

Proofpoint Supplier Threat Protection

Identifizieren Sie kompromittierte Drittanbieter-Konten und erfahren Sie, welche Risiken dadurch entstehen

Wichtige Vorteile

- Proaktive Überwachung auf Kompromittierungen bei bekannten externen und Lieferanten-Konten
- Automatisierte Benachrichtigungen über kompromittierte Lieferantenkonten, die schädliche Nachrichten an Ihr Unternehmen senden
- Priorisierung kompromittierter Lieferantenkonten zur Untersuchung und Behebung
- Identifizierung von Mitarbeitern, die kürzlich mit kompromittierten Lieferantenkonten kommuniziert haben

Proofpoint Supplier Threat Protection erweitert die Vorteile von Proofpoint Targeted Attack Protection, da die Lösung kompromittierte Lieferanten und andere externe Parteien erkennt und Ihnen hilft, den Supply Chain vor Phishing, Malware und Business Email Compromise (BEC) zu schützen.

Durch die einzigartige Kombination aus Bedrohungsdaten und KI-gestützten Verhaltensanalysen erkennt Proofpoint Supplier Threat Protection die E-Mail-Muster von bekannten Absendern, die auf eine Kompromittierung hinweisen können. Die Lösung erkennt außerdem Muster zwischen bekannten Absendern und anderen Proofpoint-Kunden, sodass Sie auch dann geschützt werden, wenn das Konto noch keine schädlichen Nachrichten an Ihr Unternehmen gesendet hat.

Sie erhalten eine detaillierte Verlaufsübersicht der E-Mail-Aktivitäten, umfangreiche Kontextdaten und eine Dashboard-Übersicht der Drittanbieter-Konten mit dem größten Risiko. Durch diese relevanten Erkenntnisse können Sie verhindern, dass Bedrohungen Ihre Anwender erreichen, sowie Risiken priorisieren, Untersuchungen vereinfachen und schnell reagieren.

Sender	Suspected Compromise	Last Malicious Message	Identity	Found Threat Category	Context
bill@supplier1.com	Observed globally 2023/03/11	-	Supplier	(2) Phishing, Malware	Frequent communication with third party domain
mary@supplier2.com	Observed in your traffic 2023/03/13	2023/03/13 13:03	Supplier	(1) Imposter	Frequent communication with third party domain

A company you interact with has an account that is sending malicious emails to other companies

Incoming traffic from a compromised account detected

Strong business relationship

Abb. 1: Proofpoint Supplier Threat Protection erkennt potenziell kompromittierte Lieferantenkonten und bietet relevante Kontextdaten.

Transparenz

Proofpoint Supplier Threat Protection identifiziert Drittanbieter-Konten, die mit Ihrem Unternehmen kommunizieren. Die Lösung erstellt eine Baseline der typischen Kommunikationsaktivitäten zwischen Mitarbeitern und Lieferanten und verwendet anschließend Bedrohungsdaten, künstliche Intelligenz sowie Maschine Learning, um verdächtiges Verhalten zu erkennen. Die entsprechenden Konten werden als möglicherweise kompromittiert angezeigt. Außerdem werden basierend auf der Häufigkeit der Interaktionen und anderen Kriterien besonders gefährdete Partner priorisiert, damit Sie sich auf diese Partner konzentrieren können.

Proaktiver Schutz

Proofpoint Supplier Threat Protection unterstützt einen proaktiven Sicherheitsansatz. Die Lösung überwacht die Daten im gesamten Proofpoint-Ökosystem und kann dadurch Aktivitäten von kompromittierten Konten Ihrer Lieferanten erkennen, selbst wenn diese noch keine schädlichen Nachrichten an Sie geschickt haben. Dies ist deshalb so wichtig, weil Ihr Unternehmen nicht immer das erste Ziel eines Angriffs sein muss.

Sie werden benachrichtigt, sobald Proofpoint Supplier Threat Protection Aktivitäten kompromittierter Konten entdeckt, die von Ihren Partnern stammen. Dadurch können Sie schnell Maßnahmen zur Blockierung oder zur absenderbasierten URL-Isolierung ergreifen. Und bei schädlichem Datenverkehr von diesen Konten können Sie sich Benachrichtigungen schicken lassen – entweder direkt per E-Mail oder über eine API an Ihr SIEM-System (Sicherheitsinformations- und Ereignis-Management).

Vereinfachte Untersuchungen

Mit Proofpoint Supplier Threat Protection können sich Ihre Sicherheitsanalysten schnell einen Überblick über die Lage verschaffen und die nächsten Schritte vorbereiten. Die Lösung bietet Erkenntnisse zum kompromittierten Lieferantenkonto, einschließlich einer detaillierten Analyse und einer Zeitleistenansicht der Aktivitäten. Dabei werden die betroffenen Empfänger und die Bedrohungen genannt, die bei ihnen eingegangen sind.

Dank der Integration intelligenter Suchfunktionen können Ihre Analysten schnell weitere Nachrichten finden, die mit dem kompromittierten Lieferantenkonto ausgetauscht wurden. Dadurch erfährt Ihr Team, ob finanzielle oder vertrauliche Daten weitergegeben wurden und welche Mitarbeiter mit diesem Konto kommuniziert haben.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter [proofpoint.com/de](https://www.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 75 Prozent der Fortune-100-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.

© Proofpoint, Inc. Proofpoint ist eine Marke von Proofpoint, Inc. in den USA und anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.