Mimecast | WildFire Integration

Reduce Risk With Layered Security

Email remains the most common and widely used attack vector for the delivery of malware. Today's malware takes many forms, ranging from commodity mass-delivered inconvenience to custom-built and highly targeted threats. More than ever, it's important for emails with file attachments to undergo thorough and detailed inspection to reduce the risk to your organization.

Mimecast & Palo Alto Networks

As a mutual customer of both Mimecast and Palo Alto Networks, you can maximize your security investments to ensure your organization optimizes malware-based threat detection for email-borne zero-day attacks, and provide your security teams with the data and context they need to combat these threats.

Mimecast Targeted Threat Protection

Mimecast Attachment Protect delivers multi-layered protection against malicious attachments sent to your organization.

Static file analysis breaks the attachment down to spot malicious activity at the code level, probing deeper than traditional sandboxing and eliminating latency typically associated with the sandboxing process.

Attachment Protect also delivers the optimum combination of speed and detection of sophisticated malware. An option to convert all inbound files to a safe file format means that attachments can be safely delivered to employees without delay – a critical first line of defense against constantly changing malware exploits.

The original file can be requested by the employee on-demand, at which time static file analysis and sandboxing are performed prior to delivery.

Administrators can select the most appropriate mode of protection for different groups, or even specific employees, in order to optimize security without impacting productivity.

Palo Alto Networks Cloud-Based Malware Detection & Analysis

Palo Alto Networks WildFire® leverages cloud-based malware detection and multiple analysis techniques to identify and protect against unknown file-based threats, while resisting attacker evasion techniques. WildFire's unique real-time signature streaming capability ensures your organization is protected against previously unknown threats in seconds after they are first discovered. In an industry first, WildFire deploys inline machine learning modules on the NGFW to identify and prevent new and unknown file-based threats, protecting users before a threat can even enter your network.

Key Benefits Of The Integration:

Through the Mimecast and Wildfire integration your organization will benefit from:

- **Optimized malware detection**
  using both the Mimecast and Wildfire scanning and sandboxing technology
- **Richer and more detailed context and intelligence**
  about detected threats, accessible through both the Mimecast and Wildfire dashboarding and reporting tools
- **Alerts and optional automated mailbox remediation**
  for message attachments found to contain malware
- **Detailed reporting**
  on threats detected, blocked and remediated by both the Mimecast and Wildfire products

Solution Overview

The Mimecast Targeted Threat Protection and WildFire integration maximizes your security investments through optimized malware detection using both the Mimecast and WildFire scanning and sandboxing technology to better protect your organization.

As email attachments are received by Mimecast, they pass through the Mimecast inspection funnel, where each file is checked against a number of proprietary and commercial anti-virus engines. Depending on policy, files not flagged by the anti-virus engines are subject to traditional sandboxing or static file analysis or both. Where there is no threat detected the file is sent to WildFire for an all-important second opinion.

In the event a file is subsequently detected as malware by WildFire, an alert is sent to a pre-defined user or group to take action. If your organization's Mimecast subscription includes the Threat Remediation feature, you can also trigger an automated mailbox remediation of the email(s) containing the malware attachment, ensuring that the threat is neutralized as soon as possible. The next time the malware is detected via email it will be automatically blocked, ensuring no further spread of the malware in your organization.

WildFire sandbox analysis is available for all files submitted by Mimecast whether they are found to be malware or benign. This analysis is available using the WildFire Reports feature.

Additionally, files detected as malware by WildFire are visible in the Mimecast Threat Dashboard where you will find detailed information about the threat from both Mimecast and WildFire.

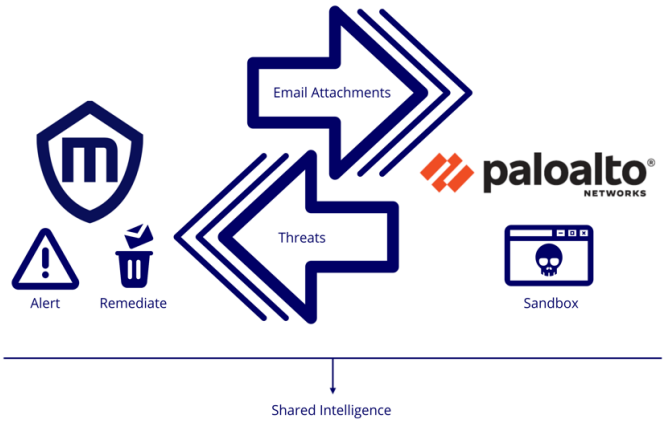

Figure 1: Integration Workflow

Use Cases

Use Case #1

Challenge
Email is one of the primary attack vectors used for the delivery of zero-day malware. Defending against these new threats is a critical yet complex task for organizations across all industries and of all sizes.

Solution
By combining sandboxing and static file analysis from Mimecast's Targeted Threat Protection with Palo Alto Networks' Cloud-Based Malware Detection and Analysis, organizations will benefit from enhanced threat detection and automated remediation for email-borne zero-day attacks.

Use Case #2

Challenge
When investigating cyber threats, visibility, attack context and forensic information is key for security teams to understand and assess impact, as well as the Visibility, context and awareness of malware-based attacks

Solution
The Mimecast and Palo Alto Networks WildFire integration provides security teams with detailed context on who is being targeted, when, and by what type of malware. Forensic information about detected malware is available in both systems, ensuring that data is always at hand.

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 Palo Alto Networks

Palo Alto Networks, a global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate.

Their mission is to be the cybersecurity partner of choice, protecting our digital way of life. They help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, they are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices.

Their vision is a world where each day is safer and more secure than the one before.

For more information, visit www.paloaltonetworks.com.