

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 Sicherheitsteams 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 Sicherheitsniveau 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	azure	120	87	⊖ 33	⊖ 18	⊕ 15	0	73%
	Azure Network Watcher	azure	31	31	0	0	0	0	100%
	Azure Resource Manager	azure	9	7	⊖ 2	0	0	⊕ 2	78%
	Azure Policy	azure	3	3	0	0	0	0	100%
	Azure SQL Database	azure	2	0	⊖ 2	⊖ 2	0	0	0%
	Azure Compute	azure	31	17	⊖ 14	⊖ 5	⊕ 9	0	55%
	Azure Storage	azure	13	0	⊖ 13	⊖ 1	⊕ 12	0	0%
	Azure App Service	azure	1	1	0	0	0	0	100%
	Azure Security Center	azure	2	0	⊖ 2	0	⊕ 2	0	0%
	Google Resource Manager	gcp	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.

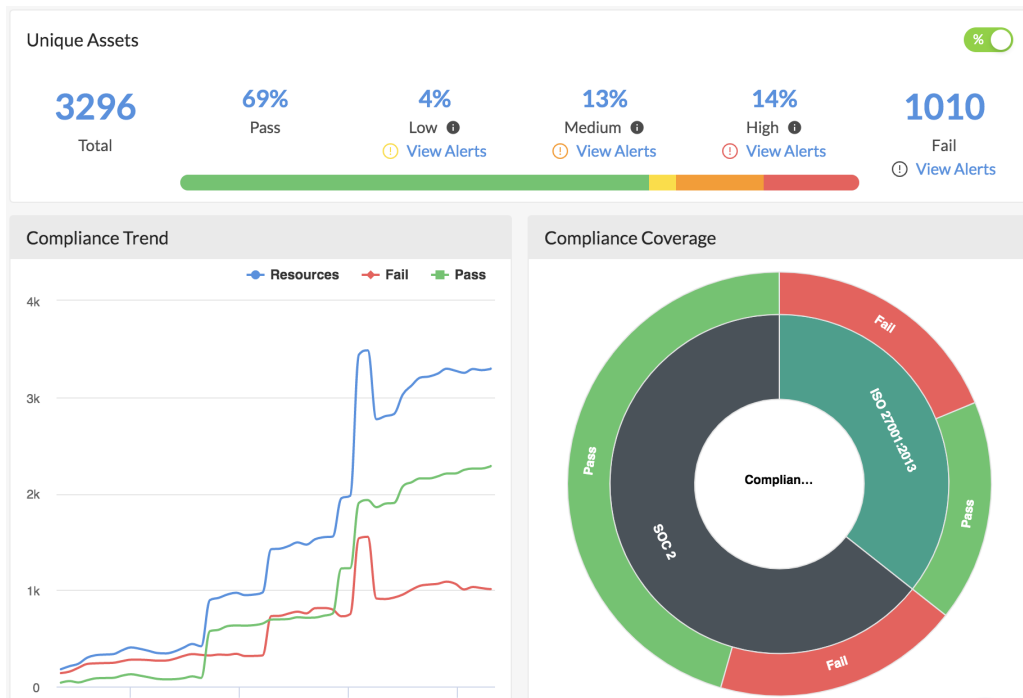


Abbildung 2: Compliedashboard

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.

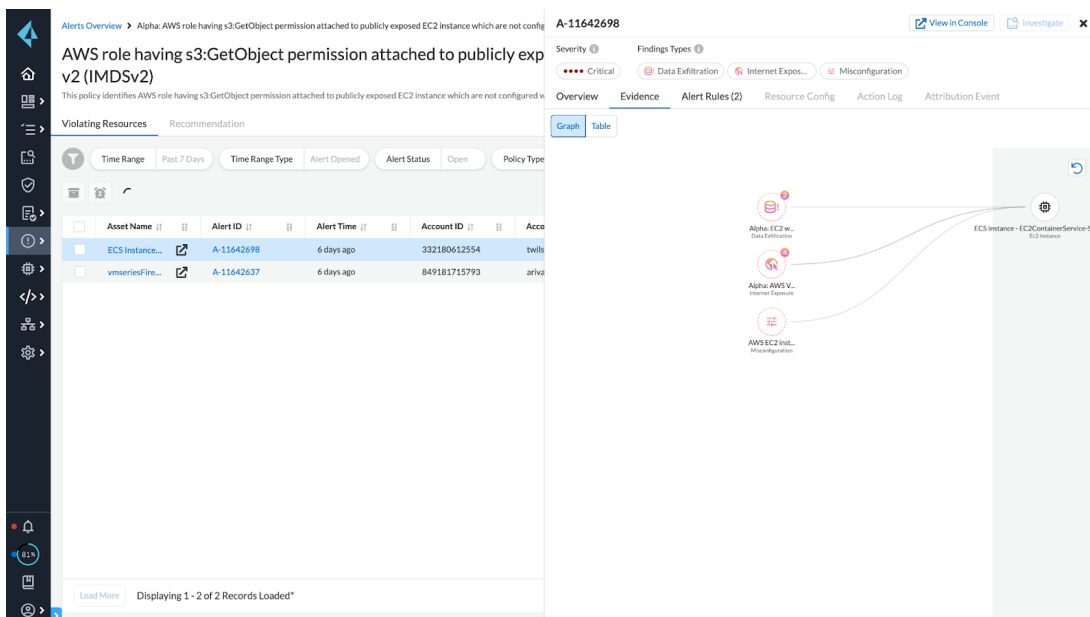


Abbildung 3: Untersuchung von Alarmen zu Angriffspfaden

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.

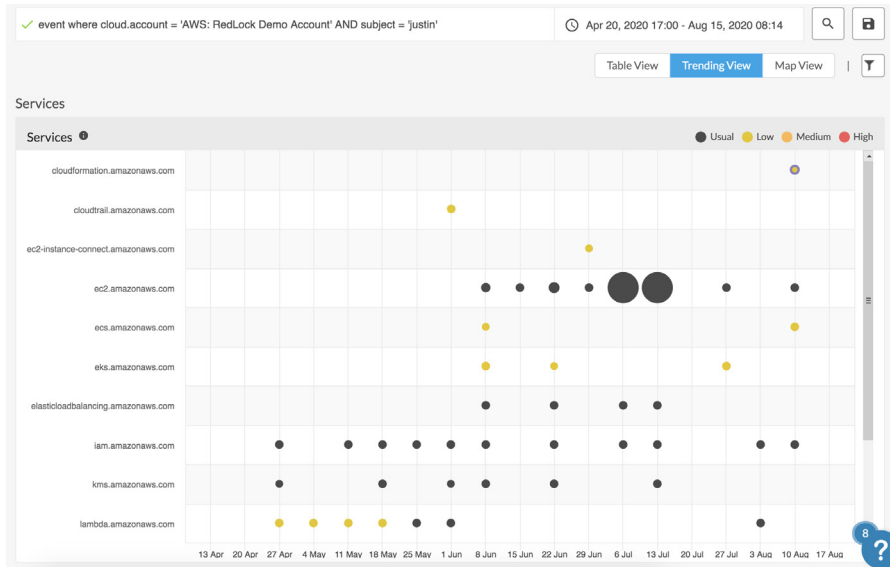


Abbildung 4: Anomaliesuche und -verfolgung

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.

The screenshot shows a detailed view of a port scan alert. The alert title is 'Port scan activity (External)'. The recommendation is to review scanned ports and fix any violating policies. The 'Violating Resources' table is shown below.

ALERT ID	RESOURCE NAME	ACCOUNT	REGION	ALERT STATUS	RATING	OPTIONS
P-45094	188.166.186.209	Azure: RedLock Demo Account	Azure East US	Open	N/A	
Violating Resources						
Modern Table (Beta) <input checked="" type="checkbox"/>						
	SOURCE HOST	SOURCE LOCATION	TARGET HOST	TARGET PORT COUNT		
	188.166.186.209	Singapore	Bastion-Host-2	1000		
	P-44786	185.39.10.14	Azure: RedLock Demo Account	Azure West US	Open	N/A
	P-44700	93.174.93.68	Azure: RedLock Demo Account	Azure East US	Open	N/A
	P-44405	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A
	P-44404	93.174.93.68	Azure: RedLock Demo Account	Azure West US	Open	N/A
	P-44403	185.39.10.54	Azure: RedLock Demo Account	Azure East US	Open	N/A
	P-44354	89.248.172.196	Azure: RedLock Demo Account	Azure East US	Open	N/A
	P-44282	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A
	P-44281	89.248.172.196	Azure: RedLock Demo Account	Azure West US	Open	N/A
	P-44280	80.82.77.214	Azure: RedLock Demo Account	Azure East US	Open	N/A

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.

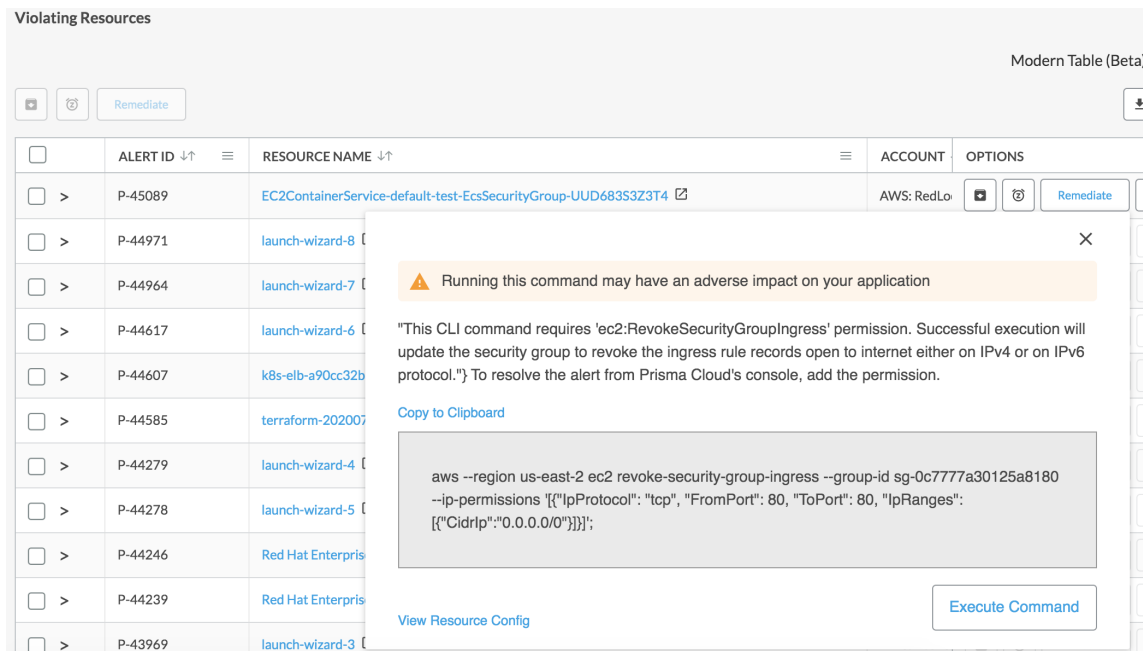


Abbildung 6: Automatisierte Untersuchung, Detailanzeige

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.

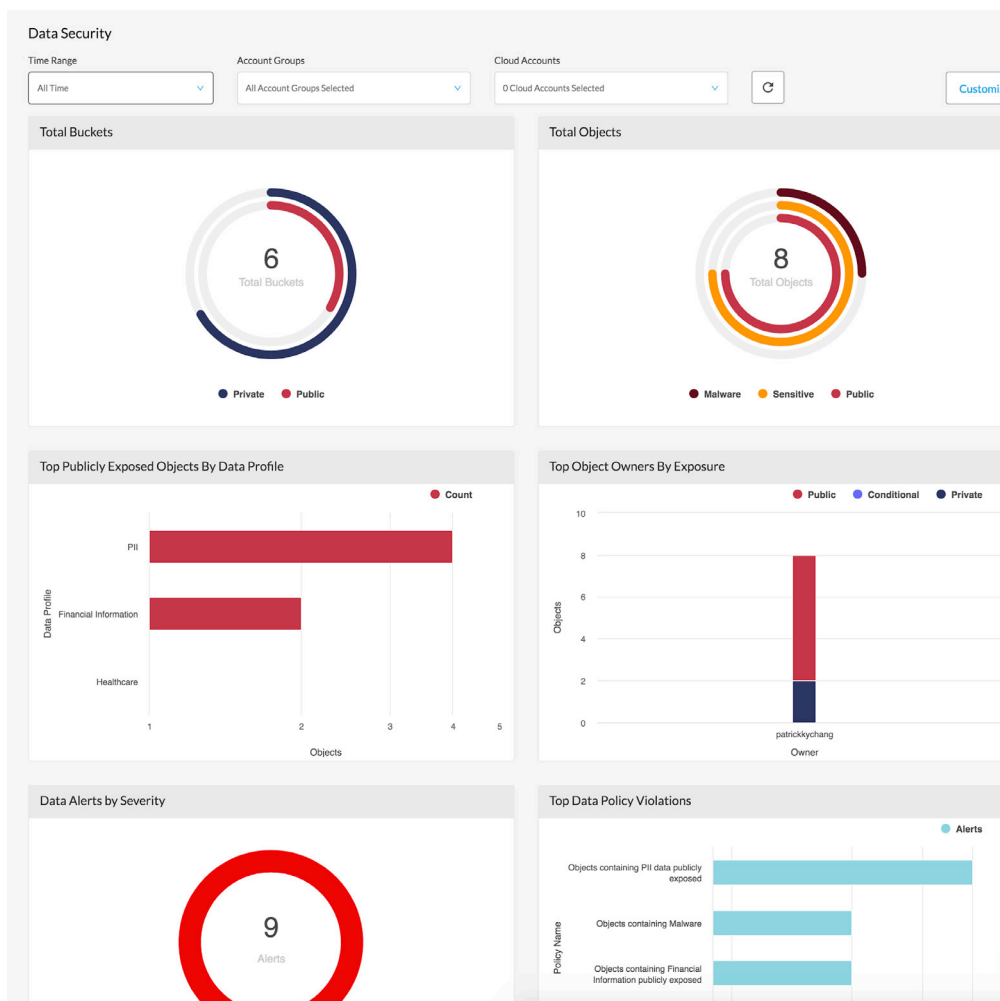


Abbildung 7: S3-Datensicherheitsdashboard

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.

Alarmer und Entstörung

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

PRISMA CLOUD Data Alerts > Objects Containing PII Data Publicly Exposed

Objects Containing PII Data Publicly Exposed
This policy creates alerts if PII data is publicly exposed

Time Range: All Time | Policy Severity: All | Sub Type: All | Alert Status: Open

Violating Objects

Alert ID	Object Name	Resource Name	Object Classification	Object ID	Object Exposure	Object Owner	Malware	Alert Status
P-1448813	Monish.pdf	prisma-dlp-dev-terra	C1	Object ID 1	Conditional	Owner Name 1	Yes	Open
P-1447472	Object Name 2	memsqlmigration	C1	Object ID 2	Private	Owner Name 2	No	Open
P-1447161	Object Name 3	pcs-dlp-dev	C1	Object ID 3	Public	Owner Name 3	No	Open
P-1445596	Object Name 4	delp-elk	C1	Object ID 4	Conditional	Owner Name 4	No	Open
P-1445243	Object Name 5	redlock-3rdparty-migr	C1	Object ID 5	Public	Owner Name 5	No	Open
P-1444969	Object Name 6	qa3-ng-app12.qa	C1	Object ID 6	Public	Owner Name 6	No	Open
P-1443688	Object Name 7	redlock-2ndparty-migr	C1	Object ID 7	Conditional	Owner Name 7	Yes	Open
P-1443685	Object Name 8	some-resource-name	C1	Object ID 8	Conditional	Owner Name 8	Yes	Open
P-1443384	Object Name 9	resource-name	C1	Object ID 9	Private	Owner Name 9	Yes	Open
P-1448456	Object Name 10	migration-qa	C1	Object ID 10	Private	Owner Name 10	No	Open
P-1441234	Object Name 11	a.resource.1	C1	Object ID 11	Conditional	Owner Name 11	No	Open
P-1449898	Object Name 12	pcs-234-dev	C1	Object ID 12	Public	Owner Name 11	No	Open
P-1446565	Object Name 13	resource-thing1	C1	Object ID 13	Public	Owner Name 12	No	Open
P-1443625	Object Name 14	name-resource-item	C1	Object ID 14	Private	Owner Name 13	Yes	Open
P-1441245	Object Name 15	some-other-resource1	C1	Object ID 15	Conditional	Owner Name 14	Yes	Open

225 Accounts | Per page: 15 | Page: 1 of 15

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](#).



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

© 2023 Palo Alto Networks, Inc. Palo Alto Networks und das Logo von Palo Alto Networks sind eingetragene Marken von Palo Alto Networks, Inc. Eine Liste unserer Marken ist unter <https://www.paloaltonetworks.com/company/trademarks.html> verfügbar. Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein. prisma_ds_cloud-security-posture-management_040423