proofpoint.   CROWDSTRIKE

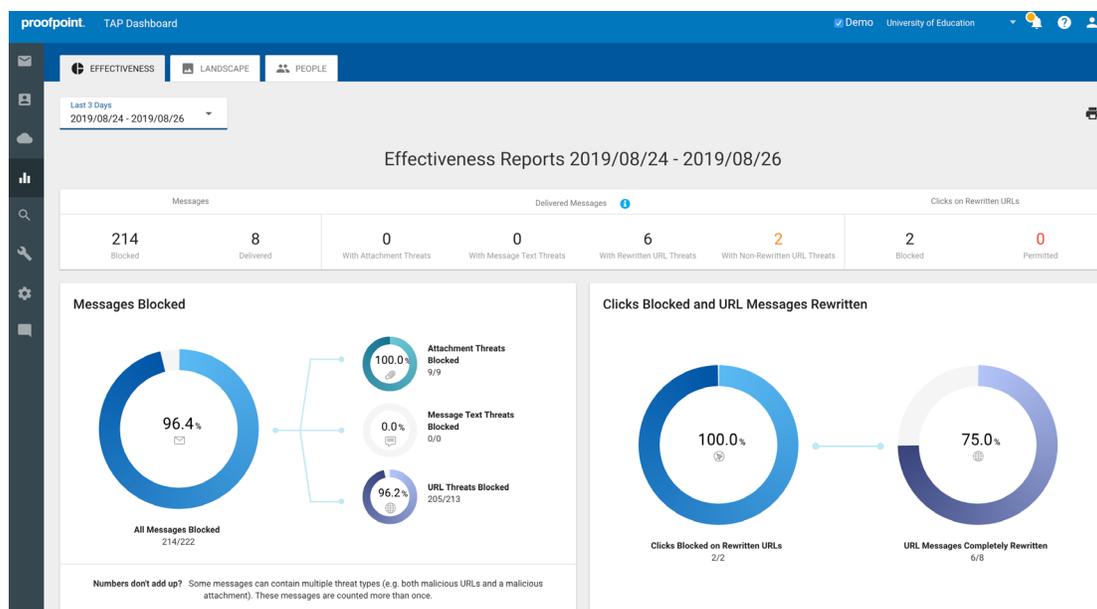# PROOFPOINT AND CROWDSTRIKE PARTNERSHIP
PROTECTING ORGANIZATIONS' PEOPLE AND THEIR DEVICES

As companies continue struggling with advanced threats targeting their organizations, new approaches are needed to help mitigate the risk of these threats. We know that over 90% of malware threats originate via the email vector.[1] Proofpoint has a range of solutions you can deploy to help protect against this barrage of attacks. Proofpoint Targeted Attack Protection (TAP) helps block attachment and URL-based malware and provides you with deep visibility into the threats that are targeting your organization and the people in it.

Invariably, there will be threats that make it to users' devices. Making sure those threats can't cause harm to the device or spread to other devices becomes very important. 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.
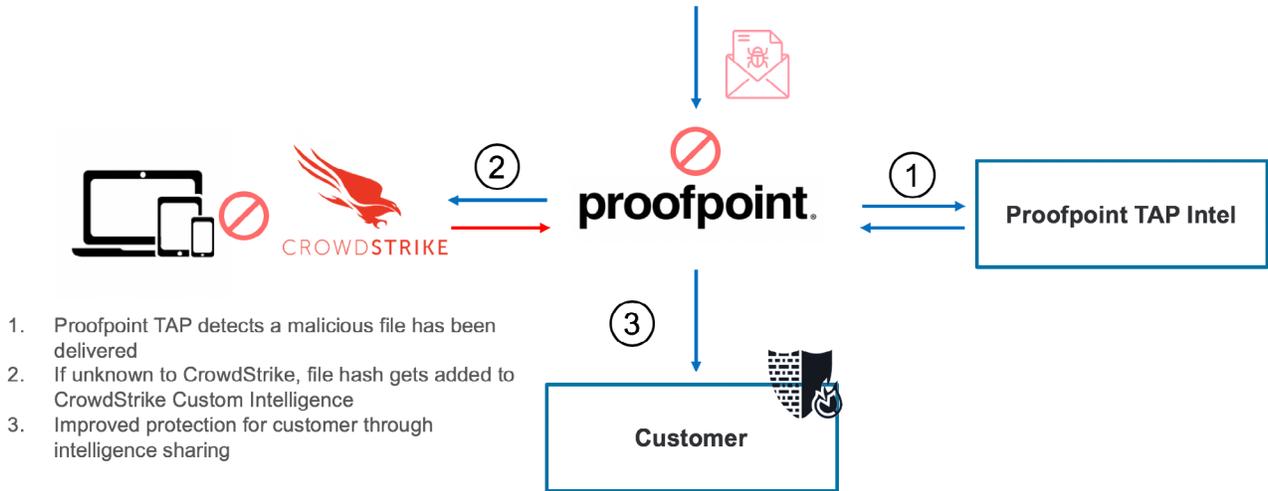
The Partnership at a Glance:
• Achieve multi-layer threat protection
• Secure organizations' devices and data against sophisticated malware and malware-free attacks
• Gain immediate visibility and context into threat adversaries and attack vectors

[1] Verizon. "2019 Data Breach Investigations Report." July 2019.

The technical partnership between Proofpoint and CrowdStrike allows our shared customers to enhance their security posture from email to the device itself. We're 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 receive the benefits of having integration with these two best-of-breed solutions.

1. Proofpoint TAP detects a malicious file has been delivered
2. If unknown to CrowdStrike, file hash gets added to CrowdStrike Custom Intelligence
3. Improved protection for customer through intelligence sharing

HOW THE INTEGRATION WORKS

As the partnership evolves, we expect to include several additional points of integration. This will more fully protect our shared customers.

The initial integration allows Proofpoint TAP to share threat information with the CrowdStrike Falcon platform. This enables more enhanced security on the device itself. When Proofpoint TAP detects that a malicious file has been delivered via email, we are able to query CrowdStrike Falcon X, the threat Intelligence module, to determine if it's 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 the CrowdStrike list of custom 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 Falcon X will help you to proactively defend against any similar future attacks seen across other endpoints in the organization.

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.