Data Sheet

mimecast

Mimecast Targeted Threat Protection

Proven Defense Against Advanced Email-Borne Attacks

Mimecast Targeted Threat Protection safeguards your organization and employees against sophisticated email-borne attacks. It helps defend against attackers trying to steal data or credentials, plant ransomware, trick employees into transferring money, and springboard to attack supply chains. These kinds of threats require advanced security measures over and above those provided by traditional email security systems.

How It Works:

- Emails pass through the Mimecast gateway and are scanned for the presence of URLs, attachments, key words/phrases, and other indicators of an attack.
- URLs are re-written and checked pre-click and on every click.
- Attachments are analyzed using a combination of static file analysis and fullsystem emulation sandboxing. Files can be converted to a safe format and delivered instantly.
- Emails are scanned for multiple indicators of compromise to protect against impersonation attacks.
- Mimecast's Threat Intelligence Dashboard provides actionable intelligence to aid incident investigation and reduce mean time to respond.

Key Benefits

- 100% cloud based provides low total cost ownership.
- Protection from ransomware, phishing, malicious URLs and attachments.
- Comprehensive protection against social engineering and impersonation.
- Remediation of newly identified threats, including emails previously delivered.
- Helps to improve users' security awareness.
- Maintain employee productivity with little to no latency.
- Granular logging and reporting to see who's being attacked, with what, and how often.
- Easily benchmark your organization's cybersecurity posture against your peers' using data available through Threat Feed, Mimecast's threat intelligence API.

Mimecast URL Protect

Mimecast Attachment Protect

Mimecast Impersonation Protect

URL Protect

URL Protect rewrites all links in inbound emails and scans the destination website at time of click to block access to malicious websites and protect from delayed exploits.

By leveraging global block lists and performing advanced heuristic analysis, malicious sites are blocked whether they are well-known or newly compromised. Also included is protection from typo-squatted domains and inspection across various non-western character sets to detect domain similarities.

Administrators can block, warn, or allow employee access to websites. Real-time logging, auditing and reporting, including a dedicated dashboard, enables administrators to monitor and track phishing attacks.

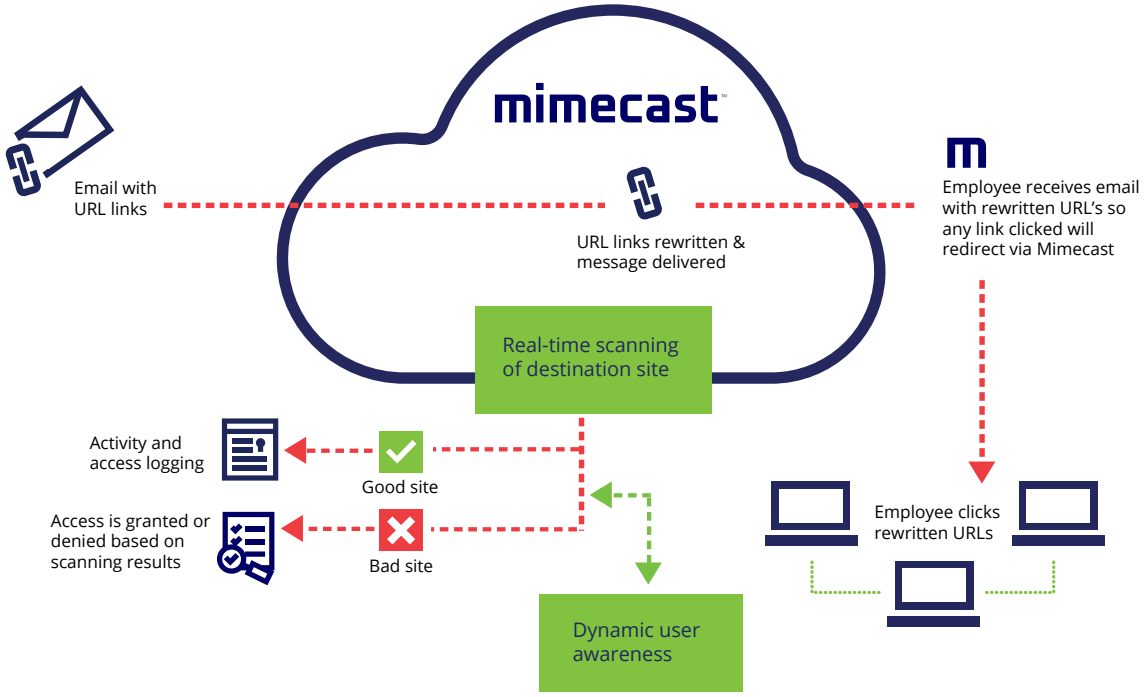
Links attempting to directly download dangerous files are automatically blocked. When URL Protect is used in conjunction with Attachment Protect, links directly downloading Office Documents and PDFs are subject to static and behavioural analysis.

Built-in dynamic user awareness training helps develop greater visibility and vigilance of the risks of spear-phishing and targeted attacks. Administrators can define the frequency of these security awareness prompts, or they can be dynamically adjusted depending on users' demonstrated security cautiousness.

Extend the protection offered by URL Protect with the Mimecast Browser Isolation service. It accesses websites using remote browsers on secure servers in the Mimecast cloud and streams only safe video to the user.

Key Capabilities

- Real-time, on-click, website scanning protects against malicious websites including delayed exploits.
- When used with Internal Email Protect, malicious URLs in inbound and outbound emails are detected and blocked.
- Administrator controlled list of Custom Monitored Domains to protect from attackers using typo-squatted domains.
- URLs within attachments are scanned at the Mimecast Gateway. Attachments containing malicious URLs are stripped from inbound emails.
- Multi-layered protection using Mimecast and third-party detection technologies.
- Protection on and off the corporate network, including mobile devices – no client software or impact on users.
- Dynamic awareness training helps develop increased employee caution and threat awareness.
- Simple, central administration and control for holistic policy management, monitoring, and reporting.



Attachment Protect

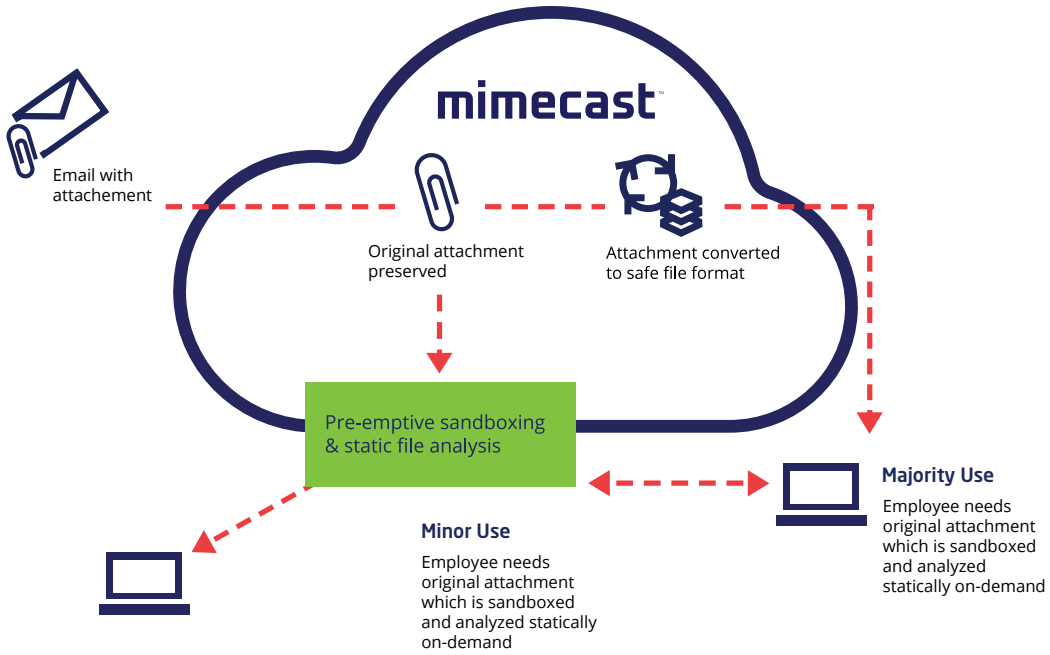
Attachment Protect delivers multi-layered protection against malicious attachments.

As attackers have continued to adapt their malware to be self-aware and recognize when it is being analyzed by traditional, virtualized sandboxing, it's become important to inspect attachments using multiple techniques. Static file analysis breaks the attachment down to spot malicious activity at the code level, probing deeper than traditional sandboxing can and eliminating latency that can result from sandboxing. Attachment Protect delivers the optimum combination of speed and detection of sophisticated, evasive malware.

The option to convert all inbound files to a safe format means 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 on-demand at which time static file analysis and sandboxing are undertaken.

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

Additionally, information about malicious files identified in your tenant by Attachment Protect is incorporated into Mimecast's Threat Intelligence Dashboard.* The Dashboard offers easily consumable, contextual and actionable insight into the malicious activity targeting your organization. Through the Dashboard, you can see which users are most at-risk, malware origin by geo-location, and recently observed Indicators of Compromise (IoCs). You will also have the ability to search for specific files or messages if needed.



Key Capabilities

- Inspection of attachments sent within the organization when used with Internal Email Protect, including remediation of undesirable, or malicious content.
- Multi-layered malicious attachment protection, including static file analysis, conversion to a safe format, and sandboxing.
- Pre-emptive sandboxing with static file analysis pre-filter can be selected by administrators and for selected senders defined by end users.
- Safe attachments are delivered without traditional sandboxing latency, helping maintain employee productivity and security.
- Granular reporting allows for real-time threat analysis.
- When used in conjunction with URL Protect, links which lead directly to file downloads are analyzed before delivery.
- Protection on and off the corporate network, including mobile devices.
- A Threat Intelligence Dashboard that provides deep insight into the malware targeting your organization.

**Threat Dashboard and Threat Intel APIs are included as standard features only for customers with the Secure Email Gateway (SEG). They are designed to consolidate information about malicious attachments detected at both the anti-virus and the Targeted Threat Protection-Attachment Protect (TTP-AP) layer of protection. Mimecast recommends as a best practice that all customers upgrade to a service that includes SEG and TTP-AP. Please contact your Mimecast representative or partner for more details on these features or to discuss an upgrade if necessary.*

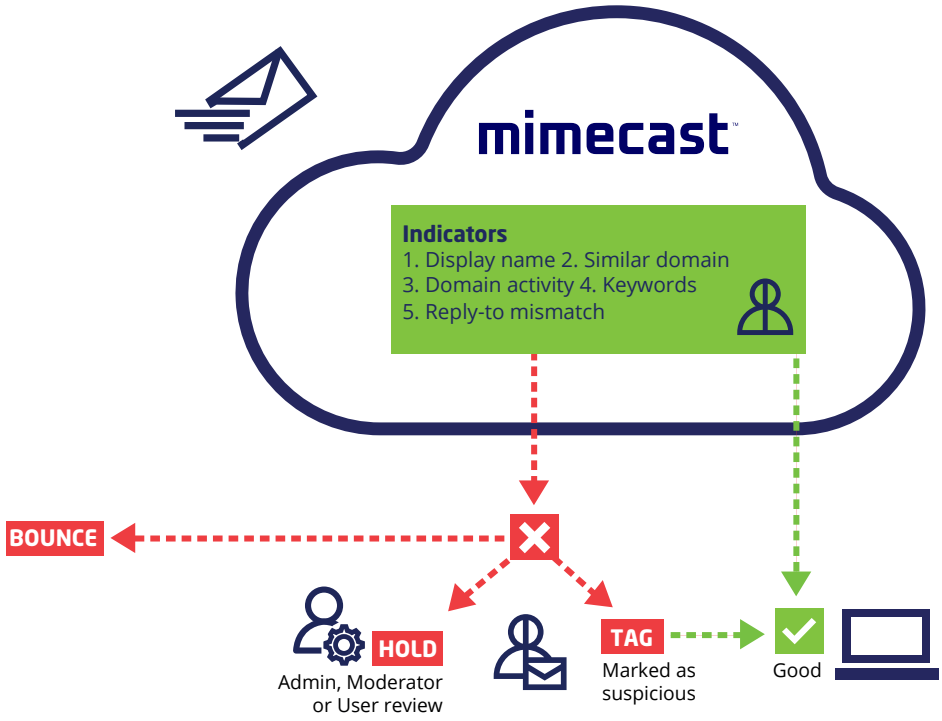
Impersonation Protect

Impersonation Protect delivers comprehensive protection against social engineering-based attacks. Often called CEO fraud, impersonation, whaling or business email compromise, these attacks are designed to evade traditional gateway checks and trick users into handing over money, company secrets, or sensitive employee information. Attackers will pose as C-level execs, supply chain partners or well-known internet brands in an attempt to exploit the relationship or trust of internal employees.

Impersonation Protect detects and prevents these types of attacks by identifying combinations of key indicators in an email to determine if the content is suspicious, even in the absence of a malicious URL or attachment.

These indicators include:

- Display name – is the attacker trying to spoof an internal sender.
- Reply-to mismatch – senders trying to hide their true sending email address.
- Domain name similarities (including homoglyph/ homograph) – attempts to use a similar domain to the target, a popular internet domain, or supply chain partner domain.
- Newly observed domains – these are more likely to be malicious.
- Key phrases e.g. “wire transfer”, or “W-2” – a Mimecast managed and customizable threat dictionary of common terms used in these types of attacks.



Key Capabilities

- Real-time protection against malware-less social engineering attacks.
- Ensures end users are protected by blocking, quarantining or visibly marking suspicious emails.
- Protects against newly observed and newly registered domains used in an attack.
- Scans for popular internet domain brand impersonation – Mimecast managed list and customer customizable for organizations they work with to monitor for typo-squatting abuse.
- A Targeted Threat Dictionary managed by Mimecast – customers can add custom terms.
- Backed by comprehensive protection from Mimecast’s threat intelligence infrastructure and the Mimecast Security Operations Center.