Solution Brief

mimecast

Mimecast Email Incident Response Solution Brief

Mimecast Email Incident Response can lower the dwell time of cyber security threats with rapid investigation, response and remediation by Mimecast's expert email security analysts. The burden of analysis of user reported suspicious emails is removed from your analysts by routing them to Mimecast's security operations center (SOC).

Users are your last line of defense and can help reduce dwell time

Dwell time is the duration between the start of a cyber intrusion and it being identified. The global median dwell time reported in 2020 was 56 days[1], during which time an attacker had free rein to:

- Perform reconnaissance, gathering information that could increase the chances of success of the next stage of the attack
- Spread the attack laterally through the organization and outbound to customers and business partners
- Gather and exfiltrate sensitive information

Enabling users to report email threats that have made it to their inbox is your last line of defense and is key to help prevent an attacker gaining a foothold in your organization. An Osterman Research survey found that all enterprises recognize this and provide users with a formal mechanism for reporting suspicious emails, and 57% make this task simple with an Outlook plugin or embedded link in the email. Reducing the friction of reporting has a major impact – those with an Outlook "button" are twelve times more likely to report an email as suspicious than those using any other method.[2]

Empowered users report more suspicious emails[2]

Almost all enterprises provide awareness training for users, with 56% doing so monthly or more frequently. Eighty-six percent reinforce this with the inclusion of banners in emails to warn users of some element of suspicion associated with the email. Combine this with technology that makes reporting easy, and it becomes clear to see why 80% of enterprises report an increase in user reported suspicious emails following awareness training. The reported rates of increase vary significantly, as can be seen in Fig 1.[3]

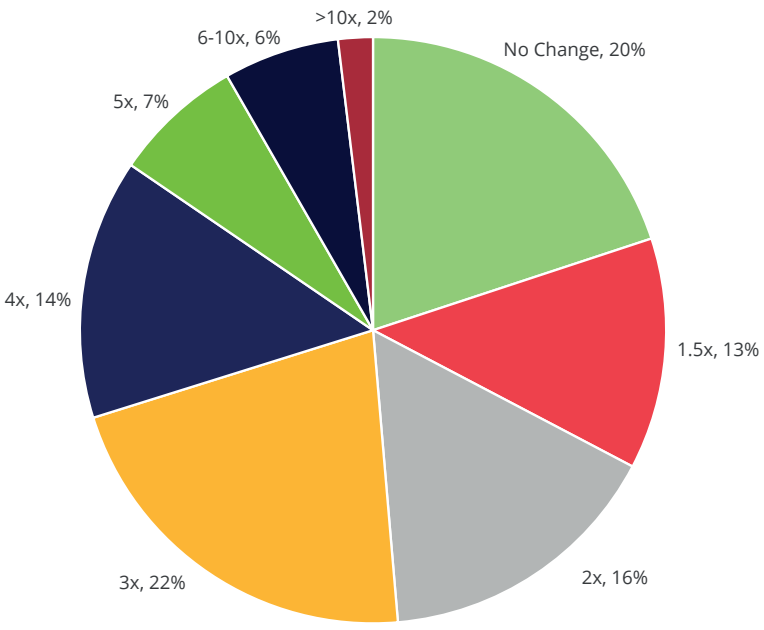


Fig 1. Percentage of enterprises that saw an increase in emails reported by users as suspicious following awareness training, with the rate of increase (n=300)

Expert human analysis provides accurate classification

Sophisticated, targeted email threats are difficult to detect. Therefore, organizations add warning banners to suspicious emails rather than risk lost productivity should a false positive occur.

Human analysis is essential to maintain low false positives and given up to 90%[4] of reported emails can be benign, users cannot be relied on. SOC analysts must perform this task.

According to Osterman, 29% of enterprises rely on human analysis only, 1% outsource the task, and the remainder use a triaging tool.[2] The available tools fall into two broad categories.

The first is an evolution of email security solutions that automatically inspect reported emails and remediate them if they are found to be malicious. They also include incident management and manually triggered remediation capabilities for those organizations that do not want to risk the false positives that could result from automating remediation.

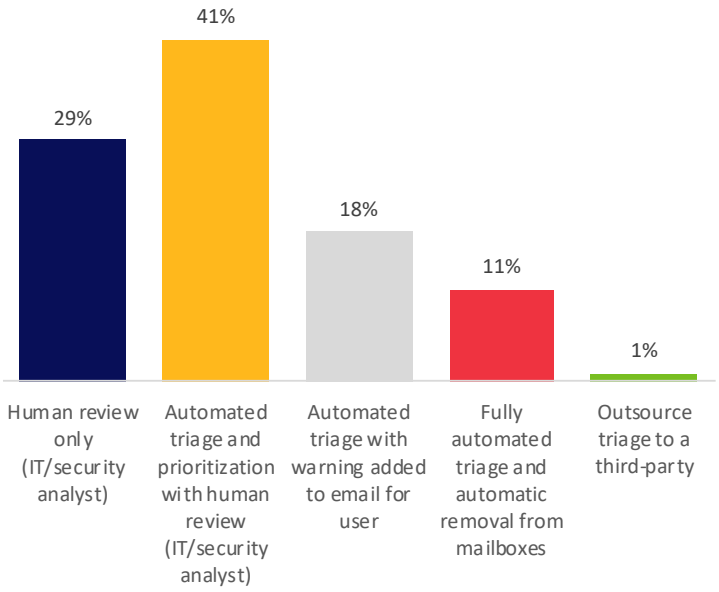


Fig 2. Methods of dealing with emails reported suspicious by users

The second category has evolved from phishing simulation platforms. These perform similar functions to the first category, but typically include no or rudimentary automated inspection for signs that the email is malicious. Only 11% of enterprises use fully automated response and remediation, the remainder relying on manual triggering of remediation following human investigation. For this function, the majority use a combination of their secure email gateway and/or integration with a SOAR platform. Shockingly, 6% rely on users manually deleting the email.[2]

These tools might help cut through the noise of those benign reported emails, but this still presents a significant diversion for analysts. In fact, 53% of enterprises consider user reported suspicious emails a diversion. Unsurprisingly this compares to just 1% of those who outsource the task.[2]

Analyzing reported emails is a drain on resources

This significant diversion is likely related to the alert fatigue suffered by security analysts and the well documented cyber skills gap. (ISC)2 reports that 64% of organizations have a shortage of cyber skills[5] and the Osterman survey found that 48% of enterprises do not have a dedicated SOC and consider cyber security part of the general IT team.

Emails reported as suspicious that are found to be benign can take far less time to classify than those that are malicious – 70% of enterprises classify them within 10 minutes, but 8% take greater than 30 minutes. Those reports that are classified as malicious, as one would expect, take far longer to investigate, with 79% of enterprises taking between 5 and 60 minutes. Surprisingly, the automated approach that relies on human review takes the longest time – almost twice as long as human analysis only. This is perhaps because the automation tool hides the context that a human analyst needs to make a final determination.[2]

Reported email threats are being disregarded

The result of the discussion above is that enterprises are failing to analyze all reported emails. If only 10% of emails that are reported are malicious, this would represent significant risk, but the 90% benign number is the extreme end of the scale – according to Osterman, the average is 49%. This means that, on average, 51% of reported emails are classified as malicious.

This represents a significant risk because only a quarter of enterprises analyze the full 100% of reported emails and more than two thirds analyze 90% or fewer. Figure 3 shows the varying degrees to which enterprises are analyzing emails. Those relying on human involvement in the analysis process analyzed just 64%, or about 10% fewer messages than those with full automation or using outsourcing.[2]

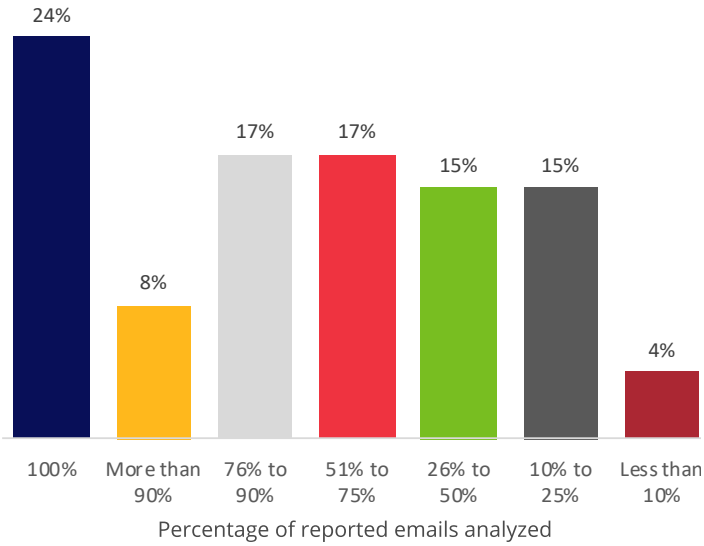


Fig 3. Enterprises and the numbers of reported emails that are analysed (n=300)

The risk here can be quantified by looking at a subset of Mimecast customers – in one week, 73 emails that were reported by users as suspicious, and subsequently classified by Mimecast as malicious, resulted in almost 14,000 similar emails being classified potentially malicious.[6] If the original reported emails are not being analyzed, this is the level of potential risk organizations are exposing themselves to.

Outsourcing can accelerate email incident response and reduce the burden on your SOC

Given the pressures on the SOC it is hardly surprising that almost 20% of organizations outsource part or all of their SOC function.[2] This will typically be to a dedicated MSSP that will be managing general alerts and incident investigation. Some may manage user reported suspicious emails and their challenge is similar to their customers' – up to 90%[1] of these reports are noise.

Outsourcing to email security experts

Mimecast has almost 20 years' experience of email security provision. Each month we process over 69B email requests for almost 40,000 customers. Our SOC is manned by expert email security analysts who analyze all reported emails to maintain low false positive and false negative rates. This is made possible by leveraging our latest threat intelligence, purpose-built tools and machine learning powered automation that has matured and evolved over many years.

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.

Automation driven by artificial intelligence

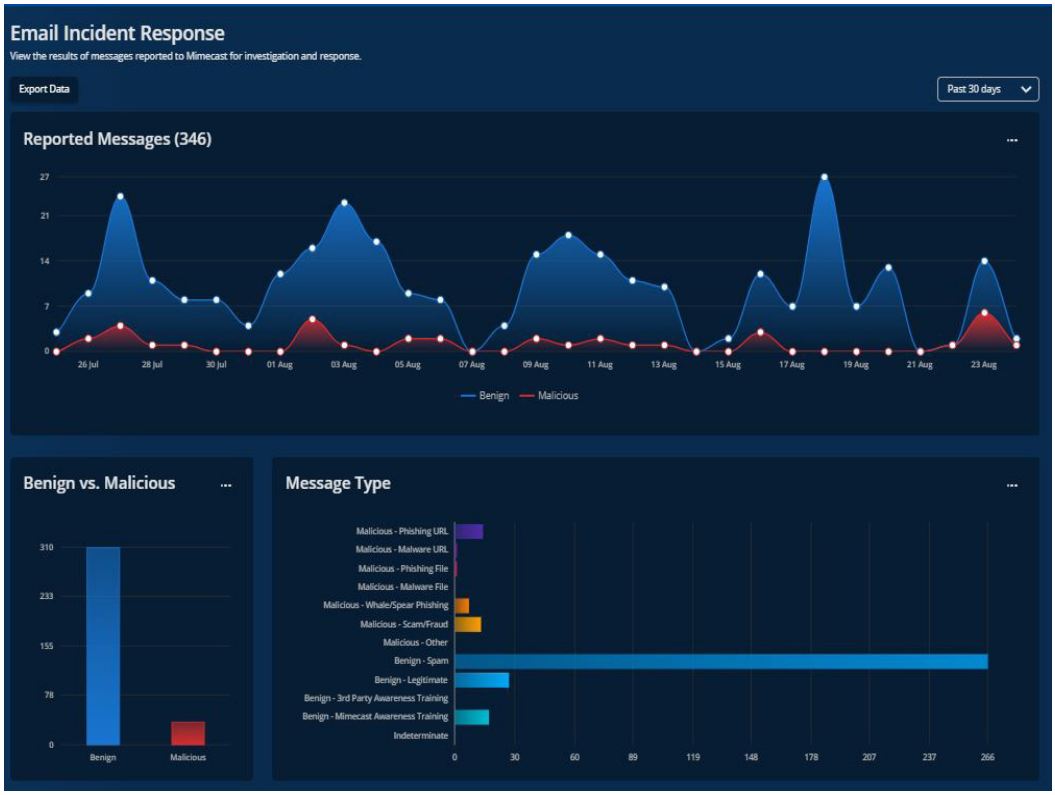
Emails ready for analysis are automatically triaged and prioritized, enabling Mimecast's expert analysts to rapidly classify threats and remediate all instances across your business. These classification decisions are fed back into the automation process, feeding machine learning models to strengthen 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.

The Email Incident Response workflow

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.

The Email Incident Response dashboard highlights user reporting accuracy, users that clicked suspicious links and threat types. These enable you to adjust your security program and processes to help you maintain the best possible security posture.



The financial impact of Mimecast Email Incident Response

Mimecast's scale and investment in email threat analysis automation, tooling and skills enables us to deliver Email Incident Response at a price point few enterprises could hope to achieve for a comparable service. The major expense incurred for an enterprise is that of the analysts themselves. Below, is an example of the staffing costs to analyze reported emails, which uses average results derived from the Osterman Research study that has been quoted extensively throughout this document. The salary of a London-based security analyst was derived from the Reed Technology Salary Guide 2021.

Average number of emails reported per user, per week	**0.33**
Percentage of reported emails that are benign	**49%**
Time to analyse a benign email (minutes)	**4.53**
Time to analyse a malicious email (minutes)	**12.39**
Fully loaded cost of a security analyst (2 x benchmark salary)	**$160,000**
Working days per annum (assume holiday, sickness and training days)	**220**

A 5000 user company would need eight analysts, and by deploying Email Incident Response could save $1M in direct staffing costs alone. Even if we reduce the number of reported emails to just 1 per-user, per-month, the saving is still $700K.

The savings above are related only to the staffing costs. Research suggests triage platforms can cost more than $20 per seat and take up to 2 weeks to install,[7] yet the Osterman study found that where human analysis is also required, triage platforms do not help reduce the time taken to analyze user reported suspicious emails. Mimecast Email Incident Response 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.

Contact Mimecast to learn more about the comparative total cost of ownership of response and remediation of user reported suspicious emails.

Mimecast Email Incident Response can lower the dwell time of email threats and reduce the burden on your SOC by routing user reported suspicious emails directly to Mimecast's SOC.

Operational Benefits

- Rapid response and remediation can prevent an attacker gaining a foothold, stopping them covering their tracks and progressing the attack over a prolonged period.
- Helps alleviate concerns around how to deal with the volumes and quality of user reported suspicious emails, while user communications engage them and positively reward their actions.
- Reduces your security team's workload, eliminating a mundane task and freeing them to focus on investigating high priority alerts and meeting MTTD/MTTR goals.
- Threats are automatically remediated from all inboxes across the business, and forensic information is reported back to your security team for further investigation, if needed.

Strategic Benefits

- The Email Incident Response dashboard highlights user reporting accuracy and users that clicked suspicious links and threat types. These enable you to adjust your security program and processes to help maintain the best possible security posture.
- Helps to overcome the challenge of finding skilled cyber security professionals and can relieve the pressure on the SOC to maintain staff morale and help retain current staff.
- Removes the requirement for costly tools to triage user reported emails and yet another console and additional processes.
- Per-user, per-annum pricing provides a fixed, dependable operating expense for budgeting purposes.

1. FireEye Mandiant M-Trends 2020 Report | 2. Osterman Research: Assessing Organizational Readiness to Deal With Increased Employee Cyber Awareness | 3. Mimecast analysis of data from Osterman Research: Assessing Organizational Readiness to Deal With Increased Employee Cyber Awareness | 4. Mimecast Security Operations Centre reporting | 5. (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2020 | 6. Mimecast MessageControl | 7. Automating Response to Phish Reporting, SANS.edu Graduate Student Research, by Geoffrey Parker - June 12, 2019