Data Sheet

mimecast

Email Threat Response and Remediation

Remediate email-based threats and elevate your SOC's focus with Email Incident Response

Security teams are inundated with alerts. Email-based threats in particular represent a massive security challenge due to their volume and complexity. With many employees now empowered to report suspicious emails, there's a never-ending backlog of security alerts that still require expert human analysis. Many of these reported emails are benign, but it takes careful attention to cut through the noise and identify real threats before they result in a successful attack. Unfortunately, this noise diverts analysts from investigating more serious alerts.

Fast and accurate remediation for malicious email

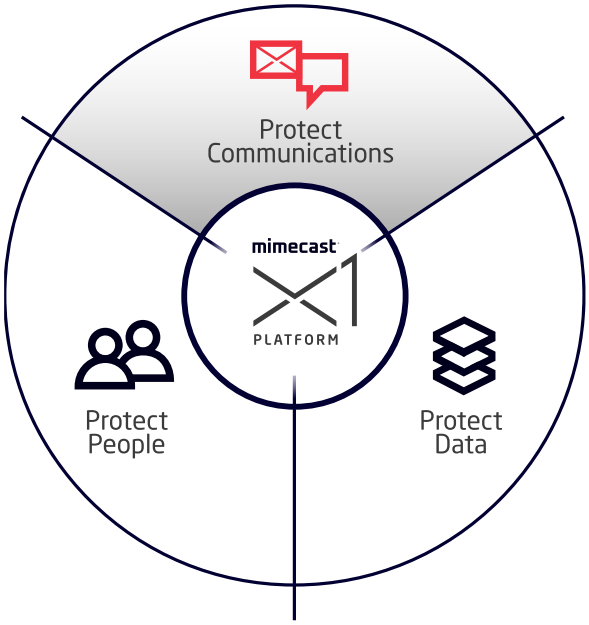
Mimecast's Email Incident Response service improves your security posture while reducing the burden on your security operations center (SOC).

Elevate your SOC's focus by routing employee-reported, email-based threats directly to Mimecast. With advanced threat intelligence, Mimecast's automated triaging and expert human analysis capabilities provide you with a trusted partner for email incidents. By quickly investigating emails to accurately identify and remediate threats, Email Incident Response empowers your security analysts to focus on more than just email.

Key Benefits

Email Incident Response

- Lowers the dwell time of email threats with rapid response and remediation, typically in 30 minutes or less
- Protects your entire organization by remediating known threats across all employee inboxes
- Reduces the burden on resource constrained SOCs, allowing your analysts to focus on high-priority incidents
- Strengthens your security posture with Mimecast expert email security analyst recommendations



Automatic triage & expert analysis

Mimecast sources data from over 40,000 customers and nearly 1.3 billion emails every day. When a suspicious email is reported using the Mimecast 'Report Message' plugin, it's triaged with the latest threat intelligence. The reported email is enriched with metadata and contextual information, including the employee's past reporting accuracy, numbers of reports of similar emails, and email risk score. This information is routed to the Mimecast SOC where expert analysts classify suspicious emails to identify real threats.

Rapid response & remediation

After triage and investigation, any emails determined to be malicious are rapidly remediated across your business. Email Incident Response works in partnership with Mimecast's Internal Email Protect solution to fully remove the identified threat from all employee inboxes. The entire process is managed by Mimecast SOC analysts and typically takes less than 30 minutes, helping you improve critical mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR) goals.

Employee & admin engagement

Communication is built into each stage of the incident workflow to ensure employees are positively encouraged to report suspicious emails. Your security and IT teams also receive valuable forensic information when an incident is closed to facilitate further internal investigation if needed. This includes email information, detailed attachment information, threat details briefed by analyst, scope of the threat, remediation logs, advice on how to prevent this threat where possible, and a list of analyst actions.

Low total cost of ownership

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