Mimecast CEO Unveils Vision for Future of Email Security at Cyber Resilience Summit in Dallas

October 29, 2019

Organizations Need to Expand From Perimeter Email Security to Pervasive Email Security to be Resilient in the New Digital Risk Reality

DALLAS, Oct. 29, 2019 (GLOBE NEWSWIRE) -- **Cyber Resilience Summit -** Mimecast Limited (NASDAQ: MIME), a leading email and data security company, announced its CEO, Peter Bauer has outlined Mimecast's vision of the future of email security at the North American Cyber Resilience Summit in Dallas, Texas. Today organizations are required to think bigger and create proactive cyber resilience postures that address the threats at the email perimeter, inside the email network, and also beyond their purview, to eliminate the threats that abuse the trust in their brands out in the wild. Organizations must also leverage the vast telemetry and threat intelligence that can be gathered at the attack surface of their email systems to make their teams and their other security investments smarter and more effective -- this what Bauer referred to as advancing from perimeter email security to pervasive email security.

Bauer further explained that the future of email security is comprised of three distinct zones, alongside an API-led approach, that organizations need to recognize:

Zone 1 – Perimeter
The email security perimeter is focused on keeping users and data safe by protecting email against spam and viruses, malware and impersonation attempts, and data leaks. Organizations need global visibility that offers rapid detection of sophisticated threats to protect their entire customer, partner and vendor ecosystem.

Zone 2 – Inside the Perimeter
Compromised users whose accounts are being taken advantage of, lateral movement using credential harvesting links, social engineering and employee errors are threats and risks that manifest inside the perimeter. Organizations should combine security inspections of internal and outbound email traffic with capabilities to build a stronger human firewall through dynamic user awareness training and testing programs. They also need rapid remediation capabilities to extract threats and shut down access to compromised accounts. This will help to ensure that an organization's internal network, made up of people and machines, is robust and capable of defending itself when attacks occur.

Zone 3 – Beyond the Email Perimeter – Pervasiveness
Organizations need the ability to protect their brands and domains from being explicitly spoofed or hijacked to defraud customers and partners. This requires the ability to implement DMARC efficiently as well as to hunt for and take action against threats where attackers present themselves fraudulently to an organization's customers or partners using deception and impersonation.

Beyond the Zones: API-driven Security Ecosystem Integration
To move from perimeter to pervasive email security requires an extensible architecture that allows organizations to fully integrate the value of the telemetry and intelligence gathered through observing email attacks with their existing technologies such as SOARs, SIEMs, endpoints, firewalls and broader threat intelligence platforms. An API-driven approach further helps deliver pervasive security throughout all zones. This allows organizations to make their teams and other security investments even more effective.

"The expanded attack surface, the proliferation of security vendors and the monetization of attacks have all increased the complexity of an organization's security infrastructure. When you consider the cyber security skills gap that most organizations face today, the threat of business disruption due to a cyber incident is certainly on the rise," said Peter Bauer, chief executive officer at Mimecast.

"Addressing complexity is as much of a priority as increasing security. Adding new solutions to your security stack to help thwart new attacks may be counter-intuitive if those solutions don't connect with each other. There's power in platform-based solutions that can give organizations the visibility they need to help reduce risk and build a stronger proactive cyber resilience posture," added Bauer.

In addition, Mimecast also announced it has engaged in strategic partnerships with DMARC Analyzer and Segasec to offer brand protection against threats outside the perimeter. Combining Mimecast defenses with DMARC Analyzer's reporting and email validation solution, helps customers stop impersonation attacks faster with self-service email channel analysis and DMARC Reporting. The strategic partnership with Segasec means customers can help protect their brands from fraudulent impersonators in the wild and neutralize attacks before they are released.

These new technology partnerships in combination with Mimecast's Cyber Resilience platform offers organizations full end-to-end detection and take down capabilities when a malicious actor conducts impersonation activities against an organization. Additionally, customers benefit from integrated, unparalleled visibility into inbound threats as well as those that exist beyond their visibility, helping to restore trust.

Mimecast is either a registered trademark or trademark of Mimecast Services Limited in the United States and/or other countries. All other products or services referenced are trademarks of their respective companies. The use of the word partner does not imply a partnership relationship between Mimecast and any other company.

About Mimecast:
Mimecast is a cybersecurity and compliance provider that helps thousands of organizations worldwide make email safer, restore trust and strengthen cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, compliance risk, human error and technical failure. www.mimecast.com

Mimecast Social Media Resources

LinkedIn: Mimecast
Facebook: Mimecast
Twitter: @Mimecast
Blog: Cyber Resilience Insights

Press Contact
Alison Raymond Walsh
Press@Mimecast.com
617-393-7126

Investor Contact
Robert Sanders
Investors@Mimecast.com
617-393-7074

mimecast®

Source: Mimecast Limited