BLOG POST

Mimecast & Crowdstrike: A Platform-to-Platform Partnership

Mimecast and CrowdStrike continue to deepen their integration, uniting email, endpoint, identity, and data protection into a single adaptive defense

AUGUST 6, 2026

Key Points

- The partnership between Mimecast and the CrowdStrike Falcon® platform has matured from a threat-sharing integration into a full platform-to-platform defense spanning email, endpoint, identity, insider risk, and human risk management.
- As adversaries adopt generative AI to craft hyper-personalized phishing and deepfake campaigns, the combined Mimecast and CrowdStrike ecosystem gives security teams the shared intelligence and automated response they need to keep pace.
- Together, the two companies address the same enduring reality: the human element sits at the center of nearly 60% of breaches, and defending it requires integrated intelligence, not disconnected tools.

Cybersecurity leaders keep learning the same lesson: protecting one layer of the infrastructure in isolation is no longer enough. Threats move across email, endpoints, identities, and data in seconds, and the tools defending each layer have to move with them. Since 2019, Mimecast and CrowdStrike have built their partnership around exactly that idea, and over the past two years, it has grown from a set of point integrations into one of the most complete platform-to-platform alliances in the industry.

From threat sharing to a unified defense

The early integration focused on trading indicators of compromise between Mimecast's email security and CrowdStrike's endpoint protection. That foundation still holds, but the scope today is far wider. Joint customers can now connect Mimecast to CrowdStrike Falcon® Insight XDR, Falcon® LogScale, Falcon® Next-Gen SIEM, Falcon® Fusion SOAR, and Falcon® Foundry, giving SOC teams a cohesive view across email, endpoint, identity, cloud workloads, and the many tools on which their operations depend.

The mechanics are straightforward but powerful. Threats detected on the endpoint through CrowdStrike instantly inform Mimecast's email defenses, and suspicious email activity triggers deeper endpoint scrutiny. When CrowdStrike flags a risky endpoint, Mimecast can automatically enforce stricter email policies or quarantine dangerous messages. Email telemetry, including URL logs, flows into the SIEM for correlation and threat hunting, letting analysts trace the full kill chain rather than piecing together isolated alerts. The result is a closed loop that

turns disconnected data points into coordinated action and dramatically shrinks the window attackers have to exploit.

Why integration matters more than ever

The urgency behind this work has only intensified. The 2025 Verizon Data Breach Investigations Report found that the human element factored into roughly 60% of breaches, and email and collaboration platforms remain a primary vector for exploiting it. What's changed is the sophistication of the attacks. Adversaries are now using generative AI to produce hyper-personalized phishing lures, and Mimecast threat analysts are tracking a surge in deepfake audio and AI-generated spear-phishing designed for psychological realism that slips past traditional filters.

Against that backdrop, integration isn't a nice-to-have. Industry research reinforces the point: 81% of organizations cite improved visibility across attack surfaces as a top benefit of integrating security platforms. The Mimecast and CrowdStrike combination delivers that visibility while automating the response, so analysts spend less time switching consoles and correlating alerts and more time on strategic remediation.

Defending the human layer

Because people remain the most targeted and unpredictable element of any security program, the partnership has expanded well beyond blocking malicious messages. The capabilities of Mimecast's Human Risk Command Center continuously assess, score, and address individual user risk based on real-world behavior and threat exposure, combining adaptive security behavior management, behavioral analytics, and dynamic risk scoring. When paired with CrowdStrike, high-risk users identified by Mimecast can trigger automated policies such as stricter endpoint monitoring or targeted phishing simulations, creating a proactive defense that accounts for both human and technical risk.

Data protection rounds out the picture. Mimecast Incydr extends the integration with insider risk detection, continuously monitoring sensitive information in use, in motion, and at rest across email and endpoints. When Incydr spots risky data movement, automated workflows can quarantine emails, restrict transfers on the endpoint, or alert the SOC, while unifying insider-threat and external-threat signals from both platforms into a single view.

A partnership built to evolve

Both companies frame this as a platform model rather than a bolt-on integration, echoing a broader industry shift toward ecosystem collaboration. Omdia's Jay McBain has observed that the typical customer journey now involves an average of seven partners in every deal, and that the organizations best positioned for the future are those that execute on a platform strategy. Mimecast and CrowdStrike have leaned into exactly that approach, and with continued innovation in AI-driven detection, automation, and cloud-native scale, joint customers get a defense that keeps evolving alongside the threat landscape.

In a world where a user can fall for a phishing email in under a minute and AI is accelerating every stage of the attack, disconnected tools simply can't keep up. The combination of Mimecast and CrowdStrike gives organizations integrated intelligence and automation that is, by design, greater than the sum of its parts.