Solution Brief

Mimecast | CrowdStrike Integration

Multi Layer Threat Protection

Challenge

In the midst of a global cybersecurity technical skills gap, organizations need to protect themselves from the increasing volume and impact of ransomware, impersonation fraud, and phishing attacks.

Solution

With the vast majority of cyberattacks starting with email, the Mimecast and CrowdStrike integration provides mutual customers with optimized threat protection on CrowdStrike managed devices without any additional costs or subscription requirements.

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

Technical Solution

The Mimecast Attachment Protect and CrowdStrike integration maximizes the organizations security investments with optimized malware detection on endpoint devices through the sharing of malware 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, a series of email hygiene and advanced security scanning techniques applied to ensure that emails are safe before they are delivered to the recipient.

2 Dependent on policy, the Mimecast Attachment Protect feature is invoked for file attachments that pass standard anti-virus scanning. These files are subject to advanced analysis using sandboxing and static file analysis.

3 When a threat is discovered by Mimecast Attachment Protect, the email message is not delivered to the recipient and the file hash (a unique identifier of the file) is shared with the CrowdStrike Falcon platform. CrowdStrike uses this information in the threat detection process on endpoint devices, optimizing the protection provided using data from email-borne attacks.

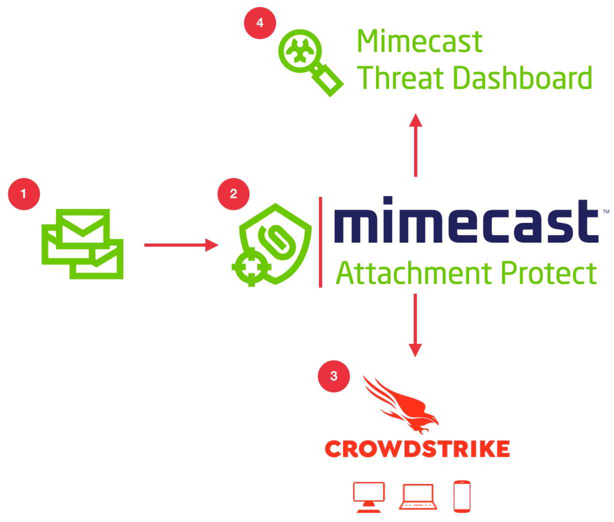

Figure 1: Integration Workflow

4 Data about the threats detected by Mimecast Attachment Protect is made available in the Mimecast Threat Dashboard. Here, security professionals will find detailed analysis of the threat, including who was targeted, when they were targeted, as well as forensic information about the malware.

Use Cases

Combat ransomware and malware-based phishing attacks on CrowdStrike managed devices

As emails with ransomware file attachments are detected by Mimecast Attachment Protect, the hash of the infected file is shared with the CrowdStrike platform. The file hash is used to protect managed devices from the threat.

Gain visibility and context about email-borne malware attacks

As email-borne threats are detected by Mimecast Attachment Protect, forensic detail about the malware and contextual data about who is being targeted is made available in the Mimecast Threat Dashboard and programmatically via the Mimecast API for ingestion into SIEM solutions.

Maintain optimal security while dealing with the cybersecurity skills gap

Achieve shared intelligence between Mimecast Targeted Threat Protection and CrowdStrike without any coding requirements and a simple wizard-based setup experience.

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 https://www.mimecast.com.

About CrowdStrike

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with 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. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches.

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