Palo Alto Networks and Mimecast

Reduce Risk with Layered Email Security

Benefits of the Integration

Together, Mimecast and Palo Alto Networks provide:

- Optimized detection and prevention of zero-day exploits and malware, driven by cloud-based analysis and globally crowdsourced intelligence.
- Richer, more detailed context and intelligence on detected threats, accessible through both Mimecast and WildFire dashboards and reporting tools.
- Alerts and optional automated mailbox remediation of messages found to contain malware.
- Detailed reporting on threats detected, blocked, and remediated by both Mimecast and WildFire.

The Challenge

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. Over the past few years, the attack methodologies have changed significantly to include hybrid-style attacks using malware elements combined from previous campaigns as well as fileless malware that attempts to hide from scanning technologies. Ransomware is increasingly being delivered through these new malware campaigns. It has been estimated that there would be more than 700 million new malware samples in 2020 alone.[1] It is now more important than ever for emails with file attachments to undergo thorough and detailed inspection to reduce the risk to organizations.

The best way to address this is to use multilayered scanning technologies to determine if attachments contain any new malware strains and protect against subsequent instances, combined with the intelligence to understand the execution techniques of the malware. It is also vitally important to be able to remediate existing malicious email should a new malware strain be found.

Mimecast Targeted Threat Protection

As attackers continue to adapt malware to recognize when it is being analyzed by traditional sandboxing, it is crucial to inspect attachments using multiple techniques. Mimecast Email Security delivers multilayered protection against malicious attachments sent to your organization.

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

Mimecast's attachment inspection capabilities are designed to deliver the optimal combination of speed and detection of sophisticated malware. An option to convert all inbound files to a safe file format means attachments can be safely delivered to employees without delay—a critical first line of defense against constantly changing malware. The original file can be requested 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 users, to optimize security without impacting productivity.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. Central to this architecture is WildFire® malware prevention service, which turns every Palo Alto Networks deployment into a distributed sensor and enforcement point to stop zero-day malware and exploits before they can spread and impact the network.

1. "Malware Statistics & Trends Report," AV-TEST, accessed March 15, 2021, https://www.av-test.org/en/statistics/malware.

Palo Alto Networks and Mimecast

Integration between Mimecast Targeted Threat Protection and Palo Alto Networks WildFire maximizes your security investments through optimized malware detection using the techniques of both technologies, with cloud-based analysis, inline machine learning-based prevention, and globally crowdsourced intelligence to better protect your organization.

As Mimecast receives email attachments, they pass through the Mimecast inspection funnel, where each file is checked against a number of proprietary and commercial antivirus engines. Files not flagged by the antivirus engines are subject to static file analysis and/or traditional sandboxing. Whether a scanned email attachment contains malware or Mimecast's attachment scanners see it as clean, the file is sent to WildFire for a second opinion.

In the event WildFire subsequently detects that a file contains malware, a predefined user or group is alerted 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 or emails 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 malicious or benign. This analysis is available using the WildFire Reports feature.

Use Case 1: Layered Security

Challenge

Malware remains the preferred methodology for malicious actors to gain access to your corporate infrastructure, and it constantly evolves as attackers attempt to stay ahead of your detection capabilities.

Solution

Layered security from both Mimecast and Palo Alto Networks employs a unique combination of malware analysis techniques backed by real-time intelligence from tens of thousands of subscribers.

Use Case 2: Threat Sharing

Challenge

Threat sharing across the security landscape typically requires investment in additional software and significant resource time in order to increase protection.

Solution

Malware-based email threats are stopped through the combination of Mimecast and WildFire. Threats are remediated from your end user mailboxes, and prevention controls are shared across your Palo Alto Networks ecosystem on the endpoint, network, and cloud. Blocking and remediation are fully automated and require no administrator intervention.

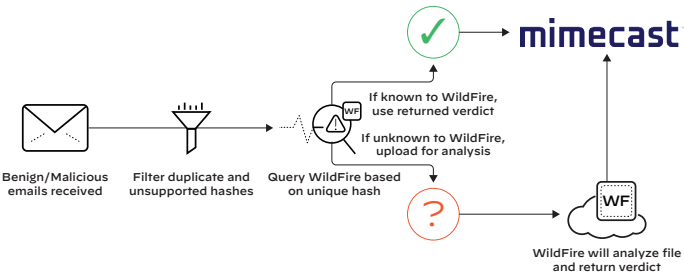

Figure 1: Mimecast integration workflow

About Mimecast

Mimecast takes on cyber disruption for our customers; putting them first, and tackling their biggest security challenges together —email. Our mission is to protect organizations from malicious activity, human error and technology failure; and help lead towards building a more resilient world. Learn more about us at www.mimecast.com.

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com