Proofpoint Cloud App Security Broker

WICHTIGE VORTEILE

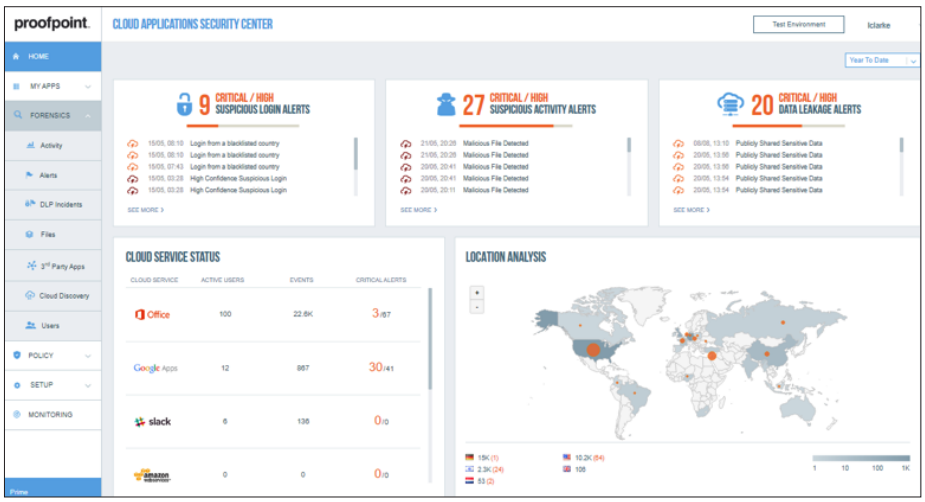
- Schutz der Cloud-Anwender durch personenorientierten Einblick in Bedrohungen und adaptive Zugriffsberechtigungen für Cloud-Anwendungen
- Beschleunigte Erkennung regulierter Cloud-Daten und Implementierung geeigneter Schutzmaßnahmen mithilfe standardmäßiger DLP-Richtlinien
- Bereitstellung konsistenter DLP-Richtlinien für E-Mail, Cloud-Anwendungen und lokale Datei-Repositorys
- Vereinfachung der täglichen Arbeit durch Bündelung der DLP-Vorfallverwaltung für mehrere Kanäle
- Erkennung von Cloud-Anwendungen und Eindämmung von Schatten-IT einschließlich Drittanbieter-OAuth-Anwendungen
- Noch schnellerer Wechsel in die Cloud dank agentenloser CASB-Architektur

Sichern Sie Ihren Wechsel in die Cloud mit Proofpoint Cloud App Security Broker (Proofpoint CASB) – dem einzigen Cloud Access Security Broker, der den Bedürfnissen von Unternehmen gerecht wird, für die Cloud-Bedrohungen, Datenverluste und Amortisierungszeit wichtige Themen sind. Mit unserem personenorientierten Ansatz kann Proofpoint CASB Ihre Anwender vor Cloud-Bedrohungen schützen, Ihre vertraulichen Daten sichern, Schatten-IT aufdecken und Cloud- sowie Drittanbieter-OAuth-Anwendungen kontrollieren.

Cloud-Sicherheit beginnt mit dem Schutz der Anwendungen, die von der IT freigegeben wurden. Dazu gehören z. B. Microsoft Office 365, Google G Suite, Salesforce, Box, AWS, Slack und andere Anwendungen, die Ihre wertvollsten Datenressourcen enthalten. Unser integrierter, personenorientierter Ansatz korreliert Bedrohungen und wendet konsistente DLP-Richtlinien (Data Loss Prevention) in E-Mail- und Cloud-Anwendungen an. Proofpoint CASB schützt Sie vor Kontenkompromittierung, versehentlicher Datenweitergabe und Compliance-Risiken in der Cloud. Unsere agentenlose Lösung bietet personenorientierte Transparenz und automatisierte Reaktionen bei Bedrohungen, umfassende Datensicherheit mit DLP sowie Kontrolle über Cloud- und Drittanbieteranwendungen.

Ausdehnung personenorientierter Transparenz auf Cloud-Anwendungen

Proofpoint CASB sorgt für personenorientierte Transparenz bei E-Mail- und Cloud-Bedrohungen, damit Sie besonders häufig angegriffene Personen (Very Attacked People™, VAPs) erkennen sowie ihre Cloud-Konten und -Daten schützen können. Wir kombinieren die Analyse von Kontextdaten und Anwenderverhalten, um verdächtige Aktivitäten zu erkennen. Zudem können Sie mit Proofpoint CASB sehen, welche Daten in Ihren Cloud-Anwendungen gegen DLP-Regeln verstoßen, wem die Daten gehören und wer sie herunterlädt, teilt oder bearbeitet.



Proofpoint CASB-Konsole

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 Risikoindikatoren, um das Anwenderverhalten zu analysieren und Anomalien in Cloud-Anwendungen und bei Mandanten zu erkennen. Durch Machine Learning und umfangreiche Bedrohungsdaten kann Proofpoint CASB genau erkennen, ob ein Cloud-Konto kompromittiert wurde. Wenn es zu Zwischenfällen kommt, können Sie in unserem intuitiven Dashboard frühere Aktivitäten und Warnungen untersuchen. Zur weiteren Analyse lassen sich forensische Daten manuell oder über REST-APIs in eine Lösung für Sicherheitsinformations- und Ereignis-Management (SIEM) exportieren.

Die personenorientierten adaptiven Kontrollen von Proofpoint CASB behandeln Cloud-Bedrohungen (einschließlich Cloud-Kontenkompromittierung, Email Account Compromise (EAC) und Datendiebstahl), ohne die Produktivität der Anwender zu beeinträchtigen. Darüber hinaus minimiert Proofpoint CASB diese personenorientierten Bedrohungen automatisch und reduziert die Wahrscheinlichkeit weiterer Angriffe. Robuste 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 alle Cloud-Anwendungen (SaaS, IaaS und Postfächer), E-Mail, Web und lokale Datei-Repositorys 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 andere Vorschriften zum Schutz personenbezogener Informationen ab. Eigene 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 Daten unter Quarantäne stellen, Berechtigungen für den Datenzugriff und -austausch begrenzen und Kontext nutzen, um Compliance sicherzustellen.

Proofpoint CASB schützt gefährdete Daten durch die Erkennung zu weit gefasster Datenberechtigungen und unzulässiger Datenweitergabe. Mit Proofpoint CASB können Sie verdächtige Anmeldungen oder falsch konfigurierte AWS S3-Buckets mit DLP-Vorfällen korrelieren. Diese Einblicke ermöglichen nützlichere DLP-Warnungen und die Automatisierung der Durchsetzung von Datenschutzrichtlinien.

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, Aufdecken von Cloud-Anwendungen und bei der Kategorisierung nach Typ und Risiko. Anhand der Bewertungsergebnisse können Sie Sicherheitsrisiken, potenzielle Schwachstellen für Datenverluste und nicht konforme Bereiche einfacher feststellen. Im weiteren Verlauf werden Sicherheitsmaßnahmen mit Firewalls und sicheren Web-Gateways koordiniert, um Schatten-IT einzudämmen. Zudem können Sie gefährliche Anwendungen blockieren oder Anwendern schreibgeschützten Zugriff auf diese Anwendungen gewähren.

Proofpoint CASB erkennt und bewertet OAuth-Berechtigungen für Drittanbieter-Anwendungen und Skripte, die auf Ihre von der IT freigegebenen zentralen Cloud-Dienste zugreifen. Die tiefgehende Analyse zeigt Ihre Risiken durch einzelne Anwendungen und Anwender auf. Dank der Kontrollfunktionen können Sie basierend auf dem ermittelten Risiko und dem Kontext geeignete Maßnahmen definieren oder automatisieren.

Schnelle Bereitstellung mit agentenloser Architektur

Mit seiner modernen agentenlosen Architektur bietet Proofpoint CASB eine unerreichte Amortisierungszeit. Leistungsstarke integrierte Funktionen interagieren mit bereits vorhandenen Cloud-Investitionen, sodass Sie Cloud-Bedrohungen schnell und automatisch verhindern, erkennen sowie beheben können. Proofpoint CASB beinhaltet risikobasierte SAML-Authentifizierung, Web-Isolierung und Zero Trust-Fernzugriffsfunktionen, um Cloud-Bedrohungen schon im Keim zu ersticken. Dank der 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. Wenn Sie Proofpoint CASB zusammen mit anderen Proofpoint-Lösungen (z. B. wie Advanced Threat Protection und Information Protection für E-Mails) verwenden, wird die Gesamtsicherheit für alle Cloud-Anwendungen, E-Mails und den lokalen Datenaustausch zusätzlich verbessert.

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.com.