Proofpoint-Lösungen und Amazon Web Services

Personenzentrierte Sicherheit und Compliance für AWS-Kunden

Produkte

- Adaptive Zugriffsberechtigungen
- Proofpoint Cloud App Security Broker (CASB)
- Sicherheitsverwaltung für Cloud-Umgebungen
- Proofpoint Email Fraud Defense
- Proofpoint Emerging Threats Intelligence
- Proofpoint Enterprise Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Threat Response Auto-Pull
- Zero-Trust-Netzwerkzugang

Wichtige Vorteile

- Vereinfachte regionenübergreifende Sicherheit und Compliance für AWS durch zentrale Verwaltung
- Erkennung und Klassifizierung vertraulicher Daten in Cloud-Repositorys
- Blockierung verdächtiger Anmeldeversuche und Verhinderung von Kontoübernahmen bei AWS-Ressourcen
- Überblick über Anwender- und Datenaktivitäten in allen AWS-EC2-Instanzen und Amazon WorkSpaces
- Sicherer Fernzugriff für Ihr Team
- Schädliche E-Mails, die vorhandene E-Mail-Filter passiert haben, werden automatisch unter Quarantäne gestellt

Cloud-Plattformen wie Amazon Web Services (AWS) haben die Geschäftswelt grundlegend verändert. Mitarbeiter nutzen sie heute, um im Homeoffice in der Cloud zu arbeiten, und Unternehmen können durch sie Kosten sparen, flexibler agieren und Innovationen schneller entwickeln. Im Zuge dieses Wandels verlagern Bedrohungsakteure ihre Anstrengungen vom alten Netzwerk-Perimeter auf die Anwender sowie die Daten, Systeme und Ressourcen, auf die sie zugreifen.
In dieser veränderten Landschaft müssen Sie sicheren Zugang zu AWS-Ressourcen gewährleisten, Datenverlust verhindern und Compliance-Vorschriften einhalten. Proofpoint verfügt über eine Reihe von Produkten, die Sie dabei unterstützen.

Unsere Lösungen helfen Ihnen mit den folgenden Problemen:

- Schatten-IT
- Kompromittierte Konten
- Compliance-Verletzungen
- E-Mail-Spoofing
- Nicht autorisierter Zugriff
- Datenverlust und -exfiltration
- Bedrohungen durch Insider
- Verdächtige Netzwerkaktivitäten

Erkennung von AWS-Ressourcen und -Konten

Proofpoint Cloud App Security Broker (CASB) kombiniert personenzentrierte Kontrollen mit der Erkennung kompromittierter Cloud-Konten, DLP und Governance für Cloud- und Drittanbieter-Anwendungen. Die Lösung hilft Ihnen, Cloud-Plattformen wie AWS zu schützen. Unser Multimodus-CASB unterstützt Bereitstellungsmodelle, die auf APIs oder Proxys basieren.

Proofpoint CASB vereinfacht die regionenübergreifende Sicherheit und Compliance für AWS durch eine zentrale Verwaltung. Sie erhalten einen Überblick über Ihre gesamten SaaS-Anwendungen (Software as a Service) und IaaS-Ressourcen (Infrastructure as a Service) in AWS.

Die Lösung bietet folgende Funktionen:

- Visualisierung von Trends bei der Ressourcenerstellung für die Suche nach Anomalien wie extrem häufige Ressourcenerstellung oder -löschung
- Anzeige weiterer Details der erkannten Ressourcen, um zu gewährleisten, dass Konten gemäß gesetzlichen Vorschriften und bewährten Methoden bereitgestellt werden
- Auswertung von Netzwerkprotokollen, um Cloud-Anwendungen sowie AWS-Konten zu erkennen, die auf Ihr Netzwerk zugreifen

Schutz vor Cloud-Bedrohungen

Die adaptiven Zugriffskontrollen von Proofpoint CASB ermöglichen Echtzeit-Sicherheitsmaßnahmen auf Grundlage von Risiko, Kontext und Rolle. Sie blockieren automatisch Zugriffsversuche von gefährlichen Standorten und Netzwerken oder Anmeldeversuche bekannter Bedrohungsakteure. Zudem werden risikobasierte Kontrollen für stark gefährdete und umfassend berechtigte Anwender durchgesetzt. Zu den risikobasierten Kontrollen gehören zum Beispiel starke Authentifizierung, Richtlinienregeln für verwaltete Geräte und VPN-Durchsetzung.

Adaptive Zugriffskontrollen blockieren verdächtige Anmeldeversuche und verhindern eine Kontoübernahme Ihrer AWS-Ressourcen.

Sie bieten folgende Funktionen:

- Blockierung des Zugriffs auf besonders gefährdete Anwenderkonten aufgrund verdächtiger Anmeldeversuche
- Erstellung einer Blocklist von Ländern, in denen Ihr Unternehmen keine Niederlassung unterhält

Identifizierung falsch konfigurierter Dienste

Die Sicherheitsverwaltung für Cloud-Umgebungen (Cloud Security Posture Management, CSPM) ist Teil des Proofpoint CASB-Angebots. CSPM hilft Ihnen bei der Überwachung und Kontrolle der Sicherheitslage Ihrer Cloud-Umgebung. Mit der Lösung können Sie Ihre Cloud-Ressourcen organisieren, konfigurieren und pflegen. Zudem hilft CSPM Ihnen, Compliance-Vorgaben einzuhalten.

Die Lösung bietet folgende Funktionen:

- Identifizierung von Sicherheitskonfigurationen und -einstellungen, die von festgelegten Basislinien abweichen
- Empfehlung bewährter Methoden zur Korrektur erkannter Fehlkonfigurationen, die ein Sicherheitsrisiko darstellen
- Vereinfachte Cloud-Sicherheit und Compliance durch zentralisierte Governance für Cloud-Ressourcen aller Konten und Regionen

Schutz vertraulicher Daten

Proofpoint Enterprise Data Loss Prevention (DLP) führt unsere DLP-Lösungen für E-Mail, Cloud sowie Endgeräte zusammen und kombiniert Telemetriedaten zu Inhalten, Verhalten und Bedrohungen aus diesen Kanälen. Das gibt Ihnen die Möglichkeit, die gesamte Bandbreite an personenzentrierten Datenrisiken zu bewältigen.

Zudem unterstützt Proofpoint Enterprise DLP Sie bei der Erkennung und Klassifizierung vertraulicher Daten in Cloud-Repositorys.

Die Lösung bietet folgende Funktionen:

- Suche nach Dateiaktivitäten, die gegen DLP-Richtlinien verstoßen
- Suche nach ungewöhnlich umfangreicher Datenweitergabe in S3-Buckets
- Erstellen von Datensicherheitsrichtlinien mithilfe von 240 integrierten Klassifizierern, einschließlich integrierter intelligenter Identifikatoren, Wörterbücher, Regeln und Vorlagen, die gemeinsam mit anderen Proofpoint DLP-Produkten genutzt werden

Schutz Ihrer AWS-Konten

Amazon GuardDuty schützt AWS-Instanzen mit Proofpoint Emerging Threats (ET) Intelligence.

Proofpoint ET Intelligence ist die schnellste und zuverlässigste Bedrohungsdatenquelle der Branche. Die Lösung kombiniert eine Datenbank global erfasster Bedrohungen und Malware-Analysen mit minutenaktuellen IP- und Domänenreputations-Feeds, damit Ihre Sicherheitsexperten die nötigen Daten und Kontext haben, um schädliche Angriffe zu untersuchen und abzuwehren.

Wir bieten Ihnen Produkte und Lösungen der nächsten Generation für Sicherheit, Compliance, digitale Risiken und Reaktion. Unsere IP- und Domänenreputationsdaten für ET basieren auf einem der umfangreichsten Angebote im Bereich der Sicherheitstechnologien und umfassen E-Mails, Mobilgeräte, soziale Netzwerke sowie SaaS- und Netzwerkumgebungen.

Umgang mit Insider-Bedrohungen

Proofpoint ITM ist Teil der Proofpoint Information and Cloud Security-Plattform und schützt vor Datenverlust, schädlichen Aktionen und Markenschädigung durch Insider. Proofpoint ITM schützt Sie vor nicht autorisierten sowie böswillig oder fahrlässig handelnden Anwendern und korreliert Anwenderaktivitäten und Datenbewegungen, um Datenschutzverletzungen durch Insider zu verhindern.

Proofpoint ITM liefert Ihnen einen Überblick über Anwender- und Datenaktivitäten in allen AWS-EC2-Instanzen und Amazon WorkSpaces.

Die Lösung bietet folgende Funktionen:

- Vollständiger Überblick über endpunktbasierte Aktivitäten, um vollständigen Kontext zu von Anwendern verursachten Zwischenfällen zu liefern
- Visualisierung des Bedrohungskontexts zu bestimmten Anwendergruppen, um Anwenderrisiken besser zu verwalten

Sicherer Fernzugriff auf Cloud-Anwendungen

Proofpoint ZTNA ist eine personenzentrierte Zero-Trust-Alternative zur VPN-Technologie. Die Lösung bietet sicheren Fernzugriff auf Unternehmensanwendungen, ganz gleich, wo die Anwendungen gehostet werden. Mit Proofpoint ZTNA erhalten Ihre Anwender sicheren mikrosegmentierten Zugriff auf hunderte Cloud-Instanzen. Mit der Lösung können Sie Cloud-zu-Cloud-Verbindungen automatisieren und hybride Cloud-Netzwerke zwischen lokalen Servern und öffentlichen Clouds aufbauen.

Proofpoint ZTNA ermöglicht Mitarbeitern, Auftragnehmern, Partnern sowie Kunden sicheren Fernzugriff auf Anwendungen, die auf AWS gehostet werden.

Die Lösung bietet folgende Funktionen:

- Verwaltung von Fernzugriffsrichtlinien für alle Unternehmensressourcen in Ihrem Rechenzentrum oder in der AWS-Cloud über eine zentrale Konsole
- Eine Zero-Trust-Alternative, die segmentierten, verifizierten und geprüften Zugriff für jeden Anwender bietet

Gestärktes Vertrauen in E-Mails

Proofpoint Email Fraud Defense (EFD) schützt Ihr Unternehmen vor E-Mail-Betrug. Die Lösung bietet Ihnen einen vollständigen Überblick über Doppelgänger-Domänen sowie E-Mails, die über Ihre Domänen verschickt werden, und hilft Ihnen bei der Minimierung von Risiken durch Lieferanten. Zudem identifiziert die Lösung Ihre Lieferanten sowie Doppelgänger-Domänen, die von Dritten registriert werden.

Proofpoint EFD schützt E-Mails, die über Amazon SES verschickt werden und unterstützt Sie mit Transparenz, Tools und Diensten bei der Autorisierung legitimer E-Mails.

Die Lösung bietet folgende Funktionen:

- Behebung falsch konfigurierter E-Mail-Versandsysteme sowie von Zustellungsproblemen in Verbindung mit Validierungsprüfungen bei der E-Mail-Authentifizierung
- Erkennung und Meldung von E-Mail-Spoofing
- Aufdeckung von Problemen mit DKIM-Signierung und SPF, von denen E-Mail-Empfänger berichten

Automatisches Verschieben schädlicher E-Mails in die Quarantäne

Die Proofpoint TRAP-Appliance (Threat Response Auto-Pull) kann auf AWS gehostet werden. Ihr Sicherheitsteam kann mit der Lösung E-Mails analysieren und schädliche Nachrichten automatisch entfernen lassen. Ebenso können unerwünschte E-Mails nach der Zustellung aus den Postfächern der Anwender unter Quarantäne gestellt werden.

Proofpoint TRAP hilft Ihnen, den Reaktionsprozess bei E-Mail-Zwischenfällen zu optimieren. Sie erhalten eine leistungsstarke Lösung, die den Zeitaufwand für die Bereinigung von E-Mails für Ihre Sicherheitsteams verringert.

Die Lösung bietet folgende Funktionen:

- Automatische Überwachung des Postfachs auf Bedrohungen
- Exponentielle Zeitersparnis für Sicherheits- und Messaging-Teams bei der Orchestrierung und Beantwortung von E-Mail-Sicherheitsfragen
- Stellt auch schädliche Nachrichten unter Quarantäne, die an Personen oder Verteilerlisten weitergeleitet wurden

Weitere Informationen über die Partnerschaft zwischen Proofpoint und AWS erhalten Sie unter **proofpoint.com/us/partners/aws**.

WEITERE INFORMATIONEN

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

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0201-023-01-01 9/21