Solution Brief

# Email Security and Automated SecOps Thwarting Phishing Attacks Faster

### Key Benefits

- Detect and stop lateral movement threats through full visibility of detection and automated response
- Multi layer Defense In Depth unifies prevention, detection, and response across email, endpoint, identity and cloud
- Immediate Visibility and Context through visualization at every stage of the kill-chain
- Improve Security Analyst Efficiency by leveraging a single user experience dashboard view
- Enrich Threat Detection from Mimecast into Stellar Cyber XDR detection analytics

Phishing attacks continue to be one of the most popular attack vectors accounting for nearly 20% of all attacks in 2022. As a result, many lean security operations teams spend much of their investigation time on phishing attacks. While investigating phishing attacks, other potentially serious attacks are left in the queue, giving attackers more time to carry out their attacks and reach their objectives. Stellar Cyber and Mimecast working together provide security teams with a new approach to combating phishing attacks, combining Mimecast's advanced email security with Stellar Cyber's automated SecOps platform to deliver faster, scalable security outcomes.

## The Security Dilemma: Technology and cyber risk are intertwined

Tactics change, increase in sophistication, new vulnerabilities are constantly being discovered and Security Operations Center (SOC) teams are stretched to the limit investigating and remediating each incident. SOC teams find themselves relying on limited data found during the investigation, accepting decisions will be made based on incomplete knowledge or drowning under the weight of information, but not having the sufficient time to act appropriately. Most of an analysts' time is spent on the collection, normalization, and prioritization of data, leaving little time to focus on solving the issue.

Security teams must find new ways to ensure their organizations are protected. Moving between systems to ensure optimal threat protection, incident investigation or responding to a threat are no longer scalable solutions. Integrated, effective threat protection across all systems is mission-critical for organizations of all sizes and across all industries.

www.mimecast.com | ©2023 Mimecast | All Rights Reserved | CS-05253

## Integrated Solution

The Mimecast and Stellar Cyber integration deliver best-of-breed threat intelligence sharing and multilayered detection analysis across email, endpoint, identities, applications and cloud. This integration automates response by sharing threat intelligence across our platforms. Together this enables security outcomes that make Security operations more effective and productive. Our out-of-the-box integration is enabled within minutes and free to any joint Mimecast and Stellar Cyber customers.

Mimecast Email Security automatically detects and quarantines emails or attachments that are deemed malicious . At the same time, alert information about a phishing attack detected by Mimecast is shared with Stellar Cyber Open XDR, which correlates Mimecast alerts across the attack surface by using AI and machine learning to create a more complete picture of a security incident or attack, and allowing analysts to invest time in more focused research. This shared intelligence is used to help limit future attacks across multiple layers across the security stack including endpoint, identity and multi-cloud environments by taking immediate response actions, including shutting down endpoints or user access.

By integrating Mimecast with Stellar Cyber, SecOps teams can standardize their incident response processes, accelerate the time it takes to detect and adaptive security measures for containing and remediating attack campaigns.

### Mimecast + Alliance Partner: Customer Use Cases

- **Protect against Phishing attacks:** Ingest threat data, including email logs across the security estate to correlate threats and automated response actions
- **Simplify Threat Detection:** AI-enabled detection simplifies threat investigation by eliminating manual steps and improving efficacy of alerts
- **Correlate Alerts Across the Attack Surface:** Security analysts are able to automatically correlate email threat data across endpoint, network, cloud, and other security tools for faster detection and response
- **Share Threat Information:** Bi-lateral alert signals exchanged between Stellar Cyber and Mimecast enriches threat intelligence, while minimizing attacker dwell time
- **Automate Incident Response:** Detected threats are automatically contained through custom playbooks that run when specific threats are detected

**About Stellar Cyber**
The Stellar Cyber Open XDR platform delivers comprehensive, unified security without complexity, empowering lean security teams of any skill to successfully secure their environments. With Stellar Cyber, organizations reduce risk with early and precise identification and remediation of threats while slashing costs, retaining investments in existing tools, and improving analyst productivity, delivering a 8X improvement in MTTD and a 20X improvement in MTTR.

Learn more at **https://stellarcyber.ai**

**About Mimecast**
Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.

Learn more at **http://www.mimecast.com**