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 that require advanced security measures over and above that 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 compromise.
- URLs are re-written and checked pre-click and on every click.
- Attachments are analyzed using a combination of static file analysis and full-system 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.
- Internal and outbound mail are inspected to block URL or attachment-based threats; DLP checks prevent sensitive information leakage.
- Malicious content is removed from mailboxes through automated or manual remediation.
- Files are constantly rechecked and removed if the latest intelligence and analysis deems them malicious.

Key Benefits:

- Full integration with Mimecast email gateway and broader cyber resilience.
- 100% cloud based.
- Inspection of inbound, outbound, and internal emails to ensure protection from every angle.
- 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.

Mimecast URL Protect

Mimecast Attachment Protect

Mimecast Impersonation Protect

Mimecast Internal Email Protect

URL Protect

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

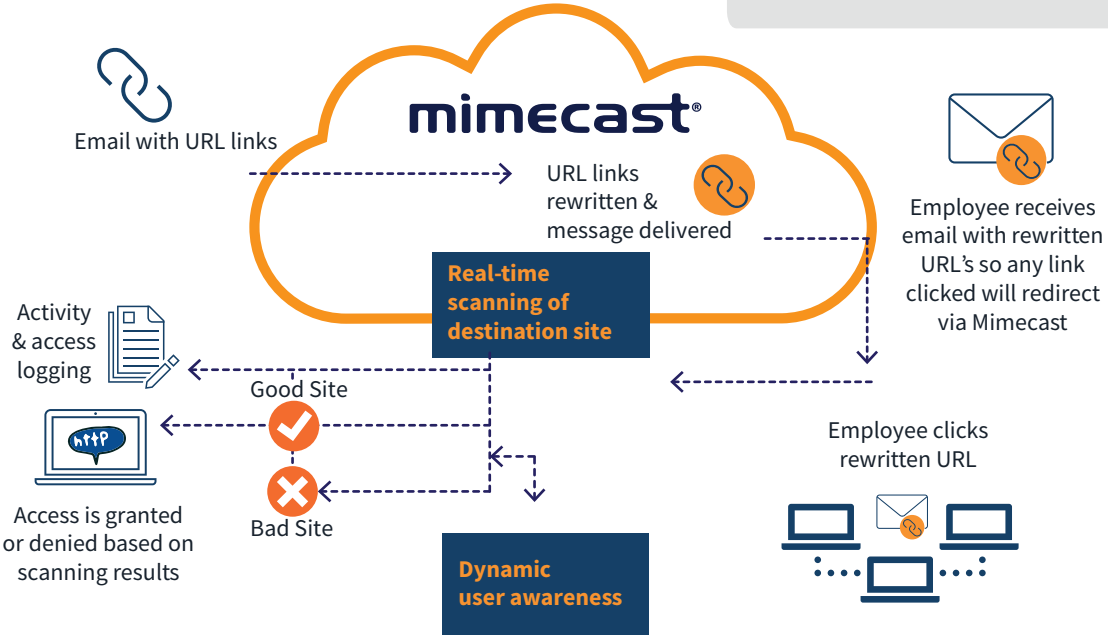
Administrators can block, warn, or allow employee access to websites. Real-time logging, auditing and reporting, including a dedicated dashboard, enables administrators to monitor and track phishing attacks.

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

Built-in Dynamic User Awareness 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.

Key Capabilities:

- Real-time, on-click, website scanning protects against malicious websites including delayed exploits.
- Malicious URLs in inbound and outbound mail are detected and blocked when used with Internal Email Protect.
- Administrator controlled list of Custom Monitored Domains to prevent attackers from typo-squatting domains they work with.
- 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 techniques alongside the Messaging Security team.
- Protection on and off the corporate network, including mobile devices – no client software or impact on users.
- Dynamic user awareness 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 sent to your organization.

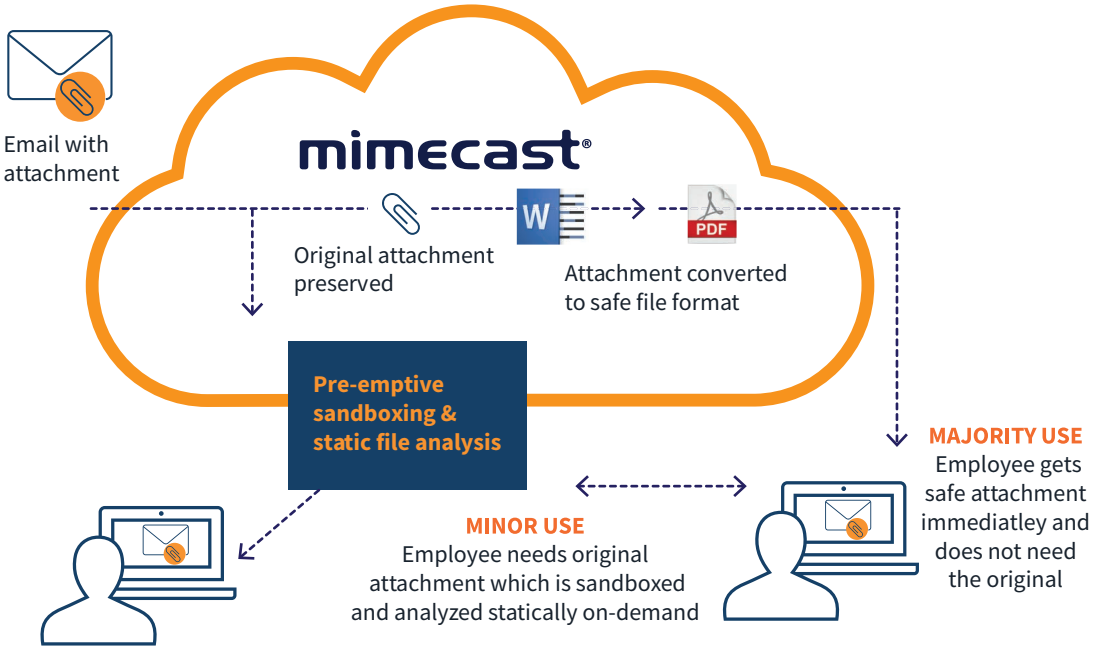
As attackers have continued to adapt their malware to be self-aware and recognize when it is being analyzed by traditional, virtualized sandboxing, it's become important to inspect attachments using multiple techniques. Static file analysis breaks the attachment down to spot malicious activity at the 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 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.

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.



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.

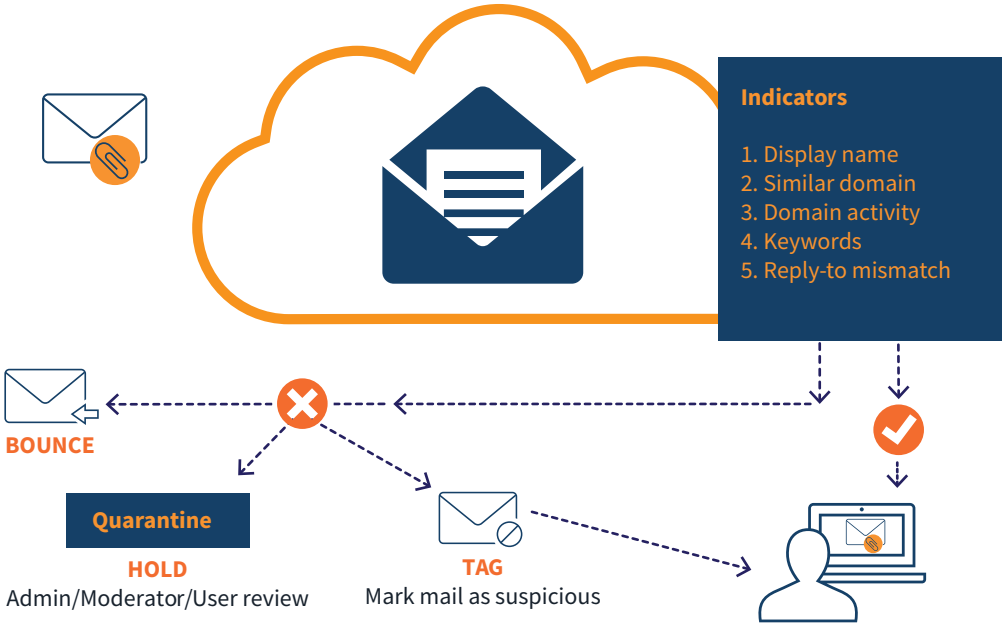
Impersonation Protect detects and prevents these types of attacks by identifying combinations of key indicators in an email to determine if the content is suspicious, even in the absence of a malicious URL or attachment.

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.



Internal Email Protect

Internal Email Protect applies best-practice security inspections to internal and outbound email, which accounts for 60% of all email traffic[i]. It allows organizations to monitor, detect, and remediate security threats that originate from within their email systems.

Such protection is critical as a recent Mimecast survey found that 80% of companies had experienced threats caused by compromised user email accounts. Careless and malicious employees are also a significant risk. 61% had malicious activity spread from one infected user to other employees via email.[ii]

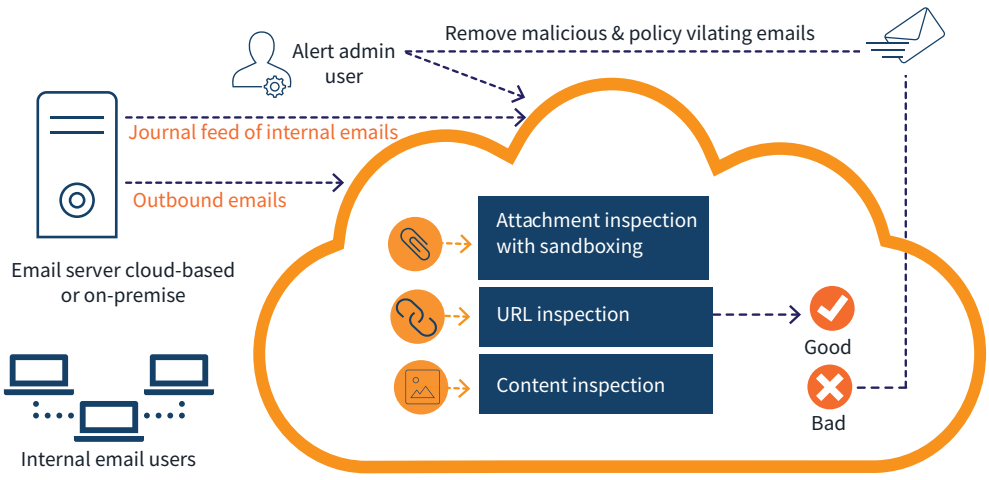
Internal Email Protect stops the spread of malware and sensitive information internally and outbound by inspecting mail for malicious attachments and URLs as well as violations of data loss prevention policies.

In addition to full integration with URL Protect and Attachment Protect, Internal Email Protect offers:

- Journaling of internal email for the inspection of threats – monitors internal and outbound email, conducts data loss prevention inspections of the content, and scans attachments and URLs.
- Content remediation – allows for automatic or manual removal of malicious content from mailboxes. Rechecks content against latest intelligence to remove newly identified malware.
- Threat Remediation Dashboard – provides detailed threat insights and trends, and allows search based on message ID and attachment file hash, as well as from and/or to address.

Key Capabilities:

- Provides comprehensive protection from threats originating internally – resulting from compromised, careless or malicious users.
- Reduces the risk of a breach or damaging security incident spreading throughout the organization.
- Identifies and prevents threats or sensitive data from leaving an organization – protecting reputation and exposure of information.
- Automates the detection and removal of internal emails that are determined to contain threats or sensitive information.
- Continuously rechecks delivered files to identify and remediate previously unidentified malware.
- Supports automatic or manual remediation of emails.
- Provides a Threat Remediation Dashboard that allows for search and remediation based on admin and/or organizational requirements.



i. Based on aggregated data from Mimecast Internal Email Protect customers. I ii. 2018 State of Email Security report