Customer Case Study

Ensemble Health Partners Safeguards Patient and Provider Data with Abnormal

Behavioral AI detects and blocks advanced credential harvesting attacks while AI automation optimizes security operations.

Ensemble Health Partners keeps providers financially healthy so they can focus on patient care. The company's customers include mid-sized to large hospitals and health systems across the country. As an award-winning end-to-end revenue cycle management company managing more than $34 billion in net patient revenue, Ensemble's expertise, best practices and approach to technology help reduce denials, accelerate collections and drive revenue lift for healthcare providers.

The Ensemble Email Security Challenge

Attackers often target healthcare organizations seeking patient data for identity theft and extortion—with potentially serious privacy and wellbeing consequences for patients. "You can get a new credit card after theft, but you can’t get a new medical record," said David Anderson, CISO and VP. "Attackers know they can leverage patient health, which has led to high-profile payouts in the industry and even facility closures." After an increase in targeted credential phishing and business email compromise (BEC) emails reaching employee inboxes, the Ensemble team decided they needed an advanced layer of protection on top of Microsoft Defender and a traditional secure email gateway (SEG).

ENSEMBLE®
HEALTH PARTNERS

Industry
Hospitals and Healthcare

Headquarters
Cincinnati, Ohio, USA

Protected Mailboxes
28,000+

Customer Key Challenges

- Protect client and patient data from AI-powered credential phishing.
- Detect and block high volumes of advanced attacks faster with automation.
- Free the security team to work on higher-level projects that add value.

Abnormal Solution Impact

- Detects subtle changes that can indicate credential phishing, account takeovers, and other attacks with human behavior AI.
- Remediates attacks immediately and at scale with AI automation.
- Integrates with other applications via API to give analysts more insight into attack trends and more time to act.

> “Adversaries are innovating with AI and automation to steal credentials from organizations, their clients, and their vendors. Traditional solutions can't keep up. Abnormal is at the forefront of new ways to identify malicious traffic and take that workload off our SOC analysts.”

David Anderson
CISO and VP

Customer Case Study

$34B
net patient revenue managed with Abnormal protection

93%
of attacks were sophisticated credential phishing

1,438
employee hours saved with graymail filtering in 30 days

The Abnormal Security Solution

Anderson was familiar with Abnormal from his role at a previous healthcare employer, and he was happy to find Abnormal already in use when he joined Ensemble. "I was interested in Abnormal's natural language processing capabilities and the additional signals used for detection."

Abnormal's AI automation capabilities aligned with his goal to help Ensemble's 22-person security team respond more efficiently to accelerating attack rates. "As adversaries do more with AI and begin to automate their processes even more, we have to automate on our side, especially to prevent credential compromise. If you don't automate, there isn't enough time to respond when a high volume of attacks hits your SOC at once."

Why Ensemble Chose Abnormal

Anderson said Abnormal's detection and automation capabilities set it apart. "I spent many years at the NSA, and traffic analysis is important. Abnormal has detected and remediated multiple compromised accounts for us, so the ROI is fantastic.

Abnormal's API integrations allow for better intelligence across the organization, Anderson added. "Connecting Abnormal with CrowdStrike and other tools creates a better mosaic of defense data for decision making." In addition, the Email Productivity module extends efficiency gains to all employees by filtering promotional emails out of the main inbox. In just 30 days, Ensemble saved 1,438 hours by eliminating the need to comb through promotional messages.

A Partnership for Safer Customer and Patient Data

Anderson sees Abnormal as an innovative partner for fighting advanced attacks and pursuing business goals. "Detection will get significantly harder, because AI is raising the quality of phishing attempts. Attackers can more easily do deep target research and engineer powerful prompts, so we need to be prepared," he said. "As the security team, we are part of the business and its goals, so we can't be the 'office of no.' We have to be able to say 'yes, and we'll do it securely.' Abnormal lets us do that so our people can focus on helping our clients and their patients."

> "Most people in healthcare want to be helpful, and attackers exploit that. Security awareness education helps train our employees, but as attack emails become precisely targeted, we need Abnormal to analyze all the data points behind each email to determine if it's safe or not."
>
> David Anderson
> CISO and VP

Abnormal Products in use:

- Inbound Email Security
- Account Takeover Protection
- Email Productivity

abnormalsecurity.com →

Abnormal