proofpoint.

SOLUTION BRIEF

Proofpoint and CrowdStrike Partnership

Protecting Your People and Their Devices

The Partnership at a Glance

- Leverage best-of-breed threat intelligence sharing
- Achieve multi-layered threat protection
- Secure organizations' devices and data against sophisticated malware and malware-free attacks
- Gain immediate visibility and context into threat adversaries and attack vectors
- Enable posture checking to ensure endpoint is compliant before accessing company resources

As companies continue struggling with advanced threats targeting their organization, new approaches are needed to help mitigate the risk of these threats. We know that over 90% of threats originate via the email vector. Proofpoint and CrowdStrike have partnered to give shared customers an enhanced security posture—from email to the device itself.

Proofpoint Targeted Attack Protection (TAP) helps you stay ahead of attackers with an innovative approach that detects, analyzes and blocks advanced threats before they reach your inbox. This includes ransomware and other advanced email threats delivered through malicious attachments and URLs. The CrowdStrike Falcon platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise. This provides you with an innovative approach to handle these threats. You gain deep, real-time visibility into endpoint activity, threat investigation and remediation to stop breaches.

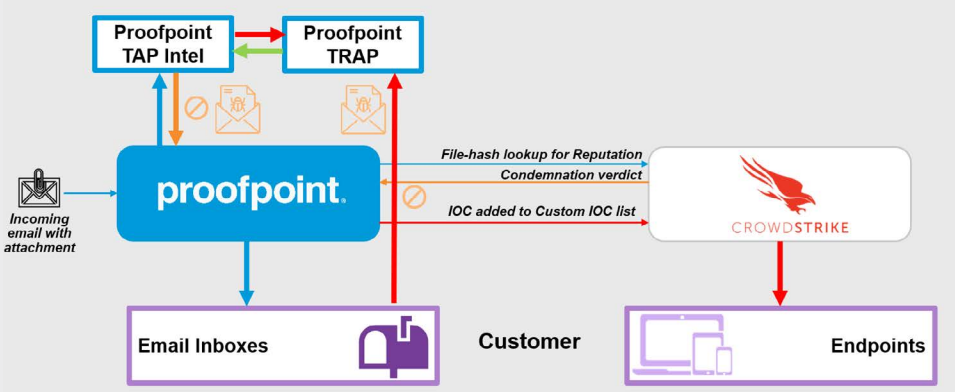
Proofpoint Meta offers an evolutionary step in networking. It's the first software-defined enterprise network-as-a-service that can securely connect your users to data centers, public and private clouds, SaaS applications and offices. And, it provides you with the agility and performance that today's enterprises need. Meta's Zero Trust architecture binds each user within a software-defined perimeter. Every user has a unique, fixed identity. It doesn't matter where they connect from to this network or which device they connect on.

With this technical partnership, we're focused on the shared vision of protecting people and their devices from today's most sophisticated threats. You get additional security benefits and expanded visibility—at no additional cost enhancing Zero Trust security. You also receive the benefits of having integration with these two best-of-breed solutions.

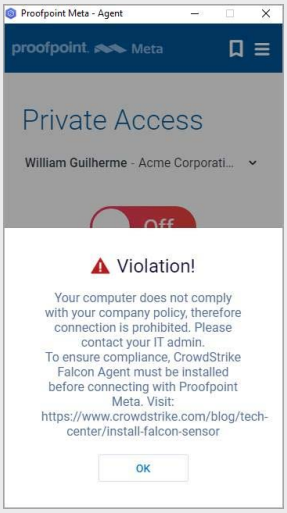
How the Integration Works

Multi-layered protection through threat intelligence sharing

As your people remain the top target for attackers, it is imperative to have a multi-layered defense to stop targeted attacks. Our existing integration that leverages Proofpoint TAP and CrowdStrike provides both pre-delivery and post-delivery protection and remediation through threat intelligence sharing.



Proofpoint + CrowdStrike: Multi-layered Protection Through Threat Intelligence Sharing



Posture Check Failure Alert

Pre-delivery email protection

When an email that contains a file is sent to a customer, TAP will begin its sandbox analysis to determine if it is malicious. At the same time, TAP will query the CrowdStrike Intelligence for file reputation. If CrowdStrike knows the file to be malicious, it will inform TAP. From there, the message and file will be condemned and blocked from ever reaching the user.

Posture checking to increase Zero Trust security

With this integration between Meta and Falcon, administrators can set up easy polices to ensure the endpoint is in compliance. We are able to check the endpoint to determine if the Falcon agent has been deployed. If the agent has not been deployed, we can disconnect the user so that they are unable to access company resources. In addition, the administrator can set up a notification letting the user know why they failed compliance and include a remediation action such as visiting a URL to install the Falcon agent. This integration helps to ensure the endpoint agent is as secure as possible before it's allowed to access potentially confidential company data or other resources.

Post-delivery protection and automated remediation

For multi-layered post-delivery protection, TAP shares threat information with the CrowdStrike Falcon platform. This provides you with enhanced security to protect your people, both through email and the device. When TAP detects that a malicious file has been delivered via email, it can alert Proofpoint Threat Response Auto-Pull to quarantine any of those delivered messages as well as query CrowdStrike Intelligence to determine if it's known. If malicious content is known, no action is taken because the device will be protected. If it's unknown, then the malicious hash information is added to the CrowdStrike list of custom indicators of compromise (IOCs). And, an alert is created if the malicious content tries to execute on the device.

The Proofpoint and CrowdStrike integration makes it easy to detect, investigate and remediate email threats—providing an enhanced level of protection for your organization and your people.

LEARN MORE

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