CrowdStrike Technology Partners

Solution Brief

CROWDSTRIKE AND PROOFPOINT INTEGRATION: ADVANCED EMAIL THREAT DETECTION

Protecting organizations, people and their devices

CHALLENGE

As companies continue to struggle with advanced threats targeting their organizations, new approaches are needed to help mitigate the risk of these threats, most of which originate through email.

SOLUTION

CrowdStrike and Proofpoint have partnered to provide joint customers with an innovative approach to handling threats, offering enhanced security posture from email to the device itself.

CrowdStrike and Proofpoint are focused on the shared vision of protecting people and their devices from today's most sophisticated threats. With this partnership, you get additional security benefits and expanded visibility — at no additional cost. You also gain the benefits of the integration of two best-of-breed solutions.

KEY BENEFITS

Gain the advantage of sharing best-of-breed threat intelligence

Achieve multi-layer threat protection

Secure your organization's devices and data against sophisticated malware and malware-free attacks

Gain immediate visibility and context into threat adversaries and attack vectors

TECHNICAL SOLUTION

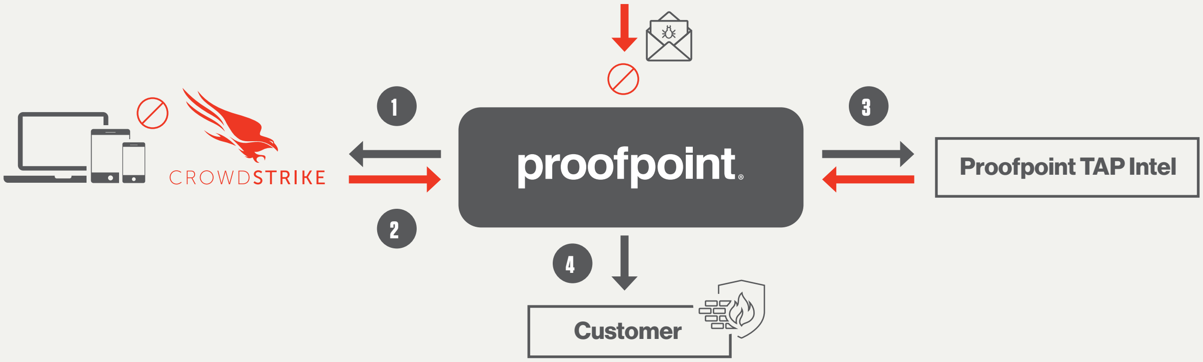
SHARED THREAT INTELLIGENCE

This integration allows Proofpoint Targeted Attack Protection (TAP) and the CrowdStrike Falcon® platform to share threat intelligence. When an email that contains a file is sent to a customer, Proofpoint TAP begins its sandbox analysis to determine if it is malicious. This helps customers 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. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, and superior protection and performance across the enterprise.

MULTI-LAYERED PROTECTION

For multi-layered protection, Proofpoint TAP shares threat information with the CrowdStrike Falcon platform. This provides more enhanced security to protect both your employees' email and their devices. When Proofpoint TAP detects that a malicious file has been delivered via email, it queries the CrowdStrike threat intelligence module to determine if the threat is known. If the malicious content is known, no action is taken because the device will be protected. If it's unknown, the malicious hash information is added to CrowdStrike's custom list of indicators of compromise (IOCs), and an alert is created if the malicious content tries to execute on the device. This customized intelligence added to CrowdStrike threat intelligence will help you to proactively defend against any similar future attacks seen on other endpoints in the organization.

How CrowdStrike Falcon and Proofpoint TAP Work Together



1 Proofpoint TAP Attachment Defense inspects the file and also queries the CrowdStrike Intelligence application programming interface (API).

2 If the file is known by CrowdStrike to be malicious, Proofpoint TAP will quarantine the file, and it won't be delivered to the end user.

3 If the file is not known to CrowdStrike but is found to be malicious by Proofpoint TAP, it will be quarantined and not delivered to the end user.

4 The customer benefits from improved protection through this sharing of threat intelligence.

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 its employees. Through the ongoing development of new integrations, this partnership will continue to add solutions to provide the best protection for Proofpoint and CrowdStrike customers.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyberattacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint to mitigate their most critical security and compliance risks across email, the cloud, social media and the web.

More information is available at **www.proofpoint.com**.

ABOUT CROWDSTRIKE

CrowdStrike Holdings, Inc. (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

Start Free Trial
of Next-Gen AV

Learn more **www.crowdstrike.com**