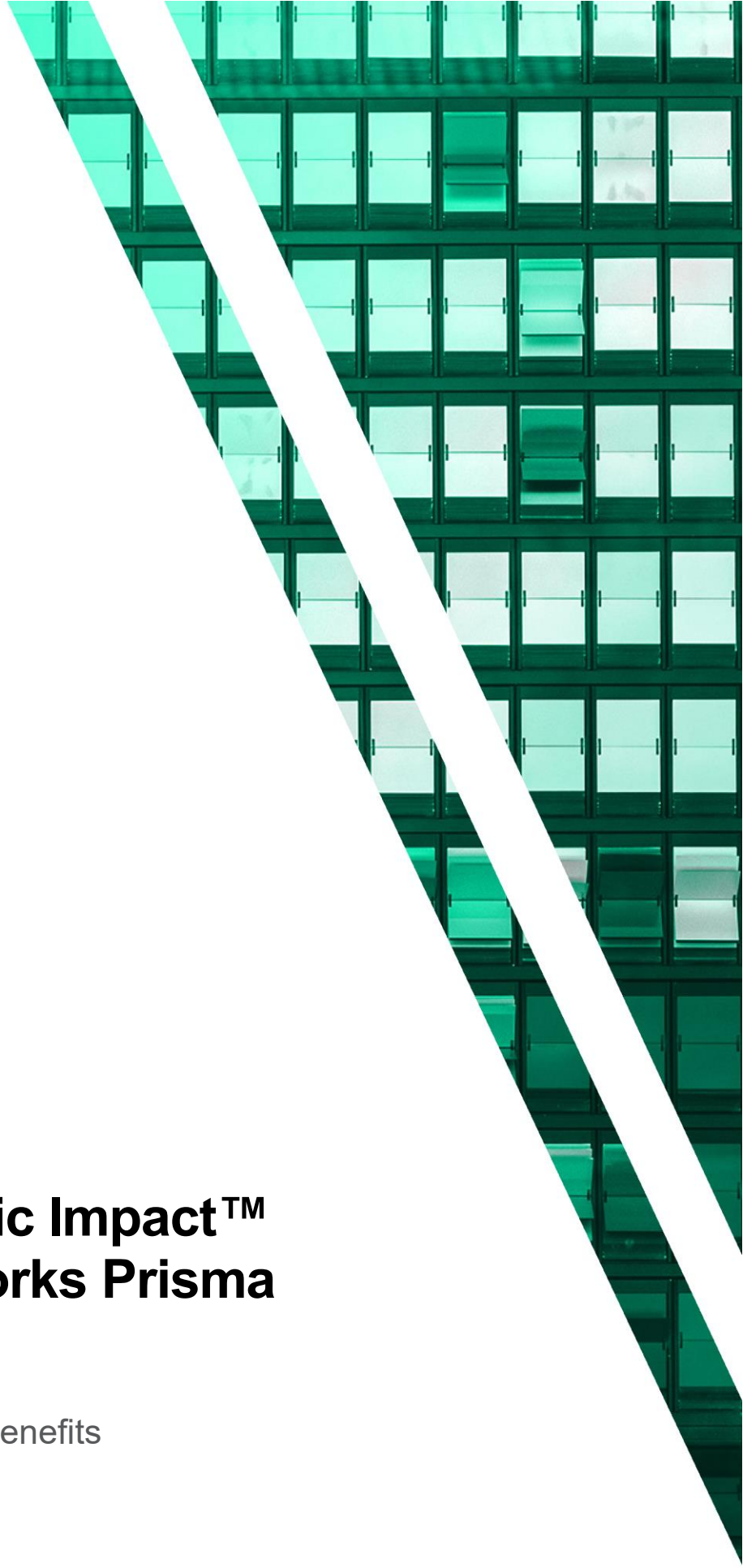
FORRESTER®



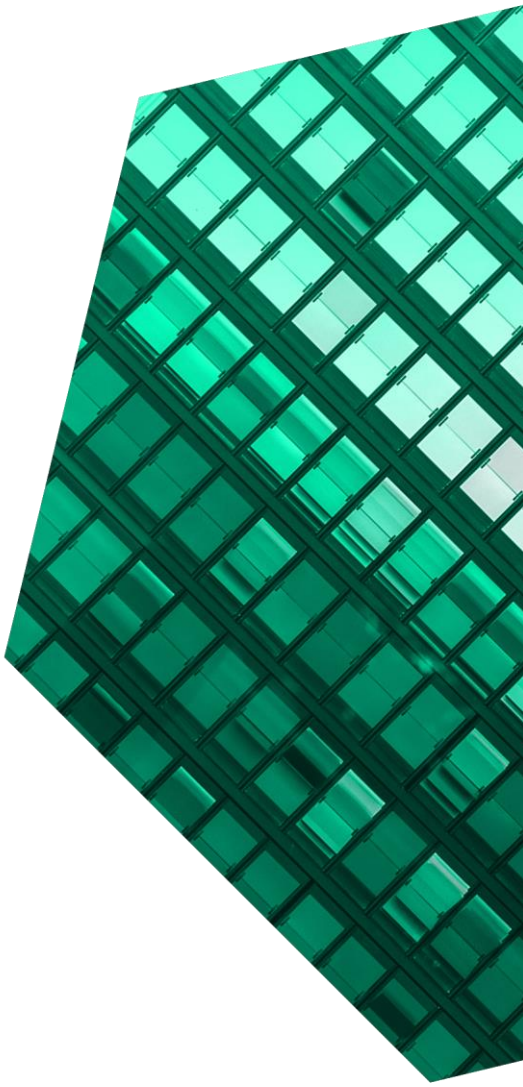
The Total Economic Impact™ Of Palo Alto Networks Prisma Cloud

Cost Savings And Business Benefits Enabled By Prisma Cloud

DECEMBER 2023

Table Of Contents

Consulting Team: Henry Huang
Marianne Friis
Luca Son



ABOUT FORRESTER CONSULTING

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

Executive Summary

Cloud technology gives companies the power to scale and adapt at speed, driving business agility, streamlining operations, and accelerating innovation. But increased reliance on the cloud and the explosive growth of cloud application development driven by AI also increase risk. Cloud security requires the use of a code to cloud platform that can eliminate vulnerabilities in development and stop exploits in runtime before they lead to a breach.

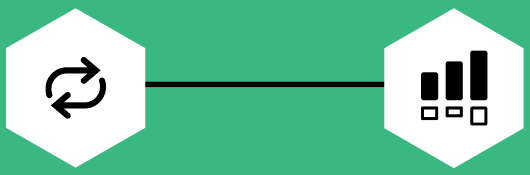
Palo Alto Networks Prisma Cloud is a cloud-native application protection platform (CNAPP) that secures applications and services across multicloud, hybrid, and private environments. It begins at the coding stage with early-stage code and pipeline scanning throughout the application lifecycle and through runtime, bringing security operations (SecOps) together with developers. The platform gives a single source of security posture state to both SecOps and developers. This combination provides visibility across development environments, accounts, and applications by monitoring and detecting threats across the clouds for a full code to cloud security platform covering cloud security posture, permissions, workloads, and detection.

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 Cloud.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Prisma Cloud on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Prisma Cloud. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization of 15,000 employees operating globally.

Prior to using Prisma Cloud, these interviewees noted how their organizations worked in a hybrid environment with assets spread across on-premises and the cloud. Having moved recently to multiple clouds, however, many of these organizations faced the issues of 1) securing these assets with proper posture management, and 2) making sure that their newly developed services, APIs, and applications that reside in the cloud are secure. There simply was not a solution to bring together cloud security management for the interviewees' organizations.

KEY STATISTICS



Return on investment (ROI)
264%

Net present value (NPV)
$6.9M

Reduction of SecOps team effort to investigate incidents
48%

After the investment in Prisma Cloud, the interviewees were able to consolidate their management of cloud security as well as secure new code developed for the cloud. Key results from the investment include the reduction of SecOps effort, reduction of DevOps effort, and a direct reduction in possible breach costs.

KEY FINDINGS

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

- **SecOps team efficiency lift for cloud enforcement.** Security professionals reduce the time they spend on cloud security investigations by 48%. Additionally, their time spent configuring and enforcing policies across multiple clouds becomes drastically easier, leading to an 80% reduction in time spent on those activities. The efficiency gained from both time savings over three years is equivalent to $3.5 million.
- **DevOps productivity lift from adopting shift-left security.** Developers collaborate with SecOps using Prisma Cloud to catch vulnerabilities during the coding stage, enabling the rise of DevSecOps. With the shift-left of security before the deployment stage, issues are eliminated, reducing the need for rework and potential future security incidents. DevOps reduces the time needed to address vulnerabilities by 60%, giving developers more time to focus on product changes rather than security issues prior to each product release. The value of reduced rework is $1.8 million over a three-year period.
- **Material breach risk reduction savings.** Risk and attack surfaces increase as the composite organization expands across clouds, where controls over security measures are more complicated than in traditional on-premises environments. With Prisma Cloud, risk is reduced for large-scale data breaches, which affect not only external customers and the organization's credibility but also the productivity of internal workers who avoid time-consuming incident response and downtime. The reduction is valued at $2.8 million over three years.
- **Compliance efficiencies uplift for reporting.** Consolidating security solutions and showing security posture in one place creates a significant efficiency boon for compliance professionals. The time to produce and verify reports alone is reduced by 90%, and audit times are reduced by up to 67%. Savings over the course of three years is $1.3 million.

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

- **Consolidation of tools.** Prisma Cloud allowed organizations to reduce tool sprawl by consolidating solutions. This improved operational efficiencies and reduced costs by eliminating licensing and training costs for multiple point products and improving time to issue remediation.
- **Ability to scale easily across multiple clouds.** Servicing policies and entitlements with Prisma Cloud is easy for organizations because security teams can deliver once and apply them to many scenarios. This provides further efficiencies when expanding to additional clouds.
- **Integration with the entire security stack.** Security assets do not operate in a vacuum, and thus, they need to integrate with other pieces in the stack such as live information feeds, security information and event management (SIEM); endpoint detection and response (EDR); and security orchestration, automation, and response (SOAR) systems. Prisma Cloud integrates quickly and seamlessly with most products on the market.

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

- **Licensing costs.** Pricing for the composite is based on usage. When computed, the estimated cost of licenses inclusive of support is $2.0 million PV.
- **Ongoing costs borne internally.** The cost comprises the increased engagement between SecOps and DevOps. Developers often require the assistance of security operations to support an environment in which code vulnerabilities and misconfigurations are remediated within the software supply chain, before reaching production. These DevSecOps investment costs amount to $550,000 PV.
- **Implementation and training costs.** Prisma Cloud is cloud native and built for the various clouds available today. The composite, therefore, can implement and connect services with minimal training. Total PV costs are $28,000, all accrued in the initial deployment year.

The representative interviews and financial analysis found that a composite organization experiences benefits of $9.4 million over three years versus costs of $2.6 million, adding up to a net present value (NPV) of $6.9 million and an ROI of 264%.

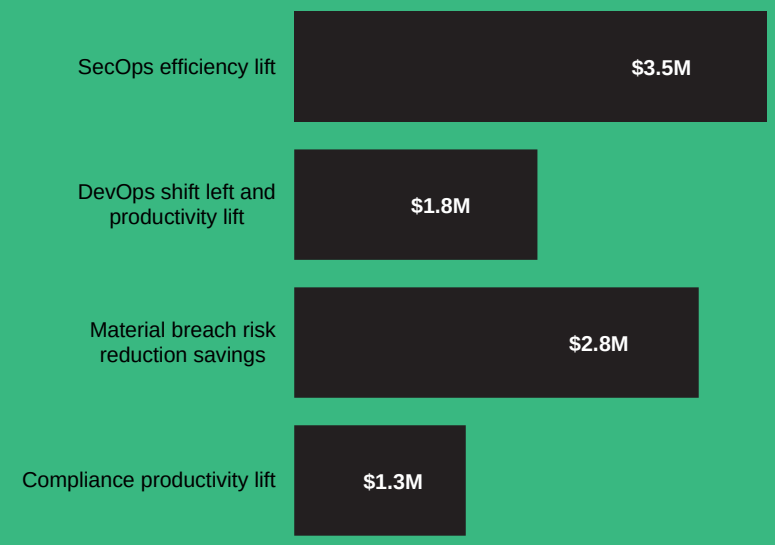
ROI
264%

BENEFITS PV
$9.4M

NPV
$6.9M

PAYBACK
<6 months

Benefits (Three-Year)



SecOps spends 80% less time on policy configuration and enforcement.

DevOps shift left on cloud development activities, reducing rework by 60%.

“There are solutions that provide metrics but not together with remediation capability, code security, and policy enforcement. Prisma Cloud is a couple of years ahead of the game.”

— Senior security analyst, financial services

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 Cloud.

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 Cloud can have on an organization.

DUE DILIGENCE

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

INTERVIEWS

Interviewed four representatives at organizations using Prisma Cloud to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviewees' organizations 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.

The Palo Alto Networks Prisma Cloud Customer Journey

Drivers leading to the Prisma Cloud investment

Interviews			
Role	**Industry**	**Region**	**Revenue**
Cloud security engineer	Healthcare	North America	$1 billion+
Senior security architect	Communication service provider	North America	$10 billion+
Senior security analyst	Financial services	Global	$5 billion+
Cloud manager	Professional services	Global	$100 million+

KEY CHALLENGES

Interviewees' organizations shifted a mounting number of workloads and data toward a multicloud environment, as each cloud presented different value propositions. Frustrations mounted as they realized the difficulty in securing these cloud assets with different cloud providers; by not having a single view of the assets, they were unable to deploy common policies and permissions across clouds. This led to an increased inability to monitor clouds — and thereby mitigate further risks — as they could not properly protect their assets in the cloud.

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

- **Too many clouds and not enough resources.** As their organizations migrated to the cloud, the interviewees realized that the cloud environment existed with multiple vendors. Because of this, they faced the issue of dealing with assets' policies and permissions across multiple, distinct clouds. The interviewees quickly discovered that handling the policies efficiently with each cloud/vendor's specific tools was nearly impossible. This led to stress among security resources as it amplified the effort required to individually manage each cloud environment.

> **"We didn't have the time to budget the money or the internal horsepower to go and get a CSPM [cloud security posture management] tool and a different container tool to solve our cloud problems."**
>
> *Senior security architect, communication service provider*

- **Lack of visibility across cloud assets.** The interviewees described how their organizations struggled with the lack of visibility across the spectrum of assets on different clouds. While they could view assets individually on the clouds, they could not see them collectively across a multicloud environment. The stark lack of visibility created risk factors, compliance issues, and customer-level liabilities.
- **Disconnected point solutions.** Organizations quickly realized that they could not bring together information on cloud threats for a central point of control. Issues resulted from both a disjointed

policy distribution and how the policies were enforced.

- **Lack of cloud and container security management solutions.** While some organizations leveraged point solutions, it was also apparent that others lacked a solution, period. There had been no vulnerability management solution at the container level for some organizations. Similarly, there was no common denominator for cloud security policy management.

"The fact was that Prisma Cloud was a unified platform with potential to add even more capabilities for our future in the cloud — not to mention [being] best of breed as well."

Senior security architect, communication service provider

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Act as a single platform for both development and security teams to foster better communication and collaboration.
- Consolidate cloud policy management into a central platform to support their code to cloud security strategy.
- Reduce the strain on SecOps with new deployments in the cloud for threat management.
- Be cloud-native and live in the cloud to interface with current and new cloud deployments.
- Protect cloud assets and scale with cloud sprawl.

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 is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The Forrester composite is a 15,000-employee global, public organization. It has numerous regulatory entities that oversee its operations. The anticipated strategy is to quickly move the organization to the cloud to not only be able to save on capital expenses but also to provide service to its distributed workforce across regions and work-from-home employees. The expectation is that SecOps will deploy 10 FTEs in the initial year, which ramps up to 20 due to newly created cloud workloads.

Key Assumptions

- **Global organization**
- **Revenue of >$10B**
- **15,000 FTEs**
- **200+ developers**
- **10+ SecOps FTEs dedicated to cloud security**
- **Heavy shift from on-prem to cloud delivery**

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	SecOps efficiency lift	$994,410	$1,346,766	$2,023,724	$4,364,900	$3,537,493
Btr	DevOps shift left and productivity lift	$468,874	$703,310	$1,062,781	$2,234,965	$1,805,980
Ctr	Material breach risk reduction savings	$668,109	$1,111,027	$1,731,859	$3,510,995	$2,826,747
Dtr	Compliance productivity lift	$501,648	$510,029	$522,600	$1,534,278	$1,270,193
	Total benefits (risk-adjusted)	$2,633,041	$3,671,133	$5,340,964	$11,645,138	$9,440,413

SECOPS EFFICIENCY LIFT

Evidence and data. The largest and perhaps most important benefit realized by the interviewees' organizations was the efficiency created for security professionals. The interviewees shared the following ways their respective SecOps teams benefited from the deployment of Prisma Cloud.

- In general, organizations were moving quickly to the cloud. Application and service delivery were shifting rapidly, especially considering the trend of moving from capital expenditure to operational expenditure with a more flexible cost model.
- A reduction in effort to manage a multicloud operation from a security perspective was necessary, especially as security operations personnel were difficult to hire. Those who leveraged multicloud environments especially saw this benefit. Deploying across multiple clouds simply was not possible with existing resources. A cloud security engineer at a healthcare company illustrated this point further, sharing, "You would need [a minimum of] three full-time people to do the work that Prisma covers."
- Utilizing Prisma Cloud, the SecOps team was able to save 48% of their work effort on defending cloud assets, attributed to the centralization of security information.
- A reduction in tools to amass the alert information made it easier to both manage and onboard new SecOps personnel as the organization changed over the years. Additionally, a single tool better identified and prioritized critical alerts and attack paths.
- Capturing vulnerabilities and misconfigurations in development so they never reach runtime saved significant SecOps time and reduced alert distraction.
- Having to deal with multiple vendors for cloud security was wasteful — not only on the procurement side but also on a continual engagement perspective. With Prisma Cloud,

Reduction in SecOps time configuring/enforcing policies

80%

interviewee organizations consolidated their vendor management.

- The senior security architect at a communication service provider said: “How many people am I going to need to implement these tools? How much time are product owners or service owners going to need to spend on three different platforms with three different vendors? We talk once a week with Palo Alto Networks and address things all at once.”

“There was no way we could manage 100 accounts without a tool like Prisma Cloud. It simply would not happen. The type of automated scanning and protecting is just not feasible without Prisma Cloud.”

Cloud security engineer, healthcare

Modeling and assumptions. Forrester modeled this benefit category based upon the customer interviews and the following additional factors:

- The composite organization increases its percentage of workloads and applications moving from on-premises to the cloud. Cloud workloads are expected to rise, with the percentage of workloads in the cloud moving from 30% in Year 1 to 68% by Year 3, when organizations expect the shift to stabilize.
- Policy deployment and enforcement are distributed from Prisma Cloud to all clouds in use.
- The composite organization is underequipped to handle the surge of cloud infrastructure investment in its legacy environment. As a result, it faces 9,900 severe cloud security incidents in the backlog, requiring manual investigation in Year 1. Without Prisma Cloud to consolidate cloud security solutions and shift proactive security measures left, the number of projected incidents scales to 14,850 in Year 2 and to 22,440 in Year 3.
- Forrester research finds that the average amount of time spent per investigation is 3.7 hours.[2]
- There is a 48% reduction in SecOps effort required to investigate incidents with Prisma Cloud.
- The composite organization’s SecOps team recaptures 90% of its productivity with Prisma Cloud as cloud security operations face a continuously growing number of demands.
- The average fully burdened hourly rate for a member of the SecOps team is $62.
- The SecOps team spends 4,160 hours configuring and enforcing policies in Year 1. Due to economies of scale, this reduces to 832 hours in Years 2 and 3.
- The composite organization sees an 80% reduction in time spent configuring and enforcing policies with Prisma Cloud.

Risks. Forrester accounts for variability and potential risks that may impact the financial model, including:

- The number of severe-level cloud security incidents that require manual investigations.
- Hourly salaries for the SecOps team.
- The ability for operators to efficiently work on matters without a confluence of tools.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $3.5 million.

SecOps Efficiency Lift

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Percentage of workloads and applications in the cloud	Interviews	30%	45%	68%
A2	Projected number of severe-level cloud security incidents requiring manual investigation or intervention in the legacy environment	Composite	9,900	14,850	22,440
A3	Hours spent per investigation	Forrester research	3.7	3.7	3.7
A4	Reduction in SecOps effort required to investigate incidents with Prisma Cloud	Interviews	48%	48%	48%
A5	Productivity recapture	Assumption	90%	90%	90%
A6	Average fully burdened hourly salary: SecOps (rounded)	TEI standard	$62	$62	$62
A7	Subtotal: Lift in SecOps productivity from reduced incident intervention rate (rounded)	A2*A3*A4*A5*A6	$981,098	$1,471,647	$2,223,822
A8	SecOps hours spent configuring and enforcing policies	Composite	4,160	832	832
A9	Reduction in time spent configuring and enforcing policies with Prisma Cloud	Interviews	80%	80%	80%
A10	Productivity recapture	Assumption	60%	60%	60%
A11	Subtotal: Lift in SecOps productivity from configuring and enforcing policies (rounded)	A8*A9*A10*A6	$123,802	$24,760	$24,760
At	SecOps efficiency lift	A7+A11	$1,104,900	$1,496,407	$2,248,582
	Risk adjustment	↓10%			
Atr	SecOps efficiency lift (risk-adjusted)		$994,410	$1,346,766	$2,023,724
	Three-year total: $4,364,900			**Three-year present value: $3,537,493**	

DEVOPS SHIFT LEFT AND PRODUCTIVITY LIFT

Evidence and data. Palo Alto Networks Prisma Cloud enhanced DevOps' visibility into its cloud development, and by doing so, it helped teams contextualize misconfigurations and vulnerabilities so they could take precise and immediate action. Through Prisma Cloud's scans and alerts, the interviewees' organizations were able to identify and resolve software vulnerabilities in a timely manner.

- Prior to using Prisma Cloud, interviewees shared that their organizations were not mature when it came to corporate cloud security and found it difficult to have knowledgeable internal people to support their organizations' evolving needs. The lack of controls meant security lapses weren't preventable; however, once Prisma Cloud was in place, its scans and hardening checks allowed teams to be more proactive. A senior security analyst at a finance organization stated: "We have [our security tooling] streamlined now with our pipeline. If we want to add a new rule, we just copy and paste a few things and distribute it. It's quick and easy."
- With the addition of Prisma Cloud and its enhanced visibility, SecOps teams were able to provide guidance to DevOps and collaborate on risk mitigation processes. A senior security analyst at a financial services organization shared how the proactive approach enhanced collaboration: "Our work this year is 70% more proactive. We're getting out in front of the development and making sure that we don't have to go back and correct it."
- This same interviewee added that the options to shift left aided in getting stakeholder buy-in on different vulnerabilities their organization faced. They said: "[Before], a developer would do a merge and realize that they had nine different issues that they didn't fix and different vulnerabilities in their packages that needed to be updated. But it's already deployed, and they can't fix it now because they've got an upcoming production release, etc., but this goes on the risk registers. [We would bring this to the executive team] and developed this process where they looked at these retrospective issues. [With Prisma Cloud], we now have a choice. We can either go down the [old] path where it's talked about every week and will be on a list until it gets corrected, or we can fix it before this, which won't go that far and potentially add risk to our deployments. It puts the ball in their court: You're accepting the risk here in going down that path, or you can fix it ahead of time."

> **"We can now fix this prior to things going to production, without having to raise issues to the executive team — this is where our cloud development is at."**
>
> *Senior security analyst, financial services*

- Interviewees also shared how Prisma Cloud helped their DevOps teams gain efficiencies and reallocate their time to value-added tasks. A cloud manager at a professional services organization explained how Prisma Cloud gave their team 35% more efficiency. They shared: "It's a little more than a third of the effort from — jokes aside — meeting reduction. That's a state we know because we track it. We had a meeting reduction [form] and when we filled it out, a third of our meetings were gone because we're not hopping on calls at 6 a.m. [anymore]."

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

- Before implementing Prisma Cloud, DevOps FTEs spend 31,200 hours addressing vulnerabilities and exposures. This scales to 46,800 hours in Year 2 and increases again to 70,720 in Year 3.
- With Prisma Cloud, there is a 10% increase in upfront time spent addressing vulnerabilities early in the software development lifecycle (SDLC).
- With Prisma Cloud, DevOps FTEs save 60% of the time they previously spent addressing vulnerabilities.
- The composite organization's DevOps team recaptures 60% of its productivity.
- The average fully burdened hourly rate of a member of the DevOps team is $68.

Risks. The expected financial impact is subject to risks and variation based on several factors, including:

- The number of hours spent addressing vulnerabilities prior to investing in Prisma Cloud.
- The level of DevOps expertise and training using Prisma Cloud.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.8 million.

"Developers use Prisma Cloud at the IDE level, which prevents faulty code from being released. That is a massive and exciting improvement."

Cloud security engineer, healthcare

"Prisma Cloud helps us find things faster and sooner. We're not expecting breaches, and it's attributed to Palo [Alto Networks] helping us find vulnerabilities before or early so we can remediate faster. We're not playing catchup."

Cloud manager, professional services

DevOps Shift Left And Productivity Lift

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	DevOps time spent addressing vulnerabilities and exposures introduced by new cloud developments (hours)	Composite	31,200	46,800	70,720
B2	Additional shift-left DevOps hours addressing vulnerabilities and exposures earlier in the development lifecycle	Interviews	3,120	4,680	7,072
B3	Reduction in time needed to address vulnerabilities due to shift-left efficiencies enabled by Prisma Cloud	Interviews	60%	60%	60%
B4	Productivity recapture	Assumption	60%	60%	60%
B5	Average fully burdened hourly salary: DevOps (rounded)	TEI standard	$68	$68	$68
Bt	DevOps shift left and productivity lift	(B1*B3*B4*B5)-(B2*B5)	$551,616	$827,424	$1,250,330
	Risk adjustment	↓15%			
Btr	DevOps shift left and productivity lift (risk-adjusted)		$468,874	$703,310	$1,062,781
	Three-year total: $2,234,965			**Three-year present value: $1,805,980**	

MATERIAL BREACH RISK REDUCTION SAVINGS

Evidence and data. Like all companies, the interviewees' organizations rely on software to power their business. But a majority of their codebases include open source software, which left their applications' code at risk due to third-party sources. Palo Alto Networks Prisma Cloud's software composition and infrastructure as code analysis tools significantly reduced the number of vulnerabilities reaching production by helping developers remediate vulnerabilities and keep libraries up to date. The result was increased cloud posture, far fewer alerts, and less misconfiguration risk for security and development teams having to spend time remediating.

- Security was top of mind for the interviewees as software vulnerability exploits were still too easy. For a cloud security engineer at a healthcare company, that risk was too great and was one of the main reasons they invested in Prisma Cloud. They shared: "We have a lot of sensitive data that flies around, so we're extremely security-conscious because of that. ... Every healthcare company must adhere to HITRUST and HIPAA, and we had to take the next steps."
- In Forrester's Security Survey, 2022, 63% of security decision-makers said that their firm's application security budget would increase in 2023.[3] Of those reporting six or more breaches, two-thirds said that their total breach costs exceeded $2 million. For the interviewees, preventative and protective application security measures were considered imperative and worth the investment. A cloud manager at a professional services organization explained: "It helps us find things faster. We're actually not going to have had any breaches, and what we attributed to get this budgeted was [that] Prisma Cloud helps us find vulnerabilities before or early, and we get them remediated faster. We're not playing catchup [where] we have to fix something because it was exploited. We're fixing something because the industry told us this could be exploited, and we take care of it beforehand. Thus far, that has served us well and justifies the cost."

Modeling and assumptions. For the composite organization, Forrester quantifies the impact of significant material data breaches and assumes the following:

- Breaches will happen, and they will sometimes go unnoticed. Forrester defines a breach as an incident resulting in the loss or compromise of data, accompanied by material remediation costs.[4] According to Forrester Consulting's Cost Of A Security Breach Survey, the average number of data breaches per year from cloud workloads in terms of impact ranges from 0.8 in Year 1 to 1.2 in Year 2 and 1.8 in Year 3.[5]
- Forrester models the cost of a material breach by factoring in the following variables:
    - **Regulatory fines.** Additive audit and security compliance costs. Response and notification to affected parties.
    - **Customer compensation, lawsuits, and punitive damage.** Customer churn, the cost of acquiring new customers, and lost revenue from loss of customers.
    - **Lost revenue from system downtime.** The cost to rebuild brand equity.
- With Prisma Cloud, organizations can expect to reduce the likelihood of a data breach by 27% in Years 1 through 3.
- The proportion of employees affected by each data breach are 10% for Year 1, 15% for Year 2, and 17% for Year 3 of total employees due to increased usage of cloud applications and services.
- Each affected employee experiences 3.6 hours of downtime and is salaried at $42 per hour.[6]

Risks. The expected financial impact is subject to risks and variation based on several factors, including:

- The size, industry, region, and other factors of an organization that may impact the value of its data assets or the likelihood of a data breach.
- The severity of a security event, the percentage of employees affected by a breach, the associated downtime duration, and the fully burdened compensation rate for business users.

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.

Material Breach Risk Reduction Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average number of data breaches per year from cloud workloads	Forrester research	0.8	1.2	1.8
C2	Average potential cost of data breach	Forrester research	$3,026,370	$3,026,370	$3,026,370
C3	Reduced likelihood of a cloud data breach with Prisma Cloud	Forrester research	27%	27%	27%
C4	Subtotal: Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs (rounded)	C1*C2*C3	$653,696	$980,544	$1,470,816
C5	Internal business users	Composite	15,000	15,000	15,000
C6	Average percentage of employees affected per breach	Composite	10%	15%	17%
C7	Diminished/eliminated internal user productivity per breach (hours)	Forrester research	3.6	3.6	3.6
C8	Average fully burdened hourly salary: business user (rounded)	TEI standard	$42	$42	$42
C9	Subtotal: Cost of reduced internal productivity	C5*C6*C7*C8*C1	$181,440	$408,240	$694,008
Ct	Material breach risk reduction savings	C4+C9	$835,136	$1,388,784	$2,164,824
	Risk adjustment	↓20%			
Ctr	Material breach risk reduction savings (risk-adjusted)		$668,109	$1,111,027	$1,731,859
	Three-year total: $3,510,995			**Three-year present value: $2,826,747**	

COMPLIANCE PRODUCTIVITY LIFT

Evidence and data. Security compliance reporting is critical to organizations to both understand and comply with standards and avoid fines and associated costs. Interviewees informed Forrester of the following:

- Due to using multiple clouds and a lack of a single point of control, auditing controls and security measures were difficult.
- Reporting was generated within different clouds, necessitating the collation of various permissions and policies.
- Internal audits generally took a month and were hindered by the number of reports and controls that were located in the individual clouds.
- Interviewees said they reduced audit time required from various groups, including internal auditors, external auditors, and DevOps and SecOps, by upward of 90%.

Modeling and assumptions. Forrester models this benefit category based on the customer interviews and the following additional factors:

- The composition of labor expended to address compliance comprises developers, control owners, and auditors. We have grouped auditors as a part of the compliance managers rows in the table below.
- Based on interviews, Forrester assumes that the composite organization is coming from a stance of using point solutions for compliance — often ones provided by the various cloud providers.
- With Prisma Cloud, the composite organization reduces the time to create, review, and consume reporting by 90%.
- External audits and the impact on internal employees are factored in.
- With Prisma Cloud, the composite organization reduces total audit time by 52%.
- The average fully burdened hourly rate for a compliance analyst is $44; for a compliance manager, it is $59.

Risks. Forrester accounts for variability and potential risks that may impact the financial model, including:

- The industry of the organization will dictate the number of regulatory and required audit measures.
- External audits will vary greatly from a cost perspective.
- Controls vary greatly between organizations.

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

> **“Internal audits are now under one week, when it used to be a month. There is no lie there.”**
>
> *Cloud manager, professional services*

Reduction in compliance reporting effort

90%

Compliance Productivity Lift

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	DevOps hours to create and document each control	Interviews	2,560	2,560	2,560
D2	Compliance analyst hours to aggregate, produce, and revise reports	Interviews	6,160	6,160	6,160
D3	Compliance manager hours to consume and validate reports	Assumption	5,280	5,280	5,280
D4	Reduction in time to create, review, and consume reporting with Prisma Cloud	Interviews	90%	90%	90%
D5	Productivity recapture	Composite	70%	70%	70%
D6	Average fully burdened hourly salary: compliance analyst (rounded)	TEI standard	$44	$44	$44
D7	Average fully burdened hourly salary: compliance manager (rounded)	TEI standard	$59	$59	$59
D8	Subtotal: Labor saved from reporting efficiencies (rounded)	[(D1*B5)+(D2*D6)+(D3*D7)]*(D4*D5)	$476,683	$476,683	$476,683
D9	Internal audit events	Composite	4	4	4
D10	Internal auditor FTEs	Composite	5	5	5
D11	Total internal audit hours per event	D10*40 hours	200	200	200
D12	External audit events	Composite	1	1	1
D13	External auditors	Composite	3	3	3
D14	Total external audit hours per event	D13*160 hours	480	480	480
D15	External compliance professional hourly rate	Composite	$250	$250	$250
D16	Reduction in total audit time due to improved evidence tracking, monitoring, and reviewing	Composite	52%	58%	67%
D17	Subtotal: Audit compliance productivity lift	[(D9*D11*D6)+(D12*D14*D15)]*D16	$80,704	$90,016	$103,984
Dt	Compliance productivity lift	D8+D17	$557,387	$566,699	$580,667
	Risk adjustment	↓10%			
Dtr	Compliance productivity lift (risk-adjusted)		$501,648	$510,029	$522,600
	Three-year total: $1,534,278			**Three-year present value: $1,270,193**	

UNQUANTIFIED BENEFITS

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

- **Consolidation of tools.** Prisma Cloud allowed organizations to reduce tool sprawl by consolidating solutions. This improved operational efficiencies and reduced costs.
- **Ability to scale easily across clouds.** Servicing policies and entitlements with Prisma Cloud is easy for organizations because security teams can deliver once and apply to many scenarios. This provides further efficiencies when expanding to additional clouds.
- **Integration with the entire security stack.** Using Prisma Cloud is integral to preventing cloud-based threats. Integrating Prisma Cloud with the existing stack, such as SIEM, further streamlines work for security professionals.

FLEXIBILITY

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

- **Extensibility.** As technology progresses, the importance of a connected stack becomes ever more important. Prisma Cloud connects to multiple solutions should there be a need to shift or adjust portions of the security stack.
- **Third-party compliance.** Organizations are inextricably connected to third parties, many of which are SaaS solutions. Interviewees indicated that the visibility provided made it possible to assess and ensure compliance measures across the value chain.

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

"Knowing that we were going multicloud, even though we're AWS-focused, the features and possibilities that Prisma [Cloud] offered just made sense for us."

Senior security analyst, financial services

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	Licensing costs	$0	$525,289	$787,934	$1,181,900	$2,495,123	$2,016,699
Ftr	Ongoing costs	$0	$141,856	$212,784	$326,269	$680,909	$549,945
Gtr	Implementation and training costs	$27,702	$0	$0	$0	$27,702	$27,702
	Total costs (risk-adjusted)	$27,702	$667,145	$1,000,718	$1,508,169	$3,203,734	$2,594,346

LICENSING COSTS

Evidence and data. Costs for licensing depend on workloads and applications being secured. The following costs from Palo Alto Networks include support and implementation services.

- Interviewees generally spoke of purchasing licensing in advance of anticipated overage to account for surges in growth or usage.
- Costs varied depending on purchase size, but they were generally more favorable in larger units of credits purchased.
- All costs assume a nominal level of discount.

Modeling and assumptions. Forrester models this cost category based upon the following:

- Licensing costs based on the workloads and applications secured for the 15,000-FTE composite organization, with characteristics listed in the Composite Organization section.
- Licensing is charged annually and based on Forrester's estimated rate of cloud usage.
- Pricing may be affected by previous purchases. As displayed, prices do not include consideration for having other Palo Alto Networks products.

Risks. Forrester factors the impact of potential differences that might influence the cost for other organizations. Possible risks include:

- The quantity of cloud workloads and the shift to move to cloud on a maturity basis.
- The level of discount from having other Palo Alto Networks products.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.0 million.

Licensing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Palo Alto Networks Prisma Cloud licensing	Palo Alto Networks		$500,275	$750,413	$1,125,619
Et	Licensing costs	E1	$0	$500,275	$750,413	$1,125,619
	Risk adjustment	↑5%				
Etr	Licensing costs (risk-adjusted)		$0	$525,289	$787,934	$1,181,900
	Three-year total: $2,495,123			**Three-year present value: $2,016,699**		

ONGOING COSTS

Evidence and data. Ongoing costs reflect internally borne costs. Interviewees expressed that:

- There were few ongoing costs from internal teams from a management perspective.
- Refinement of policies and tools on the platform averaged to require approximately 1.5 employees working full time in the steady state.
- While attaining a steady state was reasonably easy for the interviewees' organizations, the transition from existing point solutions took time — with some customers taking as long as six months.

Modeling and assumptions. Forrester models this cost category based upon the following.

- The acceleration to the cloud is assumed and reflected in the number of FTEs required to support the platform and developers.
- The assistance from SecOps to DevOps is reflected already in benefit category A, and as such, it is not duplicated here.

> **"Palo Alto [Networks] has helped us become a proactive cloud security team, which has served us well and justified the cost."**
>
> *Cloud manager, professional services*

Risks. Forrester factors the impact of potential differences that might influence the costs for other organizations. Possible risks include:

- The shift to the cloud is dependent on an organization's overarching strategy and hence can increase costs.
- Variance in cloud environment usage can add to costs, depending on the cloud provider.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $550,000.

Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	SecOps FTEs required to support developers	Interviews		1.0	1.5	2.3
F2	Average fully burdened annual salary: SecOps (rounded)	TEI standard		$128,960	$128,960	$128,960
Ft	Ongoing costs	F1*F2	$0	$128,960	$193,440	$296,608
	Risk adjustment	↑10%				
Ftr	Ongoing costs (risk-adjusted)		$0	$141,856	$212,784	$326,269
	Three-year total: $680,909			**Three-year present value: $549,945**		

IMPLEMENTATION AND TRAINING COSTS

Evidence and data. Interviewees expressed that implementation was not difficult; rather, the costs were borne of adjusting prior policies and permissions to Prisma Cloud. Forrester heard the following:

- Deployment was extremely quick, according to multiple interviewees.
- Training SecOps and DevOps took time for the implementation and deployment — generally between 10 and 20 hours per individual to become proficient.
- The time for DevOps to acclimate to writing code that is vulnerability free with Prisma Cloud is incorporated in Benefit Category A.

Risks. Forrester factors the impact of potential differences that might influence the costs for other organizations. Possible risks include:

- The complexity of applications being built for the cloud requires differing levels of training.
- SecOps maturity and the general state of security, which can affect the length of time to onboard the team.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $28,000.

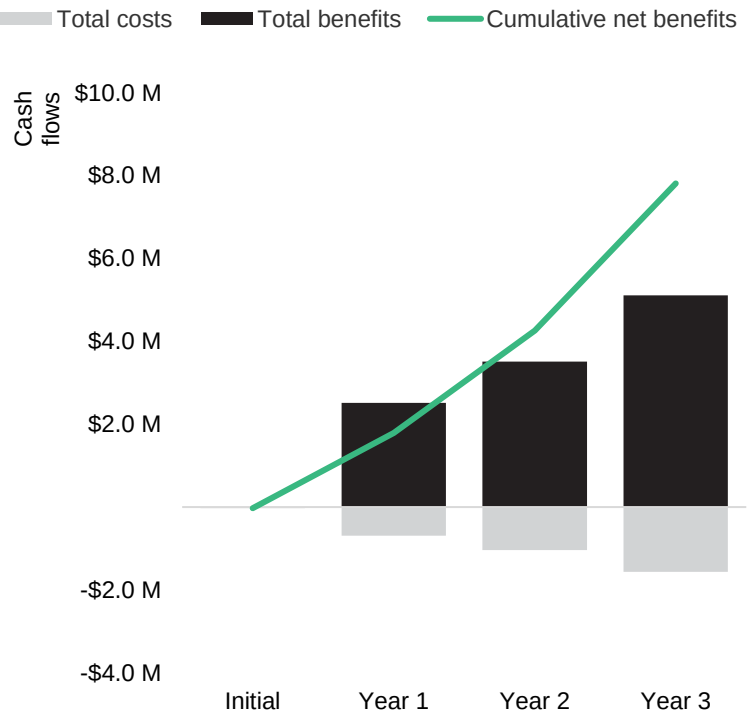
Implementation And Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Planning, implementation, and integration hours	Composite	240			
G2	Average fully burdened hourly salary: SecOps (rounded)	A6	$62			
G3	Subtotal: Planning, implementation, and integration costs	G1*G2	$14,880			
G4	Training hours per FTE	Interviews	16			
G5	SecOps training FTEs	Composite	6			
G6	DevOps training FTEs	Composite	4			
G7	Average fully burdened hourly salary: DevOps (rounded)	B5	$68			
G8	Subtotal: Training costs	(G4*G5*G2)+ (G4*G6*G7)	$10,304			
Gt	Implementation and training costs	G3+G8	$25,184	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Implementation and training costs (risk-adjusted)		$27,702	$0	$0	$0
	Three-year total: $27,702			**Three-year present value: $27,702**		

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	($27,702)	($667,145)	($1,000,718)	($1,508,169)	($3,203,734)	($2,594,346)
Total benefits	$0	$2,633,041	$3,671,133	$5,340,964	$11,645,138	$9,440,413
Net benefits	($27,702)	$1,965,896	$2,670,415	$3,832,795	$8,441,404	$6,846,067
ROI						264%
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: 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 Security Breach Survey, Q4 2020

[3] Source: "Security Survey, 2022," Forrester Research, Inc., September 12, 2022.

[4] Ibid.

[5] Ibid.

[6] Ibid.


FORRESTER®