mimecast®

DATASHEET

Mimecast Targeted Threat Protection

Impersonation Protect

Instant and comprehensive protection from the latest malware-less social engineering -based email attacks, often called CEO fraud, impersonation, whaling or business email compromise.

Not all email based attacks use malicious URLs or attachment . Business email compromise attacks are designed to trick key users, often in finance, into making wire transfers or other financial transactions to cyber-criminals by pretending to be the CEO or CFO. Some also target those responsible for sensitive employee data, for example payroll information, which could be used for identity theft.

Targeted Threat Protection with Impersonation Protect detects and prevents these types of attack. Impersonation Protect identifies combinations of key indicators in an email to determine if the content is likely to be suspicious, even in the absence of a malicious URL or attachment.

How it works

- As email passes through the Mimecast Secure Email Gateway, Impersonation Protect examines several key aspects of the message.
- Impersonation Protect examines the email's display name, domain name, domain age, reply-to information and the body of the message to determine if the email could be an impersonation attack.
- If the email fails a combination of these tests, administrators can configure Impersonation Protect to discard the message.
- Or alternatively quarantine or notify end users that the email is suspicious.

KEY FEATURES:

- Real-time protection against malware-less social engineering attacks like whaling, CEO fraud, business email compromise, impersonation or W-2 fraud.
- Protects against newly observed domain names used as part of the attack.
- Protects against display name spoofing and reply-to address mismatches.
- Ensures end users are protected at all times by visibly marking suspicious emails.
- Backed by comprehensive protection from Mimecast's threat intelligence infrastructure and Messaging Security teams.
- Complete administrative control over handling of emails; quarantine, discard or mark emails depending on your security posture.
- Works alongside URL Protect, Attachment Protect, and Internal Email Protect to provide comprehensive protection against the latest attack methods.

Protect employees from the new breed of email cyberattack.

According to the U.S. Federal Bureau of Investigation (FBI), whaling email scams alone were up 270 percent from January to August 2015. The FBI also reported business losses due to whaling of more than $1.2 billion in little over two years, and a further $800 million in the six months since August 2015. Cybercriminals are becoming ever more inventive and creative when it comes to compromising organizations.

The attacks seek to fraudulently trick employees into making wire transfers, or other sensitive data transfers, to the cybercriminals as a way of generating income for organized crime.

With Mimecast Targeted Threat Protection with Impersonation Protect organizations can protect their employees and financial assets from this type of fraud.

Impersonation Protect provides instant and comprehensive protection against this latest type of email-borne cyberattack which are often malware-less and based heavily on social engineering, thereby able to pass through traditional gateway checks.

Key indicators of threat

Impersonation Protect examines a number of indicators in an email, such as:

- Display name analysis to determine if the attacker is trying to spoof an internal email address.
- Reply-to mismatch to determine if the sender is trying to hide their true sending email address.
- The sending domain name; to detect how near a match to your existing corporate domain name the sender's domain is.
- The age of the sending domain name; newly observed domain names are more likely to be malicious in this scenario.
- Keywords in the message body; attackers will use phrases like 'wire transfer', 'bank transfer' or 'W-2' in this type of attack.

Impersonation Protect blocks, bounces or tags the email as suspicious ensuring employees are not tricked into making fraudulent wire-transfers or giving out sensitive data

Additional protection from malicious URLs and weaponized attachments

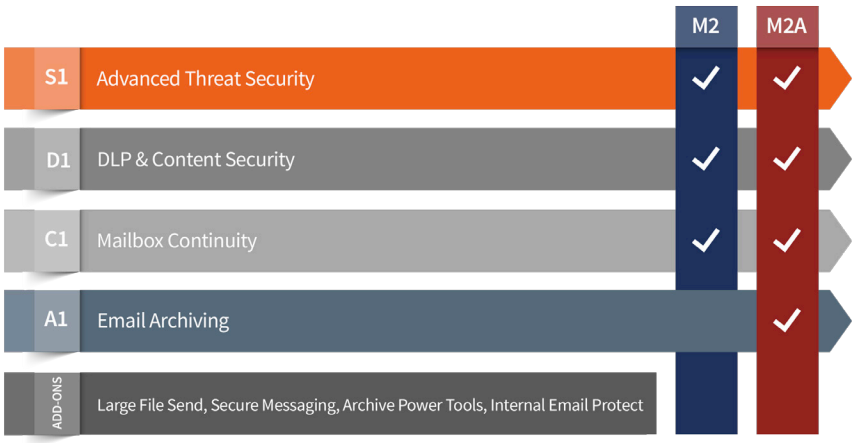
Impersonation Protect works with URL Protect, Attachment Protect, Internal Email Protect for comprehensive protection against advanced email-borne threats.

Make Email Safer for Business

Mimecast integrated service bundles deliver the ultimate in cyber security, resiliency and archiving. Get comprehensive risk management or address specific requirements - all in a single platform.

LEARN MORE

mimecast.com/products/email-management-bundles/



mimecast® Partner

Innovative Computing Systems

Innovative Computing Systems has primarily focused on the technology needs of law firms since 1989, and those skill sets have been sought out by entities such as municipalities, corporate environments and professional services organizations. Innovative Computing Systems selects only premier technology partners to provide solutions to its clients and is committed to maintaining long-term strategic relationships. Learn more at www.innovativecomp.com.

www.innovativecomp.com **sales@innovativecomp.com** **1.800.541.045**
www.facebook.com/ICSgetsIT/ **twitter.com/ICSGetsIT**