SUCCESS STORY

# Mimecast deploys Elastic to defend its systems against sophisticated cyberattacks and reduce overheads by 50%

Leading enterprise security software provider protects its own systems from cyberthreats using Elastic Security with Elastic Cloud on AWS, increasing productivity, reducing severe incidents by 95%, and accelerating detection and remediation.

**Region**
United Kingdom

**Industry**
Software & Technology

**Solution**
Elastic Security

### Accelerates data integration and use case deployment

Elastic Security enables Mimecast to integrate new data sources and build customized use cases in days rather than weeks or months for faster and more robust threat prevention that has reduces severe incidents by more than 95%.

### Lowers security management costs, increases productivity

Mimecast has reduced the time, resources, and costs needed to manage security and respond to threats by 50%, improving productivity and keeping the team focused on high-value tasks.

### Consolidates disparate systems for a unified view of security risk

Elastic Security gives Mimecast a ‘single pane of glass’ view into hundreds of services, supporting data-based decision making, and an acceleration of threat detection and remediation.

Mimecast has forged a reputation as a leading provider of secure email, data retention, and compliance and security training solutions since its inception in 2003. Email and data retention can sometimes be an afterthought in IT security but are the favorite targets of cybercriminals given the large amount of highly confidential data being shared through these applications every day.

The company's 2,000 employees across 13 global offices have helped more than 40,000 customers bolster their overall IT security with a focus on email and data retention. Mimecast must also defend its own systems from external threats to protect the business and best serve clients, especially as Mimecast can act as a custodian of its customers' most crucial assets.

## Implications of modern IT security challenges

Damian Haslam, Cybersecurity Operations Director at Mimecast, leads the team responsible for protecting the company's IT infrastructure and software.

"The threat from hackers, cybercriminals, and state-sponsored agents is dramatically increasing each year," says Haslam. "People are even using artificial intelligence to write malicious code and share it on the dark web for others to use, adding to the exploding prevalence of cyberthreats that we must stay ahead of."

Mimecast faces ongoing security demands from acquisitions, cloud adoption, new and increasingly ephemeral environments, explosive growth of data volumes and sources, and expensive security platforms built for the on-prem world. The security team foresaw these challenges as potential inhibitors of its security position.

Additionally, disparate data sets, weeks-long onboarding of new sources into their legacy Security Information and Event Management (SIEM) systems, and increasingly manual efforts to view and analyze data tied up the Mimecast team with lower-value activities. Over-reliance on human intervention came with the risk and costs of higher error rates and overhead.

"These challenges were taken extremely seriously by my team up to the executive leadership level, knowing that they could become Board-level risks if left unaddressed," says Haslam. "It was clear we needed a centralized solution to minimize attack dwell times, enhance advanced persistent threat identification, lower cyber insurance premiums, and prevent team burnout and turnover."

This proactive approach hinged on the identification of a thoroughly planned and neatly implemented solution that covered all key criteria.

## Streamlining and accelerating network security

After researching all available options, Mimecast ultimately turned to Elastic Security, deploying Elastic Cloud hosted on AWS with tight partnership and support from Elastic Consulting. Elastic Professional Services provided oversight during key phases of the project. They also trained the Mimecast team to maintain the system independently.

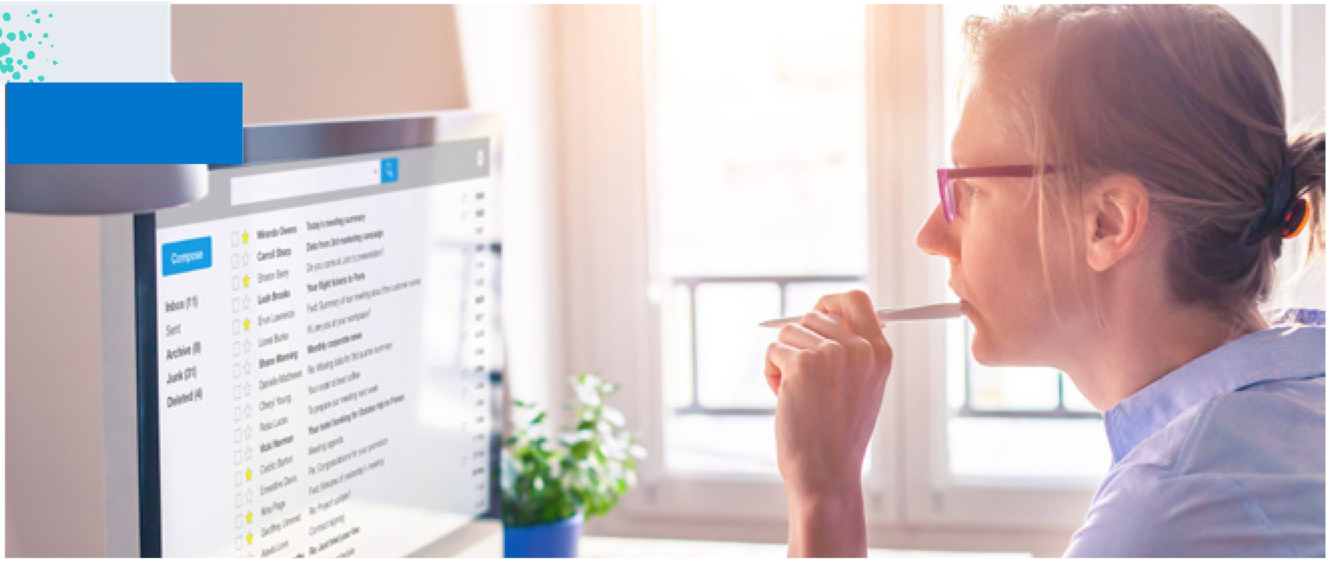
“The Elastic Professional Services team were a godsend during our migration to Elastic Cloud,” says Haslam. “If we had any issues, they got back to us immediately. Working with such a dedicated team was a revelation compared to previous experiences with other vendors.”

The migration to Elastic Security provided key wins for the Mimecast security team, including:

- Deployment aligned global business architecture in hours and days versus weeks or months,
- Significant cost savings and the ability to see new data without incurring new costs,
- Legacy transformation and future-proofed security posture in just four months,
- Dramatic shift in Security and Platform Engineering team focus from menial to high-value activities.

Elastic enables Mimecast to capture and integrate data from dozens of systems including customer-facing products and threat intelligence platforms. In doing so, Mimecast has been able to reduce unsustainable security operations costs by consolidating its security solutions and automating detection and intervention. Consolidation and automation have accelerated remediation by and reduced instances of human error.

Speed of course plays a critical role in security, as every second an intruder has access to a sensitive system translates to more compromised data. Elastic Security simplifies log ingestion from multiple sources to help speed threat identification and remediation. Haslam and his team can add new feeds in a day or less rather than the three-week sprint it took in the past, dramatically improving the development of new detections and use cases and reducing severe incidents by 95%.



> Elastic Security on Elastic Cloud gives us a unified view of our security systems and logs. It is a highly versatile data platform that we can mine for insights above and beyond a traditional SIEM system. We regularly test our systems with attack simulations. If we detect any vulnerabilities, we can build a new use case with Elastic in a matter of days rather than weeks compared with other solutions.

**Damian Haslam**
Cybersecurity Operations Director, Mimecast

Advanced automation and self-healing features provided by Elastic Security enable Mimecast to boost its network resilience while simultaneously reducing time spent managing security and responding to threats. The Mimecast security team has leveraged these capabilities to cut the number of hours its analysts need to cover this work by 50 percent.

"Using Elastic Security, our machine learning and artificial intelligence team can automate processes and use data analytics and algorithms to assess vulnerabilities and risks," says Haslam. "We can now provide a line of defense that is above and beyond a mainstream security system."

## Improving threat detection with user-friendly dashboards and centralized management

Elastic also excels in data search speed. From local searches to cross-cluster investigations, Elastic returns results from huge volumes of data in a matter of seconds. When Mimecast detects an indicator of compromise (IOC) through one of its threat simulations, it can quickly search back through its data to see if it has been compromised and shut the door on any threat.

Kibana dashboards are critical components of Mimecast's Elastic deployment, democratizing threat intelligence across the organization for better data-driven decision making.

"We really like the way that Kibana can be adapted to different contexts throughout our business," says Haslam. "We have built many dashboards that offer teams across the organization a unique view into the performance of their systems."

Elastic Agent further centralizes security management by unifying log collection and other key data points across all sources and use cases. The result is a future-proofed protective framework that improves security and platform team productivity, consolidates and unifies previously disparate systems, and alleviates the cost and resource strains of the past.

With support from the Elastic team, Mimecast can now block attacks and reduce threat exposure to a minimum. The company can continue to protect its clients knowing that its own defenses are always a step ahead of cybercriminals.

> Elastic Security goes beyond the traditional definition of a SIEM system. It is more like an enterprise-wide security environment that can be adapted to protect any area of the business. I can't imagine not having Elastic as our main line of defense.

**Damian Haslam**
Cybersecurity Operations Director, Mimecast

|