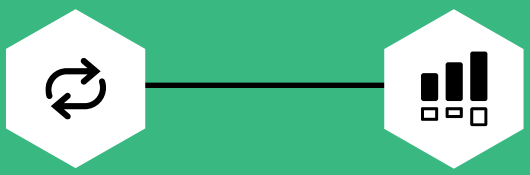
Palo Alto Networks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Prisma SASE.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Prisma SASE on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Prisma SASE. 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, of whom 33% are remote or hybrid, and $7 billion in annual revenue.

Prior to using Prisma SASE, organizations typically worked with inconsistent and incomplete security, poor user experience due to how traffic was backhauled to data centers, and poor scalability as organizations increasingly adopted hybrid work and cloud. Additionally, managing access service at their organizations meant having to install different 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. Yet this piecemeal approach left interviewees' 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.

After the investment in Prisma SASE, the interviewees shared that they were able to consolidate much of their time spent on certain management activities as well as their vendor spend, creating operational efficiencies. They were able to boost end-user productivity, specifically their remote workers and employees who were not present at their physical office sites. They also noted that Prisma

KEY STATISTICS



Return on investment (ROI)
107%

Net present value (NPV)
$9.49M

SASE in collaboration with other Palo Alto Networks solutions installed in their environment significantly reduced the likelihood of a data breach event.

Efficiency gains in managing SASE and making policy changes

75%

KEY FINDINGS

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

- **Gained 75% efficiency in SASE management and policy changes as well as in responding to security incidents, and 80% time savings related to scaling and setting up new sites.** Whereas previously, the composite organization would deploy multiple teams related to the management of their SASE solution, by using Prisma SASE, it realizes time savings and efficiencies across multiple activities for both its SecOps and network operations (NetOps) teams. Over three years, this efficiency gain is worth $2.2 million to the composite organization.
- **Improved end-user productivity with better system availability and less intrusion to their network, totaling $12.2 million in business value over three years.** The composite organization also realizes end-user productivity, especially those who are working remotely or outside their physical office site, gains by having less disruption caused by their security activities, and just overall better system availability of their environment. This is a product of better integration and compatibility of the different Palo Alto Networks solutions, as well as overall performance. Over three years, this improvement to end user productivity is worth close to $12.2 million to the composite organization.
- **Decreased likelihood of a data breach by 50% after three years.** By replacing multiple disconnected security solutions with a single integrated solution, Prisma SASE better fills previous security gaps that exist at the composite organization. As a result, it decreases the likelihood of a significant data breach. Over three years, this reduced risk from a data breach is worth close to $3 million to the composite organization.
- **Avoided and rationalized security and networking infrastructure, saving $846,000 over three years.** Using Prisma SASE also allows the composite organization to consolidate its security tech stack vendor spending. Over three years, this cost savings from vendor consolidation totals $846,000 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.** Prisma SASE allows the composite organization to better monitor traffic and actually know what is happening on its network.
- **Better employee experience.** Employees at the composite organization, either part of the security organization or general end users, also appreciate the ease and comfort of using Prisma SASE, as well as the confidence that they are well protected from potential attacks and threats. In addition to the productivity boost quantified above, this can also potentially impact their attachment to the organization and the brand of

the company 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 $436,000 over three years.** Time and labor are required to deploy and install the Palo Alto Networks solution throughout the composite organization. Deployment of Prisma SASE relative to other Palo Alto Networks solutions (i.e., NGFW and CDSS) is assumed to need 20% of the implementing staffs' time.
- **Training costs and ongoing management time investment totaling $63,000 over three years.** Palo Alto Networks requires less training than legacy solutions, and interviewees reported that the provided trainings were 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' Prisma SASE annual licensing costs totaling $8.3 million over three years.** The cost for Prisma SASE includes payment for Prisma Access, Prisma SD-WAN hardware appliance, and the subscription, all of which are impacted by the number of branches where it is installed.

The representative interviews and financial analysis found that a composite organization experiences benefits of $18.34 million over three years versus costs of $8.85 million, adding up to a net present value (NPV) of $9.49 million and an ROI of 107%.

Forrester Perspective: Merging Security And Networking Teams

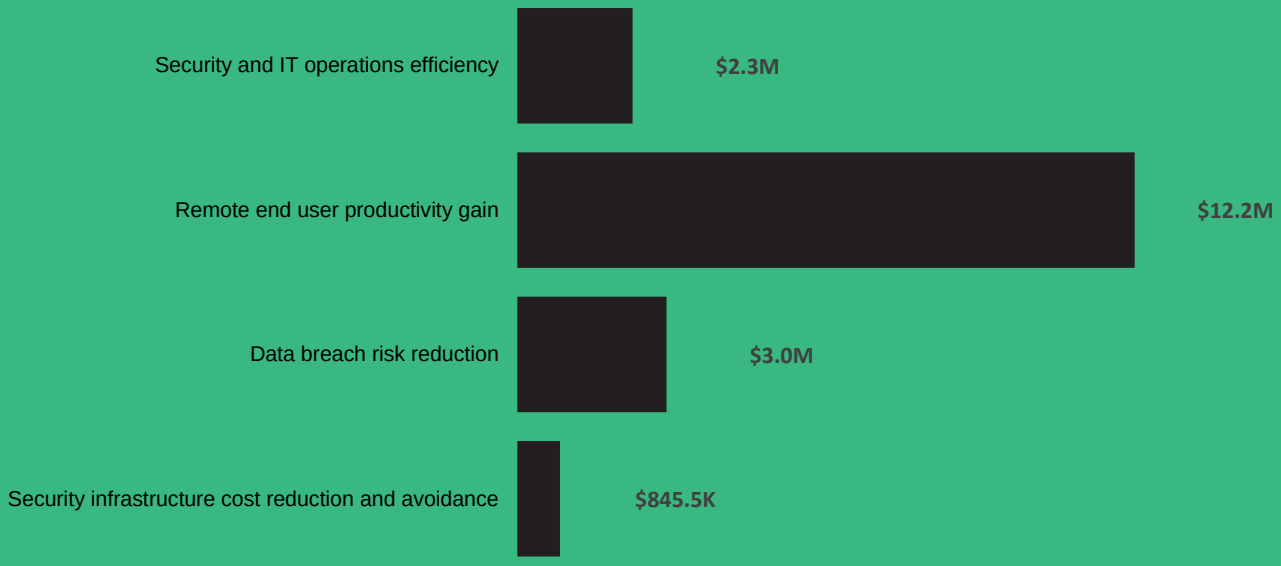
While networking and security have a long and complicated history, having a segregated approach is not an acceptable way to operate as it often sabotages the gains from digital initiatives.

Now a businesswide networking fabric interweaves business assets, customers, partners, and digital assets to connect all parts of the business ecosystem, which can only occur if security is embedded within the DNA of the network.

Source: "Introducing The Zero Trust Edge Architecture For Security And Network Services," Forrester Research, Inc., August 2, 2021.

ROI	BENEFITS PV	NPV	PAYBACK
107%	$18.34M	$9.49M	<6 months

Benefits (Three-Year)



“The productivity that users can achieve, even remotely; not having to worry about integration with other systems; and the level of security we achieve — none of that is possible without Prisma SASE.”

— Principal architect, 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 Prisma SASE.

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 Prisma SASE can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Palo Alto Networks and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Prisma SASE.

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 Prisma SASE Customer Journey

Drivers leading to the Prisma SASE investment

Interviews

Role	Industry	Revenue	Total Employees
Principal architect	Healthcare	$30 billion	15,000
Director of security architecture and engineering	Manufacturing	$17 billion	160,000
SVP of IT	Financial services	$3 billion	3,000
Senior director	Hospitality	$20 billion	380,000

KEY CHALLENGES

Prior to using Prisma SASE, the interviewees told Forrester they typically worked in an environment with inconsistent and incomplete security. They often had to backhaul their network traffic to their data centers for security policy enforcement, which resulted in negative end-user experience. Additionally, scaling into new sites or providing security to hybrid and remote workers was incredibly challenging.

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

- **The need to update security for a modern work environment.** Interviewees shared that the combining factors of growth of remote and hybrid work, adoption of cloud technologies, and cybersecurity attacks becoming increasingly more sophisticated caused them to realize security gaps in their current environment. Finding a more modern and comprehensive security system for their work environment was paramount. The principal architect in healthcare shared, “We hardly have anyone working in office full time, so we rely pretty heavily on Palo Alto networks’ Prisma SASE solutions.”

> **“One of the biggest risks that we have today is the speed of technology adoption and evolutions at 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 of security architecture and engineering, manufacturing*

- **Inconsistency in user experience with impact on productivity.** Interviewees also noted that with their previous environment, they realized a lot of disruption, either caused by cybersecurity threats 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 SVP of IT at a financial services company said: “For a user, using their laptop at home vs. the office the next day are two totally different experiences, [with] different technologies on the back end. This can cause disruption in their workflow such as needing to raise tickets or asking our operations team to investigate what’s happening. If there’s a policy mismatch or a vendor not supporting something the user is trying to do, there is a lot of the productivity cost from that standpoint.”

- **Challenges in scaling their existing security environment.** Finally, interviewees noted how their existing security system was unable to match their business growth. The senior director in hospitality said: “Our organization has grown so much. Having individually managed routers has become a nightmare to manage. Particularly when wanting to make changes to policy — historically, we have to touch every single router in the environment.”

“We had many reliability issues with our traditional VPN before moving to Prisma Access. Constant connection disruption, slow connectivity, high latency — that is a lot of lost time and productivity from an end-user standpoint.”

SVP of IT, financial services

INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that:

- **Could make their security environment more operationally efficient.** Interviewees shared wanting a solution that could either save time, money, or ideally both, which meant more resources that could potentially be repurposed for more strategic work. The principal architect in healthcare shared: “One of the reasons we went with Prisma SASE was that the configuration is 100% in the cloud. We no longer had to rely on data centers or hardware that we cared for.”

  The senior director in the hospitality industry added: “Centralized management and integration with other solutions was the main [factor] in our decision-making process [of choosing Palo Alto Networks].”

- **Had reliability and comprehensiveness in performance.** Interviewees also highlighted performance of the solution as another key factor in their decision-making. The director at a manufacturing company shared: “We chose Palo Alto Networks because they are the best of breed in terms of technology around firewalling. We wanted to bring a good quality of experience for the end user, while keeping security at the max.”

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. 33% of its workforce work remotely or hybrid. It has 400 sites including its headquarters, data center, cloud, branch offices, and retail and manufacturing locations. On average, the composite's security team responds to 1,200 incidents a week, or 62,400 in the first year, with each incident taking an average of 2 hours to resolve.

Deployment characteristics. The organization uses Palo Alto Networks Prisma SASE to connect remote networks at its retail locations and branch offices, as well as its remote and hybrid workers. 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 network security team are involved in deployment.

Key Assumptions

- **$7 billion annual revenue**
- **50,000 employees**
- **33% of employees are remote or hybrid**
- **400 sites**
- **4 data centers**

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	$911,250	$920,363	$929,475	$2,761,088	$2,287,368
Btr	End-user productivity gain	$4,925,580	$4,925,580	$4,925,580	$14,776,740	$12,249,188
Ctr	Data breach risk reduction	$1,189,320	$1,189,320	$1,189,320	$3,567,960	$2,957,663
Dtr	Security infrastructure cost reduction and avoidance	$340,000	$340,000	$340,000	$1,020,000	$845,530
	Total benefits (risk-adjusted)	$7,366,150	$7,375,263	$7,384,375	$22,125,788	$18,339,749

SECURITY AND IT OPERATIONS EFFICIENCY

Evidence and data. Interviewees noted that by moving to Prisma SASE, they were able to ease the load from members of the SecOps and NetOps team. This is a result of the managed service aspect of the solution, as well as various automation of activities that can be implemented in the process.

- The principal architect in healthcare noted: "Previously we would have multiple teams involved in SecOps. There was a software layer, a hardware layer, and an application layer. Today, those three formations have been removed. We only have application SME people. So we can rely on one or two people vs. five to 10."
- Highlighting the ease of scaling, the same interviewee told Forrester: "Scaling is a lot easier. The same policies apply. Scaling is done automatically. Without PANW, we would have to add additional gateways ourselves. We would have to increase back-end systems that deal with databases and all the back-office processing that comes with that."
- The director in manufacturing shared: "In terms of making policy changes, we went from four business days to less than 1 hour. We make around 120 changes per day (80% of time)."
- The same director also specifically noted the value their organization received from using ADEM, noting: "My networking team use ADEM for each time they receive a ticket from the help desk or the service desk around network latency. They use ADEM to understand where the problem is."
- The senior director at a hospitality company said: "With SD-WAN, setting up is a single push.

> **"Prisma SASE is a managed service at its core. It's not something that we have to keep our eyes on every day. We don't have to worry about the system, the gateways, or network latency. All that is no longer our concern."**
>
> *Principal architect, healthcare*

That's minutes or hours vs. weeks of multiple people's time. Previously, it was easily five or six people working through changes like that over a two-week period. We do two to three change cycles per quarter."

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

- The organization has 20 employees who are part of the SecOps organization and 12 employees who are part of the NetOps organization.
- The average SecOps employee spends 80% of their time (relative to their other work) managing tools and making policy changes. They spend another 10% of their time responding to security incidents.
- The efficiency gain for the SecOps team for their work due to using the Prisma SASE solution is 75% time savings.
- The average NetOps employee spends 25% of their time (relative to their other work) on scaling and setting up new sites.
- The efficiency gain for the NetOps team for their work due to using Prisma SASE is 80% of their time in Year 1. This grows to 85% in Year 2 and 90% in Year 3.
- The average annual fully burdened salary of a SecOps employee is $121,500, while a NetOps employee's is $135,000.
- A 50% productivity recapture rate is introduced, assuming that not all time saved will be reintroduced as additional productivity by the employee.

Risks. The exact benefit an organization receives in this regard may depend on:

- The size and skill set of an organization's security management team.
- The capabilities and systems that are in place before deploying Prisma SASE.
- The complexity of the security environment.
- The number of security incidents that require manual intervention before implementing Prisma SASE.
- The other tools and solutions implemented to support the work of the SecOps and IT ops team.
- The average salary of the SecOps and NetOps teams.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.3 million.

Security And IT Operations Efficiency

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Size of SecOps organization (FTEs)	Composite	20	20	20
A2	Percentage of time managing tools and making policy changes	Composite	80%	80%	80%
A3	Percentage of efficiency gain due to Prisma SASE	Interviews	75%	75%	75%
A4	Subtotal: Total time savings in managing tool and making policy changes (in FTEs)	A1*A2*A3	12	12	12
A5	Percentage of time responding to security incidents	Composite	10%	10%	10%
A6	Percentage of efficiency gain due to Prisma SASE	Interviews	75%	75%	75%
A7	Subtotal: Total time savings in responding to security incidents (FTEs)	A1*A5*A6	2	2	2
A8	Average fully burdened annual salary of SecOps employee	TEI standard	$121,500	$121,500	$121,500
A9	Subtotal: Total value of SecOps organization efficiency gain	(A4+A7)*A8	$1,701,000	$1,701,000	$1,701,000
A10	Size of NetOps organization (FTEs)	Composite	12	12	12
A11	Percentage of time spent to scaling and setting up new sites	Composite	25%	25%	25%
A12	Percentage of efficiency gain due to Prisma SASE	Interviews	80%	85%	90%
A13	Average fully burdened annual salary of NetOps employee	TEI standard	$135,000	$135,000	$135,000
A14	Subtotal: Total value of NetOps organization efficiency gain	A10*A11*A12*A13	$324,000	$344,250	$364,500
A15	Productivity recapture	TEI standard	50%	50%	50%
At	Security and IT operations efficiency	(A9+A14)*A15	$1,012,500	$1,022,625	$1,032,750
	Risk adjustment	↓10%			
Atr	Security and IT operations efficiency (risk-adjusted)		$911,250	$920,363	$929,475
	Three-year total: $2,761,088			**Three-year present value: $2,287,368**	

END-USER PRODUCTIVITY GAIN

Evidence and data. Interviewees noted that prior to using Prisma SASE, their previous security environment would sometime disrupt work done by business and end users. Sometimes this could be through investigation procedures that were too disruptive. Other times, security gaps that existed in the legacy environment resulted in cybersecurity attacks that could significantly disrupt employee productivity, especially those that work remotely.

- The SVP of IT in financial services told Forrester: "I'm 100% remote or hybrid, and there's still that percentage where they are at home. So having the same infrastructure to support that is still critical today, working three days in the office and two days at home. Those two days, everything needs to work seamlessly between when they float between: If they take a laptop, then they float from at home vs. when they float to the office and it uses on the back end different infrastructure then the office-use hardware firewall."
- The principal architect in healthcare added: "If [our employees] get attacked, they are unable to perform their work. We had an outage on a weekend because [our previous vendor] did an upgrade that wasn't completely tested. It removed our ability to connect to our network. Nobody could do anything for 8 hours."

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

- There are 50,000 employees.
- Thirty-three percent of all employees work in a remote or hybrid situation.
- Fifty percent of all employees work directly with cloud products, which are assumed to be most affected by Palo Alto Networks' solutions.
- During any system downtime, 20% 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 assumed to be $87,750.
- The composite organization recaptures 50% of the efficiency gains for productive work.

Risks. The exact benefit an organization receives in this regard 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 15%, yielding a three-year, risk-adjusted total PV of $12.2 million.

End-User Productivity Gain

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Total employees	Composite	50,000	50,000	50,000
B2	Percentage of remote/hybrid workers	Composite	33%	33%	33%
B3	Percentage of work done in the cloud	Composite	50%	50%	50%
B4	Percentage of end users impacted by system downtime	Composite	20%	20%	20%
B5	Percentage of time recaptured due to better availability/less downtime	Interviews	8%	8%	8%
B6	Average fully burdened annual salary for a business user	TEI standard	$87,750	$87,750	$87,750
B7	Productivity recapture	TEI standard	50%	50%	50%
Bt	End-user productivity gain	B1*B2*B3*B4*B5*B6*B7	$5,794,800	$5,794,800	$5,794,800
	Risk adjustment	↓15%			
Btr	End-user productivity gain (risk-adjusted)		$4,925,580	$4,925,580	$4,925,580
	Three-year total: $14,776,740			**Three-year present value: $12,249,188**	

DATA BREACH RISK REDUCTION

Evidence and data. The reduced complexity of the security environment also means reduced security risk. Whereas in their previous environment, the different point solutions didn't integrate well or talk to each other, creating potential security gaps that could lead to an increased risk of data breach, using Prisma SASE significantly reduced that risk. This was even more substantial among organizations with remote and/or hybrid workers.

- The principal architect in healthcare told Forrester: "Being able to offer services in a secure manner by having what we consider full visibility into user activities"
- The director in manufacturing noted: "Having the security perimeter be around the user instead of a closed location reduces the risk"
- The SVP of IT at a financial services company shared: "One of the value is security posture and the ability to identify what traffic is going out. Being able to easily monitor internet traffic and see what is happening on the network"

"Without PANW, we would be exposed to different kinds of attacks. When on-prem, people are behind a firewall. Now, with people remote or abroad, you lose that. Tools like Prisma SASE allow you to continue to have the same level of visibility, control, and protection."

Principal architect, healthcare

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

- According to Forrester data, the composite organization can expect to experience an average of 3.2 breaches per year when relying on point solutions.[2]
- Forrester models the cost of a breach by employee count at organizations. For the composite, this is $53 per employee, not counting the loss of worker productivity.[3] The costs include:
  - Fines to regulatory bodies.
  - Customer reimbursement/lawsuits.
  - Incident response and remediation.
  - Lost revenues.
  - Brand equity rebuild costs.
  - Cost of customer reacquisition.
- With Prisma SASE, organizations can expect to reduce the likelihood of a data breach by up to 50% after three years.
- An attribution to Prisma SASE equals the percentage of remote employees at the organization, which is 33%-.

Risks. The exact benefit an organization receives in this regard 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 associated downtime.
- The average salary for business users.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $3 million.

Data Breach Risk Reduction

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average data breaches per year	Forrester research	3.2	3.2	3.2
C2	Total employees	B1	50,000	50,000	50,000
C3	Average potential cost of data breach per employee, excluding internal user downtime	Forrester research	$53	$53	$53
C4	Reduced likelihood of a breach	Interviews	50%	50%	50%
C5	Attribution to Prisma SASE	B2	33%	33%	33%
Ct	Data breach risk reduction	C1*C2*C3*C4*C5	$1,399,200	$1,399,200	$1,399,200
	Risk adjustment	↓15%			
Ctr	Data breach risk reduction (risk-adjusted)		$1,189,320	$1,189,320	$1,189,320
	Three-year total: $3,567,960			**Three-year present value: $2,957,663**	

SECURITY AND NETWORKING INFRASTRUCTURE COST REDUCTION AND AVOIDANCE

Evidence and data. Interviewees noted that the different solutions and functionalities that they receive as a result of their investment in Prisma SASE meant being able to reduce or retire a percentage of their annual security and networking tech spend.

- The principal architect in healthcare explained all the different solutions from their organization's legacy environment that they were able to retire related to their Prisma SASE investment, telling Forrester: "We had a specific product for remote access. Then, we had what we call our H-security, or the secure gateway. That's the security for remote users. And then data loss prevention (DLP) was a separate system. These were three distinct things, separate solutions, that required different expertise, different teams. Now, it's all blended."
- The director in manufacturing added: "I was able to retire my web proxy vendor, among others. That saving was in the millions of dollars on an annual basis."

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' Prisma SASE represents 5% of the annual security tech spend.

Risks. The exact benefit an organization receives in this regard 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 $846,000.

> **"With Prisma SASE, you have one platform that does multiple things. We were able to consolidate three different solutions into one. Dollarwise, that is a significant cost saving."**
>
> *Principal architect, healthcare*

Security And Networking 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 Prisma SASE and SD-WAN	Interviews	5%	5%	5%
Dt	Security and networking infrastructure cost reduction and avoidance	D1*D2	$400,000	$400,000	$400,000
	Risk adjustment	↓15%			
Dtr	Security and networking infrastructure cost reduction and avoidance (risk-adjusted)		$340,000	$340,000	$340,000
	Three-year total: $1,020,000			**Three-year present value: $845,530**	

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 one of Prisma SASE's most valuable benefits is the enhanced visibility they now have on the condition, performance, and usage of different parts of the security organization. The principal architect in healthcare shared, "We're able to easily monitor traffic and see what is actually happening on the network."

  The SVP of IT in financial services added: "The attractive thing about Palo Alto Networks was the interface and visibility. The 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."

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

"Having PANW 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 Prisma SASE 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 longstanding impact on a company's performance, its brand, and how it copes with new and emerging threats. The enterprise network architect in The director at a manufacturing company elaborated: "Having Palo Alto Networks prepares you for the rest of the path, which is to integrate more things, such as remote networks, branch offices, CASB, etc. The next generation of tools and features that Palo Alto Networks will introduce allows us to simplify even more the way we do security designs and firewall policies."

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 Comprise 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 flavors of compute and storage infrastructure.

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**
Etr	Internal time investment for installation and deployment	$248,400	$124,200	$62,100	$31,050	$465,750	$435,960
Ftr	Internal time investment for user training and ongoing management	$950	$24,948	$24,948	$24,948	$75,794	$62,992
Gtr	Prisma SASE costs	$162,068	$3,291,750	$3,291,750	$3,291,750	$10,037,318	$8,348,163
	Total costs (risk-adjusted)	$411,418	$3,440,898	$3,378,798	$3,347,748	$10,578,862	$8,847,115

INTERNAL TIME INVESTMENT FOR INSTALLATION AND DEPLOYMENT

Evidence and data. Interviewees noted that deploying Prisma SASE was an involved process, requiring collaboration from different teams at their organizations (IT, SecOps, and NetOps) with the Palo Alto Networks team.

- The principal architect at a healthcare organization shared their setup process, telling Forrester: “After evaluating different vendors and choosing Palo Alto Networks, we set up the entire solution in one year. We had multiple teams participate from IT security, compliance, and network. We also involved the desktop support team for the deployment of agent. So in total, about 10 to 20 people dedicated about 50% of their time [to the implementation].”
- The director in manufacturing added: “We had someone from my networking team as well as the IT team. The first couple days, this was 50% of their time because most of the work was done by the Palo Alto Networks people. As soon as the tenant on the cloud was ready to use, the work became 100% of my team’s time.”
- For Prisma SD-WAN deployment, the senior director at a hospitality company shared: “We had a number of people focused on deployment full time. If done efficiently, this work can be completed with 16 to 18 people actively working on the project. The majority of them are network people, with some engineers.”

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

- For the entire Palo Alto Networks 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 loaded annual salary for a network operations employee is $135,000.
- Since organizations typically deploy Prisma SASE in conjunction with other Palo Alto

Networks solutions, the model assumes that the composite takes 20% of the total installation and deployment time for Prisma SASE.

Risks. The exact cost an organization incurs in this regard may depend on:

- The skill set of the involved internal employees.
- The complexity of the legacy environment.
- The annual salary of the involved internal employees.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $436,000.

Internal Time Investment For Installation And Deployment

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Network team working on PAN installation	Composite	10	10	10	10
E2	Time spent per network team member	Interview	80%	40%	20%	10%
E3	Annual salary: NetOps employee	TEI standard	$135,000	$135,000	$135,000	$135,000
E4	Percentage attribution to Prisma SASE	Interviews	20%	20%	20%	20%
Et	Internal time investment for installation and deployment	E1*E2*E3*E4	$216,000	$108,000	$54,000	$27,000
	Risk adjustment	↑15%				
Etr	Internal time investment for installation and deployment (risk-adjusted)		$248,400	$124,200	$62,100	$31,050
	Three-year total: $465,750			**Three-year present value: $435,960**		

INTERNAL TIME INVESTMENT FOR USER TRAINING AND ONGOING MANAGEMENT

Evidence and data. Once set up, interviewees noted varying degrees of what ongoing management would look like for Prisma SASE. For some, it was an easy platform to monitor, while others spent additional time and investment to ensure that they fully maximize what the solution has to offer for their organizations.

- The principal architect noted: “We have one or two people manning the tool to respond to policy change requests and monitor alerts. A lot of it is security application layer work.”
- The director at a manufacturing company added, “For ongoing management of Prisma SASE, I would estimate [that it involves] 10% of my team’s time. It’s really easy to operate.”
- For Prisma SD-WAN, the senior director at a hospitality company told Forrester: “We do periodic meetings with the Palo Alto Networks team to understand how their platform evolves. We exchange lessons and challenges if they exist. We have a team focused on maintaining the platform as well as another team focused on optimizing the platform.”

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

- A total of 20 hours of training is required for employees new to Palo Alto Networks. In subsequent years, 8 hours of training is required to share any new features, updates, and enhancements.
- The average fully loaded hourly 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 Prisma SASE.
- Since organizations manage NGFW and CDSS together, the model assumes that 20% of the total time spent for ongoing management is for Prisma SASE.

Risks. The exact cost an organization incurs in this regard may depend on:

- The IT organization’s size and 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**
F1	FTEs receiving training for ongoing management	Composite	10	10	10	10
F2	Hours per training session	Interviews	8	2	2	2
F3	Average fully hourly salary per IT org employee (including SecOps, NetOps, and IT operations)	TEI standard	$54	$54	$54	$54
F4	Internal time investment for user training	F1*F2*F3	$4,320	$1,080	$1,080	$1,080
F5	Percentage of time spent for ongoing management	Interviews		10%	10%	10%
F6	Value of internal time investment for ongoing management	F1*F3*2,080*F5		$112,320	$112,320	$112,320
F7	Attribution to Prisma SASE	Interviews	$0	20%	20%	20%
Ft	Internal time investment for user training and ongoing management	(F4+F6)*F7	$864	$22,680	$22,680	$22,680
	Risk adjustment	↑10%				
Ftr	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**		

PRISMA SASE COSTS

Evidence and data. The interviewees purchased hardware upfront and were able to amortize the subscription costs over the three-year contract term, providing predictable annual costs.

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

- Annual costs include both the hardware that needs to be purchased and the subscription fees for the solution.
- Subscription contracts are amortized over the three-year term.
- Pricing may vary. Contact Palo Alto Networks for additional details

Risks. The exact cost an organization incurs in this regard may depend on:

- The number of users and sites where the solution will be implemented.
- Specific add-ons that should be implemented to further strengthen performance.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $8.3 million.

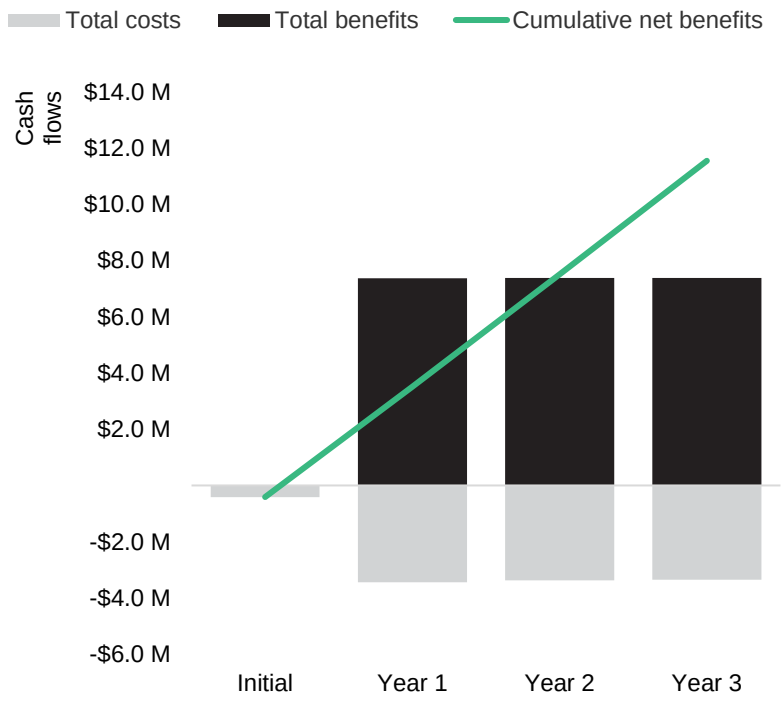
Prisma SASE Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Annual cost for Prisma SASE	Composite	$154,350	$3,135,000	$3,135,000	$3,135,000
Gt	Prisma SASE costs	G1	$154,350	$3,135,000	$3,135,000	$3,135,000
	Risk adjustment	↑5%				
Gtr	Prisma SASE costs (risk-adjusted)		$162,068	$3,291,750	$3,291,750	$3,291,750
	Three-year total: $10,037,318			**Three-year present value: $8,348,163**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($411,418)	($3,440,898)	($3,378,798)	($3,347,748)	($10,578,862)	($8,847,115)
Total benefits	$0	$7,366,150	$7,375,263	$7,384,375	$22,125,788	$18,339,749
Net benefits	($411,418)	$3,925,252	$3,996,465	$4,036,627	$11,546,926	$9,492,634
ROI						107%
Payback period						<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

"Introducing The Zero Trust Edge Architecture For Security And Network Services," Forrester Research, Inc., August 2, 2023

Appendix C: Endnotes

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

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

[3] Ibid.


FORRESTER®