Proofpoint Cloud App Security Broker IaaS Protection

Identifizierung falsch konfigurierter Cloud-Dienste und Schutz vertraulicher Daten im IaaS-Storage

HERAUSFORDERUNGEN

- Konfigurationsfehler
- Unbekannte Ressourcen und IaaS-Konten
- Datenverlust- und Compliance-Risiken
- Kompromittierte Cloud-Konten

WICHTIGE FUNKTIONEN

- Vereinfachen Sie Multi-Cloud-Sicherheit und Compliance mit zentraler Governance für alle IaaS-Ressourcen über Anbieter, Konten und Regionen hinweg
- Identifizieren Sie falsch konfigurierte Sicherheitseinstellungen, die von den veröffentlichten Baselines abweichen
- Überprüfen und analysieren Sie Anwenderverhalten, um nicht autorisierte Anmeldungen und Administrationsaktivitäten erkennen und unterbinden zu können
- Schützen Sie sensible Daten in IaaS-Speichern
- Entdecken und regeln Sie nicht genehmigte IaaS-Konten
- Schnelle Bereitstellung in der Cloud

PRODUKTE

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint CASB IaaS Protection

Die Nachfrage nach Cloud-Diensten wächst. Ebenso wie Unternehmen und IT-Teams möchten auch DevOps-Teams durch den Einsatz von SaaS-Anwendungen größer, flexibler und elastischer werden und entwickeln neue Anwendungen und Dienste auf Cloud-Infrastrukturen.

In Ihrem Unternehmen gibt es eventuell dutzende oder hunderte IaaS-Konten, die auf einem oder mehreren Cloud-Diensten arbeiten. Aufgrund der Datenschutzbestimmungen sind Sie möglicherweise dazu gezwungen, Ihre Daten in Cloud-Repositorys in verschiedenen Regionen der Welt zu speichern. Der fehlende Einblick in die Lücken in Ihrer Cloud-Sicherheitslage kann es schwierig machen, die IaaS-Sicherheit aufrechtzuerhalten und die Compliance zu gewährleisten. Außerdem können Cloud-Bedrohungen wie die Kompromittierung von Konten und der Mangel an gut geschultem Personal die Komplexität noch erhöhen.

Fehlkonfigurationen, Missmanagement und Fehler von Kunden können zu groß angelegten Sicherheitsverletzungen führen. Angriffe auf Cloud-Dienste wie Amazon Web Services (AWS), Microsoft Azure oder Google Cloud (GCP) können aus solchen Versäumnissen resultieren. Sicherheits- und Risikomanagement-Verantwortliche müssen diese Risiken identifizieren und abmildern. IaaS-Konten, Ressourcen und sensible Daten in Cloud-Speichern wie Kunden- oder Patientendaten sollten gesichert werden.

Um Ihre IaaS-Umgebungen zu schützen und Compliance zu gewährleisten, bietet Proofpoint CASB IaaS Protection (IaaS Protection):

- IaaS-Erkennung
- Cloud Security Posture Management (CSPM)
- Sicherheit der Daten
- Schutz vor Bedrohungen
- Adaptive Zugriffskontrollen

IaaS Protection ist eine Zusatzfunktion von Proofpoint CASB.

Identifizierung von Konfigurationsfehlern in IaaS-Umgebungen

IaaS Protection hilft Ihnen bei der Überwachung und Kontrolle der Sicherheitslage Ihrer Multi-Cloud-Umgebung. Diese Funktion in Proofpoint CASB erkennt Konfigurationen und Einstellungen, die von den festgelegten Basislinien in IaaS-Diensten abweichen. Dazu zählt zum Beispiel ein Root-Benutzerkonto, das keine Multifaktor-Authentifizierung verlangt. IaaS Protection überprüft die Einstellungen für virtuelle Maschinen, Storage, Netzwerke und Zugriffskontrollen anhand der folgenden vier Sicherheitsstandards:

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

Wenn die Lösung Konfigurationsfehler erkennt, die ein Sicherheitsrisiko darstellen, schlägt sie bewährte Methoden zur Korrektur vor.

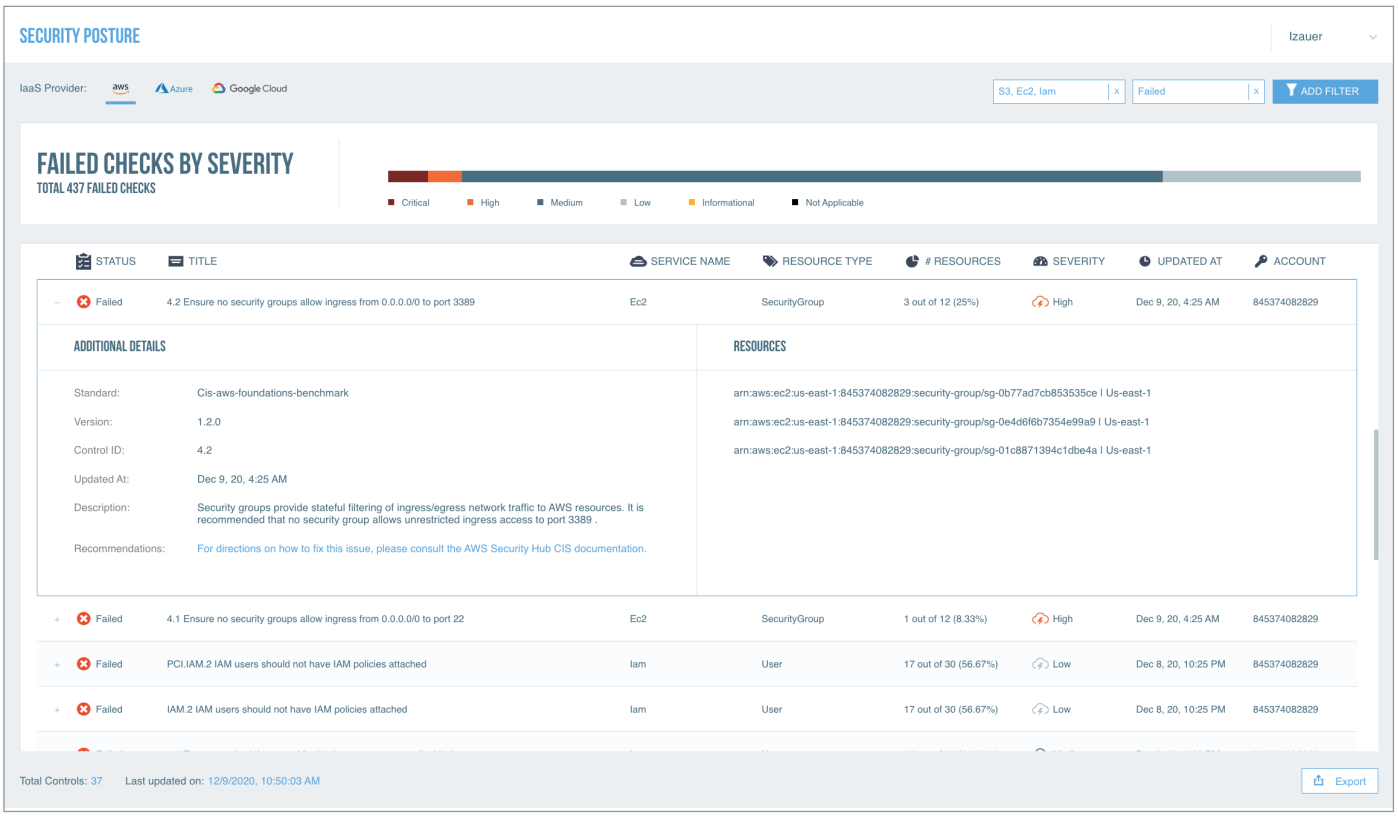

Abb. 1: Das Sicherheits-Dashboard zeigt einen Konfigurationsfehler, Anweisungen zur Erfüllung der Sicherheitsstandards und eine Liste von Ressourcen, die den Standard nicht erfüllen.

Überwachung und Kontrolle der Aktivitäten privilegierter Anwender

Anders als bei SaaS-Anwendungen handelt es sich bei den meisten Anwendern in der IaaS-Umgebung um privilegierte Anwender wie DevOps-Engineers oder Softwareentwickler, die IaaS-Ressourcen wie virtuelle Maschinen und Cloud-Storage bereitstellen, löschen und konfigurieren sowie Administratorrechte zuweisen können. Daher ist es äußerst wichtig, die Aktivitäten dieser privilegierten Anwender zu überwachen.

In Proofpoint CASB mit IaaS Protection lassen sich personenorientierte Richtlinien festlegen (Abb. 2), die auf umfangreichem Kontext basieren und nicht autorisierte Aktivitäten privilegierter Anwender melden. Der Kontext umfasst Anwenderstandort, Gerät und Netzwerk sowie jede Cloud-Anwendung, auf die zugegriffen wird. So können Sie zum Beispiel verhindern, dass Bucket-Berechtigungen von gesperrten Ländern aus geändert werden.

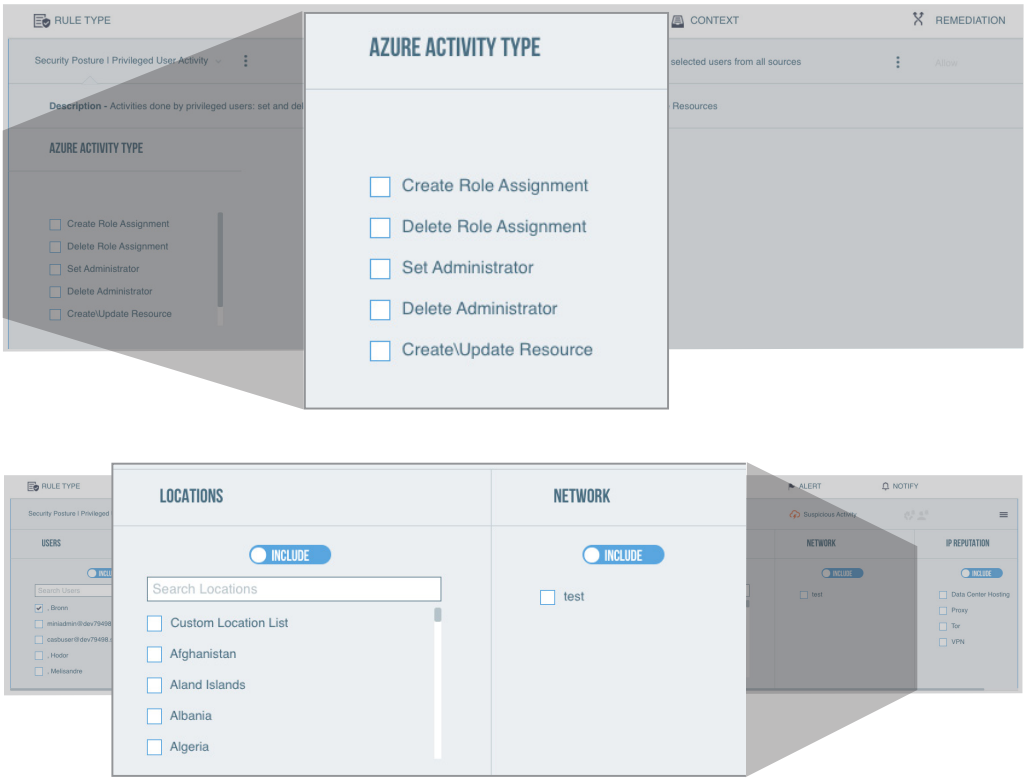

Abb. 2: Regelvorlage zur Erstellung von Richtlinien für Aktivitäten privilegierter Anwender.

Entdecken Sie alle IaaS-Ressourcen

Mit Proofpoint CASB vereinfachen Sie die Multi-Cloud- und Multi-Regionen-IaaS-Sicherheit und Compliance mit zentralem Management. Und Sie erhalten Einblick in alle Ihre SaaS-Anwendungen und IaaS-Ressourcen über IaaS-Anbieter, Konten und Regionen hinweg (Abb. 3).

Sie können Trends bei der Ressourcenerstellung visualisieren und nach Anomalien wie übermäßige Ressourcenerstellung oder -löschung suchen. Sie können die entdeckten Ressourcen auch nach Typ und Region aufschlüsseln und sicherstellen, dass die Konten gemäß den Vorschriften und Best Practices bereitgestellt werden – wenn Sie beispielsweise ein multinationales oder europäisches Unternehmen sind, können Sie die außerhalb der EU bereitgestellten Buckets überwachen, um Verstöße gegen die Datenschutzgrundverordnung zu verhindern.

Entdecken Sie unprovisionierte IaaS-Konten

Proofpoint CASB gibt Ihnen Einblick in die Schatten-IT in Ihrem Unternehmen. Dazu gehören IaaS-Konten, die nicht von der IT-Abteilung genehmigt oder dokumentiert sind (Abb. 4). Wir helfen Ihnen bei der Prüfung von Netzwerkverkehrsprotokollen. Sie können Cloud-Apps und IaaS-Konten entdecken, auf die in Ihrem Netzwerk zugegriffen wird. Dazu können von der IT genehmigte, nicht dokumentierte und möglicherweise private IaaS-Konten gehören. Wenn Sie nicht genehmigte Konten auditieren, können Sie deren Status in der CASB-Konsole verfolgen. Wenn Sie zum Beispiel undokumentierte Konten entdecken, die bei einer Fusion erworben wurden, können Sie diese nach Sicherheitsmaßstäben bereitstellen, um Compliance zu gewährleisten.

Abb. 3: Das Dashboard zu den erkannten IaaS-Umgebungen mit Ressourcen-Trends, Standorten und Typen.

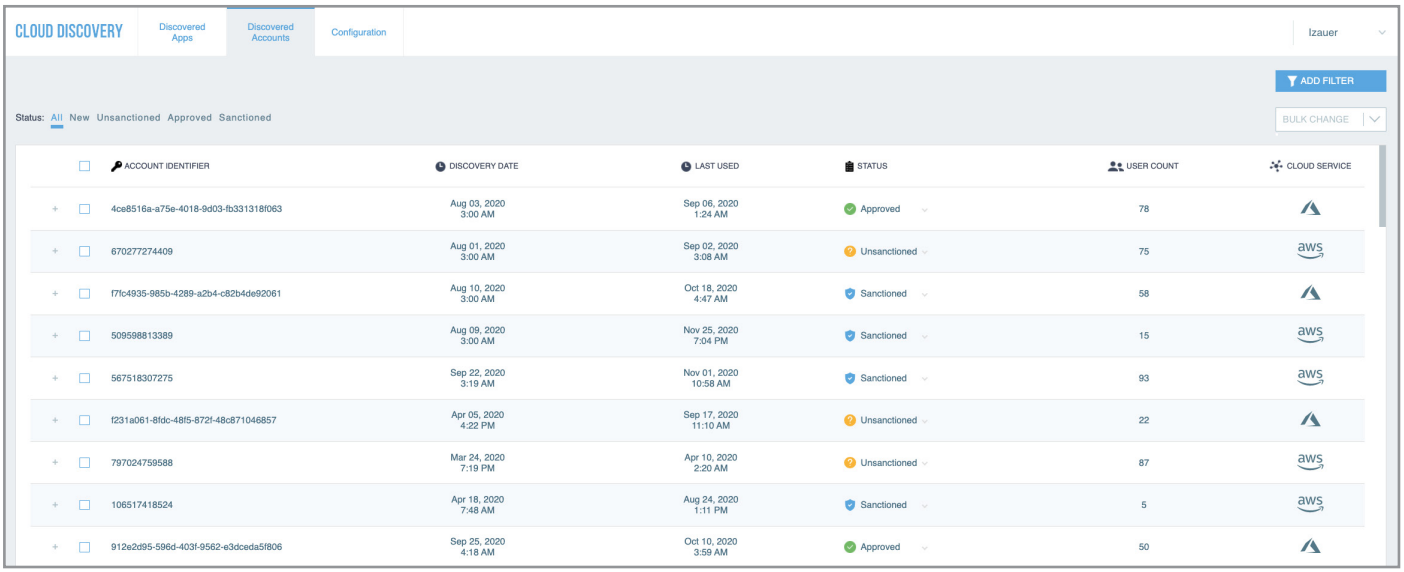

Abb. 4: Das Dashboard zeigt den Status der auf dem Netzwerk erkannten IaaS-Konten.

Schützen Sie sensible Daten im Cloud-Speicher

Proofpoint CASB mit IaaS Protection bietet Hilfe bei der Identifizierung und Klassifizierung vertraulicher Daten auf Ihren Cloud-Repositorys, z. B. AWS S3-Buckets und Azure Storage Blob-Container, und bietet folgende Funktionen:

- Überwachung von Datei-Aktivitäten auf DLP-Verstöße
- Überwachung von Buckets und Containern auf übermäßige Freigabe
- Erstellung von Datensicherheitsrichtlinien mithilfe von DLP-Klassifikatoren, einschließlich integrierter Smart Identifier, Wörterbücher, Regeln und Vorlagen, die mit anderen Proofpoint DLP-Produkten gemeinsam genutzt werden

Unsere Out-of-Box-Klassifikatoren helfen Ihnen, die Zeit zu verkürzen, um regulierte Daten in Cloud-Speichern zu entdecken und zu schützen und dabei zudem die Vorschriften einzuhalten. Mit CASB als Bestandteil von Proofpoint Enterprise DLP lassen sich einheitliche DLP-Richtlinien für alle Ihre SaaS-Anwendungen, IaaS-Buckets, E-Mails und Endgeräte festlegen. Zusätzlich ermöglicht es die zentrale Verwaltung von DLP-Zwischenfällen für diese Kanäle auf einer einzigen Konsole. Durch die Kombination der Telemetriedaten zu Inhalt, Verhalten und Bedrohung aus mehreren Kanälen können Sie einschätzen, ob der Anwender, der die DLP-Warnung ausgelöst hat, kompromittiert wurde oder böswillig oder fahrlässig agiert.

Proofpoint CASB DLP-Funktionen umfassen:

- 240 integrierte Klassifikatoren, die Gesetze wie PCI DSS und DSGVO sowie Vorschriften zu personenbezogenen Informationen und geschützten Gesundheitsdaten abdecken
- Wörterbücher und Proximity Matching zur Verbesserung der DLP-Erkennung
- Exakter Datenabgleich zur Automatisierung des Hochladens von benutzerdefinierten Wörterbüchern oder Identifikatoren, um Informationen zu erkennen, die für Ihr Unternehmen einzigartig sind, einschließlich Kontonummern und anderer strukturierter Daten aus Datenbanken
- Document Fingerprinting zur Erkennung sensibler Daten in unstrukturierten Inhalten, einschließlich Formeln, Quellcode, Formularen, Verträgen und anderem geistigen Eigentum
- Unterstützung von 300 Dateitypen und ein Dateityp-Profiler zur Unterstützung neuer, benutzerdefinierter oder proprietärer Dateitypen

Flexible Regelvorlagen ermöglichen die Erstellung von Richtlinien, die Inhalte, Benutzerverhalten und Bedrohungen berücksichtigen (Abb. 5), damit Sie kontrollieren können, wie Ihre Daten weitergegeben und hoch- bzw. heruntergeladen werden. Sie können zudem Freigabeberechtigungen für Buckets automatisch einschränken, um Compliance zu gewährleisten, z. B. indem Sie nach Buckets aus gesperrten Ländern mit ungewöhnlich hohem Datenaustausch suchen und diese sperren.

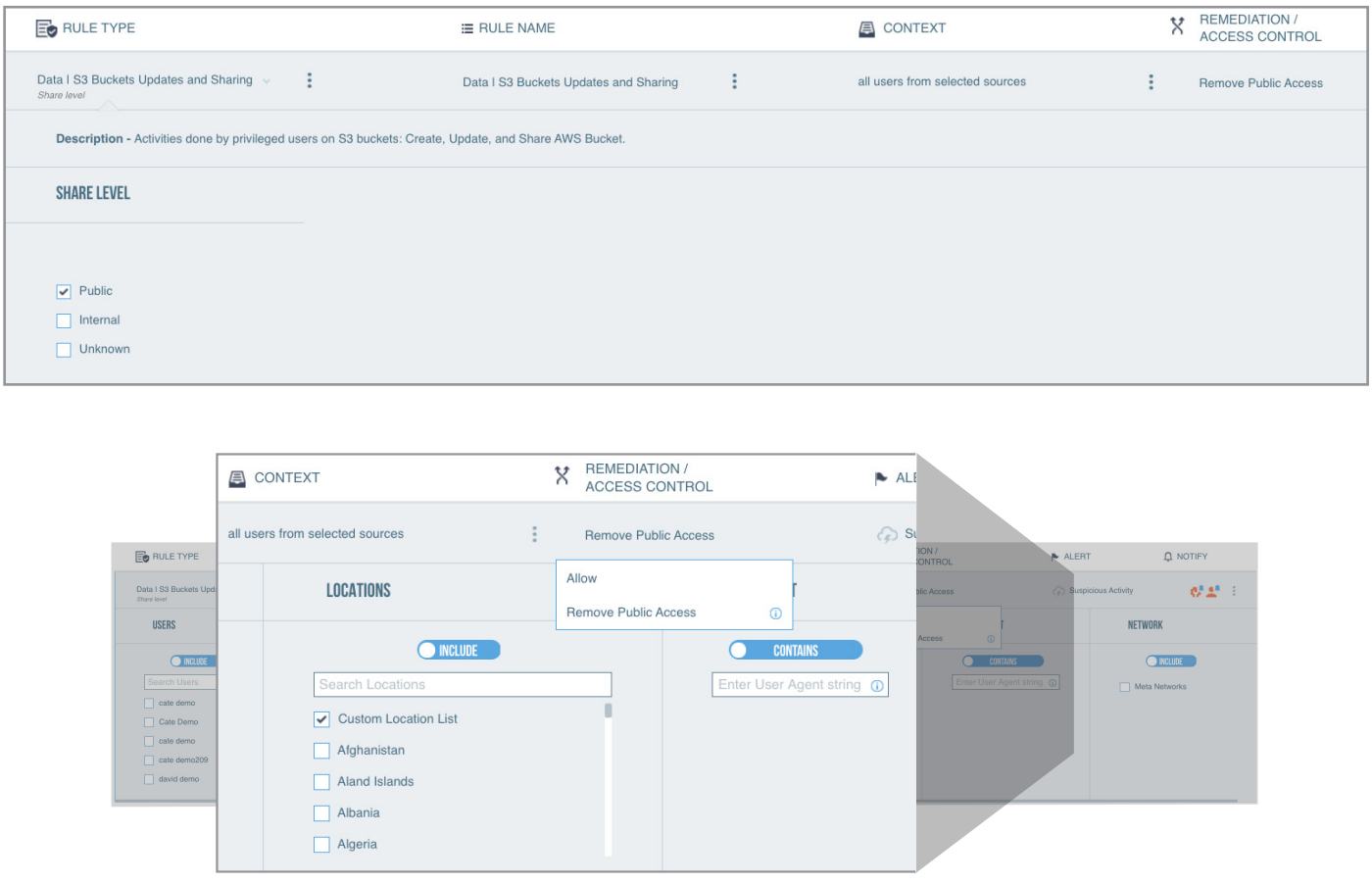

Abb. 5: Regelvorlage zur Erstellung von Richtlinien zur Überwachung von Datenweitergaben in Buckets/Containern.

Auch lassen sich DLP-Zwischenfälle leichter untersuchen, da verdächtige Logins oder falsch konfigurierte Buckets mit DLP-Zwischenfällen korreliert werden und sich Ereignisse und Warnungen für Berichte filtern lassen. Zudem können Sie Warnmeldungen abonnieren, um die Compliance genau zu überwachen.

Adaptive Zugriffskontrollen und Bedrohungsschutz

Die IaaS-Management-Konsole ist eine webbasierte Anwendung zur Erstellung und Verwaltung von Cloud-Ressourcen. Der Zugriff auf dieses leistungsfähige Tool muss streng überwacht werden. Die adaptiven Zugriffskontrollen von CASB ermöglichen Echtzeit-Sicherheitsmaßnahmen auf Grundlage von Risiko, Kontext und Rolle. Die Lösung bietet folgende Funktionen:

- Schutz Ihrer IaaS-Umgebung durch Festlegen von Richtlinien, die den Zugang von unsicheren Standorten und Netzwerken sowie durch Bedrohungsakteure sperren
- Risikobasierte Kontrollen – darunter starke Authentifizierung, Richtlinienregeln für verwaltete Geräte und VPN-Durchsetzung – für stark gefährdete und umfassend berechtigte Anwender

Proofpoint CASB kombiniert umfangreiche vektorübergreifende Bedrohungsdaten (Cloud, E-Mails u. a.) aus Proofpoint Nexus Threat Graph mit benutzerspezifischen Kontextdaten. Machine Learning hilft uns bei der Analyse der Daten auf Anwenderverhalten und der Erkennung von Anomalien in Cloud-Anwendungen und bei Mandanten. Unsere Lösungen bieten folgende Vorteile:

- Erkennung kompromittierter Cloud-Konten
- Untersuchung früherer Aktivitäten und Warnungen, z. B. verdächtige Zugriffe auf Ihre föderierten IaaS-Dienste

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.