PRISMA CLOUD
BY PALO ALTO NETWORKS

Der Business Case für cloudbasierte Bedrohungsabwehr

Zusammenfassung

Prisma™ Cloud ist ein Sicherheits- und Compliance-Service für die plattformübergreifende Bedrohungsabwehr, der die Google Cloud Platform (GCP™), Amazon Web Services (AWS®) und Microsoft Azure® abdeckt. Die innovative, auf maschinellem Lernen basierende Lösung gleicht Sicherheitsdaten aus verschiedenen Quellen miteinander ab und ermöglicht dadurch eine lückenlose Überwachung hochgradig fragmentierter Multi-Cloud-Infrastrukturen. Das erleichtert sowohl die effektive Aufdeckung von Bedrohungen als auch die Einleitung von Gegenmaßnahmen. Außerdem können Unternehmen mit Prisma Cloud die Einhaltung von Compliance-Vorgaben kontrollieren, Schutzmaßnahmen zentralisieren und einheitliche Sicherheitsprozesse in allen Public-Cloud-Umgebungen implementieren.

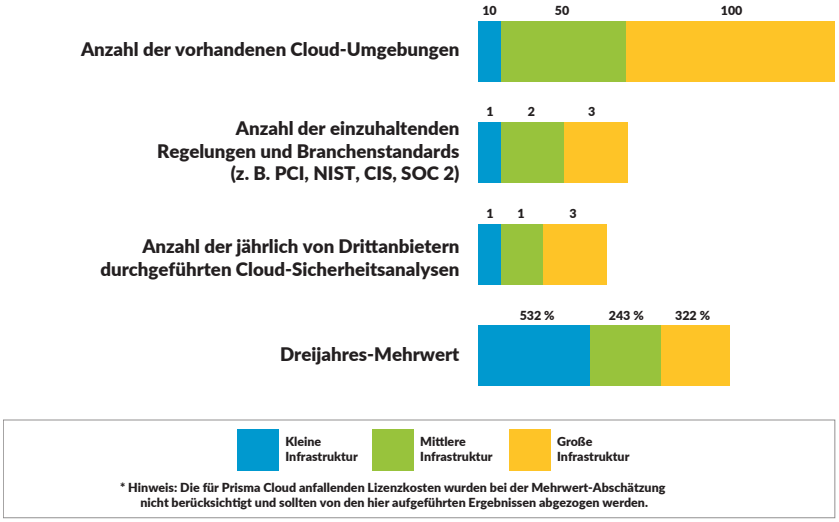
Um den finanziellen Mehrwert der Lösung und die mit der Implementierung einer cloudbasierten Bedrohungsabwehr verbundenen Vorteile, Kosten, Herausforderungen und Risiken zu ermitteln, hat Palo Alto Networks kürzlich eine Umfrage unter den Kunden von Prisma Cloud durchgeführt. Dabei hat sich gezeigt, dass Unternehmen Prisma Cloud vor allem zur Verbesserung der Transparenz, zur Zentralisierung der Sicherheitsinfrastruktur, zur Kontrolle der Einhaltung von Compliance-Vorgaben sowie zur Minimierung des Personalaufwands, der Anzahl der genutzten Drittanbieter-Tools und der mit Datenverlusten einhergehenden finanziellen Risiken einsetzen. Die folgende Tabelle bietet einen Überblick über die von den Befragten genannten Vorteile:

Bereich	Einsparungen	Vorteile
Sicherheitsprozesse	Wegfallende Kosten für die manuelle Evaluation der Cloud-Sicherheit	Vermeidung der Kosten und des Verwaltungsaufwands für Penetrationstests und andere von Drittanbietern durchgeführte Analysen
	Geringerer Arbeitsaufwand für die Untersuchung und Behebung potenzieller Sicherheitsrisiken	Schnellere Problembehebung dank aussagekräftiger, nach Risikostufe geordneter Warnmeldungen
	Vermeidung der Entwicklung und Pflege einer separaten Lösung für das Logdatei-Management	Keine Notwendigkeit zur Nutzung von intern entwickelten oder von Drittanbietern bereitgestellten SIEM-Systemen
	Geringeres finanzielles Risiko durch Sicherheitsverletzungen	Signifikante Stärkung der Cloud-Sicherheit und Minimierung der mit Sicherheitsverletzungen einhergehenden finanziellen Einbußen, Ressourcenverluste und Imageschäden
Compliance	Keine Notwendigkeit zur manuellen Ausweitung des Abdeckungsbereichs konventioneller Compliance-Kontrollen auf die Public Cloud	Verringerter zeitlicher, finanzieller und personeller Aufwand für die Überwachung der Einhaltung der DSGVO sowie von Branchenstandards wie PCI, NIST, SOC 2, HIPAA und CIS – dank vorkonfigurierter Berichtsfunktionen
	Senkung des mit der Erstellung von Prüfberichten verbundenen Arbeitsaufwands	
DevOps	Vermeidung von Verzögerungen und zusätzlichen Arbeitsschritten im Zuge der Implementierung konventioneller Sicherheitsmaßnahmen in der Public Cloud	Lückenloser Überblick über den Sicherheits- und Compliance-Status sämtlicher Public-Cloud-Umgebungen
		Integration von automatisierten Problembehebungs- und Sicherheitsmechanismen in Entwicklungsprozesse

Abbildung 1: Vorteile von Prisma Cloud

Die wichtigsten Ergebnisse der Kosten-Nutzen-Analyse zu Prisma Cloud

In Abbildung 2 finden sich Schätzwerte für den Dreijahres-Mehrwert von Prisma Cloud*, aufgeschlüsselt nach der Größe der Cloud-Infrastrukturen repräsentativer Kundenunternehmen.



Abildung 2: Möglicher Mehrwert einer Investition in Prisma Cloud, nach Größe der Cloud-Infrastruktur

Die Sicherheitsherausforderungen der Public Cloud

Da sich die Migration in die Public Cloud weiterhin mit bemerkenswerter Geschwindigkeit vollzieht, wird der weltweite Markt für Public-Cloud-Services, der bereits ein Volumen von 175,8 Milliarden US-Dollar erreichte, 2019 noch einmal um 17,3 % wachsen und einen prognostizierten Umsatz von 206,2 Milliarden US-Dollar verzeichnen.[1] Allerdings sollte dabei nicht unberücksichtigt bleiben, dass das rasante Wachstum der Cloud-Infrastrukturen von Unternehmen neue Sicherheitsrisiken mit sich bringt. Beispielsweise gehen die Analysten von Gartner davon aus, dass bis zum Jahr 2022 mindestens 95 % der in Cloud-Infrastrukturen aufgedeckten Sicherheitslücken auf Fehler und Versäumnisse des Kundenunternehmens zurückzuführen sein werden.[2]

Daher suchen die IT-Verantwortlichen vielerorts nach effektiven Lösungen zur Kontrolle der Sicherheit und Compliance von Cloud-Umgebungen. Einige erwägen den Ausbau der bereits im unternehmensinternen Rechenzentrum implementierten Maßnahmen, andere ziehen die Entwicklung eigener Tools in Betracht und eine dritte Gruppe tendiert zum Kauf von Cloud-nativen Produkten. Doch eine genauere Evaluation dieser Optionen zeigt, dass jede mit gewissen Schwierigkeiten verbunden ist: Wie aus dem von Cybersecurity Insiders erstellten Cloud Security Report[3] hervorgeht, verfügten im Jahr 2018 nur 16 % der Unternehmen über interne Sicherheitsmaßnahmen, die auch für die Cloud geeignet waren.

Zugleich erweist sich die unternehmensinterne Entwicklung einer für die Cloud ausgelegten Sicherheitslösung meist als weitaus schwieriger als ursprünglich angenommen. Und obwohl es Dutzende von Punktlösungen zum Schutz von Cloud-Umgebungen gibt, sind die meisten nicht zur Bewältigung der gängigsten und drängendsten Herausforderungen rund um die Cloud-Sicherheit geeignet:

- **Transparenz:** Herkömmliche unternehmenseigene Rechenzentren bieten den IT-Verantwortlichen umfassende Transparenz und volle Kontrolle über alle Ressourcen. Doch beim Umstieg auf die Cloud entstehen häufig tote Winkel, da verschiedene Geschäftsbereiche in Eigenregie Anwendungen und Services einsetzen, in verschiedenen Regionen Cloud-Services unterschiedlicher Anbieter genutzt werden und die Cloud eine von Natur aus dynamische Umgebung ist. All das erschwert die präzise Identifizierung akuter Risiken. Das Problem besteht also – einfacher ausgedrückt – darin, dass kaum ein Unternehmen über eine Konfigurationsmanagementsdatenbank (Configuration Management Database, CMDB) für die Cloud verfügt.
- **Compliance-Management:** Die Anbieter von Cloud-Services erweitern ihre Plattformen täglich um neue Funktionen, um den Kundenunternehmen und ihren Entwicklungsteams langersehnte Features und die Möglichkeit zur Nutzung zukunftsweisender Technologien zu bieten. Das hat zur Folge, dass sich die Cloud-Infrastrukturen der Unternehmen von Minute zu Minute verändern, und wirft die Frage auf, wie sich das aus dem Rechenzentrum gewohnte Maß an Richtlinienkonformität und -kontrolle in der Cloud erreichen lässt. Außerdem ist eine Audit-taugliche Lösung wünschenswert, die die dauerhafte Compliance der Cloud-Umgebungen anhand historischer Daten belegt.
- **Bedrohungserkennung:** Eine sichere, saubere Cloud-Infrastruktur erfordert effektive, cloudfähige Tools zur Identifizierung von geknackten Nutzerkonten, verdächtigem Netzwerk-Traffic, Insider-Bedrohungen und Ressourcen mit abweichenden Konfigurationseinstellungen. Dies ist mit konventionellen Sicherheitslösungen nicht zu leisten.
- **Bedrohungsabwehr:** Die Erfassung von Zustandsdaten aus Hunderten oder gar Tausenden verschiedenen Quellen in Ihren Cloud-Umgebungen ist eine wichtige Voraussetzung für eine schnelle und gezielte Reaktion auf Bedrohungen, reicht allein jedoch nicht aus. Für eine effektive Cyberabwehr sind zudem ein holistischer Ansatz und ein umfassender Überblick über die gesamte Cloud-Infrastruktur erforderlich. Dazu müssen die von den verschiedenen Cloud-Ressourcen bereitgestellten Daten (zu Konfigurationen, Nutzeraktivitäten, Netzwerk-Traffic, hostspezifischen Schwachstellen und Vorgängen etc.) mit Bedrohungsdaten aus externen Quellen zusammengeführt und abgeglichen werden. Nur so können die reichhaltigen Kontextinformationen zusammengestellt werden, die für aussagekräftige Warnmeldungen, die präzise Einstufung des Schweregrads erkannter Vorfälle und die Priorisierung von Gegenmaßnahmen benötigt werden.

1. „Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019“, Gartner, 12. April 2018, https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019.
2. „Gartner Survey Says Cloud Computing Remains Top Emerging Business Risk“, Gartner, 15. August 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-says-cloud-computing-remains-top-emerging-business-risk.
3. „2018 Cloud Security Report“, Cybersecurity Insiders, abgerufen am 18. Dezember 2018, https://start.paloaltonetworks.com/cloud-security-report-2018.

Abgesehen davon erfordern Planung und Aufbau einer auf die Anforderungen Ihres Unternehmens zugeschnittenen Cyberabwehr für die Cloud einen genauen Blick auf die vorhandenen Personalressourcen, Prozesse und Technologien. In diesem Zusammenhang sollten Sie sich unter anderem die folgenden Fragen stellen:

- Wie kann unser Team Sicherheitsverletzungen oder falsch konfigurierte Ressourcen identifizieren und welche Maßnahmen können in einem solchen Fall eingeleitet werden?
- Welche Hard- und Softwarelösungen sind für die Entwicklung eines unternehmenseigenen Tools erforderlich?
- Verfügt unser Unternehmen über genügend Personal, um ein intern entwickeltes Tool zu pflegen und zu warten?
- Können wir uns die Entwicklung einer eigenen Lösung leisten, wenn dieser Prozess 9 bis 24 Monate dauert?
- Kann unser Sicherheitsteam alle Cloud-Ressourcen über eine zentrale Konsole überwachen?
- Verfügen wir über die zur Planung und Einrichtung einer cloudbasierten Bedrohungsabwehr nötigen Fachkräfte?
- Welche Auswirkungen hätte ein solches Projekt auf die DevOps- und SecOps-Teams?

Prisma Cloud: Einsparungen und Vorteile

Mit Prisma Cloud lässt sich ein beträchtlicher Mehrwert erzielen, da die Lösung messbare Einsparungen und Vorteile in verschiedenen Bereichen bringt.

Weniger Arbeitsaufwand zur Einhaltung von Compliance-Vorgaben

Die Erstellung von audittauglichen Compliance-Berichten über Cloud-Ressourcen ist kompliziert, zeitraubend und teuer. Unseren Schätzungen zufolge sind anfänglich im Schnitt 480 Arbeitsstunden erforderlich, um Compliance-Kontrollen auf einen Standard auszurichten und die darin geforderten Berichte zu erstellen. In den Folgejahren müssen für die Pflege der Compliance-Kontrollen sowie die Berichterstellung und die Unterstützung von Auditprozessen durchschnittlich 240 Arbeitsstunden aufgewendet werden. Prisma Cloud enthält sofort einsatzbereite Funktionen für die Analyse der Konfigurationen von Cloud-Ressourcen im Hinblick auf die Einhaltung von DSGVO-Vorgaben und Branchenstandards wie CIS, NIST, SOC 2 und HIPAA, die diesen Aufwand erheblich reduzieren und Ressourcen für strategische Initiativen freisetzen.

Vermeidung der Kosten für von Drittanbietern durchgeführte Cloud-Sicherheitsanalysen

Die meisten Unternehmen verfügen nicht über das nötige Know-how oder die erforderlichen Tools, um ihre Cloud-Umgebungen in regelmäßigen Abständen einer Risikoanalyse zu unterziehen. Daher veranlassen die Verantwortlichen jährliche Tests durch externe Spezialisten, die Auskunft über den Sicherheitsstatus geben sollen. Wir schätzen, dass ein externer Berater für eine derartige Evaluation drei bis fünf Arbeitstage pro Cloud-Konto benötigt. Im Gegensatz dazu ermöglichen die Überwachungsfunktionen von Prisma Cloud ein kontinuierliches, lückenloses Monitoring der Cloud-Sicherheit ohne Unterstützung durch Drittanbieter.

Geringerer Arbeitsaufwand für die Untersuchung und Behebung potenzieller Sicherheitsrisiken

Die meisten SOC-Teams sind aufgrund mangelnder Erfahrung und Ausstattung nicht in der Lage, die von Cloud-Anbietern und Open-Source-Tools wie Amazon GuardDuty® oder Security Monkey gemeldeten Sicherheitsvorfälle zu überprüfen und zu beheben. Derartige Probleme werden in vielen Fällen noch dadurch verschärft, dass die betreffenden Unternehmen zur kombinierten Nutzung von GCP, AWS, Azure und anderen Cloud-Plattformen übergehen.

Prisma Cloud ermöglicht die Bewältigung dieser Herausforderungen mithilfe leistungsstarker Überwachungsfunktionen, die das im Security Operations Center tätige Team in die Lage versetzen, den Sicherheitsstatus sämtlicher Public-Cloud-Umgebungen zu überblicken und den Schweregrad erkannter Bedrohungen präzise zu bestimmen. Die von der Lösung ausgegebenen Warnmeldungen enthalten alle relevanten Informationen, darunter Angaben zu Art, Ursprung und Urheber der einzelnen Risiken und Bedrohungen sowie zu den zu erwartenden Auswirkungen auf die Cloud-Infrastruktur, zur aktuellen Gefahrenlage und zu möglichen Abwehrmaßnahmen. Dadurch können sich die SOC-Analysten auf die Vorfälle mit der höchsten Priorität konzentrieren und sofort Gegenmaßnahmen einleiten, ohne dass dafür manuelle Analysen und zusätzliche Diskussionen mit DevOps-Teams erforderlich sind. Auf diese Weise kann die Untersuchungsdauer um bis zu 75 % verkürzt werden.

Vermeidung der Kosten für Punktlösungen zur Aggregation von Log-Dateien

SIEM-Systeme bringen beträchtliche Betriebskosten mit sich, deren genaue Höhe zum einen von der Menge der eingespeisten Daten und zum anderen von der erforderlichen Hardware sowie der Zahl der benötigten Administratoren abhängt. Doch wenn Prisma Cloud die Datenaggregation übernimmt, können Sie diese Ausgaben senken, indem Sie ausschließlich relevante Warnmeldungen und Ereignisdaten in Ihr Enterprise-SIEM einspeisen und dadurch beispielsweise die Kosten für die Datenspeicherung um 95 % reduzieren. Unseren Schätzungen zufolge können Kunden auf diese Weise Hardware-, Software- und Personalkosten in Höhe von 5000 US-Dollar pro Cloud-Umgebung einsparen, da neben dem Einsatz von Punktlösungen zur Aggregation von Logdateien auch mindestens eine SIEM-Administratorenstelle hinfällig wird.

Geringeres finanzielles Risiko durch Sicherheitsverletzungen

2018 hat das Ponemon Institute eine Studie veröffentlicht, in der die durchschnittlichen Kosten einer Sicherheitsverletzung auf 3,86 Millionen US-Dollar und das Risiko einer wiederholten Infiltration innerhalb von zwei Jahren auf 27,9 % geschätzt werden.[4] Um diese Kosten und Risiken einzudämmen, versetzt Prisma Cloud die Sicherheitsteams von Unternehmen in die Lage, cloudspezifische Bedrohungen schnell und effektiv zu identifizieren, zu analysieren und zu beseitigen. Mit Prisma Cloud können Kundenunternehmen Bedrohungen und Schwachstellen im Griff behalten, die Angriffsfläche ihrer Cloud-Infrastruktur minimieren und dadurch die Wahrscheinlichkeit einer Sicherheitsverletzung im ersten Jahr der Nutzung um 50 % und in den darauf folgenden Jahren um 75 % senken.

4. „2018 Cost of a Data Breach Study", Ponemon Institute, Juli 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

Mehrwertanalyse

Auf der Grundlage der nachstehenden Annahmen und der bei unseren Kunden erhobenen Daten haben wir die geschätzten Einsparungen errechnet, die Unternehmen mit kleinen, mittleren und großen Cloud-Infrastrukturen jeweils durch einen Umstieg auf Prisma Cloud erzielen können. Die für Prisma Cloud anfallenden Lizenzkosten wurden bei dieser ROI-Abschätzung nicht berücksichtigt und sollten von den hier aufgeführten Ergebnissen abgezogen werden.

5 **Anzahl der täglichen Warnmeldungen pro Cloud-Konto**	**150.000 USD** **Jährliche Kosten für eine qualifizierte Vollzeitkraft**
250 USD **Stundensatz für externe Berater**	**24** **Anzahl der pro Cloud-Konto aufgewendeten Arbeitsstunden für externe Sicherheitstests**
60 **Durchschnittliche Dauer der manuellen Untersuchung und Behebung einer gemeldeten Cloud-Sicherheitsverletzung (in Minuten)**	**15** **Durchschnittliche Dauer der Untersuchung und Behebung einer gemeldeten Cloud-Sicherheitsverletzung mit Prisma Cloud (in Minuten)**

Abbildung 3: Grundannahmen des Modells zur Mehrwertberechnung

10	1	1
Anzahl der vorhandenen Cloud-Umgebungen	Anzahl der einzuhaltenden Regelungen und Branchenstandards (z. B. PCI, NIST, CIS, SOC 2)	Anzahl der jährlich von Drittanbietern durchgeführten Cloud-Sicherheitsanalysen

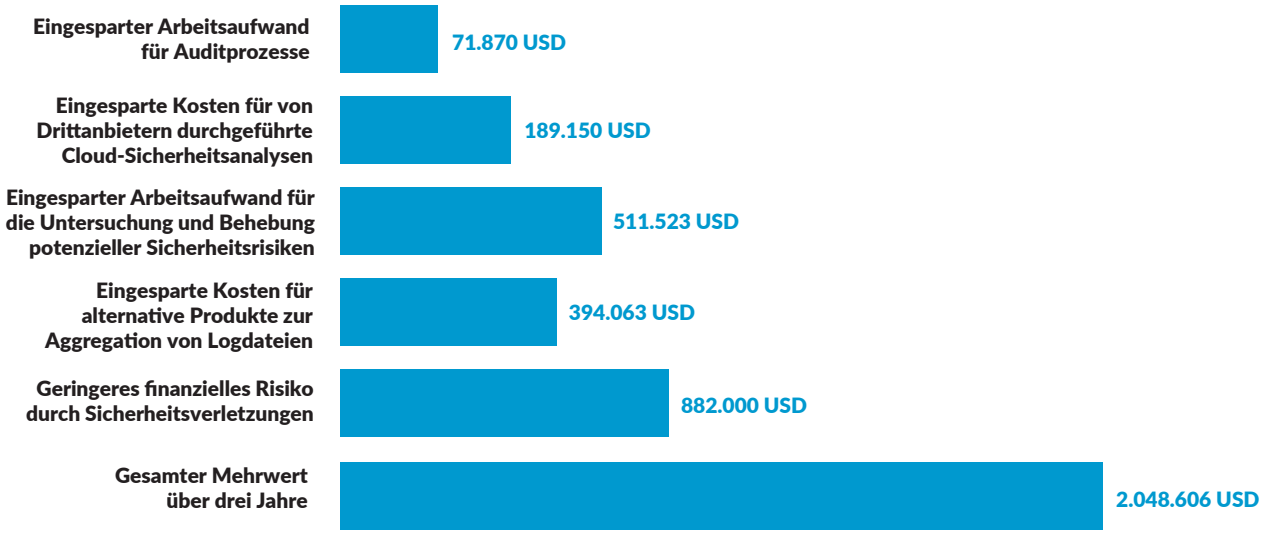


Abbildung 4: Finanzielle Vorteile für Unternehmen mit einer kleinen Cloud-Infrastruktur

50	2	1
Anzahl der vorhandenen Cloud-Umgebungen	**Anzahl der einzuhaltenden Regelungen und Branchenstandards (z. B. PCI, NIST, CIS, SOC 2)**	**Anzahl der jährlich von Drittanbietern durchgeführten Cloud-Sicherheitsanalysen**

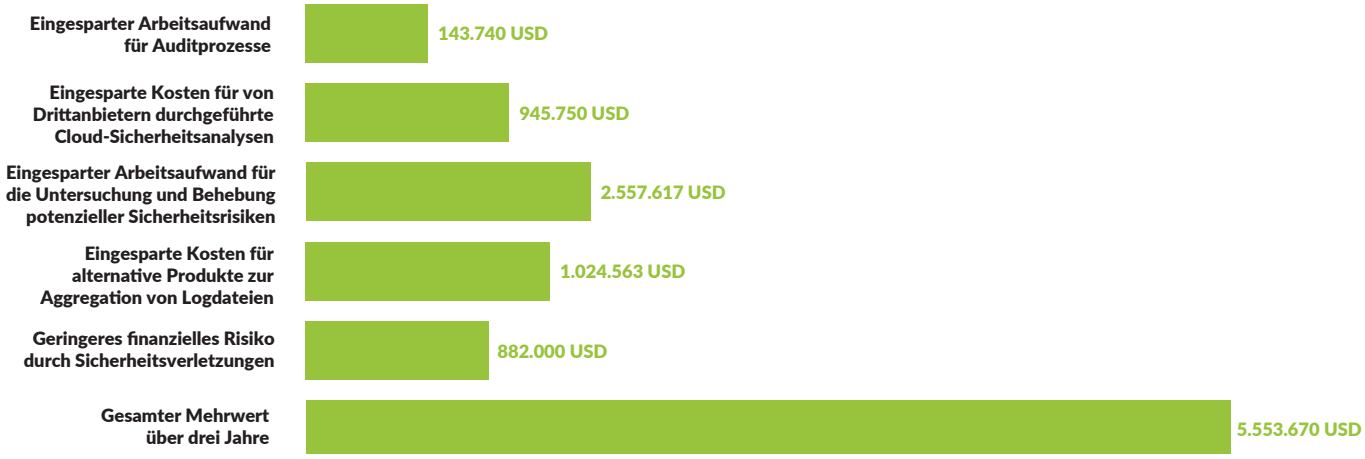


Abbildung 5: Finanzielle Vorteile für Unternehmen mit einer mittleren Cloud-Infrastruktur

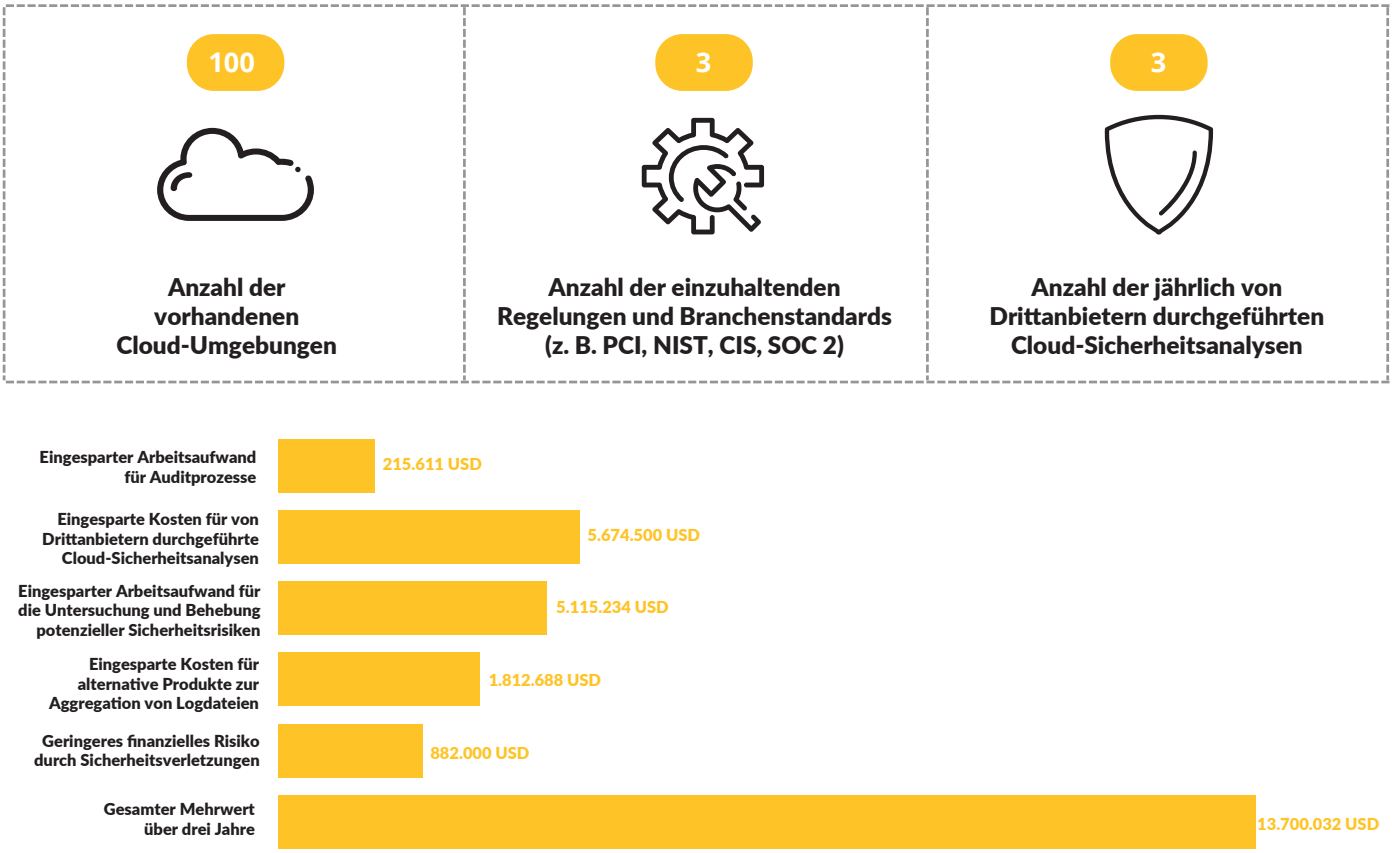


Abbildung 6: Finanzielle Vorteile für Unternehmen mit einer großen Cloud-Infrastruktur

Fazit

Mit Prisma Cloud kann Ihr Unternehmen durch die Minimierung des zeitlichen, finanziellen und personellen Aufwands für die Einhaltung von Compliance-Vorgaben und die Stärkung der Cyber-Sicherheit beträchtliche Einsparungen erzielen. Kunden profitieren sowohl von geringeren Ausgaben für externe Sicherheitsanalysten als auch von sinkenden Arbeitskosten für die Durchführung von Auditprozessen, die Untersuchung von Bedrohungen, die Administration der Tools von Drittanbietern und verschiedene weitere Sicherheitsprozesse. Darüber hinaus macht Prisma Cloud SIEM-Lösungen und andere Produkte von Drittanbietern überflüssig. Allerdings sollte über all diesen finanziellen Vorteile nicht der wichtigste Pluspunkt der Lösung aus dem Blickfeld geraten: Prisma Cloud kann die Wahrscheinlichkeit einer Sicherheitsverletzung verringern und dadurch einen entscheidenden Beitrag zum Schutz Ihrer IT-Ressourcen leisten.

Klicken Sie hier, um Prisma Cloud 30 Tage lang kostenlos zu testen.

PRISMA CLOUD
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99 -197
1101 HE Amsterdam
Niederlande

Telefon: +31 20 888 1883

www.paloaltonetworks.de