The Business Case for Cloud Threat Defense

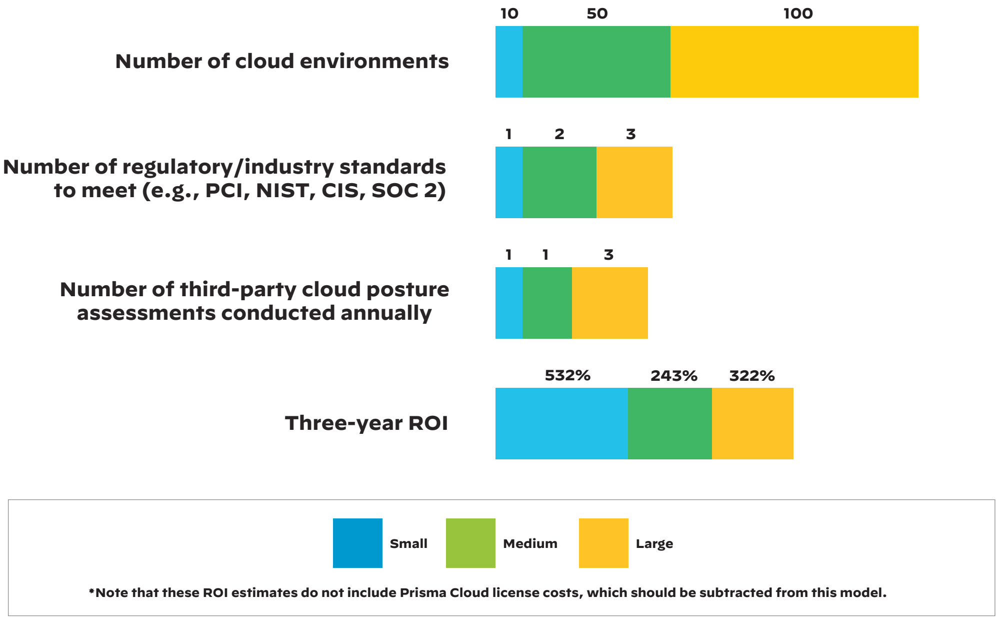
Prisma™ Cloud is a security and compliance service that enables effective threat defense across Google Cloud Platform (GCP™), Amazon Web Services (AWS®), and Microsoft Azure®. Its innovative, machine learning-assisted approach correlates disparate security data sets to provide comprehensive visibility, detect threats, and enable rapid response across the most fragmented multi-cloud environments. With Prisma Cloud, organizations can ensure compliance, govern security, and enable security operations across public cloud computing deployments.

To better understand the benefits, costs, issues, and risks associated with implementing cloud threat defense, Palo Alto Networks surveyed its Prisma Cloud customer base to understand the specific areas of savings and cost avoidance. Customers use Prisma Cloud for visibility, security governance, compliance assurance, reduction of third-party tools and labor requirements, and reduction of financial risk due to security breaches. Read on for a summary of the reported benefits.

Table 1: Prisma Cloud Benefits		
Focus Area	**Cost Avoidance**	**Benefits**
Security Operations	Avoid manual cloud posture assessment costs	Eliminate the cost, management, and overhead associated with third-party cloud posture assessments (i.e., penetration testing)
	Reduce efforts to investigate and resolve potential security risks	Shorten time to remediation with actionable alerts prioritized by risk ranking
	Avoid the need to develop and maintain a log manager	Eliminate the need for homegrown or third-party SIEM systems
	Reduce financial risk due to security breaches	Significantly reduce the probability of economic, asset, or brand loss due to security breaches in your cloud environments
Compliance	Eliminate efforts to manually map traditional compliance controls to the public cloud	Save time, resources, and money with out-of-the-box compliance reporting based on industry standards, such as PCI DSS, NIST CSF, SOC 2, HIPAA, CIS benchmarks, and GDPR
	Reduce labor to comply with audit verification requirements	
DevOps	Avoid the delays and rework that result from trying to force-fit traditional security controls into the public cloud	Give security and compliance teams continuous visibility into public cloud environments
		Integrate automated remediation into development workflows

Key Findings of Prisma Cloud Cost-Benefit Analysis

Figure 1 shows the three-year ROI estimates for Prisma Cloud* based on sample sizes of representative customer cloud environments.



*Note that these ROI estimates do not include Prisma Cloud license costs, which should be subtracted from this model.

Figure 1: Prisma Cloud ROI by environment size

Public Cloud Security Requirements

According to Gartner, the worldwide public cloud services market is projected to grow 17% in 2020 to total US$266.4 billion, up from $227.8 billion in 2019.[1] Along with this rapid growth comes new risks. To that end, Gartner also forecasts that "through 2025, 99% of cloud security failures will be the customer's fault."[2]

As you evaluate options for ensuring cloud compliance and security, you may discuss repurposing legacy data center security, building your own security and compliance options, or buying cloud native security products.

Although building a product internally may sound attractive, the reality is quite different. Dozens of cloud security point products exist, but most are ineffective at comprehensively addressing the most common and pressing cloud security challenges.

Visibility

Unlike a traditional on-premises data center, where an organization has complete visibility and precise control over all assets, migrating to the cloud introduces major blind spots. Keeping track of assets and accurately identifying risks is challenging due to the cloud's ephemeral nature, fragmented ownership by individual lines of business, multiple regions, and multiple service providers. Simply put, a configuration management database (CMDB) for the cloud typically doesn't exist in most organizations.

Compliance Management

Cloud service providers release new capabilities for their platforms daily, as organizations demand new features, and developers want to adopt the latest technologies. Environments are changing by the minute. With such speed of change, how do you map traditional compliance and regulatory controls from the on-premises era to the cloud? More importantly, how do you produce auditor-friendly historical reporting to prove these environments were always compliant?

Threat Detection

Discovering a variety of risks in the cloud is essential for a safe, hygienic environment. Detecting configuration drift, identifying account compromises or insider threats, and pinpointing suspicious network traffic are all elements of an effective cloud threat defense—yet none can be done with traditional security tools.

Incident Response

Having hundreds or thousands of data points about your cloud environments is, by itself, not enough to effectively respond to cloud threats. You must be able to respond based on a holistic view of your environments. This requires correlating disparate data from your assets, such as resource configurations, user activities, network traffic, host vulnerabilities/activities, and third-party threat intelligence sources, to produce the necessary context. Only then will you have enough information for actionable alerts, enabling prioritized response based on the severity of each issue.

Beyond these fundamental cloud security challenges are the implications of what building your own cloud threat defense program means to the people, processes, and technology in your organization. Other questions to consider are:

- When I have a breach or a misconfiguration, how will I know and how will I respond?
- What hardware and software will I need to develop a custom product?
- How will I staff the maintenance and upkeep of a custom product?
- Can I afford the 9- to 24-month cycle to build my own program?
- Can I monitor all my cloud resources from a single pane of glass?
- Do I have the right people to design and build cloud threat defense?
- What are the impacts to my DevOps and SecOps teams?

Savings and Benefits with Prisma Cloud

Prisma Cloud yields measurable savings and benefits in multiple areas to produce a strong return on your investment.

Reduce the Labor Required to Stay Compliant

Cloud resource compliance reporting and auditing are challenging, time consuming, and expensive. We estimate it initially takes 480 hours, on average, to map controls to each compliance standard and produce the required reports. In subsequent years, maintenance, reporting, and audit support take an average of 240 hours. With Prisma Cloud, mapping cloud resource configurations to compliance frameworks, such as CIS benchmarks, NIST CSF, SOC 2, PCI DSS, HIPAA, and GDPR, is an out-of-the-box feature. This can free up substantial resources for your other strategic efforts.

[1] "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17% in 2020," Gartner, November 13, 2019, https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020.

[2] "Is the Cloud Secure?" Gartner, October 10, 2019, https://www.gartner.com/smarterwithgartner/is-the-cloud-secure.

Avoid Third-Party Cloud Posture Assessment Costs

Most organizations do not have the in-house expertise or tools to periodically—or effectively—assess risks in their cloud environments. As such, these organizations rely on third-party specialists to conduct these tests annually. We estimate such assessments take three to five business days of a consultant's time per cloud account. With continuous security monitoring, Prisma Cloud eliminates the need for third-party assessments.

Reduce Labor to Investigate and Resolve Security Risks

SOC teams typically lack the expertise or the tools to investigate and act on security alerts generated from cloud service providers or other open source security tools, such as Amazon GuardDuty® and Security Monkey. This problem only becomes worse with organizations adopting multiple cloud platforms, such as GCP™, AWS®, or Azure®.

Prisma Cloud addresses these challenges by giving security operations center teams the unified ability to monitor, measure, and prioritize risks across all public cloud environments. Prisma Cloud alerts contain all the relevant information, including but not limited to the nature of individual risks, when they were introduced and by whom, their impact on the environment, exploitation status, and details on how they can be remediated. Armed with this information, and by focusing on the highest-priority alerts, SOC analysts can take action without engaging in out-of-band conversations with DevOps or using multiple tools to manually investigate, reducing investigation times by 75%.

Avoid Third-Party Log Aggregation Costs

Security information and event management (SIEM) systems are expensive to use, as their costs are driven by the amount of data they ingest, in addition to associated hardware costs and system administrators to maintain them. With Prisma Cloud, this data aggregation is included, enabling you to feed only the relevant alerts into your enterprise SIEM as well as reduce storage costs by 95%. We estimate this can help customers avoid $5,000 per cloud environment in hardware and software costs for log aggregation, in addition to the cost of at least one SIEM administrator.

Reduce Financial Risk Due to Security Breaches

According to the 2019 Cost of Data Breach Report from Ponemon Institute and IBM Security, the global average cost of a data breach has grown 12% since 2014, to $3.92 million.[3] With Prisma Cloud, organizations can comprehensively identify cloud security risks, use in-depth analytics to quickly understand the exact nature and ramifications of the risks, and resolve issues more quickly. By getting ahead of the threats and vulnerabilities, Prisma Cloud can reduce the likelihood of breaches by up to 50% in the first year of operation, and 75% in the second year and beyond, once outstanding security exposure is addressed.

[3] "2019 Cost of a Data Breach Report," Ponemon Institute, July 2019, https://www.ibm.com/downloads/cas/ZBZLY7KL.

Financial Analysis

With these customer-based estimates, the following models represent the detailed Prisma Cloud savings for three different environments. Note that these ROI estimates do not include Prisma Cloud license costs, which should be subtracted from these models.

5
Alerts per cloud, per day, on average

$150,000
Yearly cost of a full-time employee

$250
Third-party consulting hourly rate

24
Hours per cloud account for third-party testing activity

60
Minutes it takes to investigate and resolve each cloud alert manually

15
Minutes it takes to investigate and resolve each cloud alert with Prisma Cloud

Figure 2: Assumptions used to build out the models

10	1	1
Cloud environments	Regulatory/Industry standard to meet (e.g., PCI DSS, NIST, CIS, SOC 2)	Third-party cloud posture assessment conducted annually

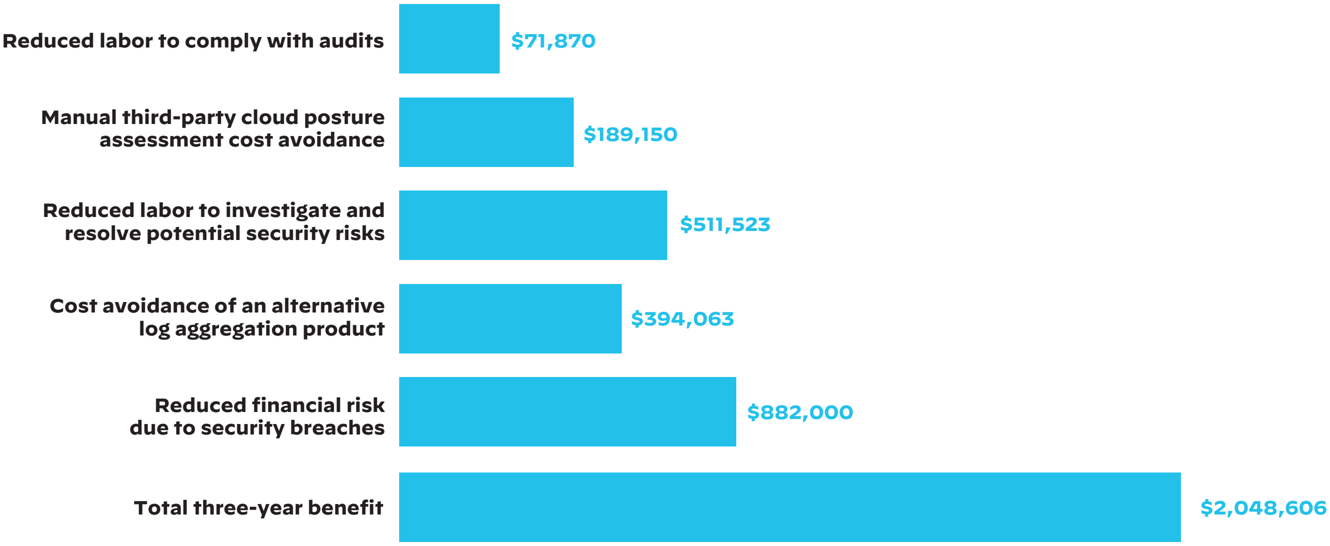


Figure 3: Small cloud environment at a glance

50	2	1
Cloud environments	Regulatory/Industry standards to meet (e.g., PCI DSS, NIST, CIS, SOC 2)	Third-party cloud posture assessment conducted annually

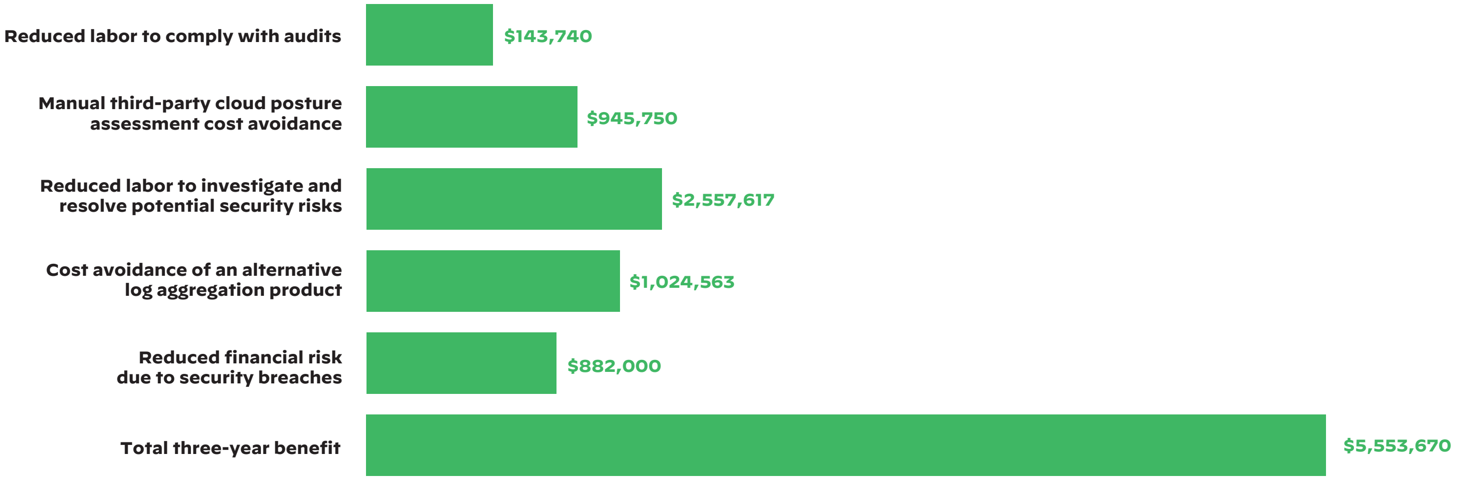


Figure 4: Medium cloud environment at a glance

100

Cloud environments

3

Regulatory/Industry standards to meet (e.g., PCI DSS, NIST, CIS, SOC 2)

3

Third-party cloud posture assessments conducted annually

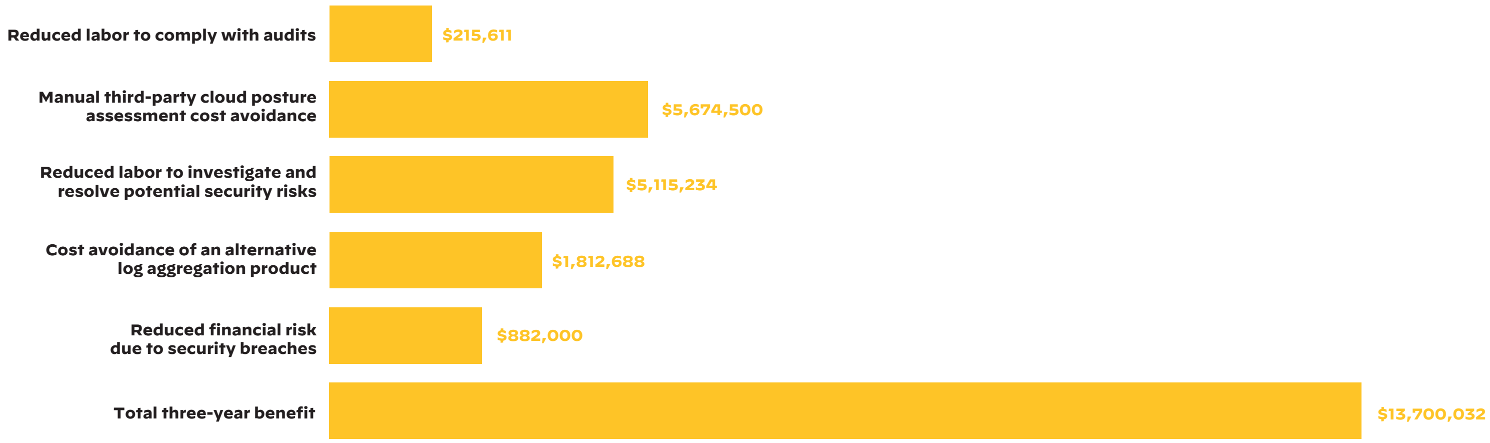


Figure 5: Large cloud environment at a glance

Conclusion

With Prisma Cloud, your organization can expect to save substantial money, time, and resources while ensuring compliance as well as maintaining a strong security posture. Savings accrue in many areas, including reduced labor associated with audits, third-party posture assessment, threat investigation, and third-party tool management. Ancillary systems, such as third-party SIEMs, can be avoided altogether. Perhaps most importantly, Prisma can reduce the likelihood of a security breach, further protecting your assets.

Click here to sign up for your free, 30-day trial.

Contact us @ https://secureitconsult.com/contact for all things Prisma Cloud, and Palo Alto Networks.

paloalto
NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com