Customer Case Study

Healthfirst Prioritizes Quality with AI Automation for Email Security

New York State's largest not-for-profit insurer relies on Abnormal to prevent advanced threats that prey on human behavior.

healthfirst
Health Insurance for New Yorkers

Industry
Hospitals and Health Care

Headquarters
New York, New York, USA

Protected Mailboxes
11,200+

Nearly 2 million New Yorkers and 40,000+ healthcare providers trust Healthfirst's innovative approach to insurance and value-based care. What makes Healthfirst different is that in-network providers are compensated based on patient outcomes, fostering excellent care. "We're leading the industry with quality, and we're also a non-profit model," said Brian Miller, CISO. "So every penny that's saved goes back to providing our members with the care they need and driving better health outcomes."

The Healthfirst Email Security Challenge

As a healthcare organization, Healthfirst's main security challenge is safeguarding protected health information (PHI). That challenge is more urgent since a successful cyberattack on a major health payment processing company, which may have exposed millions of healthcare records. "Those claims have everything you need to steal the identity of a member. So we have a heightened awareness around identity verification," Miller said.

Business email compromise (BEC) is another concern. "Microsoft and our SEG struggled with blocking sophisticated attacks," he added. "Attackers were getting into vendor systems and hijacking legitimate email chains to submit invoices with different routing numbers, which would send our payments to accounts controlled by the bad actors."

Customer Key Challenges

- Protect PHI and prevent socially-engineered attacks that used data stolen from other companies.
- Detect and stop BEC attacks sent from compromised email accounts.
- Reduce finance and security team time spent vetting invoice emails.

Abnormal Solution Impact

- Quickly modeled human behavior to flag anomalies that could indicate account takeovers and fraud.
- Dramatically reduced false positives and stopped advanced attacks through behavioral AI.
- Analyzed incoming emails and user-reported messages at scale through AI automation—allowing teams to focus on their core tasks.

> "When I first heard about Abnormal, I thought maybe we didn't need it, but I endorsed the security team looking at it. I'm glad we did because just in the pilot phase, Abnormal detected a major BEC attack that was nearly successful. Stopping that attack alone saved us half a million dollars."

Brian Miller
CISO

$500K
Saved by detecting a major BEC attack during POV.

Zero
Missed attacks or false positives in 30 days.

123
Vendors identified as high risk on integration.

The Abnormal Security Solution

Although Miller wasn't sure that Healthfirst needed Abnormal, he encouraged his team to check it out. "We started piloting Abnormal and my team came to me and said, 'Abnormal found something we ought to look at.'" That single instance prevented a BEC attack that would have cost the company half a million dollars.

Abnormal's AI automation capabilities also appealed to Miller. "As I consider any tool, I look at whether I can use it to take effort away from my team and allow them to scale." Ease of setup and integration was also a plus. "Once I moved forward to get full funding, everybody wanted to know how long it would take to implement Abnormal, and I told them, 'It's done.' It was very easy."

Why Healthfirst Chose Abnormal

Abnormal's ease of use, AI-enabled efficacy, and API architecture appealed to Miller. So did Abnormal's quick integration with CrowdStrike. "With the CrowdStrike-Abnormal integration, we have higher fidelity information going back and forth, and we're getting better information right at the edge of our network so we have enriched data that's going to our SIEM. As a result, I'm getting higher fidelity alerts and the ability to automate more of the process before I alert our analysts," Miller said.

"Having Abnormal as part of my automation strategy allows my team to triage events and incidents at scale," he added. By feeding Abnormal data into Healthfirst's SOAR, Miller estimates that his machine learning stack triages "about a billion events a week" down to only 30 to 60 for his analysts to review.

An AI-Native Security Solution That Protects People

Abnormal makes life easier for Miller and his team and more secure for Healthfirst's employees, providers, and members. "My team now works at a higher level. I have a happier staff and less risk to the business. It's a lot of goodness."

Miller credits Abnormal's unique human behavior AI, which continuously evolves as new threats emerge. "A lot of vendors bolt on large language models, but effective security needs to be built with AI from the ground up. Abnormal has done that. They've created a highly-tuned AI platform that's purpose-built for longevity."

> "Abnormal prevents attackers from taking advantage of our goodwill, our trust, and the connections that we have with others. For perfect end-user security, you have to create a paranoid workforce, and that's not very productive. I'd rather use Abnormal."

Brian Miller
CISO

Abnormal Products in use:

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

abnormalsecurity.com →

Abnormal