mimecast®

DATASHEET

Mimecast Targeted Threat Protection

Attachment Protect

Next-generation attachment sandboxing for advanced protection from spear-phishing and other targeted email attacks.

Targeted attacks in email have rapidly increased in volume and sophistication. Attackers are using multiple ways to infiltrate organizations in order to achieve their goals, that may include stealing data, staging ransomware demands or even a springboard attack on another company. Protecting against these unknown threats requires advanced security measures over and above standard email security filters.

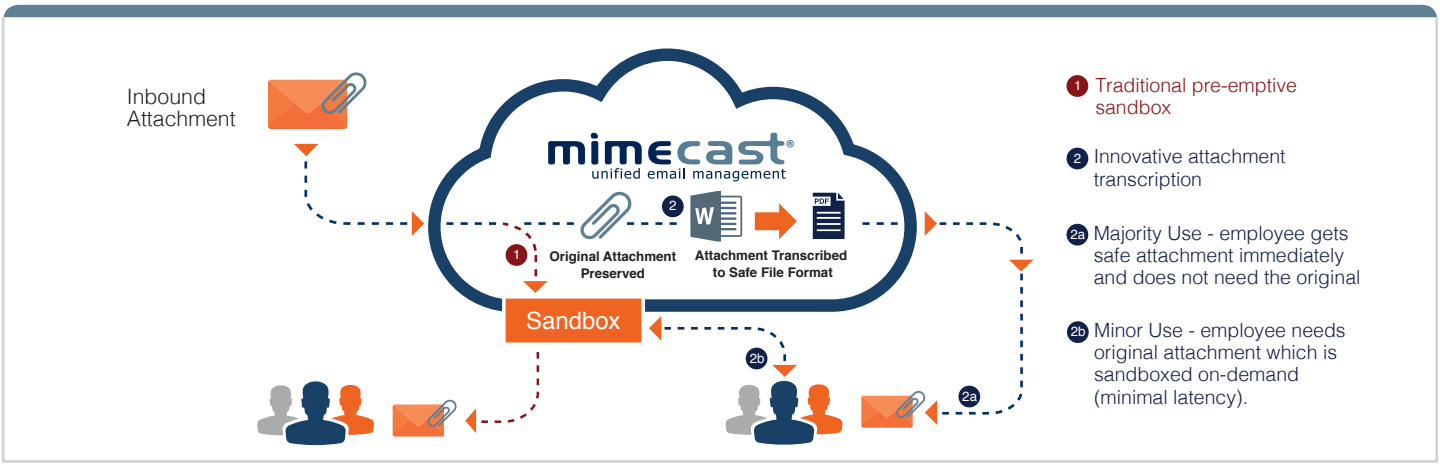
Mimecast Targeted Threat Protection, with Attachment Protect delivers end-to-end protection against spear-phishing and targeted email attacks. It extends URL-based attack defences through URL rewriting provided by Mimecast URL Protect, to include comprehensive protection against zero-hour weaponized attachments.

How it works

- Choose from traditional pre-emptive sandboxing of attachments or an innovative attachment transcription and on-demand sandbox alternative - or a combination for different groups of employees.
- On-demand sandboxing removes attachments that could potentially contain malicious code (e.g. PDF or Microsoft Office files) from inbound emails and replaces them with transcribed, safe versions – neutralizing any malicious code.
- Employees have instant access to these safe attachments.
- If they require read / write access, a link in the email can be used to request the original file via a leading, cloud based sandbox.

KEY FEATURES:

- Multi-layered zero-hour attachment protection – conversion to a safe format plus sandboxing
- Safe attachments are delivered without traditional sandboxing latency, helping maintain employee productivity
- The sandbox is only deployed if an editable version of the attachment is requested
- A pre-emptive sandbox, without initial attachment transcription, is also available
- Granular reporting allows for end-to-end, real-time threat analysis
- Protection on and off the corporate network, including mobile devices
- Protect against impersonation attacks, often called CEO fraud or Whaling with an additional service included with URL Protect or Attachment Protect



Multi-layered protection

As malware-laden attachments increase, sandboxing has become a critical defense in the war on spear-phishing and zero-hour advanced persistent threats. However, an arms race between sandbox vendors and malware authors has seen a growing number of attacks successfully penetrating traditional sandboxes to infect their targets.

With Mimecast Targeted Threat Protection - Attachment Protect, organizations can pre-emptively sandbox attachments before they are delivered to employees. This traditional approach helps defend against weaponized attachments, but introduces some delay to email delivery.

Attachment Protect also offers an innovative alternative that ensures safe attachments are delivered to employees without delay by combining attachment conversion, or transcription, with on-demand sandboxing to provide comprehensive, multi-layered protection. Transcribing vulnerable attachments to a safe format as they pass through the email gateway delivers a critical first line of defense against exploits.

In many cases, employees only ever need to view attachments rather than edit them. In fact approximately 51% of attachments are read-only PDF files to start with, followed by 17% Word, 9% Excel and 3% Powerpoint.[1]

Selectively sandboxing attachments on-demand, adds a second layer of defense for when the original, editable document is needed.

Combining transcription with on-demand sandboxing allows administrators to choose the best mix of safety, performance and functionality for their organization.

Flexible deployment

Mimecast allows organizations to select the most appropriate level of protection for different groups of employees.

They can optimize email delivery performance without impacting security by configuring attachment transcription with on-demand sandboxing for the majority of employees. They get instant access to safe attachments, while still being able to request the original if required.

Alternatively, defined groups of employees can be enabled with pre-emptive sandboxing, meaning attachments pass through the sandbox before being delivered to employees – if deemed safe.

For comprehensive zero-hour threat protection, combine Mimecast Targeted Threat Protection – Attachment Protect, with our URL Protect service.

Additional protection from malware-less threats

Not all email based attacks use malicious URLs or weaponized attachments, and are increasingly sophisticated and convincing in their efforts to use social engineering tactics against users. Whaling attacks, Business Email Compromise or CEO fraud as they are sometimes known do exactly this. They trick key users, often in the finance team, into making wire transfers or other financial transactions to cyber-criminals by pretending to be the CEO or CFO in a spoofed email.

Targeted Threat Protection includes a capability that provides dedicated protection against these types of attack. Impersonation Protect can be configured to ensure your end users are not affected by whaling style attacks.

Impersonation Protect identifies combinations of key variables in an email to determine if the content is likely to be suspicious, even in the absence of a URL or attachment. Administrators can bounce, quarantine or visually mark the email if it is determined likely to be fraudulent.

For comprehensive advanced attack protection, combine Impersonation Protect with Target Threat Protection's URL Protect and Attachment Protect services.

1.Source: Analysis of 1 terabyte of Mimecast platform data, 2015