Management des Cloud-Sicherheitsniveaus

Gewährleistung der Compliance für Anwendungen, Workloads und Daten

Prisma Cloud reduziert die Komplexität und schützt Ressourcen in Hybrid- und Multi-Cloud-Umgebungen. Mehr als 1.900 führende Unternehmen auf der ganzen Welt vertrauen bereits auf unsere umfassende cloudnative Plattform für den Anwendungsschutz (Cloud-Native Application Protection Platform, CNAPP), die über sieben Milliarden Cloud-Ressourcen schützt und täglich mehr als eine Billion Ereignisse analysiert. Prisma Cloud leuchtet tote Winkel aus und erkennt Bedrohungen, die anderen Tools entgehen. Damit sorgt es für umfassende Transparenz sowie die lückenlose Erkennung und automatisierte Behebung von Bedrohungen.

Umfassendes Management des Sicherheitsniveaus in modernen Multi-Cloud-Umgebungen

Effektive Cloud-Sicherheit erfordert einen lückenlosen Überblick über alle implementierten Ressourcen und absolutes Vertrauen in deren Konfiguration und Compliance. Das ist jedoch nicht einfach, denn je intensiver cloudnative Methoden und flexible Multi-Cloud-Architekturen genutzt werden, desto mehr, oft nicht miteinander kompatible Tools generieren relevante Sicherheitsdaten, die zueinander in Beziehung gesetzt werden müssen. Deshalb benötigen DevOps- und Sicher-heitsteams eine einheitliche, integrierte Lösung wie Prisma Cloud.

Diese Plattform nutzt einen neuen und bislang einzigartigen Ansatz für das Management des Cloud-Sicherheitsniveaus (Cloud Security Posture Management, CSPM), der über das Compliance- und Konfigurationsmanagement hinausgeht. Bedrohungsdaten aus über 30 Datenquellen liefern klare Informationen über kritische Sicherheitsprobleme und Sicherheitsmaßnahmen im Entwicklungsprozess verhindern, dass unsichere Konfigurationen in die Produktion gelangen.

CSPM-Funktionen

Transparenz, Compliance und Governance

Verzeichnis der Cloud-Ressourcen

Mit Prisma Cloud haben Sie einen umfassenden Überblick und die Kontrolle über das Sicherheits-niveau jeder implementierten Ressource. Im Gegensatz zu einigen anderen Lösungen, die Ressourcendaten lediglich zusammenfassen, analysiert und normalisiert Prisma Cloud die Daten aus verschiedenen Datenquellen, um Risiken so klar wie möglich darzustellen.

Amazon EFS	aws	24	0	24	0	24	0	0%
AWS Secrets Manager	aws	7	7	0	0	0	0	100%
Amazon EKS	aws	1	0	1	0	1	0	0%
Amazon SQS	aws	5	0	5	0	5	0	0%
Amazon S3	aws	66	0	66	66	0	0	0%
Azure Virtual Network		120	87	33	18	15	0	73%
Azure Network Watcher		31	31	0	0	0	0	100%
Azure Resource Manager		9	7	2	0	0	2	78%
Azure Policy		3	3	0	0	0	0	100%
Azure SQL Database		2	0	2	2	0	0	0%
Azure Compute		31	17	14	5	9	0	55%
Azure Storage		13	0	13	1	12	0	0%
Azure App Service		1	1	0	0	0	0	100%
Azure Security Center		2	0	2	0	2	0	0%
Google Resource Manager		114	91	23	12	11	0	80%

Abbildung 1: Ressourcenverzeichnis

Überwachung und Protokollierung der Compliance

Prisma Cloud überwacht die Cloud-Compliance kontinuierlich und unterstützt die Erstellung von Berichten per Mausklick von einer zentralen Konsole aus. Mehr als 65 Complianceframeworks sind vorkonfiguriert, Sie können aber auch eigene Frameworks erstellen.

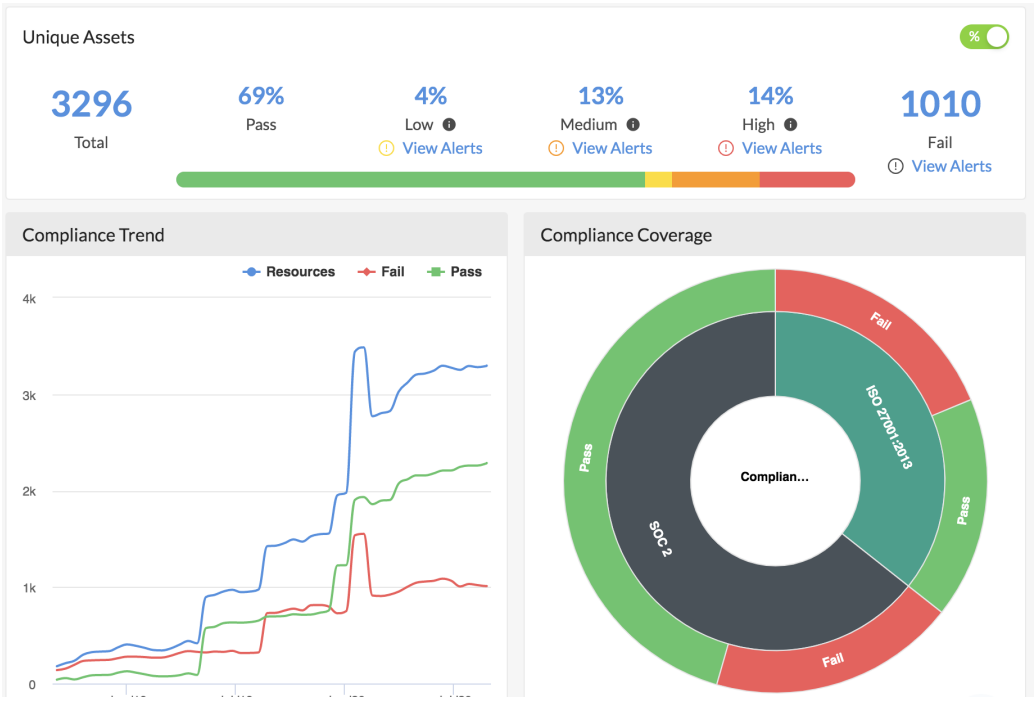

Abbildung 2: Compliancedashboard

Kontextabhängige Risikopriorisierung

Während Punktlösungen meist nur bestimmte Fehlkonfigurationen erkennen, gleicht Prisma Cloud eine breite Palette von Daten ab, um Risiken besser zu priorisieren. Die Plattform analysiert Fehlkonfigurationen, Zugangspunkte zu Netzwerken, übermäßige Berechtigungen und Schwachstellen auf Kombinationen, die potenzielle Angriffspfade eröffnen. Mithilfe der kontextabhängigen Engine von Prisma Cloud identifiziert diese risikobasierte Analyse mehrere Schwachstellen in einer Cloud, die in einem ausgeklügelten Angriff ausgenutzt werden könnten.

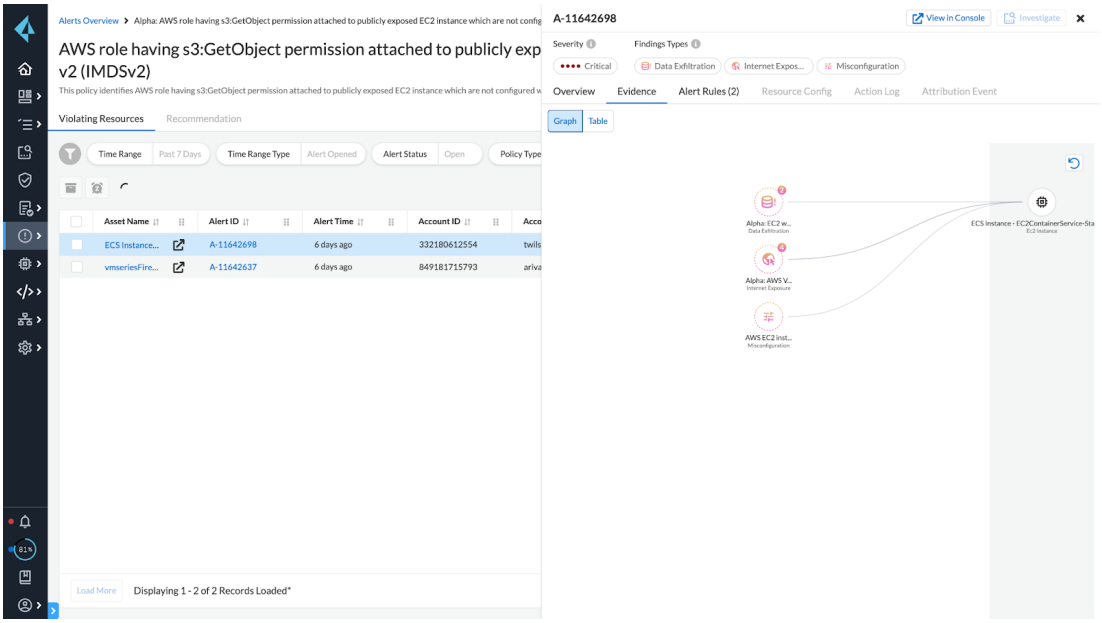

Abbildung 3: Untersuchung von Alarmen zu Angriffspfaden

Bedrohungserkennung

Analyse des Anwender- und Objektverhaltens (UEBA)

Prisma Cloud analysiert Millionen von Auditereignissen und nutzt maschinelles Lernen (ML), um ungewöhnliche Aktivitäten zu identifizieren, die eventuell auf kompromittierte Konten, Insiderbedrohungen, gestohlene Zugriffsdaten oder andere Sicherheitsverstöße hinweisen.

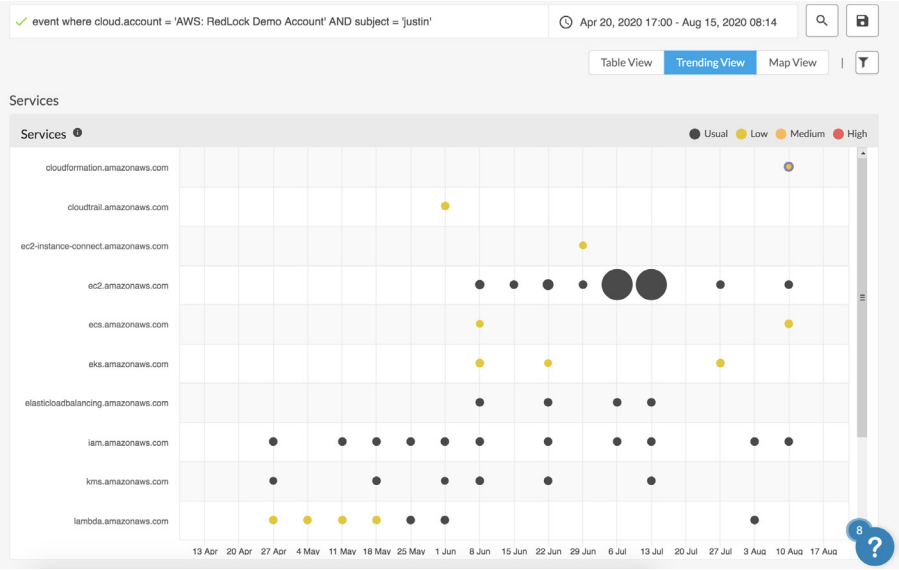

Abbildung 4: Anomaliesuche und -verfolgung

Erkennung von Netzwerkanomalien und Bedrohungen

Prisma Cloud überwacht das Netzwerkverhalten und nutzt ML sowie erweiterte Threat-Intelligence-Feeds, um Netzwerkanomalien und Bedrohungen zu erkennen. Mit Prisma Cloud erkennen Sie verdächtige Aktivitäten an Servern oder Hosts, wie z. B. Portscans und Portsweeps, sowie Bedrohungen, die im DNS-Datenverkehr (Domain Name System) versteckt sind, wie z. B. Domain-Generierungsalgorithmen (DGA) und Cryptomining-Aktivitäten.

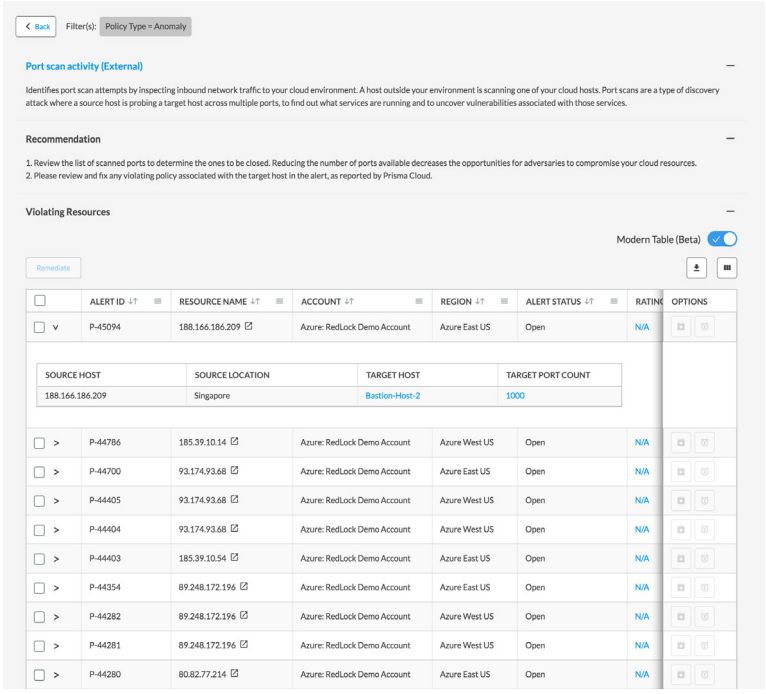

Abbildung 5: Portscan-Aktivitäten, Detailanzeige

Automatisierte Untersuchung und Reaktion

Prisma Cloud beinhaltet Funktionen für die automatisierte Behebung und eingehende forensische Untersuchung von Vorfällen sowie zur Erkennung von Zusammenhängen zwischen Ereignissen. Die aus verschiedenen Workloads, Netzwerken, Benutzeraktivitäten, Daten und Konfigurationen gewonnenen Erkenntnisse werden miteinander kombiniert, um die Untersuchung und Behebung von Vorfällen zu beschleunigen.

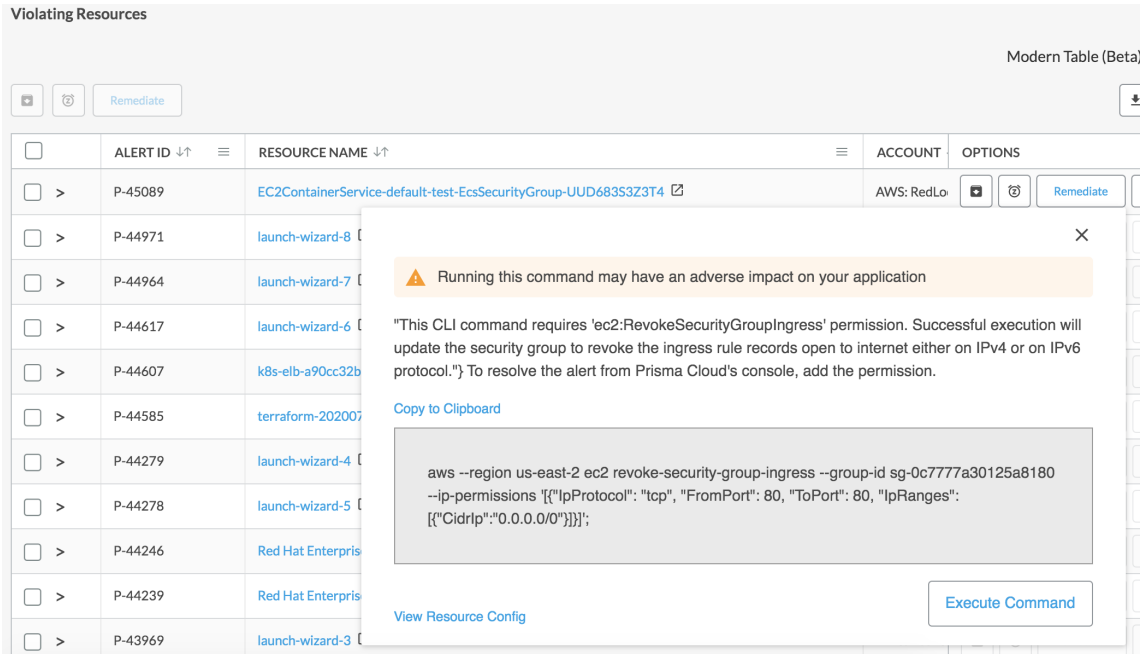

Abbildung 6: Automatisierte Untersuchung, Detailanzeige

Datensicherheit

Datentransparenz und -klassifizierung

Prisma Cloud bietet einen vollständigen Überblick über Buckets und Objekte im Amazon S3 und Microsoft Azure Storage. Diese können wahlweise auch nach Region, Eigentümer und Risikoniveau geordnet oder gefiltert angezeigt werden. Sie können Identifikatoren für Personalausweis-, Fahrerlaubnis-, Sozialversicherungs-, Kreditkartennummern usw. definieren, um sensible Inhalte zu identifizieren und zu überwachen.

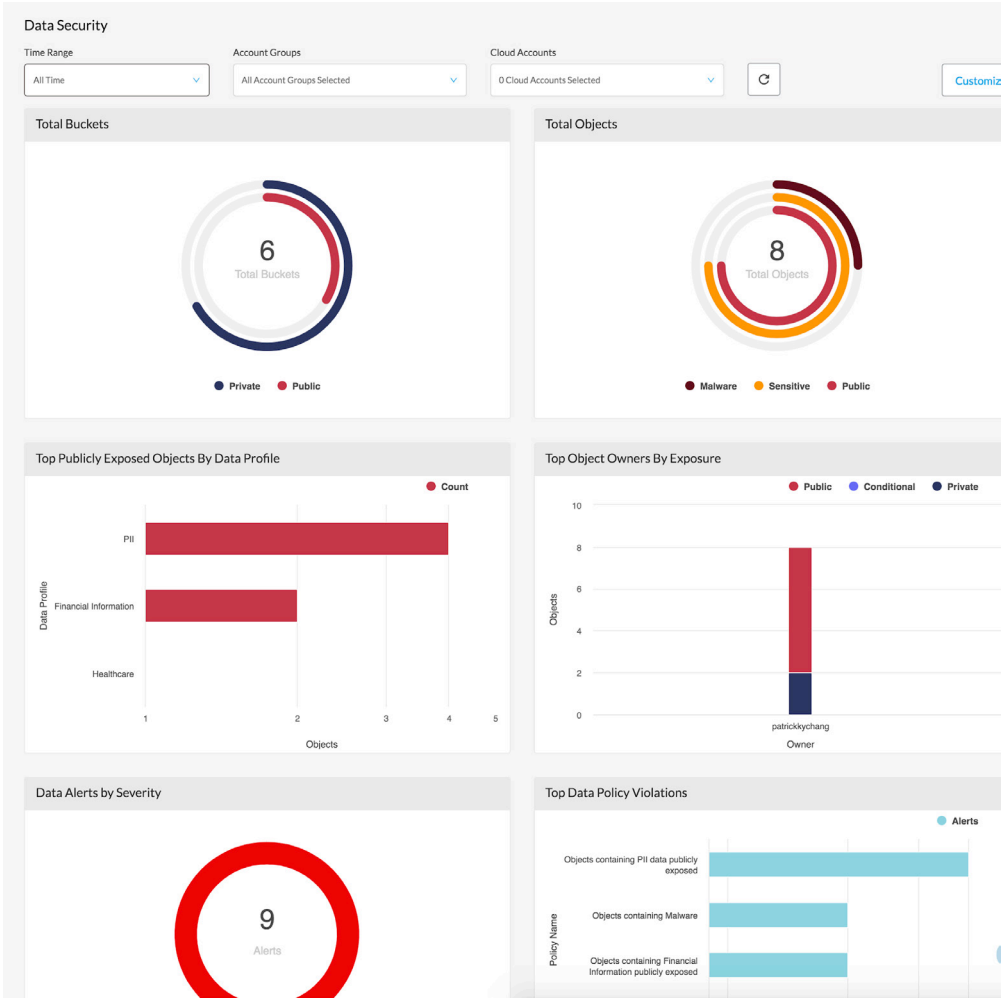

Abbildung 7: S3-Datensicherheitsdashboard

Daten-Governance

Prisma Cloud beinhaltet spezifische Datenrichtlinien, mit denen Sie Ihr Risikoprofil aufgrund der Datenklassifizierung und -sichtbarkeit bzw. des Dateityps ermitteln können. Sie können Bewertungsprofile für verschiedene Complianceframeworks Ihren Anforderungen entsprechend aktivieren bzw. deaktivieren (z. B. PCI, DSGVO, SOC 2 und HIPAA) und per Mausklick für Audits geeignete Berichte erstellen.

Malwareerkennung

Mit Prisma Cloud können Benutzer bekannte und neue dateibasierte Bedrohungen erkennen und stoppen, die in S3-Buckets und den Azure Storage Blob eingeschleust wurden. Dabei wird der Malwareschutzdienst WildFire genutzt, um Objekte zu identifizieren, die Malware enthalten.

Alarme und Entstörung

Prisma Cloud generiert unter Berücksichtigung der Datenklassifizierung, der Datensichtbarkeit und des Dateityps automatisch Alarme für jedes Objekt. So können Analysten schnell geeignete Gegenmaßnahmen einleiten, individuelle SecOps-Teams auf Sicherheitsverstöße aufmerksam machen und umgehend Objekte löschen, die Malware enthalten.

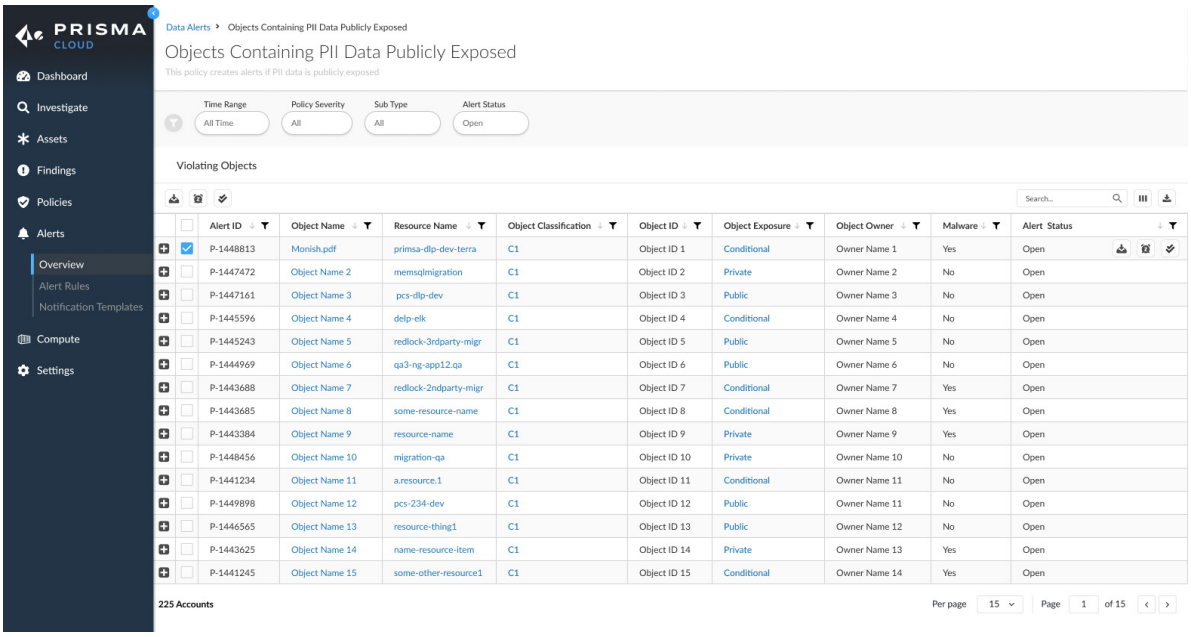

Abbildung 8: Ergebnisse eines Objektscans nach personenbezogenen Daten

„Als Manager schlafe ich ruhiger, seit ich weiß, dass dieses Tool unsere Umgebung pausenlos für mich überwacht. Meine Teams nutzen es sehr intensiv, manche arbeiten jeden Tag damit. Es hat die Art und Weise, wie wir für Compliance und Transparenz sorgen, grundlegend verändert."

– John Hluboky, Vice President of Information Security, Veradigm Health
Lesen Sie die vollständige Fallstudie.

Info zu Prisma Cloud

Prisma® Cloud ist eine umfassende Plattform zum Schutz cloudnativer Anwendungen, die mit branchenführenden Sicherheits- und Compliancefunktionen Anwendungen, Daten und den cloudnativen Technologiestack während des gesamten Entwicklungszyklus in Multi-Cloud- und Hybrid-Cloud-Umgebungen schützt. Mit ihrem integrierten Ansatz überwindet Prisma Cloud die mit cloudnativen Architekturen einhergehenden Einschränkungen bezüglich der Sicherheit, statt sie nur zu maskieren. Über den gesamten Anwendungslebenszyklus hinweg werden voneinander isolierte Sicherheitsprozesse miteinander verknüpft, was die Einführung eines DevSecOps-Ansatzes und schnellere Reaktionen auf sich ändernde Sicherheitsanforderungen in cloudnativen Architekturen ermöglicht.

Weitere Informationen finden Sie auf unserer Website und in dieser Demo.

paloalto® NETWORKS

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

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de