Proofpoint Cloud App Security Broker

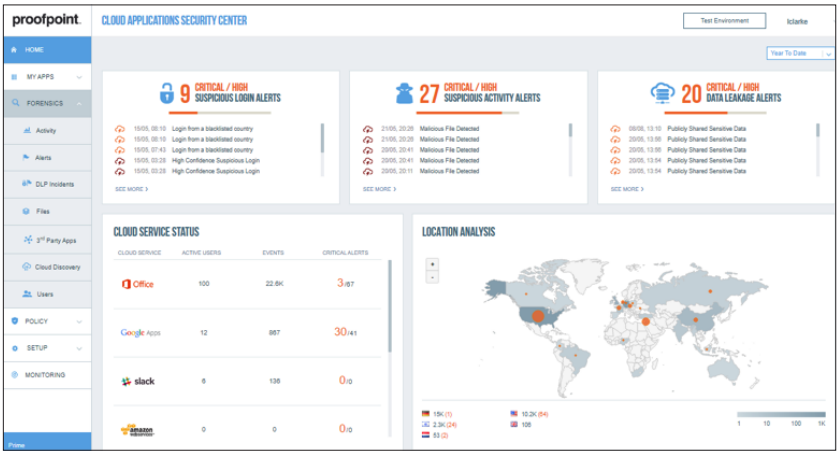
Mehr Überblick und Kontrolle über Ihre Cloud-Anwendungen

WICHTIGE VORTEILE

- Schutz der Cloud-Anwender durch personenorientierten Einblick in Bedrohungen und adaptive Zugriffsberechtigungen für Cloud-Anwendungen
- Beschleunigte Erkennung regulierter Cloud-Daten und Implementierung geeigneter Schutzmaßnahmen mithilfe standardmäßiger DLP-Richtlinien
- Schutz vertraulicher Daten und Vereinfachung von Abläufen mit genauem und einheitlichem Schutz vor Datenverlust für die wichtigsten zwei Vektoren – Cloud-Anwendungen und E-Mails
- Erkennung von Cloud-Anwendungen und Eindämmung von Schatten-IT einschließlich Drittanbieter-OAuth-Anwendungen
- Suche nach IaaS-Konten und -Ressourcen, Überwachung von Konten auf verdächtige Aktivitäten und Verbesserung der Cloud-Sicherheitslage
- Installation innerhalb von Tagen und nützliche Ergebnisse in weniger als vier Wochen

Cloud Computing befindet sich auf dem Vormarsch – von Unternehmensseite ebenso wie vonseiten der Mitarbeiter selbst. Eine Netzwerkperipherie, hinter der sich die Anwender, Anwendungen und Daten befinden, existiert nicht mehr. Oftmals haben die IT-Abteilungen in den Unternehmen keinen Überblick darüber, wie Ihre Mitarbeiter vertrauliche Daten weitergeben – und ob sie dafür auch private Geräte verwenden. Die Gewährleistung der Sicherheit der Daten ist in diesem Umfeld eine enorme Herausforderung. Gleichzeitig entwickeln sich Cyberangriffe immer weiter. Cyberkriminelle kompromittieren Cloud-Konten und stehlen Geld und Daten. Proofpoint Cloud App Security Broker (Proofpoint CASB) schützt Ihre Anwender und Ihre vertraulichen Daten mit einem personenorientierten Ansatz vor Cloud-Bedrohungen. Die Lösung hilft Ihnen auch dabei, Schatten-IT aufzudecken und Cloud- sowie Drittanbieter-OAuth-Anwendungen zu verwalten.

Cloud-Sicherheit beginnt mit dem Schutz der Anwendungen, die von der IT freigegeben wurden. Dazu gehören z. B. Microsoft 365 (Office 365), Google G Suite, Salesforce, Box und andere Anwendungen. Das allein reicht aber nicht aus. Sie benötigen einen integrierten, personenorientierten Ansatz, der Bedrohungen korreliert und konsistente DLP-Richtlinien (Data Loss Prevention) in E-Mail- und Cloud-Anwendungen durchsetzt. Proofpoint CASB schützt Sie vor Kontenkompromittierung, versehentlicher Datenweitergabe, Konfigurationsfehlern in IaaS- und PaaS-Ressourcen und Compliance-Risiken. Unsere agentenlose Lösung bietet Ihnen personenorientierte Transparenz von Bedrohungen, eine anpassbare Zugriffssteuerung, automatisierte Reaktionen und umfassende Datensicherheit mit DLP. Sie umfasst darüber hinaus die Governance von Cloud- und Drittanbieter-OAuth-Anwendungen, einschließlich des Managements der Cloud-Sicherheitslage.



Proofpoint CASB-Konsole

Ausdehnung personenorientierter Transparenz auf Cloud-Anwendungen

Proofpoint CASB bietet personenorientierte Transparenz bei E-Mail- und Cloud-Bedrohungen. Wir helfen Ihnen dabei, Ihre Very Attacked People™ (VAPs) zu identifizieren und ihre Cloud-Konten und Daten zu schützen. Zudem können Sie sehen, welche Daten in Ihren Cloud-Anwendungen gegen DLP-Regeln verstoßen, wem die Daten gehören und wer sie herunterlädt, teilt oder bearbeitet.

Dank unserer leistungsstarken Analysen und adaptiven Kontrollen können Sie Ihren Endnutzern und Drittanbieter-OAuth-Anwendungen die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen.

Schutz der Anwender vor Cloud-Bedrohungen

Proofpoint CASB kombiniert unsere umfangreichen kanalübergreifenden Bedrohungsdaten (Cloud, E-Mail usw.) mit anwenderspezifischen Kontextdaten, um das Anwenderverhalten zu analysieren und Anomalien in Cloud-Anwendungen und bei Mandanten zu erkennen. Durch Machine Learning und umfangreiche Bedrohungsdaten können Sie erkennen, ob ein Cloud-Konto kompromittiert wurde. Wenn es zu Zwischenfällen kommt, können Sie in unserem intuitiven Dashboard frühere Aktivitäten und Warnungen untersuchen. Dies umfasst verdächtige Datei- und Administrationsaktivitäten. Zur weiteren Analyse lassen sich forensische Daten manuell oder über REST-APIs in eine Lösung für Sicherheitsinformations- und Ereignis-Management (SIEM) exportieren.

Unsere personenorientierten anpassbaren Kontrollen sind auf zahlreiche Cloud-Bedrohungen ausgerichtet. Wir schützen vor Email Account Compromise (EAC), der missbräuchlichen Nutzung von IaaS-Ressourcen und vor Datendiebstahl – ohne dabei die Produktivität der Anwender zu beeinträchtigen. Unsere robusten Richtlinien weisen in Echtzeit auf Probleme hin, behandeln kompromittierte Konten, stellen schädliche Dateien unter Quarantäne und sorgen dafür, dass die erforderliche Authentifizierung basierend auf dem aktuellen Risiko basiert. Sie haben die Möglichkeit, Ihre Identitätsverwaltungslösungen über die SAML-Authentifizierung (Security Assertion Markup Language) zu integrieren.

Bündelung von DLP für Cloud-Anwendungen und andere Kanäle

Proofpoint CASB teilt DLP-Klassifizierer (einschließlich integrierter intelligenter Identifikatoren, Wörterbücher, Regeln und Vorlagen) mit anderen Proofpoint-Produkten, sodass Sie schneller mit dem Erkennen und Schützen vertraulicher Daten beginnen können. Sie können einheitliche DLP-Richtlinien schnell für Ihre SaaS-Anwendungen, IaaS-Buckets und E-Mail-Postfächer bereitstellen und die DLP-Vorfallverwaltung auf der Proofpoint CASB-Konsole für mehrere Kanäle bündeln. Die mehr als 240 integrierten Klassifizierer decken DSGVO, PCI DSS sowie anderen Vorschriften zum Schutz personenbezogener Informationen ab. Eigene kontextbasierte Regeln und moderne Erkennungstechnologien wie der exakte Datenabgleich ermöglichen die Entwicklung eigener DLP-Richtlinien, mit denen Sie das Austauschen und Herunterladen von Daten kontrollieren. Sie können den Datenzugriff von nicht verwalteten Geräten einschränken, Dateien unter Quarantäne stellen und Freigabeberechtigungen für Dateien und Buckets reduzieren, um Compliance zu gewährleisten.

Sie können gefährdete Daten durch die Erkennung zu weit gefasster Datenberechtigungen und unzulässiger Datenweitergabe schützen und verdächtige Anmeldungen oder falsch konfigurierte AWS S3-Buckets mit DLP-Vorfällen korrelieren.

Kontrolle über Cloud- und Drittanbieter-Anwendungen

Mit Proofpoint CASB erhalten Sie einen Überblick über die Schatten-IT im gesamten Unternehmen. Wir unterstützen Sie beim Prüfen von Netzwerk-Traffic-Logs und Aufdecken von Cloud-Anwendungen. Unser Katalog umfasst 46.000 Anwendungen mit über 50 Attributen pro Anwendung. Die Cloud-Anwendungen können nach Typ und Risiko kategorisiert werden. Anhand der Bewertungsergebnisse können Sie Sicherheitsrisiken, potenzielle Schwachstellen für Datenverlust und nicht konforme Bereiche einfacher feststellen. Zudem können Sie gefährliche Anwendungen blockieren oder Anwendern schreibgeschützten Zugriff auf diese Anwendungen gewähren.

Wir erkennen und bewerten OAuth-Berechtigungen für Drittanbieter-Anwendungen und Skripte, die auf Ihre von der IT freigegebenen zentralen Cloud-Dienste zugreifen. Unsere tiefgehende Analyse hilft Ihnen, riskante sowie schädliche Anwendungen zu identifizieren, und so Ihre Angriffsfläche zu reduzieren. Basierend auf dem ermittelten Risiko und Kontext können Sie geeignete Maßnahmen definieren oder automatisieren.

Durch zentrale Verwaltung vereinfachen Sie den IaaS-Schutz und die Compliance mehrerer Clouds und Regionen. Die IaaS-Cloud-Sicherheitslage lässt sich über eine einzige Konsole verwalten. Wir helfen Ihnen dabei, genehmigte und nicht genehmigte IaaS-Konten und -Ressourcen zu erkennen sowie Konfigurationsfehler und Compliance-Probleme zu ermitteln.

Schnelle Bereitstellung mit agentenloser Architektur

Unsere agentenlose Architektur ermöglicht eine bislang unerreichte Amortisierungszeit. Leistungsstarke integrierte Funktionen interagieren mit bereits vorhandenen Cloud-Investitionen, sodass Sie Cloud-Bedrohungen schnell und automatisch verhindern, erkennen sowie beheben können. Dank der risikobasierten SAML-Authentifizierung und Web-Isolierung lassen sich Cloud-Bedrohungen schon im Keim ersticken. Und durch die Integration mit Cloud-Dienst-APIs, hybriden Identitätsverwaltungstools und Produkten für die Koordinierung von Sicherheitsmaßnahmen (einschließlich Proofpoint Threat Response) werden alle Bedrohungen, die dennoch durchkommen, erkannt und eingedämmt.

WEITERE INFORMATIONEN UND MÖGLICHKEIT ZUR REGISTRIERUNG FÜR EINE KOSTENLOSE TESTVERSION:

proofpoint.com/de/products/cloud-app-security-broker

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. 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 personenorientierten 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.