Proofpoint Supplier Threat Protection

Identify compromised third-party accounts and gain insights into the risks they pose

Key Benefits

- Proactively monitor exposure and detect compromised known third-party and supplier accounts
- Get automated notification of compromised vendor accounts sending malicious messages to your company
- Prioritise compromised supplier accounts to investigate and remediate
- Identify those employees who recently communicated with the compromised supplier account

Proofpoint Supplier Threat Protection extends the power of Proofpoint Targeted Attack Protection by detecting compromised suppliers and other third parties to help defend your supply chain against phishing, malware and business email compromise (BEC).

Through a unique blend of threat intelligence and behavioural artificial intelligence (AI), Supplier Threat Protection detects email patterns from known senders to your organisation that suggest an account may have been compromised. It also detects patterns between known senders and other Proofpoint customers to keep you protected even if the account has not yet sent threats to you directly.

You get a detailed history of email activity, rich contextual data and a dashboard showing those third-party accounts that pose the greatest risk. This actionable insight equips you to prevent threats from reaching your users, prioritise risks, streamline investigation and respond quickly.
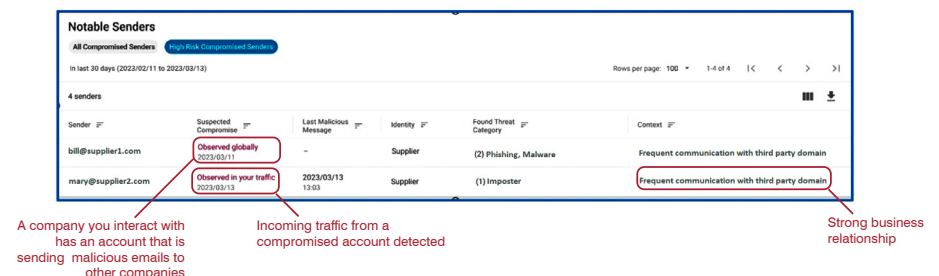

Figure 1: Proofpoint Supplier Threat Protection detects suspected compromised supplier accounts and provides relevant contextual information.

Visibility

Supplier Threat Protection identifies third-party accounts that communicate with your organisation. It establishes a baseline of communication activities between employees and suppliers. It then uses threat intel and AI/ML to detect suspicious behaviour. And it displays accounts that are likely to have been compromised. It also prioritises high-risk partners based on interaction frequency and other criteria. This lets you focus on those partners to whom you are most exposed.

Proactive Defense

Supplier Threat Protection allows you to take a proactive stance to security, rather than a reactive one. It monitors data from throughout the Proofpoint ecosystem. It detects compromised account activity from vendors with whom you interact. It can do so even if a vendor has not yet sent threats to you directly. This is important because your company might not always be the first target of an attack. If Supplier Threat Protection spots compromised account activity from your partners, you can get early notification. You can then block or create sender-based isolation if you choose. And if you do receive traffic from one of these accounts, you can receive email alerts or have notifications sent to your security information and event management (SIEM) system by an API.

Simplified Investigations

With Supplier Threat Protection, your security analysts can quickly understand what happened and what actions to take next. It provides insights about the compromised supplier account. It gives you Proofpoint's analysis and a timeline view of activity. And it identifies the targeted recipients and the threats that were sent to those targets.

Integration with Smart Search enables your analysts to quickly find other messages that were exchanged with the compromised supplier account. This lets your team see if financial or sensitive data was exposed to the account. And it identifies other employees who may have communicated with it.

LEARN MORE
For more information, visit **proofpoint.com**.

---

proofpoint.