DATASHEET

Mimecast Offshore Targeted Threat Protection

URL Protect

Instant and comprehensive protection from spear-phishing and targeted email attacks

Mimecast® Targeted Threat Protection, with URL Protect is an advanced email security technology that protects email users from spear-phishing and targeted attacks in email, extending our existing Secure Email Gateway anti-spam and anti-virus services.

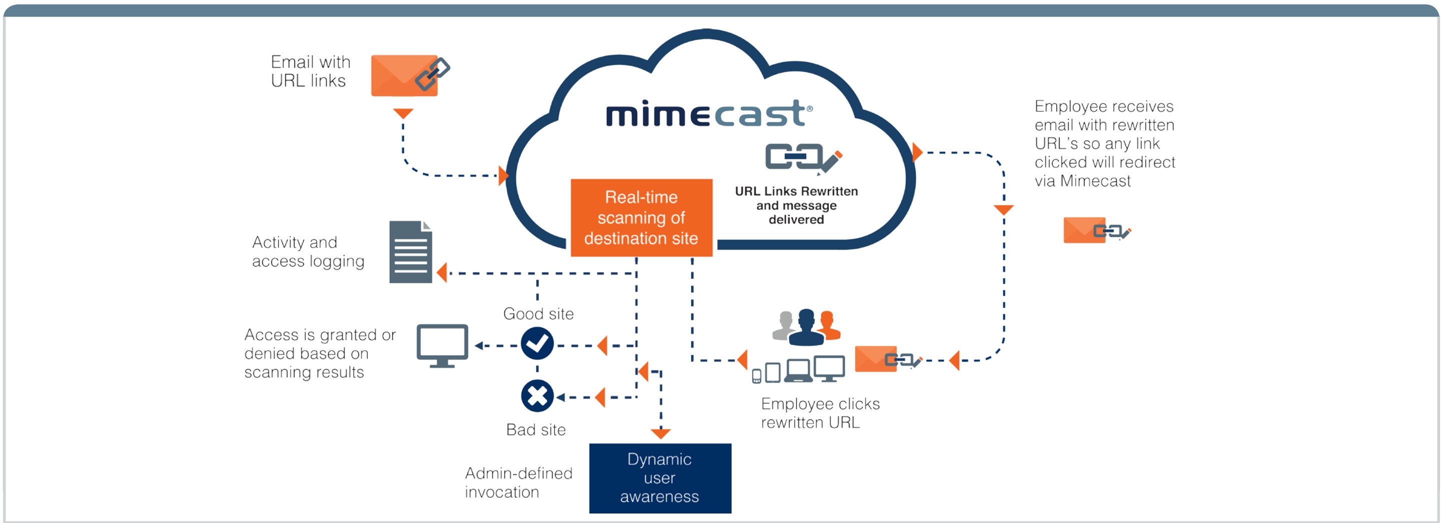
Targeted Threat Protection – URL Protect rewrites all links in all inbound emails, then scans the destination website in real-time when clicked by the user to help ensure phishing and spear-phishing websites are blocked, regardless of the client or device used to access email. Before the user is given access to the URL, domain security checks are performed on the destination, validation and assessment of the URL is also undertaken, making use of both real-time and cached feeds and also employing advanced heuristic analysis. Lastly, Mimecast uses global allow/block lists based on our own threat intelligence. In short Mimecast performs URL sandboxing for each and every click before redirecting the user to the requested site. It can be deployed alongside Mimecast Attachment Protect which adds protection against malicious attachments.

How it works

- As email passes through the Mimecast Secure Email Gateway, URL Protect rewrites all URLs in every email – removing any uncertainty about whether or not users are protected.
- On a click, these rewritten links point back to Mimecast's threat intelligence infrastructure which scans the site before delivering the page to determine if the destination website is likely malicious.
- Employees are permitted access to clean sites without delay, while access to malicious sites is blocked.
- Administrator enabled dynamic user awareness helps drive a mentality of user caution.

KEY FEATURES:

- Real-time, on-click, website scanning protects against good websites turning bad, or delayed exploits
- Comprehensive protection with Mimecast's threat intelligence infrastructure and Messaging Security teams
- 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
- Rapid deployment - no software, hardware or added IT overhead
- Simple, central administration and control for easy, holistic policy management, monitoring and reporting


Email with URL links
mimecast®
URL Links Rewritten and message delivered
Real-time scanning of destination site
Employee receives email with rewritten URL's so any link clicked will redirect via Mimecast
Activity and access logging
Good site
Access is granted or denied based on scanning results
Bad site
Employee clicks rewritten URL
Admin-defined invocation
Dynamic user awareness

Every URL, every click, every device

Mimecast URL Protect rewrites all URLs in all inbound emails, meaning users are protected on every device and client; whether they use Microsoft Outlook or any other email software, their corporate smartphone or their own BYOD device or personal computer. Mimecast URL Protect provides comprehensive protection across all devices and inboxes, removing the need to deploy additional protection for mobile or BYOD devices. Protection even extends to URLs within emails that have been retained within the Mimecast Archive, helping to ensure employees do not fall victim to older exploits.

Administrator control

Administrative control is maintained through the Mimecast Administration Console, with policies integrated into the wider security policy framework. Administrators can specifically block, warn or allow employee access to websites.

Real-time logging, auditing and reporting is maintained in the Mimecast Administration Console, which allows administrators to monitor and track phishing attacks. The URL Protect dashboard shows real time hits against positive phishing websites that users have been directed to through their emails, and where Mimecast has protected them from compromise, while administrative notifications keep your IT team firmly in control.

Dynamic user awareness

Administrators can enable an automated user awareness capability to help make users more aware of the risks of spear-phishing and targeted attacks - driving increased caution. Administrators can define the minimum frequency these security awareness prompts appear, helping ensure employee productivity is not impacted. The frequency of prompts is also dynamically adjusted depending on user security vigilance. For example, repeat offenders that click bad links will get more frequent prompts until their behavior changes. The IT team can track employee behavior from the Mimecast administration console and target additional security training as required. Mimecast URL Protect with user awareness helps users understand their role as your 'human firewall' and enhances their ability to spot dangerous emails and potentially suspicious URLs.

For comprehensive threat protection, combine Mimecast Targeted Threat Protection – URL Protect, with our Attachment and Impersonation Protect services.

Additional protection from malware-less threats

Not all email based attacks use malicious URLs or malware 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.

Mimecast's security, archiving and continuity cloud services make business email safer. Mimecast protects the email of millions of users worldwide.