Proofpoint Information and Cloud Security-Plattform

Personenzentrierte Zugriffssteuerung, Bedrohungsschutz, Datensicherheit und Schutz vor Insider-Risiken für die hybride Cloud

Produkte

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access
- Proofpoint Insider Threat Management
- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Email Data Loss Prevention

Wichtige Vorteile

- Cloud-native Plattform mit einheitlichen Verwaltungs- und Reaktionsfunktionen
- Personenzentrierte Transparenz und Kontrolle für E-Mail, Cloud, Web und Endpunkte
- Erstklassige Funktionen zur Erkennung von Bedrohungen, Inhalten und Verhaltensweisen in Kombination mit hochentwickelten Analysen
- Einheitliche Datenklassifizierer und Inhaltsprüfungen für E-Mail, Cloud, Web und Endpunkte
- SASE-fähige Sicherheitsarchitektur mit flexiblen Bereitstellungsmodellen

Der Perimeter Ihrer Unternehmensnetzwerke verschwimmt immer mehr. Stattdessen werden die Netzwerkgrenzen durch Ihre Mitarbeiter bestimmt, die heute überwiegend remote arbeiten und dabei ihre privaten Geräte und nicht verwaltete Anwendungen nutzen. Gleichzeitig befinden sich die kritische Infrastruktur sowie wichtige Daten in der öffentlichen Cloud. Zudem nehmen Cyberangreifer mehr denn je gezielt Menschen ins Visier. Diese dynamische Umgebung erfordert einen personenzentrierten Ansatz für den Schutz Ihrer Cloud und Ihrer Daten.

Ihre Anwender benötigen sicheren Zugriff auf das Web, Cloud-Dienste und private Anwendungen. Dazu benötigen Sie eine Kombination mehrerer Lösungen, die Zugriffssteuerung, Bedrohungsschutz, Datensicherheit, Governance von Anwendungen und Zero-Trust-Richtlinienkontrollen umfassen. Um Anwender- und Datenaktivitäten auf Endpunkten schützen zu können, müssen diese Kontrollen von Sensoren durchgesetzt werden, die sich auf allen Kanälen befinden. Außerdem müssen sie durch einheitliche Analysen, Untersuchungen und eine Plattform zur Richtlinienverwaltung unterstützt werden.

Die Proofpoint Information and Cloud Security-Plattform erfüllt all diese Anforderungen. Sie kombiniert viele unserer Produkte, mit denen Sie sicheren Zugriff gewähren, Datenverlust verhindern und Risiken durch Insider reduzieren können. Die Plattform bietet nicht nur erstklassige Funktionen zur Erkennung von Bedrohungen, Inhalten und Verhaltensweisen, sondern auch personenzentrierte Transparenz sowie Zugriffssteuerung für Web, Cloud und private Anwendungen. Zudem verfügt sie über eine einheitliche Konsole für Verwaltungs- und Reaktionsfunktionen und ermöglicht hochentwickelte Analysen, um Abläufe zu vereinfachen und Reaktionszeiten zu verkürzen.

Die leistungsstarke und Cloud-native Proofpoint Information and Cloud Security-Plattform verfügt über eine SSE-Architektur (Secure Service Edge). (Dieser Branchenstandard gewährleistet sicheren Anwendungs- und Datenzugriff sowie Bedrohungsschutz – ganz gleich, wo sich die Anwender befinden und welches Gerät sie nutzen.) Unsere Plattform ist global ausgelegt, kann Daten jedoch auch lokal speichern, damit sie weltweit regionsspezifische Compliance-Vorgaben einhalten.

Die Plattform umfasst folgende Produkte:

- Proofpoint Enterprise DLP
- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Email DLP und Proofpoint Email Encryption
- Proofpoint Insider Threat Management (ITM) mit Proofpoint Endpoint DLP
- Proofpoint Web Security mit Proofpoint Browser Isolation
- Proofpoint Zero Trust Network Access (ZTNA)

Bedrohungsabwehr und sicherer Zugriff auf die Cloud, Web-Dienste und private Anwendungen

Proofpoint Cloud Security ist global ausgelegt, Cloud-nativ und bietet einheitliche Funktionen für personenzentrierte Zugriffssteuerung, Bedrohungsschutz und Zero-Trust-Netzwerke. Die Lösung ermöglicht mit folgenden Komponenten sicheren Zugriff auf Cloud-Dienste, das Web und private Anwendungen:

- **Granulare Kontrollen.** Dazu gehören erweiterte Authentifizierung, Lesezugriff durch Browser-Isolierung und Anwendungszugriff mit Mikrosegmentierung.
- **Umfangreiche, vektorübergreifende Bedrohungsdaten**, die das Risiko der Anwender zeigen.
- **Hochentwickelter Bedrohungsschutz.** Kompromittierte Konten und schädliche OAuth-Anwendungen werden erkannt und behoben. Der Schutz umfasst zusätzlich Malware-Abwehr sowie Analysen des Anwenderverhaltens (User Behavior Analystics, UBA), um riskante Änderungen zu erkennen.
- **Inline-DLP in Echtzeit.** Diese Funktionen verhindern nicht autorisierten Zugriff auf vertrauliche Daten in der Cloud und gewährleisten die Einhaltung von Compliance-Vorschriften.
- **Transparenz** zu Schatten-IT, Governance von SaaS-Cloud-Anwendungen und OAuth-Anwendungen von Drittanbietern. Außerdem ist für IaaS-Services (Infrastructure as a Service) Sicherheitsverwaltung für Cloud-Umgebungen enthalten.
- **Multimodus-Architektur** für Transparenz und adaptive Kontrollen.

Unsere Plattform bietet die Möglichkeit, für besonders gefährdete Anwender strengere Kontrollen durchzusetzen. Bei diesen Anwendern kann es sich um besonders häufig angegriffene oder gefährdete Personen oder um Anwender mit umfangreichen Berechtigungen wie Administratoren und VIPs handeln.

Schutz vertraulicher Daten und Verwaltung von Insider-Risiken für alle wichtigen Kanäle

Proofpoint Information Protection erkennt vertrauliche Daten in der Cloud und verhindert Datenverlust für E-Mail, Cloud-Anwendungen, Web und Endpunkte. Mit unseren einheitlichen Datenklassifizierern, Detektoren und dem Tagging-Framework können Sie für das gesamte Unternehmen konsistente Richtlinien einrichten. Wir kombinieren Telemetriedaten zu Inhalten, Verhalten und Bedrohungen aus diesen Kanälen, damit Sie schnell ermitteln können, ob der Anwender, der die DLP-Warnung ausgelöst hat, kompromittiert wurde oder böswillig bzw. fahrlässig handelt. Außerdem vereinheitlichen wir die Verwaltung von DLP-Zwischenfällen für diese Kanäle, sodass Sie Warnungen besser priorisieren und schneller darauf reagieren können.

Risiken durch Insider und Datenverlust auf Endpunkten hängen zusammen. Mit unserer Plattform können Ihre Sicherheitsteams besonders gefährdete Anwender priorisieren, Insider-Risiken erkennen und schneller

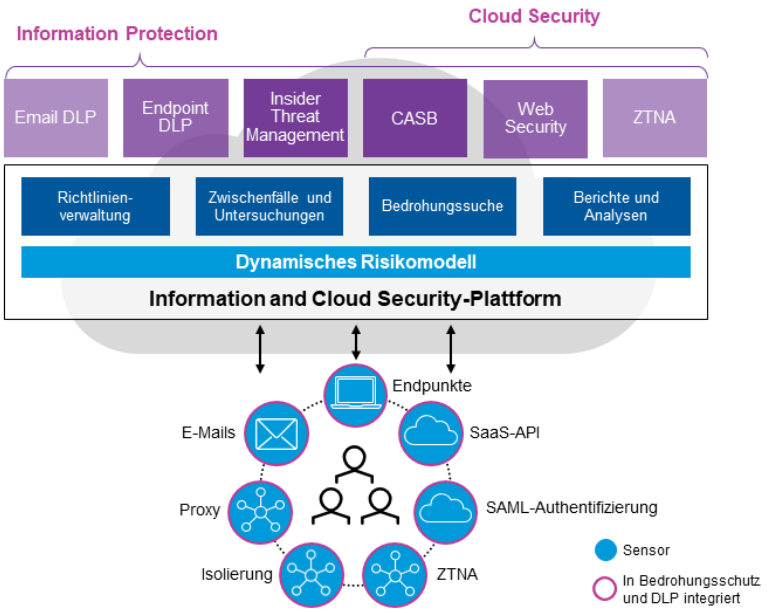

Abb. 1: Proofpoint Information and Cloud Security-Plattform.

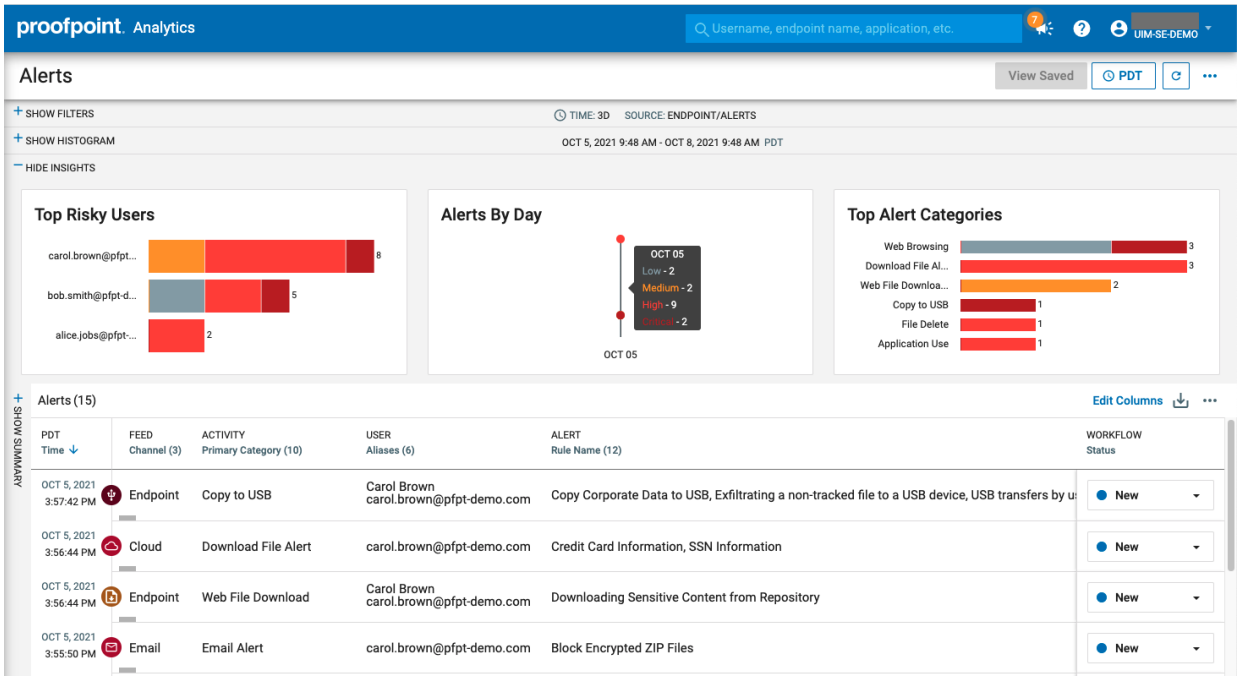

Abb. 2: Eine einheitliche Konsole für Verwaltungs- und Reaktionsfunktionen.

auf Bedrohungen reagieren. Wir bieten einen granularen Echtzeit-Überblick über die Aktivitäten Ihrer Anwender sowie einheitliche Warnmeldungen zu Datenverlust und Insider-Risiken auf allen Kanälen. Dadurch können Sie die Fragen nach dem Wer, Was, Wo, Wann und Warum zu jedem Ereignis und jeder Warnmeldung schnell beantworten.

Einheitliche Konsole mit hochentwickelten Analysetools

Unsere einheitliche Konsole für Verwaltungs- und Reaktionsfunktionen beschleunigt mit den folgenden modernen Tools Ihre Untersuchungen:

- Richtlinienverwaltung
- Workflows für die Untersuchung und Behebung von Zwischenfällen
- Bedrohungssuche und -analyse
- Berichte und Analysen
- Verwaltungs- und Datenschutzfunktionen

Richtlinienverwaltung

Die Plattform bietet diese Vorteile:

- Verwaltung aller Cloud- und Datenzugriffsrichtlinien über eine zentrale Konsole
- Erstellung komplexer Regeln für mehrere Kanäle basierend auf:
  - Einheitlichen Datenklassifizierern (intelligente IDs, Wörterbücher)
  - Detektoren (Näherungsabgleich)
  - Detektor-Sets (für Anwendergruppen, Regionen, Anwendungsfälle, Kanäle)
  - Sensitivitätskennzeichnungen
  - Hochentwickelter Bedrohungsanalyse und -erkennung

Workflows für die Untersuchung und Behebung von Zwischenfällen

Die Plattform bietet diese Vorteile:

- Erfassung von Warnmeldungen zu Bedrohungen, DLP-Ereignissen und Anwenderverhalten in einer einheitlichen Verwaltungsübersicht, sodass Sie ein ganzheitliches Risikoprofil für relevante Anwender erhalten
- Schnelle Antworten zum Wer, Was, Wo, Wann und Warum zu jedem Sicherheitsereignis
- Untersuchung von Anwenderverhalten, um deren Motive und den Schweregrad des Risikos zu verstehen
- Verwaltung des Warnmeldungsstatus für alle Bereiche von der Erkennung bis zur Behebung

Bedrohungssuche und -analyse

Die Plattform bietet diese Vorteile:

- Proaktive Suche nach neuen Bedrohungen, einschließlich Kompromittierung von Cloud-Konten, Datenexfiltration, Datenlecks, Insider-Risiken, nicht autorisierte Nutzung von Anwendungen usw.
- Einrichtung von Überwachungslisten zur Organisation und Priorisierung von Anwendern anhand des Risikoprofils (z. B. Führungskräfte, Very Attacked People™ (VAPs), entlassene/gekündigte Mitarbeiter, Anwender mit besonderen Berechtigungen, Mitarbeiter der Personalabteilung, externe Auftragnehmer) sowie von Mitarbeitern, die sich auf der Überwachungsliste der Personalabteilung befinden
- Suchfunktionen mit leistungsstarken Filtern, mit denen die integrierten Untersuchungsfunktionen angepasst werden können

Berichte und Analysen

Die Plattform bietet diese Vorteile:

- Anzeigen von Anwendern und Datenaktivitäten für mehrere Kanäle mithilfe intuitiver Zeitleistenansichten
- Berichte zu riskanten Aktivitäten basierend auf Anwendermotiven und Weitergabe dieser Berichte an Geschäftspartner
- Korrelation von Aktivitäten und Warnmeldungen zu mehreren Kanälen mit Daten aus anderen Sicherheits-tools durch nahtlose Integration mit SIEM-Systemen (Sicherheitsinformations- und Ereignis-Management), SOAR-Systemen (Koordinierung und Automatisierung von Sicherheitsmaßnahmen) und Ticket-Systemen

Verwaltungs- und Datenschutzfunktionen

Die Plattform bietet diese Vorteile:

- Funktionsübergreifende Verwaltung von Warnmeldungen und Untersuchungen mit rollenbasierter Zugriffssteuerung
- Gewährleistung von Datenschutz mit granularer, attributbasierter Zugriffssteuerung
- Authentifizierung von Plattformnutzern bei Ihrem Single Sign On (SSO)-Anbieter (z. B. Microsoft, Okta Identity Cloud, Google Cloud IAM) per OAuth

Produkte

Die Proofpoint Information and Cloud Security-Plattform führt die folgenden Produkte zusammen: Proofpoint CASB, Proofpoint Email DLP, Proofpoint ITM und Proofpoint Endpoint DLP, Proofpoint Web Security mit Browser Isolation und Proofpoint ZTNA. Nachfolgend wird jedes Produkt kurz vorgestellt.

Proofpoint CASB

Proofpoint CASB kombiniert personenzentrierte Kontrollen mit der Erkennung kompromittierter Cloud-Konten, DLP und Governance für Cloud- und Drittanbieter-Anwendungen und unterstützt Sie beim Schutz von Microsoft 365, Google Workspace, Box, Salesforce, AWS, Azure, Slack und anderen Anwendungen. Unser Multimodus-CASB unterstützt Bereitstellungsmodelle, die auf APIs oder Proxys basieren.

Proofpoint Email DLP

Proofpoint Email DLP verringert das Risiko für über E-Mail begangene Datenschutzverletzungen. Die mehr als 240 integrierten Klassifizierer decken DSGVO, PCI DSS sowie andere Vorschriften zum Schutz personenbezogener Informationen und Gesundheitsdaten ab. Sie erhalten Transparenz sowie Funktionen zur Durchsetzung von Richtlinien ohne die Komplexität und Kosten separat eingesetzter Einzellösungen.

Proofpoint ITM und Proofpoint Endpoint DLP

Mit Proofpoint ITM und Proofpoint Endpoint DLP erhalten Sie Schutz vor Datenverlust und Markenschädigung durch Insider. Die Lösungen verhindern Datenexfiltration über USB-Geräte, Cloud-Synchronisationsordner, Ausdrucke und andere Kanäle. Die Produkte schützen Sie vor nicht autorisierten sowie böswillig oder fahrlässig handelnden Anwendern und bieten einen vollständigen Überblick über die Dateninteraktionen auf Endpunkten. Zudem korrelieren sie Anwenderaktivitäten und Datenbewegungen, um Datenschutzverletzungen durch Insider zu verhindern und die Reaktion auf Zwischenfälle zu beschleunigen.

Proofpoint Web Security mit Browser Isolation

Proofpoint Web Security schützt Ihre Mitarbeiter beim Surfen im Web vor hochentwickelten Cyberbedrohungen. Die Lösung verhindert Datenverlust und ermöglicht personenzentrierte Richtlinien, um Risiken zu minimieren. Proofpoint Web Security bietet dynamische Zugriffs-steuerung, hochentwickelten Bedrohungsschutz sowie DLP-Richtlinien und nutzt die erstklassigen Proofpoint-Bedrohungsdaten, die auf dem Nexus Threat Graph basieren. Web Security ist Cloud-nativ und ermöglicht granulare Kontrollen, um unbekannte, verdächtige oder privat genutzte Websites (z. B. Webmail) zu isolieren.

Proofpoint ZTNA

Proofpoint ZTNA ist die Zero-Trust-Alternative zur VPN-Technologie und bietet sicheren Fernzugriff zu allen Unternehmensanwendungen, ganz gleich, wo diese gehostet werden. Mit unserer personenzentrierten Lösung können Sie Ihren Anwendern mikrosegmentierten sicheren Zugriff auf hunderte Cloud-Instanzen gewähren. Mit der Lösung können Sie zudem Cloud-zu-Cloud-Verbindungen automatisieren und hybride Cloud-Netzwerke zwischen lokalen Servern und öffentlichen Clouds aufbauen.

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**.