



Mimecast launches AI-enabled solution designed to help organizations protect against the most evasive and hard-to-detect email threats

July 14, 2021

The Mimecast CyberGraph™ solution uses AI to help improve detection and reduce risk

LEXINGTON, Mass., July 14, 2021 (GLOBE NEWSWIRE) -- [Mimecast Limited](#) (NASDAQ: MIME), a leading email security and cyber resilience company, today announced the Mimecast CyberGraph™ solution, a new add-on for Mimecast Secure Email Gateway (SEG) that is engineered to use Artificial Intelligence (AI) to help detect sophisticated phishing and impersonation attacks. CyberGraph creates an identity graph which is built to store information about relationships between all senders and recipients. The graph is designed to detect anomalies and leverages machine learning technology to help organizations stay one step ahead of threat actors by alerting employees to potential cyber threats.

"Phishing and impersonation attacks are getting more sophisticated, personalized and harder to stop. If not prevented, these attacks can have devastating results for an enterprise organization," said Josh Douglas, VP, Product Management for Threat Intelligence at Mimecast. "Security controls need to be constantly updated and improved to outsmart threat actors. CyberGraph leverages our AI and machine learning technologies to help keep employees one step ahead with real-time warnings, directly at the point of risk. What makes this exciting is that we are embedding the technology for existing email security customers, they do not need to look for other vendors to fill the gap with technologies that only work to solve part of this challenge."

The workplace is always the top target of cybercriminals, but in the remote working era, the problem has intensified. "[The State of Email Security Report](#)" found that email threats rose by 64% and employees are clicking on three times as many malicious emails as they had before the COVID-19 pandemic. Security controls need to evolve to help evade cybercriminals' relentless and crafty approach. CyberGraph includes three key capabilities engineered to help prevent cyber threats:

- **Renders embedded trackers useless** – During the reconnaissance phase of an attack, threat actors embed trackers into emails that communicate with an illegitimate remote server, disclosing important information that can be used to create a targeted social engineering attack. CyberGraph is built to block this communication, mask the email recipient's location, and prevents attempts to understand engagement levels with the email content.
- **Uses machine learning to protect from targeted email threats** – CyberGraph is designed to create an identity graph by learning about relationships and connections between all senders and recipients. This intelligence is combined with the outputs from machine learning models to detect anomalies that could be indicative of a malicious email.
- **Engages users with contextual, dynamic warning banners** – CyberGraph is engineered to engage users at the point of risk with color-coded banners that indicate the potential nature of a threat. Users are empowered by seeing whether an email is safe or potentially nefarious. CyberGraph is built to "crowd-source" threat intelligence, which helps to reinforce the machine learning model. As the risk associated with any given delivered email changes, banners embedded in any similar emails are updated with the latest information, providing ongoing engagement and protection for users.

Availability

CyberGraph for Mimecast SEG is available now in the US and the UK, with more regions to follow.

Mimecast: Relentless protection. Resilient world.™

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world. Learn more about us at www.mimecast.com.

Mimecast Social Media Resources

LinkedIn: [Mimecast](#)

Facebook: [Mimecast](#)

Twitter: [@Mimecast](#)

Blog: [Cyber Resilience Insights](#)

Press Contact

Tim Hamilton

Press@Mimecast.com

603-918-6757

Investor Contact

Robert Sanders

Investors@Mimecast.com

Mimecast and Cybergraph are either registered trademarks or trademarks of Mimecast Services Limited in the United States and/or other countries. All other products and/or services referenced are trademarks of their respective companies.

Safe Harbor for Forward-Looking Statements

Statements in this press release regarding management's future expectations, beliefs, intentions, goals, strategies, plans or prospects, including, without limitation, the statements relating to the effectiveness of the features and functionality in Mimecast Cybergraph™ technology, the future financial impact of the new features and functionality in Mimecast Cybergraph technology, and the overall impact of the Cybergraph technology on Mimecast's business and operations, may constitute forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995 and other federal securities laws. All statements, other than statements of historical fact, are statements that could be deemed forward-looking statements, including statements containing the words "predicts," "plan," "expects," "anticipates," "believes," "goal," "target," "estimate," "potential," "may," "might," "could," "see," "seek," "forecast," and similar words. Mimecast intends all such forward-looking statements to be covered by the safe harbor provisions for forward-looking statements contained in Section 21E of the Exchange Act and the Private Securities Litigation Reform Act of 1995. Such forward-looking statements involve known and unknown risks, uncertainties and other factors including those risks, uncertainties and factors detailed in Mimecast's filings with the Securities and Exchange Commission. As a result of such risks, uncertainties and factors, Mimecast's actual results may differ materially from any future results, performance or achievements discussed in or implied by the forward-looking statements contained herein. Mimecast is providing the information in this press release as of this date and assumes no obligations to update the information included in this press release or revise any forward-looking statements, whether as a result of new information, future events or otherwise.