proofpoint.

KURZVORSTELLUNG

# Proofpoint Supplier Threat Protection

Erkennung und Blockierung von Bedrohungen durch kompromittierte Lieferantenkonten, bevor sie Schaden verursachen

## Wichtige Highlights

- **Automatisierte Erkennung und Überwachung der Kommunikation mit der Supply Chain**
- **Proaktive Erkennung und Blockierung von Bedrohungen durch kompromittierte Lieferantenkonten**
- **Anpassbare Steuerelemente mit Hinweisen für Anwender zu sicheren Entscheidungen**
- **Schnellere Reaktion auf Risiken, da Kompromittierungen von Lieferantenkonten kanalübergreifend dem Angriffspfad zugeordnet werden**

## Überblick

Da Unternehmen agentenbasierte Arbeitsplätze einführen, gehen Lieferantenbeziehungen nun über E-Mail hinaus und betreffen Collaboration-Tools sowie weitere Kanäle. Durch dieses erweiterte Ökosystem stehen Bedrohungsakteuren neue Möglichkeiten zur Verfügung, mit denen sie gekaperte Drittanbieter- und Lieferantenkonten ausnutzen können. Bei diesen Angriffen nutzen die Angreifer das Vertrauen der Menschen aus, um kanalübergreifenden Supply-Chain-Betrug zu starten, Anmeldedaten zu stehlen und Daten zu exfiltrieren. Da Nachrichten von legitimen Konten gesendet werden, umgehen diese Bedrohungen oft Schutzmaßnahmen, die auf Domain-Überprüfungen und Authentifizierungen setzen.

Mit Proofpoint Supplier Threat Protection (in Proofpoint Collaboration Security Prime enthalten) erhalten Sie kontinuierliche Transparenz zu Kompromittierungen von Lieferantenkonten sowie aktiven Schutz vor Supply-Chain-Angriffen. Die Lösung nutzt Proofpoint Nexus™ AI sowie unsere globalen Bedrohungsdaten und lernt Ihre normalen Lieferanten-Kommunikationsmuster. Dadurch erkennt sie subtile Veränderungen im Anwendungsverhalten – selbst bei Nachrichten von legitimen, authentifizierten Domains.

Sicherheitsteams können auch kompromittierte Lieferanten über Kanäle und Angriffsphasen hinweg verfolgen, um die dringendsten Bedrohungen schnell zu finden und einzudämmen. Das verringert nicht nur Ihr Risiko für Sicherheitsverstöße über die Supply Chain, sondern hilft Ihnen auch beim Schutz vertrauenswürdiger Partnerbeziehungen.

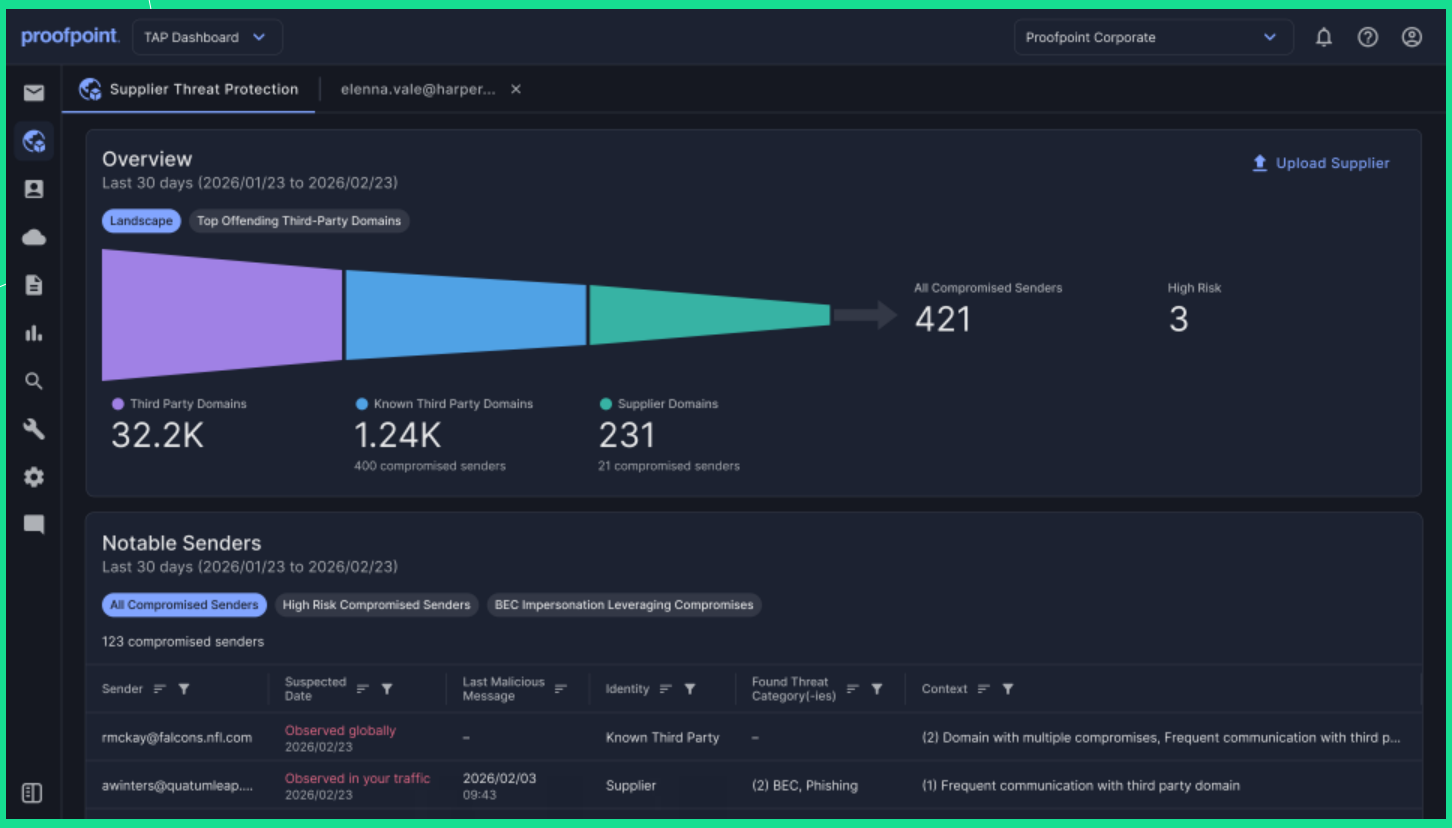


**Abb. 1:** Proofpoint erkennt potenziell kompromittierte Lieferantenkonten und bietet relevante Kontextdaten.

# Umfassender Schutz vor Supply-Chain-Angriffen

Proofpoint schützt mit mehrschichtigen, KI-gestützten Maßnahmen vor Supply-Chain-Angriffen. Schädliche Lieferanten-E-Mails werden blockiert, bevor sie die Anwender erreichen. Die Erkennungsgenauigkeit liegt bei 99,999 %. Gleichzeitig überwacht verhaltensbasierte KI vertrauenswürdige Lieferantenbeziehungen, um subtile Anzeichen für eine Kompromittierung zu erkennen. Dies schließt legitime, authentifizierte Domains ein. Dadurch können sich Angreifer nicht hinter einem vertrauenswürdigen Konto verstecken, um Ihre Schutzmaßnahmen zu umgehen.

Wenn eine Nachricht riskant, aber nicht eindeutig schädlich ist, wendet Proofpoint adaptive Schutzmaßnahmen wie Warnhinweise in der E-Mail und Browser-Isolierung an. Dadurch können Anwender sichere Entscheidungen treffen, ohne legitime Geschäftsnachrichten zu stören. Verdächtige Links werden automatisch isoliert oder blockiert, selbst wenn Anwender darauf klicken. Durch die Kombination von Blockierung vor der Zustellung mit intelligenten, Anwenderschutzmaßnahmen zum richtigen Zeitpunkt bietet Proofpoint echten mehrschichtigen Schutz während des gesamten Supply-Chain-Angriffszyklus.

# Umfassende Transparenz zu Ihrem Lieferanten-Ökosystem

Mit Proofpoint erhalten Sicherheitsteams tiefgehende, kontinuierliche Einblicke in das Supply-Chain-Risiko in Ihrem gesamten Drittanbieter-Ökosystem, sodass Sie dieses Risiko proaktiv reduzieren können, statt nur auf Zwischenfälle zu reagieren. Sie erhalten genaue Einblicke zu jeder Lieferantendomain, die mit Ihrem Unternehmen kommuniziert, einschließlich aktive Anbieter, neu beobachtete Drittanbieter sowie Domains, die zuvor mit Kompromittierungen in Verbindung gebracht wurden. Dies ermöglicht eine stets aktuelle Übersicht über das Supply-Chain-Risiko in Ihrem Unternehmen.

Dabei kennzeichnet Proofpoint nicht nur schädliche E-Mails, sondern liefert zudem wichtigen Kontext, damit Sie die Interaktionen der Lieferanten mit Ihrem Unternehmen verstehen. Sie können Details zu Finanztransaktionen wie Rechnungsstellung, ungewöhnliche Empfänger, Veränderungen in Kommunikationsmustern und verdächtige Themen beobachten.

Proofpoint Nexus analysiert mehr als 2,1 Billionen E-Mails von mehr als 2,8 Millionen Kunden, um kompromittierte Lieferantenkonten überall im Ökosystem aufzudecken – oft bevor diese Konten Sie überhaupt angreifen. Dank dieser Transparenz können Sie Ihr Lieferantennetzwerk erweitern, ohne am modernen agentenbasierten Arbeitsplatz Risiken einzugehen.

# Vereinfachte Untersuchungen für maximale Effizienz

Proofpoint Supplier Threat Protection zentralisiert die Erkennung von kompromittierten Lieferantenkonten und die Reaktion innerhalb von Proofpoint Collaboration Security Prime. Dadurch können Sicherheitsteams sowohl die Zahl der Vorfälle reduzieren als auch die für deren Untersuchung benötigte Zeit verkürzen. Schädliche Lieferanten-E-Mails werden vor der Zustellung blockiert und Nachrichten mit erhöhtem Risiko erhalten Warnhinweise und werden per Browser-Isolierung geschützt. So erreichen Analysten weniger Vorfälle und es gibt weniger von Lieferanten verursachte Ereignisse, die eine manuelle Überprüfung erfordern. Und da sich Sicherheitsteams weniger mit routinemäßiger Triage beschäftigen müssen, können sie sich auf besonders kritische Risiken konzentrieren.

Wenn es zu einem Vorfall kommt, findet Ihr Team alle für die Untersuchung erforderlichen Daten an einem Ort. Die Aktivitäten der Lieferanten werden automatisch mit zugehörigen E-Mail- und Cloud-Signalen verknüpft, die auf eine Kontoübernahme hinweisen. Ihr Team erkennt sofort, ob das Problem isoliert oder Teil eines größeren, mehrstufigen Angriffs ist. Die Prime Threat Protection Workbench visualisiert die Bewegung eines Angriffs über alle Kanäle, sodass das Verständnis der Auswirkungen und die Priorisierung von Reaktionen auf einen Blick vereinfacht wird.

Teams können eine detaillierte Historie der Kommunikation und des Verhaltenskontexts anzeigen sowie Durchsetzungsmaßnahmen ergreifen – alles über eine einzige Konsole und ohne zwischen mehreren Tools wechseln zu müssen. Das beschleunigt die Eindämmung und bedeutet auch, dass Sie klare Beweise an betroffene Lieferanten weitergeben können, um Behebungsmaßnahmen zu koordinieren, Wiederholungen zu verhindern und Ihre Geschäftsbeziehungen zu stärken.

# Weitere Informationen

Weitere Informationen finden Sie unter **proofpoint.com/de**.

proofpoint.