

Multi-Layered Threat Protection & Shared Intelligence

Mimecast and CrowdStrike protect organizations at both the Secure Email Gateway and on Endpoint devices. Now joint customers can enhance threat protection through the integration of these industry leading platforms.

The integration shares intelligence derived from malware detected at the Mimecast Secure Email Gateway with the CrowdStrike Falcon® platform.

Business Needs

Effective threat protection across all systems is mission-critical for organizations of all sizes and across all industries.

In the midst of a global cybersecurity technical skills gap, the volume and sophistication of cyber attacks such as ransomware, impersonation fraud, and phishing continue to increase on a daily basis. Organizations must find new ways to ensure they are protected.

From basic email hygiene through to highly sophisticated and targeted attacks, organizations need security platforms that reduce complexity, minimize risk, and decrease the demand on an already over-taxed and under-skilled security team. Jumping between systems to ensure optimal threat protection, investigate an incident, or respond to a threat simply no longer scales.

Key Benefits

- Protect the organization's devices from threats detected via Email
- Enhance threat detection with best-in-class shared intelligence from the Mimecast Secure Email Gateway and CrowdStrike Endpoint Protection platforms
- Gain a deeper understanding of the threats targeting the organization

Mimecast and CrowdStrike help organizations protect against cyber attacks with an integrated solution that works at the Email and Web gateways as well as on Endpoint devices. With email remaining the most highly leveraged attack vector in a cyber attack, the Mimecast Secure Email Gateway is often the first system to detect new threats. On the other hand, Endpoint security is the organization's last line of defense.

Through the sharing of intelligence from the Secure Email Gateway to the Endpoint, joint customers can be confident that their devices will be protected by CrowdStrike's threat detection capabilities as well as from zero-day email-borne threats detected by Mimecast.

Within minutes of new malware being detected by Mimecast, all CrowdStrike managed devices will be aware of the threat and will prevent the infected file from executing, better protecting the organization and preventing an incident that could take hours, days or even worse to investigate and recover from.

Technical Solution

The Mimecast Targeted Threat Protection and CrowdStrike integration maximizes the organizations security investments with optimized threat detection on Endpoint devices through the sharing of threats detected at the Mimecast Secure Email Gateway with the CrowdStrike Falcon® platform.



¹ As inbound emails are received by Mimecast on behalf of the organization, they are subject to analysis by the Mimecast inspection funnel, where a series of email hygiene and advanced security scanning techniques are applied, to ensure that emails are safe before they are delivered to the recipient.

² Any infected messages detected are not delivered to the intended recipient, protecting the organization immediately.

³ As these threats are detected by Mimecast Targeted Threat Protection, key threat identifiers are shared with the CrowdStrike Falcon® platform.

⁴ CrowdStrike uses this information in the threat detection process on Endpoint devices, infected files detected on Endpoint devices are prevented from executing, optimizing the protection provided using data from email-borne attacks.

Future Investment

As the Mimecast and CrowdStrike partnership grows additional capabilities will be added to the integration. These include:

- Enhancing threat sharing to be bi-directional, where threats detected by CrowdStrike will be shared back to the Mimecast Secure Email Gateway
- Adding additional threat indicators such as known malicious / suspicious URLs and IP addresses used to distribute malware and phishing emails
- Mimecast Threat Intelligence Dashboard Integration

About Mimecast

For organizations concerned about cyber risk and struggling to attract and retain sufficient cybersecurity expertise and budget, Mimecast delivers a comprehensive, integrated solution that protects the #1 cybersecurity attack vector – email.

Mimecast also reduces the time, cost and complexity of achieving more complete cybersecurity, compliance and resilience through additional modules, all while connecting seamlessly with other security and technology investments to provide a coherent security architecture.

Learn more at <http://www.mimecast.com>

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, provides an endpoint protection platform built from the ground up to stop breaches. 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, preventing attacks on endpoints on or off the network. With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

Learn more at <https://www.crowdstrike.com>.