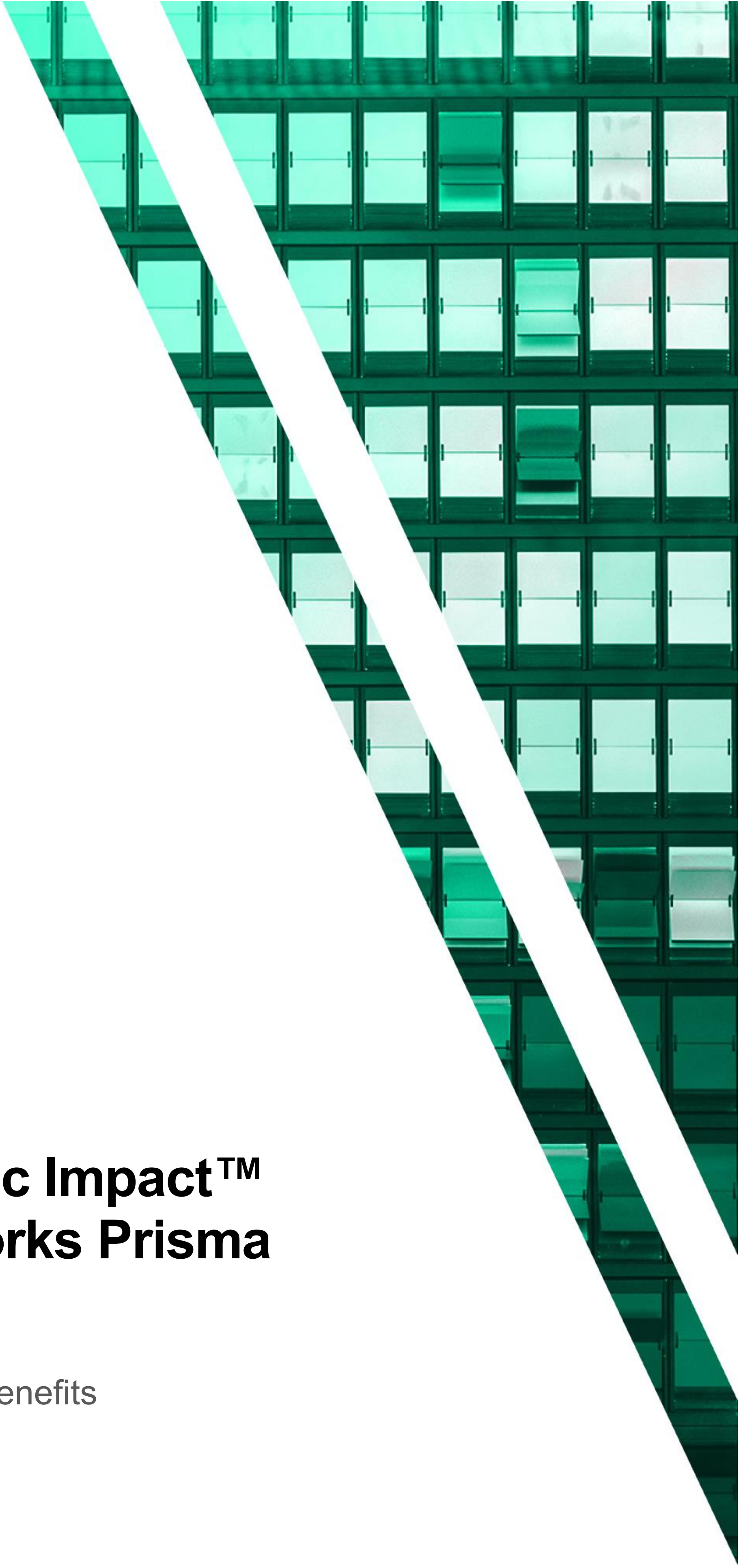
FORRESTER®



The Total Economic Impact™ Of Palo Alto Networks Prisma Cloud

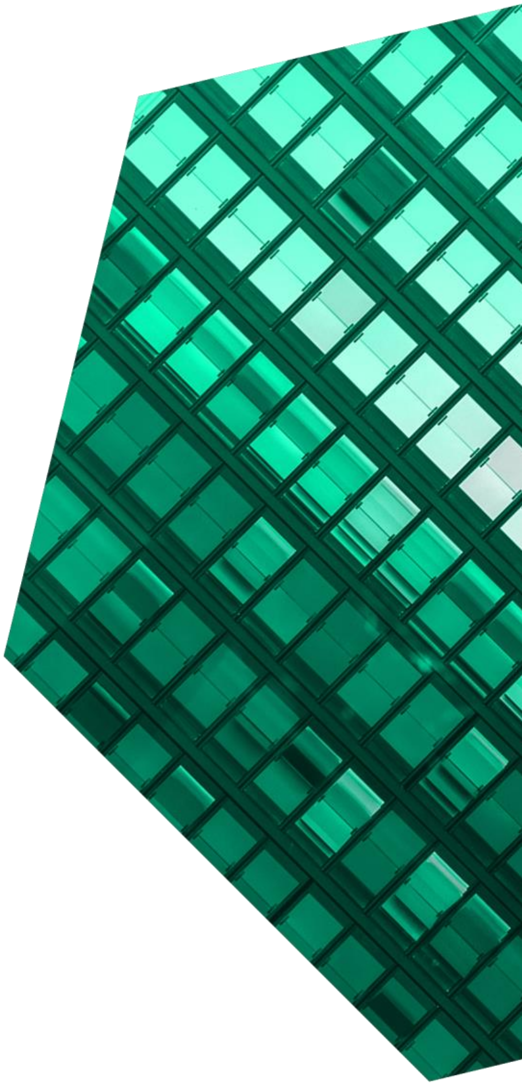
Cost Savings And Business Benefits
Enabled By Prisma Cloud

JUNE 2021

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

Table Of Contents

Consulting Team: *Luca Son*
Henry Huang



Executive Summary

> As organizations seek to modernize and transform their IT infrastructures and operations into the cloud, gaps in cloud visibility arise and attack surfaces widen, which threatens organizational security and compliance. To bridge those gaps, organizations must consider a cloud-native security solution that provides preventative security across clouds, applications, data, networks, and users.

Palo Alto Networks Prisma Cloud is a cloud-native security platform (CNSP) that helps organizations secure cloud infrastructure and cloud-native applications through cloud security-posture monitoring, threat detection and response, and cloud workload protection. Organizations struggle with maintaining visibility as accounts and applications move into the cloud, putting them at risk of having vulnerabilities and misconfigurations exploited by attackers. Prisma Cloud is a comprehensive cloud security solution covering multicloud and hybrid-cloud environments from a centralized location.

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. 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 six decision-makers from five organizations with experience using Prisma Cloud. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

Prior to using Prisma Cloud, the customers had either no solution, third-party point-solutions, or they relied on cloud service provider (CSP) tooling. Prior solutions yielded limited success, leaving the customers with little to no cloud security posture visibility, siloed developer and security processes and teams, and poor compliance and reporting.

KEY STATISTICS

Return on investment (ROI)	Net present value (NPV)
276%	**$5.81M**

After the investment in Prisma Cloud, the customers improved cloud security compliance, transformed security and developer operation agility, reduced the risk of breaches, and improved compliance efficiency.

KEY FINDINGS

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

- **Improved SecOps effort to investigate incidents with Prisma Cloud by 44%.** The increased visibility into cloud security posture gives SecOps professionals continuous visibility, improved risk measurement, it reduces the time needed to distinguish false alerts, and it ultimately improves SecOps efficiency. In addition, out-of-the-box Prisma Cloud policies and custom policy setting features reduce the time spent configuring and enforcing policies by 80%. Over three years, improved SecOps productivity equate to $2.1 million in savings.

- **Improved DevOps efforts fixing vulnerabilities and misconfiguration by 60%.** Prisma Cloud's cloud workload protection facilitates collaboration between SecOps and DevOps, and it allows DevOps to identify and fix vulnerabilities more efficiently before issues reach production environments. By resolving vulnerabilities earlier in the software development life cycle (SDLC), DevOps deploy safer software and avoid vulnerability issues further down in the workstream. DevOps productivity savings account for $1.1 million in savings.
- **Reduced likelihood of significant material data breaches by 27%.** Prisma Cloud reduces the probability of material security breaches that lead to the loss or compromise of data. This helps organizations avoid associated internal and external costs. Avoided costs include business user downtime, costs of remediation, brand rebuilding, customer resolution, and all other external-facing data breach costs. The reduction in risk of material data breaches leads to savings of $3.9 million.
- **Reduced time to create, review, and consume compliance reporting by 90% and improved audit efficiency by up to 64%.** Prisma Cloud allows compliance professionals to create, revise, and review evidence through easily accessible and automated reporting. This enables organizations to avoid manual, ad hoc, and follow-up work. The improved productivity of internal and external compliance professionals saves nearly $840,000.

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

- **Ability to scale cloud security efforts.** Prisma Cloud integrates SecOps and DevOps collaboration and processes. This allows organizations to meet the rising demands of increasing cloud adoption with a more efficient centralized DevSecOps group
- **Ease of integration with other tooling.** Prisma Cloud integrates efficiently with tools such as security information and event management (SIEM), security orchestration, automation, and response (SOAR), and ticketing and reporting applications. This makes information more readily accessible and digestible for security teams.
- **Improved reporting.** Prisma Cloud improves reporting across various functions, from SecOps and DevOps to compliance.
- **Improved implementation time-to-value.** The customers' time to implement and receive value from Prisma Cloud was as short as two weeks.

Costs. Risk-adjusted PV costs include:

- **Licensing costs totaling $1.6 million over three years.** Organizations pay licensing costs depending on their usage.
- **Ongoing costs totaling $437,000 over three years.** Ongoing costs include SecOps labor required to operationalize DevSecOps and to support for DevOps efficiency.
- **Implementation cost totaling $26,000.** Implementation costs include planning, implementation, and integration of Prisma cloud with other tooling.

The customer interviews and financial analysis found that a composite organization experiences benefits of $7.91 million over three years versus costs of $2.10 million, adding up to a net present value (NPV) of $5.81 million and an ROI of 276%.

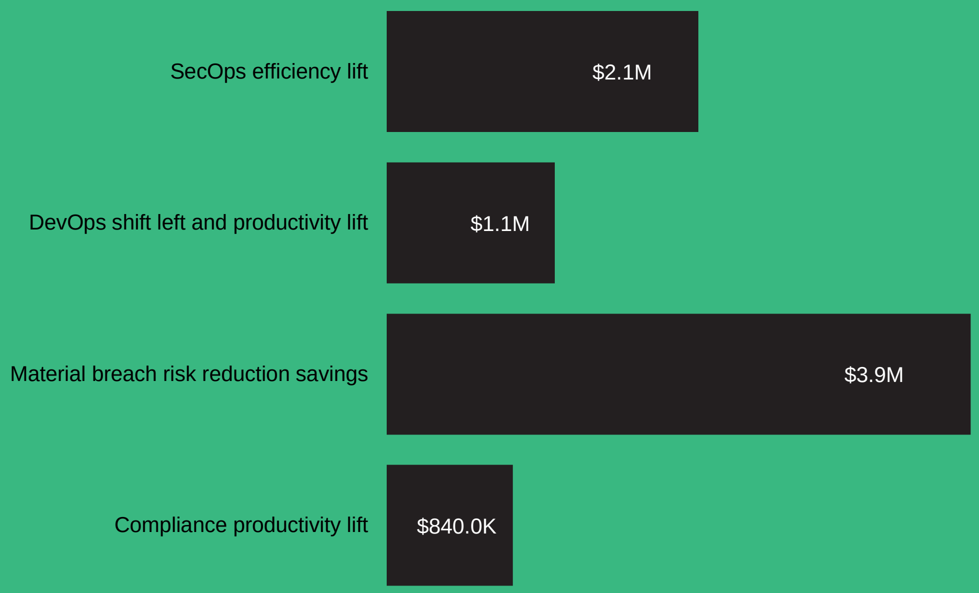
ROI
276%

BENEFITS PV
$7.91M

NPV
$5.81M

PAYBACK
<6 months

Benefits (Three-Year)



> **“Prisma Cloud gives you the [cloud security] visibility that you cannot have with other platforms, especially when you want to diagnose or get into detail of what happened. It pays for the application itself.”**
>
> — Cloud and systems security, automotive

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 the Prisma Cloud.

CUSTOMER INTERVIEWS

Interviewed six decision-makers at organizations using Prisma Cloud to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

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

FINANCIAL MODEL FRAMEWORK

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

CASE STUDY

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

DISCLOSURES

Readers should be aware of the following:

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

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

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 Cloud Customer Journey

🟩 Drivers leading to the Prisma Cloud investment

Interviewed Organizations

Industry	Region	Interviewee(s)	Revenue
Retail	North America HQ, global	Security engineering manager	$25 billion+
Automotive	EMEA HQ, global	Cloud and systems security lead	$10 billion+
Financial technology	EMEA HQ, global	Security architect	$5 billion+
Healthcare	North America HQ, global	Director of product management Senior security architect	$5 billion+
Software	North America HQ, global	Engineering security manager	$1 billion+

KEY CHALLENGES

Forrester interviewed six decision-makers from five organizations with experience using Palo Alto Networks Prisma Cloud. Before investing in Prisma Cloud, the interviewees' organizations had either no prior multicloud security tooling or third-party point solutions, or they leveraged rudimentary CSP-supplied tools with ad hoc policy management. The interviewees' organizations struggled with common challenges, including:

- **Little to no visibility into cloud environments and a lack of security controls.** As the interviewees' organizations increased their cloud footprints, decision-makers noticed a stark lack of visibility into cloud misconfigurations, vulnerabilities, and risks. A security architect at a financial technology organization stated: "Back then, when we had those near misses, we didn't have anything that would tell us what was going on in the cloud. Literally, we had nothing. It was just developers in the cloud doing whatever the heck they wanted to do."

- **Disconnect between security and cloud development teams.** Interviewees said their organizations lacked the right tooling to unify security and DevOps collaboration and processes. For example, without risk visibility into cloud workloads, security teams were unable to provide DevOps guidance. The security architect at the financial technology organization said: "We never had anything to provide answers before Prisma Cloud. There were no reports and no information. Developers were just being told to try not to do bad things."

  A security engineering manager at a retail organization explained: "Our security teams had a lack of control and visibility, especially into the unknown. For example, when development teams would go off and do their own thing, we didn't know what sort of data they were using, what was flowing through the application, what was being stored and where, [and whether or not] there was authentication in front of it, is there encryption at rest, and is there encryption in transit. The scariest part was not having control over the types of data that teams were essentially putting in unsanctioned areas."

> **“We had no good visibility, and we struggled to find a good tool that let us interact with the development teams in a way that made sense to them.”**
>
> *Security engineering manager, retail*

- **Inefficiencies addressing misconfigurations and vulnerable code.** Without tooling to provide constant cloud workload protection, DevOps professionals were at risk of deploying vulnerabilities and misconfigured software into the production environment. This would increase the burden on developer reworks and backlogs.

  A senior security architect in a software organization said: “Our traditional scanners don’t do a lot of scanning activity of the development system. Our security teams were always disconnected from the development organizations, and filtering information to them was never efficient. By the time it got to the development organization, they [would] have many weeks or months of retrace work and backlog. It was an age-old problem.”

- **Poor compliance visibility.** The interviewees’ organizations struggled to maintain sufficient compliance visibility. A cloud and systems security lead at an automotive organization told Forrester: “Our board had zero visibility about what was happening with the cloud deployments. When we did the first report, we were straightforward and told them we were 30% to 35% compliant with our previous security policy. [The board members] were completely flabbergasted.”

- **Inefficient reporting and auditing.** Before investing in Prisma Cloud, the interviewees said their organizations’ reporting was either nonexistent or ridden with inefficiencies. The director of product management at a healthcare organization said: “Before [Prisma Cloud], reporting was all manual and the process effectively didn’t exist. We either were not compliant or we spent hours of ad hoc work per event if we were going to deploy something. Every time we went to go deploy something, it would be a unique event figuring out how to scan stuff for it to be compliant. Emails would fly back and forth and that kind of thing.”

- **Inability to scale security efforts using disjointed legacy tooling.** The security architect at the financial technology organization said their organization’s homegrown solution was unable to meet its cloud security needs. They said: “We’ve come leaps and bounds in the maturity of our cloud deployment. It is now a massively large state to manage. Doing a homegrown solution to collect this data and look for bad things is just not practical on any scale.”

  The interviewees told Forrester that CSP security tooling fell short in capabilities and efficacy. In addition, their organizations could not scale existing tooling across multiple clouds. The senior security architect with the healthcare organization said: “A lot of our previous solution involved static-code scanning. We leveraged a lot of open source [technology], but we found that there was a gap in tooling when it came to container images in the whole container technology stack. When we were looking at the problem, the traditional security vendors just didn’t even have solutions for the most part.”

INVESTMENT OBJECTIVES

The interviewees said their organizations searched for a solution that could improve their efforts to:

- **Improve the digital transformation journey.** Interviewees said their organizations looked to Prisma Cloud to ensure the secure and successful migration and creation of workloads and applications into multicloud environments. The engineering security manager at the software company told Forrester: "[My organization] is only just dipping its toes in the multicloud environment. The expectation is to eventually to be multicloud."
- **Integrate DevOps and security teams and shift-left testing.** Shifting left is defined as having the ability to identify, address, and resolve issues earlier in a workstream cycle, thereby improving efficiencies and savings. Interviewees said their organizations sought the ability to shift left and transform their cloud DevOps processes using the visibility and scanning Prisma Cloud offers. The senior security architect of a healthcare organization said: "Our investment driver was about the security gap, but we definitely wanted to think about CI/CD (continuous integration/continuous delivery) and shift left."
- **Improve compliance and minimize risk.** Improving overall cloud security compliance was a crucial objective for the interviewees' organizations. The cloud and systems lead at the automotive company stated: "We want to have the biggest compliance score that we can with everything we put into the cloud. The cloud is an abstract and dangerous thing. Since we don't control what happens in the cloud, we are always trying to mitigate or minimize the risk we incur every time we put a workload in the cloud."

> **"How do we ensure that we're giving teams the ability to build whatever they want and as quickly they want and as scalable as they want, but also ensure that they're building it securely? Prisma Cloud is exactly how we do that. And the integrations with our reporting platform [allow us to] do that. And that [takes] about 30 seconds."**
>
> *Security engineering manager, retail*

> **"Prisma Cloud is a must have. It's not an option for an organization of our size. You've got to have this if you're operating in the public cloud or something like it. There is no way that we could operate safely and stay compliant without it."**
>
> *Security architect, financial technology*

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 interviewees' organizations, 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 large enterprise with 50,000 employees and $10 billion in annual revenue. The composite is pursuing a broader digital transformation journey to modernize its applications and infrastructure. The composite organization migrates and develops 20% of its workload and applications into the cloud each year, from 20% Year 1 to 40% in Year 2 and 60% in Year 3. Consequently, the number of severe cloud incidents that cloud security teams address scales in proportion to the workloads in the cloud. The same scale applies to the time the composite organization's cloud DevOps teams spend ensuring compliant and secure development.

Before investing in Prisma Cloud, the composite organization had no prior cloud-native security platform. It leveraged a mix of CSP tooling and custom and third-party tooling to work to achieve cloud-security monitoring and compliance.

Deployment characteristics. The composite organization deploys the full Prisma Cloud stack with an emphasis on Prisma Cloud's Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) to empower its cloud-security and DevOps teams.

Key assumptions

- $10B annual revenue
- 50K FTEs
- Year 1 workloads in cloud: 20%
- Year 2 workloads in cloud: 40%
- Year 3 workloads in cloud: 60%

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	$491,363	$835,063	$1,244,391	$2,570,817	$2,071,758
Btr	DevOps shift left and productivity lift	$232,128	$464,256	$696,384	$1,392,768	$1,117,912
Ctr	Material breach risk reduction savings	$629,248	$1,650,458	$2,594,202	$4,873,907	$3,885,120
Dtr	Compliance productivity lift	$327,889	$338,443	$348,996	$1,015,328	$839,992
	Total benefits (risk-adjusted)	$1,680,628	$3,288,220	$4,883,973	$9,852,821	$7,914,782

SECOPS EFFICIENCY LIFT

Evidence and data. Interviewees told Forrester that Palo Alto Networks Prisma Cloud gave their security teams visibility into vulnerabilities and threats across all cloud environments in one centralized location. Prisma Cloud pulled, correlated, and prioritized disparate data that improved the organizations' quality and fidelity of data. This gave better context to security professionals to drive incident response efficiency.

For example, the cloud and systems security lead said their organization gained the ability to reduce false alarms by using Prisma Cloud alerts. During a breach attempt, Prisma Cloud provides the organization's security teams with more accurate information, which they can apply rules to stop. Prisma Cloud provides a better understanding of risks and an ability to more quickly identify if an incident is a true positive or false positive.

- The cloud and systems security lead with the automotive organization said: "With Prisma Cloud, I was able to show our executive leadership that we could determine what systems were talking to one another during a certain period of time and what the communication was that was going from point A to point B. That was absolutely critical in selling [leadership] the tool because that demonstrates control and visibility above and beyond what any other tool in the market can provide."
- Interviewees noted the efficiency of having a single console that covers every cloud account. The security architect at the financial technology organization told Forrester: "The information that comes from Prisma Cloud is brilliant. It's across every single account we've got. I have all the data I need. For example, the people who run it call us. They don't have a list of dynamically allocated public IPs, but they can easily get it can through the Prisma Cloud API because it sees all. It's genius."

> **"There's no way we would get the same quality and richness and information if we tried to do this ourselves."**
>
> *Security architect, financial technology*

> **“There’s no doubt whatsoever of Prisma Cloud’s value. The number of teams that would be needed to keep an eye on our cloud environments without Prisma Cloud is significant. When you’ve got 2 million instances of [virtual servers] deployed into public cloud, how many good teams does it take to keep an eye on that? It’s not going to happen.”**
>
> *Security architect, financial technology*

The engineering security manager at the software organization stated: “Prisma Cloud now centralizes our account management in a single console. It definitely saves time because we have it all in one place. The SOC analysts used to have to compile reports manually, which used to take up considerable time.”

- The interviewees also praised the quantity and quality of Prisma Cloud’s out-of-the-box policies. With Prisma Cloud, SecOps teams could proactively configure and enforce more policies faster to automatically protect against certain scenarios.

  The security architect at the financial technology organization said: “The native rules that come with Prisma Cloud are excellent. They’re going to pick up stuff that you wouldn’t have thought of. [Prisma Cloud has] about 680 rules that I know of. If we were to try and build those rules ourselves, we’d be lucky to come up with 60. The actual IP and the thought process that went into Palo Alto generating those rules is incredibly important because it picks up stuff that we just didn’t think of.”

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

- The composite organization’s workloads in the cloud as a percentage of all workloads is 20% in Year 1, 40% in Year 2, and 60% in Year 3.
- The composite organization has 10,200 severe-level incidents in Year 1. That scales to 20,400 in Year 2 and 30,600 in Year 3.
- Forrester research revealed that the average amount of time spent per investigation is 3.7 hours.[1]
- Each FTE turns 50% of their time saved into productive tasks.
- SecOps teams spend 4,160 total hours configuring policies in Year 1 and 832 hours in years 2 and 3 due to economies of scale effect.
- The average fully burdened salary for a SecOps FTE is $121,500 annually, or $58 per hour.

Reduction in time to investigate severe cloud incidents:

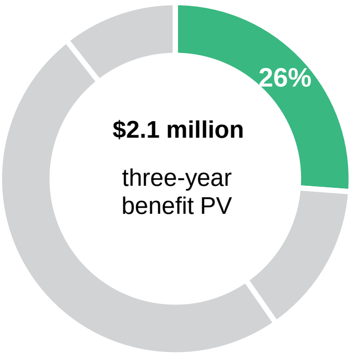
44%

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

- The number of severe-level cloud-security incidents and the hours per investigation.
- The labor required to configure and enforce policies.
- The average fully burdened rate of SecOps FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,997,180.

SecOps Efficiency Lift



SecOps Efficiency Lift

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Percentage of workloads and applications in the cloud	Composite	20%	40%	60%
A2	Number of severe-level cloud-security incidents requiring manual investigation or intervention	Composite	10,200	20,400	30,600
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	44%	44%	44%
A5	Productivity recapture	Assumption	50%	50%	50%
A6	Average fully burdened hourly salary: SecOps FTE (showing rounded value)	$90,000*1.35 (benefit load)/2,080 hours per year	$58	$58	$58
A7	Subtotal: Uplift in security productivity from reduced incident intervention rate (showing rounded value)	A2*A3*A4*A5*A6	$481,562	$963,125	$1,444,687
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	50%	50%	50%
A11	Subtotal: Uplift in SecOps productivity from configuring and enforcing policies	A8*A9*A10*A6	$96,512	$19,302	$19,302
At	SecOps efficiency lift	A7+A11	$578,074	$982,427	$1,463,989
	Risk adjustment	↓15%			
Atr	SecOps efficiency lift (risk-adjusted)		$491,363	$835,063	$1,244,391
	Three-year total: $2,570,817		**Three-year present value: $2,071,758**		

DEVOPS SHIFT LEFT AND PRODUCTIVITY LIFT

Evidence and data. Palo Alto Networks Prisma Cloud gave DevOps professionals visibility and contextual evidence of misconfigurations and vulnerabilities in their cloud developments. By integrating Prisma Cloud vulnerability scanning and hardening checks in developer environments, DevOps teams from the interviewees' organizations were more proactive in identifying and resolving software vulnerabilities. This helped the organizations to:

- Prevent security lapses and minimize configuration drift.
- Eliminate time-consuming ad hoc work addressing vulnerabilities in production environments.
- Improve vulnerability turnaround time by months, as was the case for the healthcare organization.
- Enable a DevSecOps approach to cloud development and security.
- Accelerate cloud-native application development.

> **"With Prisma Cloud, we've shrunk the time to fix vulnerabilities way down. We give developers visibility much earlier, and as long as what they're creating is a container image, we can see it with Prisma Cloud. … They are getting feedback much earlier so they can fix [issues] and they are no longer dumping masses of problems into production."**
>
> *Senior security architect, healthcare*

> **"When misconfigured code would be released, it would build a backlog for the next release. [SecOps teams] would then have to communicate that to developers to get it prioritized. It was a broken process. Now, we're releasing more secure code and improving our risk profile."**
>
> *Senior security architect, healthcare*

- The manager of cybersecurity at the retail organization explained how Prisma Cloud allowed SecOps to effectively collaborate with DevOps earlier. They said: "Each team has access to the Prisma console to view alerts when they're building, no matter what environment they're building in. We're getting involved as left as we can, and as soon as they spin up a cloud resource, it's scanned right away against a number of policies, including custom ones. It'll identify any misconfigurations very early."
- The director of product management in the healthcare industry explained that their organization was able to eliminate manual work. They said: "When fixing a vulnerability, you eventually have to strike down and the track down the development team. That is all ad hoc work. It's emails and phone calls. We are now operationalizing that, and it is multiple orders of magnitude better. … That process went from completely broken to [taking] eight days [to complete]."

The senior security architect at the same organization noted that the additional security step was nonintrusive and more efficient when brought up earlier. They said: "Developers will now frequently fix vulnerabilities within 30 days just to avoid a second step of additional work, so it's a very quick turnaround. Fixing vulnerabilities earlier on is no big deal because they're already working on this stuff."

- The security architect at the financial technology organization told Forrester that developers easily understand alerting information in Prisma Cloud. They said: "As part of the information from Prisma Cloud connected to our reporting via APIs, developers can click through to both the rationale of why they're seeing that rule and what they need to do to fix it. They get a mini-tutorial as part of the reports, which is absolutely genius. If it weren't for this information, developers would be calling us up and asking way more questions than they do now. Developers are fixing issues at inception, which means the time wasted later near delivery doesn't exist."

> **"Prisma Cloud spans both development work and continuous monitoring work, and that's very rare to find. Usually, it's one or the other."**
>
> *Senior security architect, healthcare*

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

- Before implementing Prisma Cloud, DevOps FTEs spent 20,800 hours addressing vulnerabilities and exposures, scaling proportionally to the amount of new cloud developments each year.
- Using Prisma Cloud, there is a 10% increase in upfront time spent addressing vulnerabilities early in the SDLC.
- With Prisma Cloud, DevOps FTEs save 60% of the time they previously spent addressing vulnerabilities.
- Each FTE recaptures 50% of their time saved into productive tasks.
- The average fully burdened salary for a DevOps FTE is $129,600 annually, or $62 per hour.

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.
- The fully burdened rate of DevOps FTEs.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $1,117,912.

Reduction in DevOps time addressing vulnerabilities:

60%

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	20,800	41,600	62,400
B2	Additional shift left DevOps hours addressing vulnerabilities and exposures earlier in the development lifecycle	B1*10%	2,080	4,160	6,240
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	50%	50%	50%
B5	Average fully burdened hourly salary: DevOps FTE (showing rounded value)	$96,000*1.35 benefit load/2,080 hours per year	$62	$62	$62
Bt	DevOps shift left and productivity lift	(B1*B3*B4*B5)-(B2*B5)	$257,920	$515,840	$773,760
	Risk adjustment	↓10%			
Btr	DevOps shift left and productivity lift (risk-adjusted)		$232,128	$464,256	$696,384

Three-year total: $1,392,768 **Three-year present value: $1,117,912**

MATERIAL BREACH RISK REDUCTION SAVINGS

Evidence and data. Interviewees noted that Palo Alto Networks Prisma Cloud significantly reduced the likelihood of material data breaches because it increased cloud posture visibility, improved alerting, and allowed for quicker remediation of misconfigurations and vulnerabilities in cloud environments.

- The manager of cybersecurity with the retail organization stated: "Prisma Cloud absolutely helps reduce the risk of breaches. Misconfigurations of resources were caught and fixed quickly. For example, if a key vault was completely exposed to the internet with no authentication, Prisma Cloud would be able to catch that and report it quickly to our reporting platform. That would be a critical vulnerability that would need to be fixed within a certain amount of time depending on our vulnerability remediation policy."

> **"We can say: 'Show me all the open [storage]. Show me all the things that haven't applied this policy. Show me all the images that are more than 90 days old.' We had none of that. It just didn't exist. Our organization was at real risk of significant breaches. Now, we are confident that we can see what is going on. Before we got Prisma Cloud, the chance of a breach was 100%."**
>
> *Security architect, financial technology*

- The cloud and systems security lead at the automotive organization noted: “The biggest impact that Prisma Cloud has is our ability to minimize risks when deploying stuff in the cloud. We are continuously monitoring those deployments, and we have visibility into most development instances.”

  The same interviewee told Forrester that Prisma Cloud delivers richer contextualization of cyberattacks. They said: “We have about 50,000 instances that don’t exist anymore. The good thing is since we have been getting the data logs from Prisma Cloud, we are able to cross-reference that information in Prisma Cloud with the information that we have stored in the logs to check historic trends and to see if that system was breached in the past. We can actually diagnose what happened because we have telemetry that will allow us to replay that attack anytime we want.”

Reduced likelihood of a cloud data breach with Prisma Cloud:

27%

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.[2] 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 0.5 in Year 1 to 1.1 in Years 2 and 1.6 in Year 3.[3]

- 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 to acquire near 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, 2, and 3.

- The number of employees affected by each data breach are 10% for Year 1, 14% for Year 2, and 16% 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.[4]

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 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 $3,885,120.

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	0.5	1.1	1.6
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	Composite	27%	27%	27%
C4	Subtotal: Avoided costs of remediation, customer resolution, fines, brand rebuild, and all other external-facing costs (showing rounded value)	C1*C2*C3	$408,560	$898,832	$1,307,392
C5	Number of internal business users	Composite	50,000	50,000	50,000
C6	Average percentage of employees affected per breach	Composite	10%	14%	16%
C7	Diminished/eliminated internal user productivity hours per breach	Forrester research	3.6	3.6	3.6
C8	Average fully burdened hourly salary: Business user (showing rounded value)	$65,000*1.35 (benefit load)/2,080 hours per year	$42	$42	$42
C9	Subtotal: Cost of reduced internal productivity	C5*C6*C7*C8*C1	$378,000	$1,164,240	$1,935,360
Ct	Material breach risk reduction savings	C4+C9	$786,560	$2,063,072	$3,242,752
	Risk adjustment	↓20%			
Ctr	Material breach risk reduction savings (risk-adjusted)		$629,248	$1,650,458	$2,594,202
	Three-year total: $4,873,907			**Three-year present value: $3,885,120**	

COMPLIANCE PRODUCTIVITY LIFT

Evidence and data. Interviewees told Forrester that Palo Alto Networks Prisma Cloud transformed their organizations' compliance control settings, reporting, and audit efforts. By leveraging the data in Prisma Cloud, DevOps and compliance professionals could produce, track, review, and validate evidence through automated reporting. This helped them avoid hours of ad hoc, manual, and follow-up work.

- The director of product management at the healthcare organization told Forrester that their organization's compliance and audit professionals previously spent hours of ad hoc work per event. With Prisma Cloud, the interviewee said: "The reporting aspect is all automated. We have systems set up where our

> **"We needed a way to trust but verify — especially when our teams have free rein to build and scale as they please. There would be no way to continuously audit without Prisma Cloud. Without an automated solution, there is no way we could keep up across our almost 150 cloud accounts with tens of thousands of resources."**
>
> *Security engineering manager, retail*

Prisma Cloud scans and filters data through our reporting tools. That’s 90% automated at this point.”

- The security architect with the financial technology organization stated: “[Compliance professionals] have access to our cloud environments, and they require a clean report before going live. With Prisma Cloud, they are getting clean reports, and they no longer have to go in there and manually look at everything. They have all the information they need to decide as to whether it can go live. They are now saying: ‘Yet another clean report. Excellent! Let’s move on to more interesting topics.’”
- The engineering security manager with the software organization echoed similar benefits, stating: “Prisma Cloud gives us the ability to pretty quickly produce stats and the compliance status of any of our accounts, which reduces the need for compliance officers to actually investigate the environment themselves. We no longer have to provision access for officers in the in the public cloud accounts. They are pretty satisfied just having the actual Prisma Cloud monitoring and the reporting.”

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

- There are 220 new annual controls.
- DevOps FTEs spend an average of 8 hours to create each control.
- Compliance analysts spend an average of 7 hours aggregating, producing, and revising each control.
- Compliance managers spend an average of 2 hours consuming and validating each control.
- The composite organization conducts a quarterly internal audit process and an annual external audit.

Reduction in total audit time:

Up to 64%

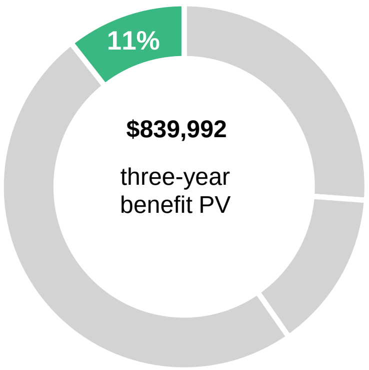
- The average fully burdened salary for a compliance analyst FTE is $91,800 annually, or $44 per hour.
- The average fully burdened salary for a compliance manager FTE is $122,850 annually, or $59 per hour.
- External auditors charge the composite organization a $250 hourly rate.

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

- Variation in compliance frequency and effort.
- The fully burdened rate for compliance professionals.
- The billing rate for external auditors.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $60,839.

Compliance Productivity Lift



Compliance Productivity Lift

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	DevOps time to create and document each control (hours)	Composite	1,760	1,760	1,760
D2	Compliance analyst time to aggregate, produce, and revise reports (hours)	Composite	6,160	6,160	6,160
D3	Compliance manager time to consume and validate reports (hours)	Composite	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	50%	50%	50%
D6	Average fully burdened hourly salary: Compliance analyst (showing rounded value)	$68,000*1.35 (benefit load)/2,080 hours per year	$44	$44	$44
D7	Average fully burdened hourly salary: Compliance manager (showing rounded value)	$91,000*1.35 (benefit load)/2,080 hours per year	$59	$59	$59
D8	Subtotal: Labor saved from reporting efficiencies	[(D1*B5)+(D2*D6)+(D3*D7)]*(D4*D5)	$311,256	$311,256	$311,256
D9	Internal audit events	Composite	4	4	4
D10	Total internal audit hours event per event	Composite	200	200	200
D11	External audit events	Composite	1	1	1
D12	Total external audit hours per event	Composite	480	480	480
D13	External compliance professional hourly rate	Composite	$250	$250	$250
D14	Reduction in total audit time due to improved evidence tracking, monitoring, and reviewing	Composite	48%	56%	64%
D15	Subtotal: Audit compliance productivity lift	[(D9*D10*D6)+(D11*D12*D13)]*D14	$74,496	$86,912	$99,328
Dt	Compliance productivity lift	D8+D15	$385,752	$398,168	$410,584
	Risk adjustment	↓15%			
Dtr	Compliance productivity lift (risk-adjusted)		$327,889	$338,443	$348,996
	Three-year total: $1,015,328		**Three-year present value: $839,992**		

UNQUANTIFIED BENEFITS

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

- **Ability to scale cloud security efforts.** Several interviewees noted that Prisma Cloud enabled their security teams to efficiently scale as cloud workloads increased, particularly due to improved collaboration and the operationalization of DevSecOps. The director of product management in healthcare stated: “Prisma Cloud is allowing us to scale. We’re a centralized security architect team of [about] 40 people looking at application security for an 8,000-developer organization. To achieve scale, we have to be plugged into the pipelines the way the developers work. Prisma Cloud is the first tool to do that.”

  Prisma Cloud gives SecOps control without hindering DevOps workflow. The security engineering manager at the retail organization told Forrester: “If we didn’t have a Prisma Cloud, we wouldn’t be able to monitor configuration drift. That largely has to do with our intent to give cloud subscription owners the ability to deploy cloud resources within their subscriptions and within their cloud accounts pretty freely.”

- **Ease of integration with other tooling.** Multiple interviewees said Prisma Cloud easily integrates with other tools (e.g., SIEM, SOAR, ticketing and reporting applications), enabling a more effective security stack. The engineering security manager with the software company noted: “[Prisma Cloud] integrates well with our public cloud. There are a number of integrations that we’ve leveraged, like [one] for message queuing. It integrates with email. It integrates with [our business communication platform]. The integrations are pretty good.”

> **“The easy accessibility and customizability of the API is incredibly important to us. It’s got its own query language, which means we can build our own rule sets — which we have — and we do that for policy components that Prisma Cloud may not consider putting into their central product.”**
>
> *Security architect, financial technology*

- **Improved reporting**. Reporting was leveraged both through the Prisma Cloud console and custom reports combined with other tooling information using API connections. The security architect with the financial technology organization stated: “[Our security team] gets an email straight away for any high or critical alerts and a weekly report on top of that. The reports show them everything including what’s new and what’s been remediated from the last report. Our central people pull monthly reports and compare the divisions. That’s key to us.”

- **Improved implementation time-to-value.** Spinning up Prisma Cloud was a quick exercise for the interviewees’ organizations. The cloud and systems security lead in the automotive industry told Forrester their organization doubled its cloud compliance score two weeks after implementing Prisma Cloud. The engineering security manager with the software organization said: “We recently added a second tenant of Prisma Cloud, which is a completely new instance for another side project. We have a good relationship with our account manager. It simply [took] an email to request it, and [it required] probably about one week's turnaround time for a new tenant. It was pretty seamless."

FLEXIBILITY

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

- **Providing multicloud strategy.** A core value proposition of Prisma Cloud is that it covers multicloud environments. The security architect in the financial technology industry explained how Prisma Cloud will facilitate their organization's adoption of a new CSP. They said: "Being able to customize our own policies, use the rule sets that come out of the box, and apply them across three different clouds is invaluable."

- **Unlocking additional use cases.** Organizations can expound on new capabilities that are unlocked with new insights from Prisma Cloud. The security architect in the financial technology industry said: "The use cases do expand. We also use the data for other things like understanding who's been patching our images and who hasn't, even though that's not a native component. The fact that [Prisma Cloud] provides the data for us is absolutely genius."

- **Improving compliance scores of other software-as-a-service (SaaS) solutions.** The cloud and systems security lead in the automotive industry said the improved visibility from Prisma Cloud allowed their organization to enforce higher security standards with other cloud technology vendors. They said: "Prisma Cloud gave us the visibility so we could generate a report, send that report back to the vendor, and say: 'Why isn't this [new application] meeting our compliance requirements? Correct this.' By bringing this up with our vendors, we ended up getting a big increase in the security of the container images themselves."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	Licensing costs	$0	$445,500	$603,900	$980,100	$2,029,500	$1,640,455
Ftr	Ongoing costs	$0	$133,650	$187,110	$213,840	$534,600	$436,798
Gtr	Implementation and training costs	$25,802	$0	$0	$0	$25,802	$25,802
	Total costs (risk-adjusted)	$25,802	$579,150	$791,010	$1,193,940	$2,589,902	$2,103,055

LICENSING COSTS

Evidence and data. Palo Alto Networks calculates the licensing costs for Prisma Cloud using the number of workloads protected in cloud environments.

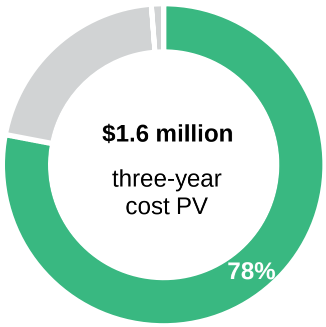
Modeling and assumptions. For the composite organization, Forrester assumes that:

- The composite organization only pays for the number of workloads in the cloud, which increases during Year 1 and Year 2.
- The modeled licensing costs reflect the composite organization's expanding cloud usage.

Risks. The expected financial impact is subject to risks and variation based on several factors including the number of workloads that need protecting.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1,640,455.

Licensing costs



Licensing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Palo Alto Networks Prisma Cloud Licensing	Composite	$0	$405,000	$549,000	$891,000
Et	Licensing costs	E1	$0	$405,000	$549,000	$891,000
	Risk adjustment	↑10%				
Etr	Licensing costs (risk-adjusted)		$0	$445,500	$603,900	$980,100
	Three-year total: $2,029,500			**Three-year present value: $1,640,455**		

ONGOING COSTS

Evidence and data. The interviewees told Forrester that their organizations utilized SecOps FTEs to support DevOps efforts to address vulnerabilities early on. The SecOps FTEs helped address questions, explained configuration requirements, and implemented DevSecOps processes to ensure faster and more secure deployments.

- The security architect with the financial technology organization said built-in Prisma Cloud tutorials sufficiently answered most DevOps questions, and the organization only needed two security FTEs to support all of the organization's developers. The interviewee stated: "Now, there are only two people supporting questions on Prisma Cloud in the organization for thousands of developers. And it's not even a full-time role thing. That's how efficient it's become."

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

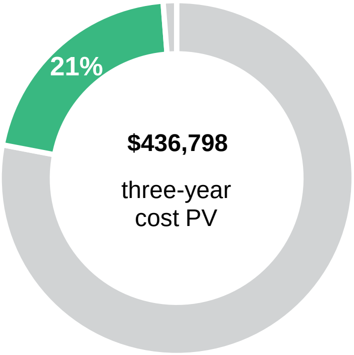
- The composite organization utilizes one SecOps FTE in Year 1, and that scales that to 1.4 FTEs in Year 2 and 1.6 FTEs in Years 3 to support increased cloud migration and development.
- The average fully burdened salary for a SecOps FTE is $121,500 annually, or $58 per hour.

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

- The amount of SecOps support needed.
- The fully burdened rate for SecOps professionals.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $436,798.

Ongoing Costs



Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	SecOps FTEs required to support developers	Composite	$0	1.0	1.4	1.6
F2	Average fully burdened salary: SecOps FTE (showing rounded value)	Assumption	$0	$121,500	$121,500	$121,500
Ft	Ongoing costs	F1*F2	$0	$121,500	$170,100	$194,400
	Risk adjustment	↑10%				
Ftr	Ongoing costs (risk-adjusted)		$0	$133,650	$187,110	$213,840
	Three-year total: $534,600			**Three-year present value: $436,798**		

IMPLEMENTATION AND TRAINING COSTS

Evidence and data. Interviewees said the time and effort required for implementation was minimal, and their organizations were able to spin up new tenants of Prisma Cloud in a matter of weeks.

- Implementation efforts included planning, coordinating among cross-organizational teams, and integrating with other tools.
- One interviewee said a two-day training session for core SecOps and DevOps personnel kickstarted their organization's adoption of Prisma Cloud.

Modeling and assumptions. Forrester assumes the composite organization conducts a two-day training for key SecOps and DevOps FTEs.

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

- The implementation requirements and skill sets available.
- The amount of training required.
- The fully burdened rate of SecOps and DevOps FTEs.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $25,802.

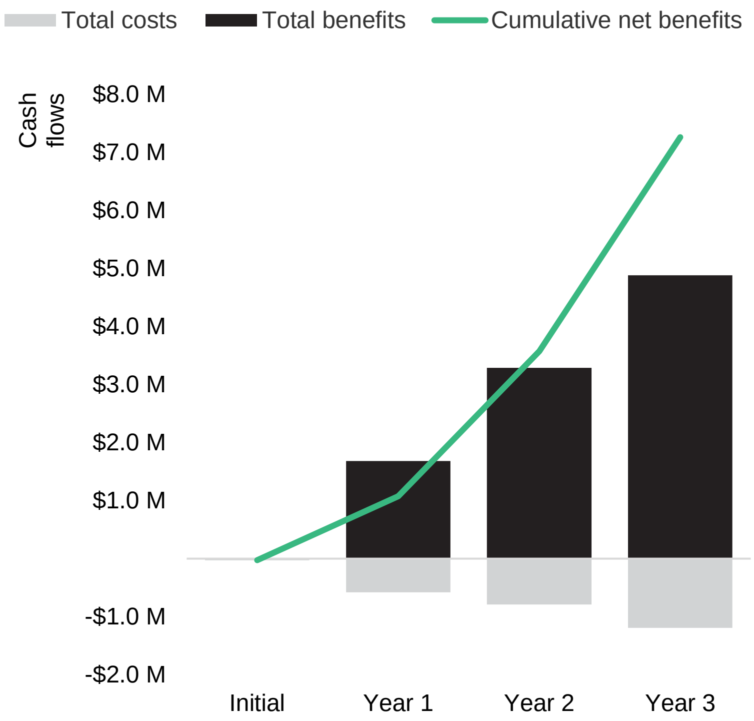
Implementation And Training Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Planning, implementation, and integration time (hours)	Composite	240	0	0	0
G2	Average fully burdened hourly salary: SecOps (showing rounded value)	Assumption	$58	$0	$0	$0
G3	Subtotal: Planning, implementation, and integration costs	G1*G2	$13,920	$0	$0	$0
G4	Training time (hours)	Interviews	16	0	0	0
G5	SecOps FTEs requiring training	Composite	6	0	0	0
G6	DevOps FTEs requiring training	Composite	4	0	0	0
G7	Average fully burdened hourly salary: DevOps FTE (showing rounded value)	$96,000*1.35 (benefit load)/2,080 hours per year	$62	$0	$0	$0
G8	Subtotal: Training costs	(G4*G5*G2)+(G4*G6*G7)	$9,536	$0	$0	$0
Gt	Implementation and training costs	G3+G8	$23,456	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Implementation and training costs (risk-adjusted)		$25,802	$0	$0	$0
	Three-year total: $25,802			**Three-year present value: $25,802**		

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	($25,802)	($579,150)	($791,010)	($1,193,940)	($2,589,902)	($2,103,055)
Total benefits	$0	$1,680,628	$3,288,220	$4,883,973	$9,852,821	$7,914,782
Net benefits	($25,802)	$1,101,478	$2,497,210	$3,690,033	$7,262,919	$5,811,727
ROI						276%
Payback period (months)						<6

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix C: Endnotes

[1] Source: Forrester Consulting Cost Of A Security Breach Survey, Q4 2020.
[2] Ibid.
[3] Ibid.
[4] Ibid.

FORRESTER®