proofpoint | CROWDSTRIKE

SOLUTION BRIEF

Proofpoint + CrowdStrike

Securing humans.
Empowering the agentic SOC.

Coordinated response. Unified visibility.

Proofpoint threat research shows that 94% of today's human-targeted attacks begin in the inbox. But the modern attack chain doesn't end there. Adversaries pivot from email to cloud applications and endpoints, then they move laterally across the enterprise. Security teams that rely on siloed tools miss the connections between these events. And that means attackers have the time they need to escalate and exfiltrate.

The Proofpoint and CrowdStrike partnership addresses this challenge head-on. Together, we deliver complete protection for people and the agentic security operations center (SOC).

Proofpoint's human-centric security platform, combined with CrowdStrike's world-class endpoint and identity intelligence, delivers correlated detection across payload, SaaS, and identity threats, along with coordinated automated responses and unified visibility for SOC teams.

Stop Malicious Payloads at Every Stage of Delivery

The global average cost of a data breach reached $4.44M in 2025.[1] Because phishing and malware remain common ways attackers gain an initial foothold, stopping malicious files before they reach users can help reduce the risk of a costly compromise. Proofpoint Payload Intelligence, powered by the Nexus® AI threat platform, combines sandboxing with CrowdStrike Falcon Intelligence reputation lookups to detect and block malicious files before delivery or execution.

Key Benefits

- Correlated detection across malicious payloads, SaaS, and identity
- Coordinated response across Proofpoint and CrowdStrike platforms
- Unified visibility via shared log data in CrowdStrike LogScale
- Reduced mean time to detection and remediation

Threat Protection	Data Security
URL and attachment sandboxing When an email with an attachment is received, Proofpoint sandboxes it. At the same time, it also queries CrowdStrike Falcon Intelligence for file reputation. If either verdict is malicious, Proofpoint condemns the email beforehand.	**ITM file upload + CrowdStrike Falcon Intelligence** Proofpoint Insider Threat Management (ITM) monitors file uploads to cloud services and calls CrowdStrike Falcon Intelligence for file reputation. Malicious uploads are automatically quarantined. This closes the gap between email-borne threats and data exfiltration via cloud applications.

[1] IBM. *Cost of a Data Breach Report*. 2025.

Protect Cloud Access and Detect Lateral Movement

Attackers who reach an inbox don't stop there. They exploit compromised identities to access cloud applications, and then they move laterally across the network, escalating privileges. Proofpoint's Account Takeover (ATO) Protection works with CrowdStrike to intercept their moves at every step.

App access control	Data Security	Lateral movement detection
Proofpoint Account Takeover Protection + Crowdstrike Falcon Next Gen Identity Security When a user requests cloud access, Proofpoint's ATO queries CrowdStrike Falcon Identity Protection for a real-time user risk score. Based on the score, Proofpoint applies allow, isolate, or block policies—preventing compromised or high-risk identities from accessing sensitive applications.	**Crowdstrike Falcon Insight XDR → Proofpoint ITM** CrowdStrike endpoint intelligence alerts Proofpoint ITM when a device shows signs of compromise. ITM automatically restricts the user's ability to move data—preventing exfiltration while the endpoint is being contained and remediated.	**Proofpoint Shadow → Crowdstrike Falcon Insight XDR** Proofpoint Shadow puts high-fidelity deceptions on endpoints to catch lateral movement by humans or malware. When an attacker engages with a deception, a high-confidence alert is sent to CrowdStrike Falcon XDR, which isolates the compromised host in real time.

Achieve Unified Visibility Across the Full Attack Chain

Proofpoint and CrowdStrike customers can now see and search the complete attack chain in a single, unified view—from initial email delivery through lateral movement and endpoint activity. Proofpoint's Core Email Protection shares detection and response log data with Crowdstrike Falcon Logscale via the SIEM API. As a result, SOC teams can correlate events across both platforms without switching consoles.

This shared telemetry powers the agentic SOC, giving automated workflows the context they need to detect, investigate, and respond at machine speed. So, SOC teams spend less time correlating alerts manually and more time on the highest-priority investigations.

Correlated detection with coordinated response	Unified visibility
Intelligence and actions flow bi-directionally across payload, SaaS, and identity. This ensures that a threat detected at one control point automatically triggers the right response at every other.	Proofpoint's SIEM API streams log data into Crowdstrike Falcon LogScale. So, your SOC has a single, searchable timeline of every attack across email, cloud, and endpoint.

Future-Proof Your Security Operations

Both the Proofpoint human-centric security platform and CrowdStrike Falcon platform are built to evolve with the threat landscape. As AI-powered attacks grow in volume and sophistication, the shared intelligence between Proofpoint Nexus and CrowdStrike's AI-native platform means that your defenses get smarter automatically. New threat indicators discovered by either platform can be shared quickly, reducing the window of exposure.

Together, Proofpoint and CrowdStrike help you to maximize automated threat responses, optimize your security team's efforts, and build an agentic SOC that operates at scale.

Learn more

proofpoint.com/us/partners/crowdstrike
marketplace.crowdstrike.com/partners/proofpoint

proofpoint.