Case Study

Centrax fires up its cybersecurity with a complete set of defenses

1 day

Centrax neutralized a major look-alike domain attack within 1 day of going live with Mimecast.

48%

of all inbound emails, on average, are flagged as spam or suspicious and are therefore rejected.

29 times

Malware is detected and blocked an average 29 times per weekday.

> “Our customers and suppliers want to know we have resilient cybersecurity measures in place before doing business with us, and thanks to Mimecast we can give them that peace of mind.”
>
> **Daniel Mortimore, IT support analyst at Centrax**

Business case

With ransomware and phishing attacks on the rise, Centrax bolstered its cyber defenses across the organization to better detect and neutralize threats while keeping its customers’ critical power-generation processes running.

Results

Armed with the complete suite of Mimecast solutions, Centrax took down the phishing attack overnight, shored up protection against future threats, and trained employees to be more proactive in protecting their data and email. The subsequent addition of Mimecast’s AI-powered CyberGraph reinforced Centrax’s security posture.

> “Having a complete set of security solutions keeps our business safe by filtering out bad emails, blocking suspicious sites, and keeping our employees on their toes, all while taking pressure off our IT team.”
>
> **Daniel Mortimore, IT support analyst at Centrax**

CENTRAX

Overview

From French energy giant ENGIE, which use a Centrax gas turbine to heat the city of Versailles, to German chemical giant BASF, which uses a Centrax generator package to fuel its manufacturing processes, businesses around the world rely on Centrax to power their organizations and the communities they serve.

But that’s not all that ties them together. Every one of Centrax’s customers need to ensure its services are secure and dependable.

“Without our products, national grids and critical manufacturing processes would go down, potentially affecting millions of people,” says Daniel Mortimore, IT support analyst at Devon, England-based Centrax. “Uptime and security are non-negotiable for our customers, which is why we provide them with comprehensive maintenance contracts, dedicated in-country teams, and the highest possible standard of cybersecurity.”

In fact, security is a top priority for Centrax, not just to protect its customers’ interests but also as a value-add for new prospects. To that end, Centrax partnered with Mimecast to build on its existing security solutions with a complete suite of cyber defenses, ranging from email protection, to employee awareness training, to advanced data protection fueled by artificial intelligence (AI).

“Our customers and suppliers want to know we have resilient cybersecurity measures in place before doing business with us, and thanks to Mimecast we can give them that peace of mind,” Mortimore says.

Learn more about Mimecast’s complete suite of security solutions, the role of AI in cybersecurity, and how to separate fact from fiction.

For more on Centrax Gas Turbines, visit its website **here**.

Advanced Threats Require Advanced Protection

Centrax had been working with Mimecast for over 10 years, starting with Mimecast's Email Security and Cloud Archive products, but the turning point for its cybersecurity strategy came in early 2021, when one of its biggest clients was hit by a major look-alike domain attack. Realizing they didn't have the solutions in place to take down the fake domain, Centrax's IT team shored up the company's security portfolio with Mimecast's Brand Exploit Protect and upgraded their existing Mimecast Email Security.

Within a day of implementation, the team was able to neutralize the attack. That would be the first of many wins for Centrax's IT team, which has since become increasingly proactive and effective at defending the business and its customers against cyber threats.

"That first attack was escalated all the way to the Centrax boardroom. It was a high-profile test of our team's threat response when supported by a complete suite of Mimecast security solutions, and we passed with flying colors," Mortimore says. "Our organization's appetite for advanced threat protection has only grown since."

A Stronger Defense Built on Awareness

In addition to taking on a complete suite of Mimecast solutions, Centrax knew it needed to empower its employees to protect themselves, their emails and their data. Mimecast Security Awareness Training has been instrumental in helping teams across the business to recognize and manage attacks that might otherwise slip through the cracks.

"You can implement as many systems as you want to filter out suspicious emails and phishing attempts, but at the rate we see attacks today there's no way to catch everything with software alone," Mortimore says. "Mimecast's Awareness Training helps our employees to recognize and avoid attacks and then flag them to our IT team so we can take the necessary action."

This focus on training continues to grow in importance at Centrax as it enhances its defenses and drives security awareness among employees. This also takes the burden off Mortimore and the relatively small IT team to fight cyber threats on their own.

Adding AI to the Mix

The growing volume and complexity of attacks has also led Centrax to explore a new frontier in cybersecurity: AI. In March 2022, the company adopted Mimecast CyberGraph to fend off email attacks at scale. The solution automatically detects and flags spy trackers embedded in employees' emails, ensuring that suspicious messages are treated with the appropriate level of scrutiny.

"Interestingly, we're seeing attacks get simpler as hackers look to slip malicious messages through our more sophisticated email filters," Mortimore says. "AI is perfectly suited to catching these quick and dirty attempts, which can snowball into major problems if left undetected."

As it continues to grow and adopt new IT systems to fuel its business, Centrax has positioned itself to stay one step ahead of security threats and ensure its customers' critical processes run securely, without disruption.

"The number of IT systems we use to do our jobsand serve customers has increased dramatically, and the more systems you use, the higher the potential for abuse," Mortimore says. "Having a complete set of security solutions keeps our business safe by filtering out bad emails, blocking suspicious sites, and keeping our employees on their toes, all while taking pressure off our IT team."