KURZVORSTELLUNG

proofpoint.

PROOFPOINT CLOUD APP SECURITY

SCHUTZ FÜR IHRE CLOUD-BENUTZER. SCHUTZ FÜR IHRE DATEN.

HERAUSFORDERUNGEN

- Kompromittierte Anmeldedaten
- Malware
- Datenverlust und Compliance-Risiken

WICHTIGE FUNKTIONEN

- Schutz für Benutzer und Daten vor Kontenkompromittierung und hochentwickelten Bedrohungen in der Cloud
- Integration von Funktionen für Bedrohungserkennung und Zugangskontrolle von E-Mails bis zur Cloud
- Kontrolle des Cloud-Zugangs mithilfe von Benutzerverhaltensanalysen und Mehrfaktor-Authentifizierung (MFA)
- Schutz vor Datenverlust dank integrierter Bedrohungserkenntnisse
- Kontrolle von Drittanbieter-Add-On-Anwendungen
- Schnelle Bereitstellung in der Cloud

PRODUKTE

- Targeted Attack Protection (TAP)
- Cloud App Security Broker (PCASB)
- Email Data Loss Prevention and Encryption

Der Schutz Ihrer Mitarbeiter und der Daten, die sie generieren, ist schwieriger – und wichtiger – als je zuvor.

Benutzer, Anwendungen und Daten werden nicht mehr durch Ihre Netzwerkperipherie geschützt. Stattdessen arbeiten Angestellte heute zu Hause, im Café oder unterwegs im Zug und nutzen Cloud-basierte E-Mails sowie Anwendungen wie Microsoft Office 365, Google G Suite und Box. Diese Anwendungen verarbeiten vertrauliche Daten und sind mit zahlreichen Add-Ons von Drittanbietern verbunden.

Gleichzeitig richten sich heutige Cyberangriffe nicht mehr gegen die Infrastruktur, sondern gegen die Menschen. Viele Attacken richten sich gezielt gegen bestimmte Unternehmen oder Personen. Sie imitieren raffiniert Ihre Arbeitsweise und verleiten die Benutzer trickreich zum Öffnen unsicherer Dateien, zum Klicken auf böswillige Weblinks sowie zum Installieren riskanter Add-Ons. Das führt zu kompromittierten Anmeldedaten, unkontrollierten Malware-Ausbrüchen, Datenverlusten und Compliance-Verstößen.

Der Weg zu besserer Sicherheit besteht in einem integrierten Ansatz, der die Menschen in den Mittelpunkt stellt. Für eine sichere Migration in die Cloud benötigen Sie Bedrohungserkennung, Zugangskontrollen sowie Datensicherheit, wobei diese Maßnahmen alle Ihre Cloud-basierten E-Mail- und Produktivitäts-Tools abdecken müssen.

Proofpoint Cloud App Security schützt vor Kontenkompromittierung, schädlichen Dateien, Datenverlusten sowie Compliance-Risiken in der Cloud. Unsere umfassende Lösung hat den Menschen im Mittelpunkt und sichert E-Mails, Speicher, Anwendungen für Zusammenarbeit usw. ab. Dabei kombiniert sie diese wichtigen Funktionen:

- Hochentwickelter Schutz vor schädliche Dateien
- Erkennung und Behebung kompromittierter Konten
- Zugangskontrollen für Benutzer und Drittanbieter-Anwendungen
- Schutz vor Datenverlust (DLP)
- Analysen und Mehrfaktor-Authentifizierung

Mithilfe dieser leistungsstarken Funktionen können Sie auch gezielte Angriffe zuverlässig abwehren, Ihre Informationen schützen und die Compliance-Vorschriften in der Cloud einhalten.

SCHUTZ VON CLOUD-BENUTZERN VOR HOCHENTWICKELTEN BEDROHUNGEN

Nicht nur Benutzer wechseln in die Cloud, sondern auch Cyberangriffe. Ransomware, Bank-Trojaner, Anmeldedaten-Diebe sowie Phishing sind nur einige der zahlreichen hochentwickelten Bedrohungen, die Benutzer per E-Mail und über andere Cloud-Anwendungen angreifen.

Ein schädliches Dokument, das auf ein Cloud-Laufwerk hochgeladen wird, kann per Enterprise File Sync and Share (EFSS) innerhalb kürzester Zeit in Ihrer Umgebung verteilt werden. Daher ist eine frühe Erkennung unverzichtbar. Herkömmliche Tools haben jedoch Schwierigkeiten, polymorphe Malware und schädliche Links (die jeweils viele Varianten besitzen) zu erkennen.

Cloud App Security erkennt, analysiert und blockiert schädliche Dateien sowie URLs. Die Lösung nutzt eine Kombination aus Sandbox-Analyse, Bedrohungsdaten und kanalübergreifender Bedrohungskorrelation, um verborgene Bedrohungen aufzudecken und abzuwehren.

Sandbox-Analysen

Mit unseren Sandbox-Analysen und prädiktiven Analysen können wir Bedrohungen schnell und zuverlässig abwehren – noch bevor Schaden entsteht. Die gesamte Angriffskette wird mithilfe statischer und dynamischer Techniken untersucht. Wir analysieren Verhaltensweisen, Code sowie Protokolle, um schädliche Dateien aufzudecken.

Unsere Technologie kann Angriffe nicht nur erkennen, sondern auch davon lernen. Sie erfasst die Muster, Verhaltensweisen sowie Techniken der einzelnen Angriffe, damit wir den nächsten Angriff noch schneller identifizieren können.
Dank automatischer Quarantäne und anderer Behebungsfunktionen können Sie Bedrohungen in Echtzeit eindämmen.

Bedrohungsanalyse

Cloud App Security korreliert Informationen zu Angriffskampagnen gegen unterschiedliche Branchen und geografische Regionen. Wir nutzen Erkenntnisse aus Proofpoint Emerging Threats (ET) Intelligence – der aktuellsten und genauesten Quelle für Bedrohungsdaten auf dem Markt. Unser Bedrohungs-Dashboard zeigt Ihnen:

- Wer in Ihrem Unternehmen angegriffen wird
- Wer die Angreifer sind und welche Mittel sie nutzen
- Worauf es die Angreifer abgesehen haben

Anhand dieser Informationen können Sie mühelos erkennen, ob es sich um einen breit gefächerten Angriff oder eine gezielte Attacke gegen Führungskräfte und andere wichtige Mitarbeiter handelt.

Kanalübergreifende Korrelation

Cloud App Security korreliert Bedrohungsaktivitäten von E-Mails bis zur Cloud. Diese Erkenntnisse geben Ihnen einen wichtigen Überblick über gefährdete Benutzer und Sicherheitsverletzungen. In unserem Dashboard können Sie leicht die Verbindung zwischen E-Mail-Angriffen mit Anmeldedaten-Phishing und verdächtigen Anmeldungen ziehen, um besonders gefährdete Benutzer zu priorisieren. Sie können diese Cloud-Konten genauer überwachen oder sie mit schärferen Zugangskontrollrichtlinien schützen, um Kontenkompromittierungsversuche abzuwehren.

Top User at Risk
Last 30 days

User	Suspicious Logins	Failed Logins Attemps	Email Threats	Phishing Threats	Permitted Clicks	Last User Activity
Joe Greene Jgreene@acme.com	14	0	0	0	0	Jul 10 12:47 PM
Abby Boyle aboyle@acme.com	12	0	0	0	0	Jul 04 12:33 PM

Cloud App Security erlaubt die Korrelation von Benutzeraktivitäten und kontextbezogenen Risiken.

ÜBERWACHUNG UND KONTROLLE DES CLOUD-ZUGANGS

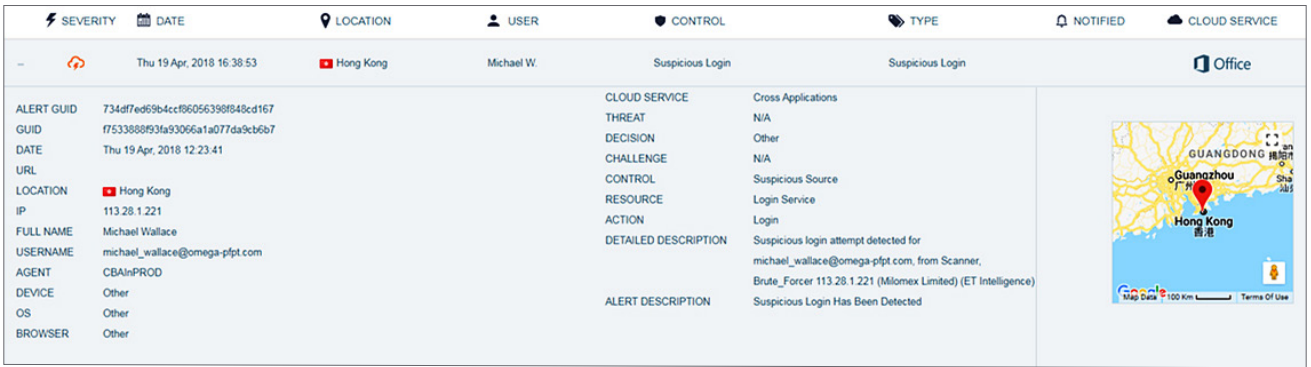
Die Mitarbeiter von heute erwarten zu jeder Zeit, an jedem Ort und mit jedem Gerät Zugriff auf die Cloud. In einer solchen Umgebung ist die Überwachung des Benutzerverhaltens in Cloud-Anwendungen absolut unverzichtbar. Alles beginnt mit der Festlegung sicherer Basislinien. Ungewöhnliches Benutzerverhalten kann darauf hindeuten, dass es Angreifern gelungen ist,

- Benutzerkonten zu kompromittieren
- Informationen zu stehlen
- Daten zu zerstören

Anhand von Risikoindikatoren können Sie sofort Maßnahmen ergreifen. Erstellen Sie Richtlinien, um den Zugang zu Cloud-Diensten zu kontrollieren, und setzen Sie Benutzervalidierung mithilfe von Mehrfaktor-Authentifizierung durch. Mit unseren leistungsfähigen Verhaltensanalysen in Verbindung mit starker Authentifizierung können Sie die Benutzeridentität überprüfen und so Benutzern sowie Drittanbieter-Add-Ons die erforderlichen Zugriffsrechte einräumen.

Verhaltensanalysen

Cloud App Security verbindet Kontextdaten und Analysen des Benutzerverhaltens. Der Kontext umfasst den Standort eines Benutzers, Gerät und Netzwerk sowie jede Cloud-Anwendung, auf die der Benutzer zugreift. Zu ungewöhnlichen Verhalten gehören extreme Aktivitäten, unübliche Zugriffsversuche u. a.



Wir suchen anhand von erfassten Spuren, Schwellenwerten und hochentwickeltem Machine Learning nach Anomalien. Sie haben folgende Möglichkeiten:

- Festlegen, dass nur unternehmenseigene Geräte, die Ihre Standards für Endgerätesicherheit erfüllen, Cloud-Zugriff erhalten
- Einschränken von Berechtigungen auf schreibgeschützten Zugriff
- Einschränken der Daten, die vom Benutzer heruntergeladen werden können

Cloud App Security korreliert kanalübergreifende Bedrohungsdaten mit benutzerspezifischen Risikoindikatoren. Mithilfe dieser Erkenntnisse können Sie verdächtige Aktivitäten schon früh erkennen, Warnungen priorisieren und eine Überflutung mit Meldungen vermeiden. Mit unseren intuitiven Dashboards und Filtern haben Sie auch die Möglichkeit, frühere Aktivitäten und Warnungen zu untersuchen. Mit unseren zuverlässigen Richtlinienvorlagen erhalten Sie Ergebnisse in Echtzeit und können anschließend je nach Bedarf risikobasierte Authentifizierung festlegen und Berechtigungen einschränken. Dadurch verhindern Sie, dass Ihre Anwendungen missbraucht und Ihre Daten kompromittiert oder gelöscht werden.

Mehrfaktor-Authentifizierung

Mit unserem SAML-Proxy können Sie vorhandene Identitätsverwaltungslösungen integrieren. Unsere Mehrfaktor-Authentifizierung überprüft zudem Benutzeridentitäten vor der Anmeldung und kontrolliert weitere riskante Aktivitäten. Mit unserer Multimodus-Architektur können Sie Schutz per API oder per Forward/Reverse Proxy aktivieren.

CLOUD APP SECURITY BIETET SCHUTZ FÜR:

CLOUD-E-MAILS

- Office 365 Exchange Online
- Gmail

CLOUD-DIENSTE

- Office 365 Exchange Online (gespeicherte Daten)
- Office 365 SharePoint Online
- Office 365 OneDrive
- Google Drive
- Google Cloud
- Box
- Dropbox
- Salesforce
- Amazon Web Services S3

VERHINDERUNG VON DATENVERLUSTEN IN DER CLOUD

Immer mehr Unternehmensdaten werden in der Cloud gespeichert. Das gilt auch für vertrauliche Inhalte. Die Hälfte der gemeldeten Datenschutzverletzungen sind die Folge gestohlener oder schwacher Anmeldedaten. Die Kompromittierung von Anmeldedaten erfolgt häufig durch Datenschutzverletzungen, Phishing, Anmeldedaten-Diebe und Brute-Force-Angriffe. Zur Erkennung und Verhinderung von Datenschutzverletzungen in der Cloud benötigen Sie risikobewusste Datensicherheit sowie starke Authentifizierung.

Cloud App Security vereint kanalübergreifende Bedrohungserkennung mit der Visualisierung vertraulicher Daten und DLP-Kontrollen. Die auf Benutzer ausgerichtete Transparenz und Verhaltensüberwachung deckt angegriffene Personen sowie Aktivitäten verwaister oder kompromittierter Konten schnell auf. Proofpoint DLP scannt folgende Elemente, um den Zugang zu vertraulichen Daten darzustellen:

- Übertragene E-Mails
- Gespeicherte E-Mails
- Cloud-Speicher
- Von anderen Cloud-Anwendungen gespeicherte Daten

Anhand dieser Informationen können Sie schnell festlegen, welche Benutzer mit hoher Priorität geschützt werden müssen, und so Verluste vertraulicher Daten sowie Schäden minimieren. Datensicherheitsregeln können für gefährdete Benutzer automatisch E-Mails verschlüsseln, Dateizugangsberechtigungen einschränken sowie die Mehrfaktor-Authentifizierung aktivieren.

Schutz vor Datenverlust

Proofpoint DLP bietet mehr als 80 vordefinierte Datensicherheitsrichtlinien. Sie können automatisch vertrauliche Daten erkennen und klassifizieren. Außerdem können Sie DLP-Verletzungen in Cloud-basierten E-Mails und Anwendungen beseitigen, um vertrauliche Daten schneller zu erkennen und abzusichern. Dazu stehen folgende Funktionen zur Verfügung.

- Einheitliche Datenklassifizierung zur Nachverfolgung übertragener und gespeicherter Daten
- Integrierte Klassifizierer zur Einhaltung von DSGVO, PCI und HIPAA sowie anderen Vorschriften zum Schutz personenbezogener Informationen
- Wörterbücher- und Näherungsabgleich zur besseren Erkennung vertraulicher Daten und automatisierten Vorschriften-Compliance
- Exakter Datenabgleich zur einfachen Aktualisierung von benutzerdefinierten Wörterbüchern bzw. Identifikatoren, damit unternehmensspezifische Informationen (z. B. Kontonummern und andere strukturierte Daten aus Datenbanken) zuverlässig erkannt werden
- Dokumentfingerabdruck zur Erkennung vertraulicher Daten innerhalb unstrukturierter Inhalte, z. B. Formeln, Quellcode, Formulare, Verträge sowie andere Arten von geistigem Eigentum
- Bereits standardmäßig Scans von 300 Dateitypen, mithilfe des Dateityp-Profilers für neue, benutzerdefinierte oder proprietäre Dateitypen erweiterbar

Flexible benutzerdefinierte Regeln ermöglichen die Erstellung eigener DLP-Richtlinien, mit denen Sie kontrollieren können, wie Ihre Daten versendet, freigegeben und heruntergeladen werden dürfen. Sie können mithilfe kontextbasierter Verschlüsselung, Quarantänen und Dateifreigabe-Berechtigungen riskante oder nicht autorisierte Zugriffe auf E-Mails und Dateien kontrollieren und so die offene Weitergabe vertraulicher Daten verhindern. Zudem können Sie die Vorschriften-Compliance mithilfe von Warnmeldungen, Ereignisfiltern und Benachrichtigungen über Berichte genau überwachen.

AUTOMATISIERTE KONTROLLEN FÜR DRITTANBIETER-ANWENDUNGEN

Marktplätze für Cloud-Anwendungen bieten hunderte Drittanbieter-Add-Ons mit Funktionserweiterungen für Microsoft Office 365, Google G Suite, Box und andere Plattformen an. Durch die unglaubliche Vielfalt dieses Ökosystems stellt der Drittanbieter-Zugriff auf Ihre Daten ein gewaltiges Compliance-Risiko dar.

Einige Add-Ons zur E-Mail- und Datei-Bearbeitung verlangen vollständigen Zugriff auf E-Mails, Kontakte und Dateiinhalte. Zudem speichern sie diese Dateien häufig in verschiedenen geografischen Regionen und verstoßen damit möglicherweise gegen DSGVO-Vorgaben und andere Vorschriften zum Schutz personenbezogener Informationen.

Unsere umfassende und anbieterunabhängige Analyse schützt Sie vor unsicheren Drittanbieter-Add-On-Anwendungen und -Skripten. Wir gewährleisten die Produktivität Ihrer Benutzer und minimieren Risiken, indem wir die erforderliche Transparenz ermöglichen und Kontrollmöglichkeiten bereitstellen. Mithilfe von Warnmeldungen werden Sie über neu hinzugefügte riskante Anwendungen und Skripte benachrichtigt. Dank der Kontrollfunktionen können Sie basierend auf Analyseergebnissen und der Risikoeinstufung der Anwendung Aktionen definieren oder automatisieren. Und mithilfe von Richtlinien können Sie festlegen, welche Berechtigungen mit den zugewiesenen Zugriffs-Token gewährt werden. Alternativ können für Anwendungen oder Skripte, die festgelegte Schwellenwerte überschreiten, OAuth-Zugangsanfragen abgelehnt werden.

SCHNELLE BEREITSTELLUNG IN DER CLOUD

Cloud-Plattformen benötigen Cloud-Schutz. Unsere Cloud-Architektur lässt sich schnell bereitstellen, sodass Sie sofort von den Vorteilen profitieren. Sie können innerhalb von Tagen – nicht Wochen oder Monaten – hunderte oder tausende Benutzer schützen. Wir aktualisieren unsere Software zudem täglich über die Cloud, um neue Funktionen hinzuzufügen und sicherzustellen, dass Sie den Angreifern einen Schritt voraus bleiben. Unsere Cloud-Bereitstellung bietet auch die notwendige Flexibilität, um Benutzer in jedem Netzwerk oder auf jedem Gerät zu schützen.

PRODUKTE

Proofpoint Targeted Attack Protection (TAP) erkennt, analysiert und blockiert hochentwickelte Attacken, die Personen über E-Mails (TAP for Email) und Cloud-Anwendungen (TAP SaaS Defense) angreifen. Wir erkennen bekannte Bedrohungen ebenso wie neue, noch völlig unbekannte Angriffe, die schädliche Dateien und unsichere URLs verwenden. TAP ist wie keine andere Lösung in der Lage, gezielte Angriffe zu stoppen, die mit polymorpher Malware, manipulierten Dokumenten und Phishing-Techniken zum Diebstahl von Anmeldedaten versuchen, auf vertrauliche Informationen zuzugreifen. Weitere Informationen finden Sie unter proofpoint.com/de/product-family/advanced-threat-protection.

Proofpoint Cloud App Security Broker (PCASB) schützt Benutzer von Cloud-Anwendungen vor hochentwickelten Bedrohungen, unbefugtem Zugriff, Datenverlust und Compliance-Risiken. PCASB bietet für Anwendungszugriffe und die Datenverarbeitung einen detaillierten Überblick, der den Menschen im Mittelpunkt hat. Unsere Lösung kombiniert Schutz vor hochentwickelten Bedrohungen, Zugangskontrollen, Schutz vor Datenverlust (DLP), Governance für Drittanbieter-Anwendungen sowie Mehrfaktor-Authentifizierung, um Microsoft Office 365, Google G Suite, Box und andere Plattformen abzusichern. Dank unserer leistungsstarken Analyse können Sie Ihren Benutzern und Drittanbieter-Anwendungen die Zugangsberechtigungen zuweisen, die den für Sie relevanten Risikofaktoren entsprechen. Weitere Informationen sowie die Möglichkeit, sich für eine kostenlose Risikoanalyse zu registrieren, finden Sie unter proofpoint.com/us/products/cloud-app-security-broker.

Proofpoint Email Data Loss Prevention and Encryption verhindert den Verlust vertraulicher Daten durch E-Mails und schützt vertrauliche E-Mails sowie Anhänge mit automatischer Klassifizierung und richtlinienbasierter Verschlüsselung – ohne dass dabei die Komplexität und Kosten entstehen, die für herkömmliche Lösungen typisch sind. Weitere Informationen finden Sie unter proofpoint.com/de/product-family/information-protection.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.