Proofpoint Supplier Threat Protection

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

Key Benefits

- Defend against impersonation threats that lead to financial loss and data extortion
- Improve visibility by proactively detecting suspected compromised third-party and supplier accounts
- Get automatically notified of suspected compromised accounts sending malicious messages to your company
- Add layers of protection by limiting user communications with suspected compromised accounts
- Better manage team resources through prioritised, high-risk suspected compromised accounts to investigate and remediate
- Identify which employees recently communicated with the suspected compromised accounts

Proofpoint Supplier Threat Protection keeps your supply chain safe from impersonation threats that lead to advanced phishing, malware and business email compromise (BEC) attacks. It checks your suppliers and known third parties for signs that their accounts may have been compromised. Using threat intelligence and behavioural artificial intelligence (AI), it spots suspicious emails containing impersonation threats from these compromised accounts and enables adaptive security controls to limit their communications. But Supplier Threat Protection extends its visibility beyond just your own communications. It also observes patterns between suspect accounts and other Proofpoint customers, and it can notify you even if the account has not yet sent you an attack.

Supplier Threat Protection is a unique impersonation risk solution for your supply chain that defends against email threats before they are launched. It uses adaptive controls, such as browser isolation and email warning tags, to limit a potentially compromised account from accessing your users. It also gives you a record of email activity, rich contextual data and a dashboard that displays the third-party accounts posing the most risk. These help you to prioritise the handling of risk, streamline investigations and respond quickly.

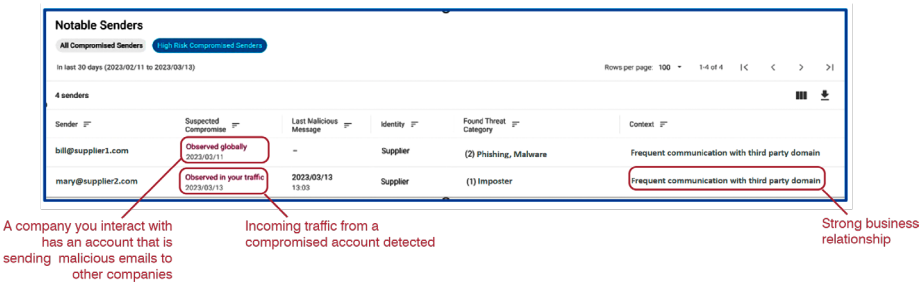

Figure 1: Proofpoint Supplier Threat Protection detects suspected compromised supplier accounts and provides relevant contextual information.

This solution set is part of Proofpoint's integrated Human-Centric Security platform, mitigating the four key areas of people-based risks.

Unmatched Visibility

Supplier Threat Protection gives you in-depth visibility into impersonation risk from suspected compromised accounts messaging your people. It also reveals compromised accounts Proofpoint sees globally that have not yet sent threats to your users. With these insights, you can enable better security measures for specific users as well as take precautionary action.

Supplier Threat Protection automatically identifies third-party accounts that communicate with your organisation. It also establishes a baseline of mail activities between your workers and suppliers. It then uses threat intel and AI/ML to spot suspicious behaviour. The solution displays accounts that may have been compromised and ranks high-risk partners. The ranking is based on interaction frequency, patterns of bad behavioural and other factors. It helps you focus on partners that are the most risky.

Proactive Protection

Supplier Threat Protection allows you to take a proactive stance to security. If it spots compromised-account activity from your partners in our ecosystem, it provides you with quick alerts in the dashboard. It also deploys adaptive controls to protect your users. These controls include Proofpoint Isolation, which opens links from suspect accounts in a safe, isolated browser. It also includes customisable email warning tags that notify users of suspected compromised accounts. This helps prevent users from forwarding sensitive information, downloading malicious files or uploading their credentials.

When you receive an alert, you can create more sender- or domain-based security policies. If you get traffic from one of these accounts, you can set Supplier Threat Protection to send email alerts or you can have an API send notifications to your security information and event management (SIEM) system.

Simplified Investigations

Supplier Threat Protection helps your security analysts. It allows them to quickly understand what happened, what actions were taken and what to do next. It streamlines investigations, saves time and creates operational efficiencies for your team.

The solution provides insights about suspected compromised supplier accounts. These insights include Proofpoint analysis, context around sender-recipient relationships and a timeline view of message activity. It also shows the controls that were triggered and recommends actionable next steps in the investigative process.

Integration with Smart Search allows your analysts to identify the recipients who were targeted and with what. They can find other messages that were exchanged with the suspect supplier account. They can also see financial or sensitive data that was exposed as well as other employees who may have communicated with the account—all without leaving the Supplier Threat Protection dashboard.

Proofpoint's Ecosystem Advantage

Supplier Threat Protection monitors data from throughout the Proofpoint ecosystem. It relies on our ability to see a large portion of the world's global email traffic (more than 3.1 billion messages a day) to identify accounts that may have been compromised and are sending impersonation threats.

After discovering third parties and suppliers with whom you interact, Supplier Threat Protection keeps track of their communications with you and other Proofpoint customers. This allows us to notify you of suspect suppliers before you are attacked. This is important because your company may not always be the first target.

LEARN MORE

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