Customer Case Study

Vituity Protects Patients' Data and Doctors' Time with Abnormal

Physician-owned group innovates for stronger security and greater efficiency to serve 8 million patients.

Vituity supports continuous innovation in healthcare by helping hospitals reduce costs, improve care quality, increase operational efficiency, connect with their communities, and improve patient flow through the care process. Vituity has more than 5,000 clinicians serving in 450 practice locations, providing their partner hospitals with critical care, neurology, psychiatry, and other practice specialties.

Industry
Healthcare

Headquarters
Emeryville, CA, USA

Employees
7,000+

Protected Mailboxes
9,400+

The Vituity Email Security Challenge

"Healthcare data is a prime target for adversaries, so attackers are always looking for ways in," said Jeff McDonald, Senior Vice President of Technology Services. "Our main concern right now is business email compromise, ransomware, and account takeover attacks that can lead to a lateral spread within our email environment."

Even with native email security tools available in Microsoft 365 and a secure email gateway, spear phishing and other malicious messages were reaching executive, physician, and employee inboxes. The security team manually remediated these reported attacks, but the time required raised the risk that a recipient would engage before the threat was addressed.

Customer Key Challenges

- Stop advanced spear phishing attacks from reaching executives' and physicians' inboxes to protect internal data, including patient data.
- Reduce clinician and executive time spent dealing with graymail and spam.
- Free security team from manual investigation and remediation work to enable focus on other security projects.

Abnormal Products

- Inbound Email Security
- Email Account Takeover Protection
- Abuse Mailbox Automation
- Email Productivity

"Email threats don't just put our company at risk. They also endanger our patients' privacy, safety, and potentially their lives. Abnormal has helped us secure the most significant vector putting our patient data at risk."

Jeff McDonald
Senior Vice President of Technology Services

Customer Case Study

Zero
Missed attacks or false positives in 30 days.

61
High-risk vendor compromises detected upon integration.

200+
Employee and executive hours saved on graymail in 90 days.

Why Vituity Chose Abnormal

To solve the problem, McDonald wanted a security layer that could evolve with the threat landscape. “Adversaries are changing from year to year and toolset to toolset, and we have to shift constantly as well. Our school of thought is if attackers now are using sophisticated techniques like AI, we should be using AI to combat that.”

He also wanted an API-based solution for quick deployment and integration. Abnormal met both requirements. “When we learned about Abnormal, we were surprised that it fit exactly how we needed it to. We didn’t need to replace our security stack, and we could set it up in five minutes,” McDonald said.

The Abnormal setup was seamless and the results were quick, said Donato Cabal, Director of Information Security. “Abnormal was catching many messages that our existing security tools were missing. It really surprised us how effective Abnormal was.” McDonald agreed: “Our existing tools filtered out a lot of mass-generated attacks but let the scariest problems go right through. Abnormal is exactly what we needed.”

The Abnormal Threat Log gives Cabal and his team better visibility into attack trends, and Cabal also checks the statistics on blocked graymail messages as Vituity rolls out Email Productivity. McDonald said the executive test group’s response has been positive, because it saves them time and it also helps reduce background noise that can mask threats.

Vituity Secures the Future with Abnormal

Abnormal’s approach to security is a good fit for Vituity’s innovation-focused mindset. McDonald views Abnormal as an effective solution for email security now and a potential resource for security issues in the future. “We're excited to see what new products are on the horizon as Abnormal expands its portfolio of AI and ML solutions, and to see how our current security can be augmented with next-generation techniques and tooling.”

> “Abnormal has helped us meet our security requirements by effectively remediating malicious emails. With the time Abnormal saves us on manual investigation and remediation, my team now spends more time focused on other potential areas of compromise and working on an infinite number of security projects across other areas of the organization.”
>
> Donato Cabal
> Head of Information Security

abnormalsecurity.com →

Abnormal