Customer Case Study

Medical Equipment Management Company Adopts Behavioral AI to Protect Its Email

Fast-growing medical equipment management and services provider strengthens defenses, protects client data with Abnormal.

This thriving player in the medical equipment and services sector operates on the philosophy that every healthcare interaction can change a life. The company helps ensure that hospitals and healthcare systems have properly working equipment—from patient beds to surgical lasers—so providers can focus on patient care. To enable its thousands of customers to optimize patient outcomes and maximize cost savings, the organization deploys 300,000+ medical devices and operates 150+ service centers.

The Company's Email Security Challenge

Because healthcare is a major target for criminals seeking data and money, the organization continually works to protect customer interactions. "We embrace zero-trust across the enterprise and cloud-first solutions to provide comprehensive security," said the Senior Manager of Cyber Security. "We treat the data our clients provide carefully, including protected health information."

The company was using Microsoft Exchange Online's security tools for Microsoft 365 and conducting awareness training, but advanced credential phishing and business email compromise attacks were still landing in inboxes. The organization was also investing significant time in email investigations, reporting, and remediation.

Industry
Medical Equipment

Headquarters
Midwest, USA

Employees
5,500+

Customer Key Challenges

- Protect company and client data, including PHI, from ongoing credential phishing and BEC attacks.
- Reallocate security team time to other projects by automating email security functions.
- Save VIP and employee time with automatic graymail filtering and management.

Abnormal Products

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox
- Email Productivity

> "The bad guys are using AI to get better at creating more complex threats faster. It's important to fight the machines with machines, and I think as time goes on we're going to rely more and more on capabilities like Abnormal's AI."
>
> VP & CISO

974

Employee and VIP hours saved on graymail in 90 days.

Zero

False positives among 5,000+ attacks stopped in 30 days.

20

Security team hours saved per month on manual email management.

Seeking an Effective Security Remedy

The VP and CISO knew the company needed additional email security to support a more proactive stance, and he knew he didn't want to add a secure email gateway (SEG). "Before joining this company, I was CISO at a bank where we implemented three different legacy SEGs in four years. I have scars and nightmares from those experiences because legacy gateways make you get deeply into rules and they break."

He also knew the emergence of AI-based attacks meant that humans would never be able to keep pace with the evolution and volume of threats. After discussing options with their IT vendor and industry peers, he and his team decided to try Abnormal.

Why the Company Chose Abnormal

Not only did Abnormal's cloud-based, behavioral AI-driven solution check all the boxes, but it was also easy to use and provided better visibility. "The API integration took minutes to get up and running," the VP and CISO said. "Before the Proof of Value we had no real visibility into the email based threats present in our ecosystem," the Senior Manager added. The Account Takeover module easily integrated into their Microsoft email system to identify anomalies and inform the security team, without generating false positives. "If we get an alert from Abnormal, there's a good reason," said the Senior Manager.

Additionally, Abnormal's automated phishing reporting and responses save the team hours each week and help inform employee training. The Email Productivity module also saves more than 900 hours per quarter companywide by filtering graymail.

Safer Email Interactions, Greater Productivity

This medical equipment and services provider now has an email solution that stops advanced threats. Users have also noticed the reduction in spam and graymail taking up space in their inboxes. And the VP and CISO has avoided the "scars and nightmares" of dealing with a SEG. "I've been a vocal supporter of Abnormal in CISO groups I belong to because I understand the difficulty of integration and lower effectiveness of legacy SEGs. If you're only using a SEG, you need to look at Abnormal. It's like going from zero to 200 mph in terms of increased capability."

> "We've realized a lot of value by integrating Abnormal with our anti-phishing program. Abnormal's dashboard shows us real threats, so we tailor our training to address those risks instead of theoretical ones. Every now and then we get reports of suspicious emails, and I use them as a coaching opportunity. Our people now have an automated tool to diagnose email that they think is suspicious: Use the report button and get feedback in minutes."
>
> VP & CISO

abnormalsecurity.com →