proofpoint.

KURZVORSTELLUNG

Proofpoint Active Exploits Protection

Stoppen Sie Exploits in der ersten Phase, noch bevor sie ausgeführt werden.

Wichtige Vorteile

- Erstklassiger Exploit-Schutz in der ersten Phase, damit Exploit-Aktivitäten schon im E-Mail-Postfach identifiziert und gestoppt werden – noch bevor die Schaddaten ausgeführt oder Endpunkte kompromittiert werden können
- Priorisierung von Schwachstellen basierend auf aktiven Exploits, die im Umlauf sind
- Reduzierung von Risiken vor der Patch-Bereitstellung sowie Schutz vor Exploit-basierter Malware und Command-and-Control-Aktivitäten
- Schnellere Untersuchungen mit aktuellem und historischem Bedrohungskontext sowie kontinuierlich aktualisierten Bedrohungsdaten
- Vorbereitung auf KI- und agentengestützte Sicherheitsabläufe

Überblick

Die Geschwindigkeit und der Umfang von Ausnutzungen nehmen zu. Neue Schwachstellen werden in Rekordzahlen offengelegt und von Angreifern immer schneller missbraucht. Klassische Lösungen für Schwachstellen- und Risikomanagement priorisieren häufig auf Basis von Schweregraden und theoretischen Risiken, berücksichtigen jedoch nicht, welche Exploits tatsächlich aktiv von Angreifern ausgenutzt werden.

Proofpoint Active Exploits Protection ändert dieses Modell.

Proofpoint bietet Einblicke zu Exploits, die per E-Mail und im Netzwerkverkehr übertragen werden, sodass Unternehmen schädliche Aktivitäten identifizieren können, bevor die Schaddaten ausgeführt werden. Die Lösung kombiniert reale Exploit-Informationen, angreiferorientierte Priorisierung und sofortige Schutzmaßnahmen, damit Sicherheitsteams sich auf das Wesentliche konzentrieren und das Risiko schneller reduzieren können. Mit diesem Ansatz lassen sich Exploits proaktiver abwehren und Angriffe früher in der Angriffskette verhindern.

© Proofpoint, Inc. 2026

Die Lösung: Exploit-Informationen in der ersten Phase sowie sofortiger Schutz

Proofpoint Active Exploits Protection verwandelt reale Exploit-Informationen in entscheidungsrelevanten Schutz und priorisierte Reaktionen. Die Lösung kombiniert angreiferorientierte Exploit-Informationen, die Erkennung von E-Mail- und Netzwerkbedrohungen sowie operative Integrationen, damit Unternehmen Exploit-Aktivitäten vor der Ausführung identifizieren und stoppen können.

Dank hervorragender Exploit-Erkennung in E-Mails – wo viele moderne Angriffe beginnen – kann Proofpoint Exploit-Übermittlungsversuche und das Verhalten echter Angreifer in der frühesten Phase der Angriffskette identifizieren, bevor die Schaddaten ausgeführt und Endpunkte kompromittiert werden oder laterale Bewegungen stattfinden.

Mit Proofpoint Active Exploits Protection können Unternehmen diese einzigartigen Schwachstelleninformationen nutzen und profitieren von der breiten Abdeckung netzwerk- und exploitbasierter Bedrohungen. Das hilft, aktiv ausgenutzte Schwachstellen zu priorisieren, die Risiken während Patch-Fenstern zu reduzieren und Untersuchungen mit entscheidungsrelevanten Bedrohungsdaten zu beschleunigen.

Priorisieren aktiver Exploits statt theoretischer Risiken

Konzentrieren Sie die Behebungsmaßnahmen nicht nur auf Basis hoher CVSS-Werte, sondern auf Schwachstellen, die aktiv ausgenutzt werden.

Proofpoint Active Exploits Protection verknüpft Exploit-Informationen mit beobachtetem Angreiferverhalten aus globalen Telemetriequellen, damit Unternehmen schnell erkennen können, welche Schwachstellen ein unmittelbares operatives Risiko darstellen.

Dieser angreiferorientierte Ansatz hilft Sicherheitsteams, unwichtige Informationen zu reduzieren, die Priorisierung zu verbessern und Ressourcen auf die größten Ausnutzungsrisiken zu konzentrieren.

Folgende Funktionen sind enthalten:

- Priorisierung von Asset-Patches basierend auf aktiv ausgenutzten CVEs
- Unterscheidung zwischen dringenden Bedrohungen und weniger priorisierten Risiken
- Patch-Priorisierung anhand von klarem, entscheidungsrelevantem Bedrohungskontext, einschließlich Echtzeitinformationen zu IP-Adressen und Domain-Reputationsdaten
- Verbesserung des operativen Fokus, indem die Priorisierung mit realen Angreiferaktivitäten abgestimmt wird

Sofortiger Schutz auch während des Patch-Vorgangs

Patchen benötigt Zeit. Proofpoint Active Exploits Protection hilft Unternehmen, während dieses Zeitraums die Risiken zu reduzieren, indem die Lösung kontinuierlich aktualisierte Exploit-Informationen bereitstellt und sofortigen Schutz für den E-Mail- und Netzwerkverkehr ermöglicht.

Proofpoint bietet aktuelle, hochpräzise Erkennungslogik für hochentwickelte Bedrohungen, einschließlich:

- Malware-Übertragung
- Command-and-Control-Kommunikation
- Exploit-Kits
- Anmeldedaten-Phishing
- Angriffsverbreitung
- Ransomware, Botnets
- Anomalien in Protokollen und Anwendungen
- Coin-Mining
- DDoS-Angriffe (Distributed Denial of Service)
- SCADA-Angriffe (Supervisory Control and Data Acquisition)

Folgende Funktionen sind enthalten:

- Kontinuierlich aktualisierte Exploit-Informationen, die den Schutz in früheren Phasen der Angriffs-Kette verbessern
- Netzwerkbasierte Erkennungsregeln für IDS, IPS, NGFW und verwandte Sicherheitskontrollen
- Hochpräzise Signaturen für Malware-Callbacks, Dropper, Command-and-Control, Obfuskation, Exploit-Kit-Bedrohungen und Exfiltration
- Tägliche aktualisierte Regeln, um mit der dynamischen Bedrohungslandschaft Schritt zu halten
- Abdeckung wichtiger Malware-Familien, Angriffskampagnen und netzwerkbasierter Bedrohungsvektoren
- Unterstützung für weit verbreitete IDS- und IPS-Formate, einschließlich Suricata- und Snort-kompatible Bereitstellungen

© Proofpoint, Inc. 2026

Globale Bedrohungsdaten zur Anreicherung von Sicherheitstools

Proofpoint Active Exploits Protection bietet entscheidungsrelevante Informationen, die sich in eine Vielzahl von Sicherheitstools integrieren lassen, darunter Firewalls, IDS, IPS, NGFW, UTM, SIEM, Authentifizierungssysteme, Plattformen für Bedrohungssuche, Workflows für die Reaktion auf Zwischenfälle und eigenentwickelte Sicherheitstools.

Die Lösung liefert Reputations- und Bedrohungsdaten zu verdächtigen und schädlichen IP-Adressen, Domains, Malware, Signaturen, Kampagnen und verwandten Angriffsaktivitäten.

Folgende Funktionen sind enthalten:

- Aktuelle und historische Bedrohungsdaten zu IP-Adressen, Domains, Malware-Hashes, Signaturen und Nachrichtentexten
- Reputationsfeeds zu IP-Adressen und Domains, organisiert nach Bedrohungskategorie und Vertrauensgrad
- Häufige Feed-Updates mit aggressiver Alterung, um aktuelle Aktivitäten widerzuspiegeln
- Durchsuchbare globale Bedrohungsdatenbank für Daten-Pivotierung, Detailanalysen und Untersuchungen
- Mehrere Feed-Formate für die operationale Integration, einschließlich TXT, CSV, JSON, IDS und komprimierte Formate
- API-basierte Anreicherung zur Unterstützung von Tools für SIEM, TIP, Reaktion auf Zwischenfälle sowie interne Tools

Verbesserte Erkennungsgenauigkeit und weniger irrelevante Informationen

Proofpoint Active Exploits Protection nutzt die Ergebnisse von realen Bedrohungsbeobachtungen, Malware-Analysen, globalem Sensorfeedback und dedizierter Bedrohungsforschung, um hochpräzise Erkennungen zu ermöglichen und Fehlalarme in bestehenden Netzwerksicherheitstools zu reduzieren.

Folgende Funktionen sind enthalten:

- Erkennungsinhalte, die auf Untersuchungen und beobachteten Bedrohungen basieren
- Malware-Sandbox-Analysen, die das Netzwerkverhalten nach der Ausführung erfassen
- Globales Sensorfeedback zur Optimierung der Erkennungsgenauigkeit
- Signaturbeschreibungen, Referenzen und Dokumentationen zur Unterstützung von Analysten-Workflows
- Kategoriebasierte Durchsetzung von Richtlinien, die an den unternehmensspezifischen Prioritäten ausgerichtet sind

Skalierung mit KI-gesteuerten Workflows

Proofpoint Active Exploits Protection ist darauf ausgelegt, moderne, datengestützte Sicherheitsabläufe zu unterstützen. Zukünftige Funktionen sollen den Zugang zu Bedrohungsdaten über MCP- und agentenbasierte Workflows ermöglichen und auf diese Weise API- und KI-gestützte Anwendungsfälle unterstützen.

Diese Workflows sollen den Teams helfen, priorisierte Bedrohungsdaten direkt in automatisierte Sicherheitsabläufe einzubetten, Entscheidungen zu beschleunigen und den manuellen Triagebedarf zu reduzieren.

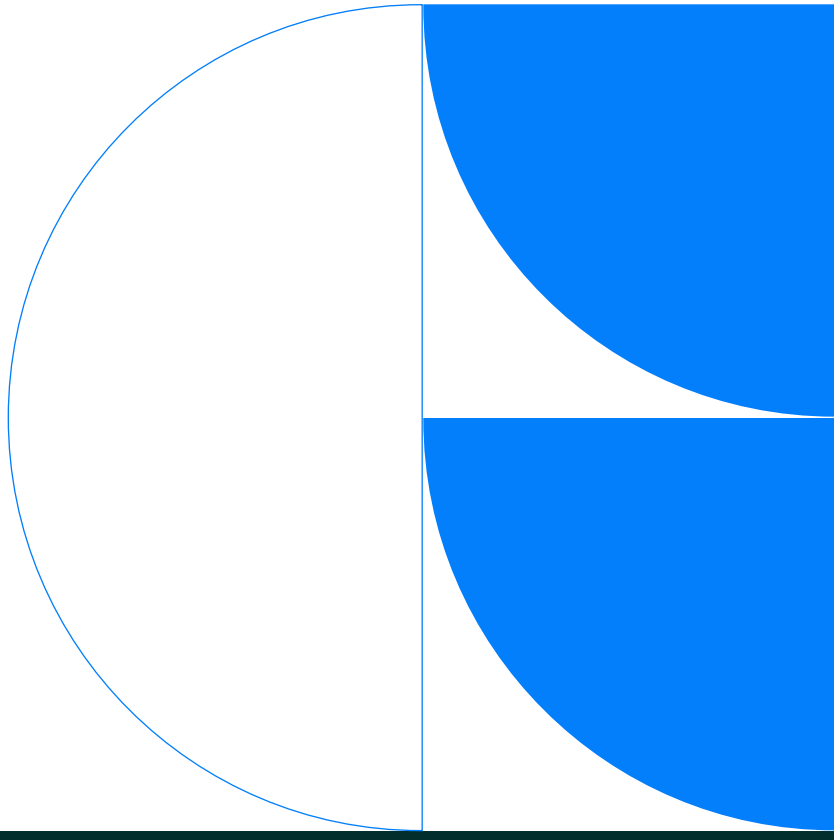
© Proofpoint, Inc. 2026

Zusammenfassung

Proofpoint Active Exploits Protection hilft Unternehmen, Exploit-basierte Angriffe vor einer Kompromittierung zu verhindern, indem Exploit-Erkennungen in E-Mails, angreiferorientierte Exploit-Informationen und sofort wirksame Schutzfunktionen kombiniert werden.

Anstatt sich ausschließlich auf Schweregrad-Einschätzungen für Schwachstellen oder theoretische Risikomodelle zu verlassen, können Sicherheitsteams mit Proofpoint Active Exploits Protection ihre Prioritäten basierend darauf setzen, was Angreifer tatsächlich ins Visier nehmen.

Durch die Vereinheitlichung von Priorisierung, Schutz und Untersuchung hilft Proofpoint Active Exploits Protection den Sicherheitsteams, sich auf das Wesentliche zu konzentrieren, sofort Schutz zu gewährleisten und schneller Untersuchungen durchzuführen.



Über Proofpoint, Inc. Proofpoint, Inc. ist ein weltweiter Marktführer bei personen- und agentenzentrierter Cybersicherheit und schützt Verbindungen zwischen Anwendern, Daten und KI-Agenten über E-Mail, Cloud und Collaboration-Tools. Proofpoint ist ein vertrauenswürdiger Partner für mehr als 80 Prozent der Fortune 100, über 10.000 große Unternehmen sowie für Millionen kleinerer Firmen und stoppt Bedrohungen, verhindert Datenverlust und sichert die Interaktionen zwischen Anwendern und KI-Workflows ab. Die Collaboration- und Datenschutzplattform von Proofpoint hilft Unternehmen jeder Größe, ihre Mitarbeiter zu schützen und zu unterstützen, damit sie KI sicher und bedenkenlos einsetzen können. Weitere Informationen unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

Proofpoint ist eine eingetragene Marke bzw. ein registrierter Handelsname von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.

proofpoint.