CASE STUDY

Mimecast: Source of Better Actionable Intelligence in the Quest to Secure the Network

CUSTOMER BENEFITS

Gigamon Insight Cloud-Based Security Solution

- Provides near real-time insights into the entire network
- Sends easy-to-set alerts on particular events of interest
- Offers a single-pane view of network activity across monitored segments, improving mean time to detection significantly
- Quick, painless deployment with results in less than two hours
- Constant background updates from Gigamon provide new detection capabilities
- Zero maintenance requirements
- Named Technical Account Managers extends the customers security expertise
- Gigamon Applied Threat Research (ATR) adds value to detections with leading-edge threat research

Challenges

Fast detection of suspicious activity at the network perimeter is a critical priority for the Mimecast IT security team. Mimecast, a cloud cybersecurity and resilience provider for IT service organizations, tried using a series of tools, many of them open source, to discover and analyze possible threats against its corporate network. However, they found that juggling multiple solutions was both limiting their visibility and delaying their team's incident response time.

Wanted: A Single Source for Threat Intelligence Visibility

"Part of the issue was collating the various logs and the various sources into a consistent view of what's really happening," says Mark O'Hare, Chief Information Security Officer at Mimecast.

"We often had to go to three or four different sources to collate the information to get a better picture." What they needed was a single source for better visibility and that includes rich contextual data to better understand what was happening at their network perimeter.

Given its cybersecurity business focus, Mimecast is proactive about protecting its own corporate network and sets high standards for any third-party technologies it considers. It was essential for any security solution to pass its rigorous governance, risk and compliance (GRC) process.

Solution

The Mimecast team was seeking a solution that was free of dependencies on other tools for data collection and analysis but also capable of integrating with their existing security stack, including their security information and event management (SIEM) system.

They selected Gigamon® Insight, a cloud-based security solution, to meet these challenges. Insight consolidates threat hunting, detection, and incident response in a single solution that rapidly scales to meet customer needs. Insight uses strategically placed physical, virtual or cloud sensors to collect detailed network activity information and transmit relevant metadata to the specialized cloud-based data platform. The data is then correlated, normalized, enriched with additional intelligence information from Gigamon Applied Threat Research (ATR) and analyzed for actionable threat detection.

Customers like Mimecast can both access this information directly using a web portal or send the data to their preferred analytics and incident management tools using Insight API integration capabilities.

"Gigamon Insight is giving us better insight to our network from a single pane."

"Insight doesn't rely on any vendor's tooling to actually get visibility to this information," O'Hare says. "I could imagine deploying this in other locations, too, and it would give the same level of visibility, which is really impressive."

Gigamon Insight in Just Two Hours

Mimecast deployed sensors in 5 different locations – UK (x2), South Africa, Australia and North America, and connected to span ports on their perimeter switches. Soon after the sensors were deployed, network metadata began flowing to the Gigamon Insight cloud-based data platform, where it was analyzed for malicious activity and began delivering new and more complete threat information to the Mimecast team.

The team was pleasantly surprised by how easy Gigamon Insight was to roll out. "The actual deployment was very painless," says O'Hare. With just two IT staffers on the task, it took less than two hours for Mimecast to start seeing results.

O'Hare appreciated how Gigamon treated Mimecast from the beginning of the process, taking feedback into careful consideration. "I really enjoy working with the people," he says. "We're treated and taken seriously, rather than being just another client."

Results

Faster Mean Time to Detection

Once Insight was deployed, Mimecast immediately gained greater context into network threats. Instead of juggling the output from multiple tools, they could use Insight to get a single pane-of-glass view into what's happening across the network. That helped deliver a much faster mean time to detection than it had with Mimecast's previous solutions.

"We've learned to rely on Gigamon Insight. We can take what we see at face value."

Alerts and Triggers that Work

One crucial way Gigamon Insight keeps Mimecast informed is via easy-to-set alerts and triggers that notify security staff about Indicators of Compromise (IoC). Because Insight is a SaaS solution, Gigamon constantly works in the background to improve it by adding new features, new alerts and new insights into the threat landscape with no maintenance from you.

"It's given us better visibility to our network from a single pane," says O'Hare, "along with near real-time monitoring and alerts to particular events and particular characteristics in a better coordinated way."

"We've learned to rely on Gigamon Insight," O'Hare concludes. "We can take what we see at face value."

About Mimecast

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure. www.mimecast.com

About Gigamon

Gigamon® is the recognized leader in network visibility solutions, delivering the powerful insights needed to see, secure and empower enterprise networks. Our solutions accelerate threat detection and incident response while empowering customers to maximize their infrastructure performance across physical, virtual and cloud networks. Since 2004 we have cultivated a global customer base which includes leading service providers, government agencies as well as enterprise NetOps and SecOps teams from more than 80 percent of the Fortune 100.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com