Data Sheet

mimecast

Mimecast Email Incident Response

Mimecast Email Incident Response can lower the dwell time of email threats and reduce the burden on your SOC. User reported suspicious emails are routed to Mimecast's SOC, where they are automatically analyzed, triaged and prioritized for expert analyst classification and remediation.

Email Incident Response Frees You to Focus on High-Priority Alerts

Email users have become part of organizations' defenses against sophisticated, targeted email threats. Awareness training, phishing simulation exercises and warning banners in emails combine to engage and empower them. The result is that IT teams and SOCs are becoming inundated with user reported suspicious emails. Unfortunately, 90% of these are benign, and this noise is diverting analysts from investigating other potentially more dangerous alerts.

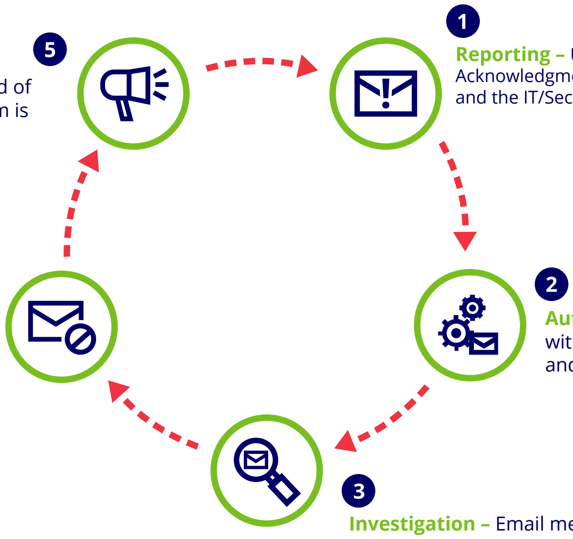
Key Benefits

- Lower the dwell time of email threats with rapid response and remediation
- Reduce the burden on resource constrained SOCs, allowing your analysts to focus on high-priority incidents
- Thirty-minute service level objective helps you meet your MTTD and MTTR goals
- Leverage Mimecast reported forensics for further investigation
- Strengthen your security posture with Mimecast expert email security analyst recommendations
- Low TCO and dependable per-user, per annum pricing provides easy opex budgeting

Leveraging Mimecast Intelligence

Mimecast crowd sources data from almost 40,000 customers. When an email is reported suspicious, it is first inspected using the latest threat intelligence, which is used to enrich the email metadata, along with contextual information. E.g. the reporter's past reporting accuracy, numbers of reports of similar emails and email risk score.

How it Works



1. **Reporting –** User reports a suspicious email. Acknowledgments are emailed to the reporter and the IT/Security team.

2. **Automation –** The reported email is inspected with the latest threat intel, automatically triaged and prioritized.

3. **Investigation –** Email meta data that is enriched to help rapid classification is queued for analysis.

4. **Remediation –** All instances of emails across the customer's estate that are classified as malicious are remediated.

5. **Notification –** The reporter is notified of the outcome, and the IT/Security team is provided with the threat details and remedial actions taken.

Automation Driven by Artificial Intelligence

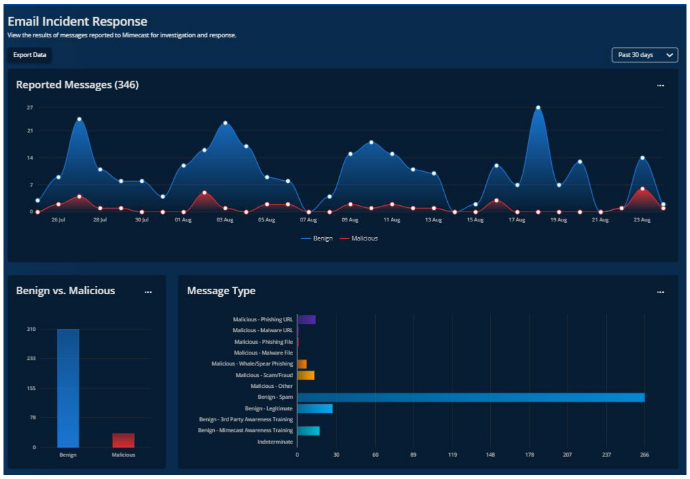
Emails ready for analysis are automatically triaged and prioritized, enabling Mimecast's expert analysts to rapidly classify threats and remediate all instances across your business. These classification decisions are fed back into the automation process, reinforcing machine learning models to strengthen future decisions. Finally, threat intelligence is updated, and future instances of the same threat will now be blocked by Mimecast Email Security before they reach your users.

Effective Communications Engage Users and Inform Your Analysts

Communications are built into each stage of the incident investigation workflow to ensure users are positively encouraged to report suspicious emails. Your security and IT teams are also part of the workflow communications and receive valuable forensic information when an incident is closed, to help with any further internal investigation.

Realize a Low Total Cost of Ownership

Mimecast's scale and investment in email threat analysis automation and tooling allow us to deliver Email Incident Response at a price point few enterprises could hope to achieve for a comparable service. It removes the requirement for yet another console. There is no installation, configuration or training required, and you are still in complete control—empowered by incident forensics and a dashboard that provides full visibility of service performance.



Email Incident Response

View the results of messages reported to Mimecast for investigation and response.

Note: Email Incident Response is available to customers with Mimecast Email Security and Internal Email Protect.