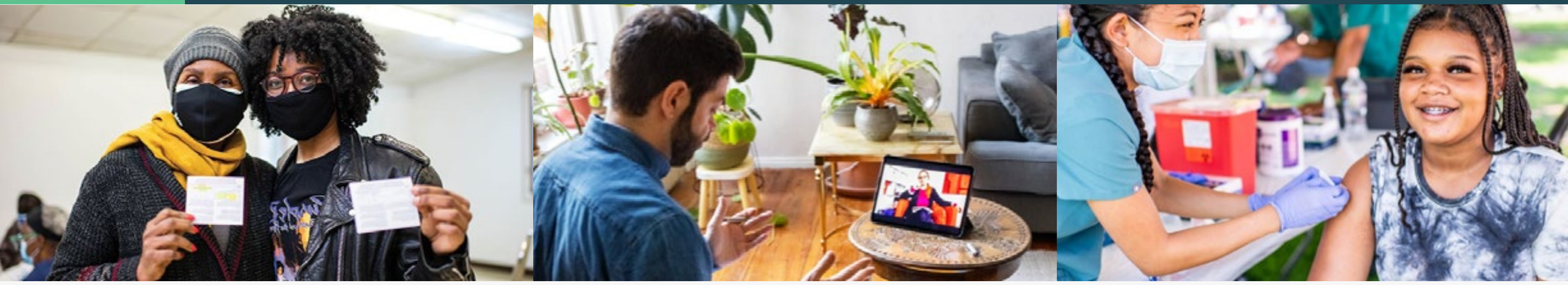
Customer Case Study



Sentara Improves Health, Security, and Trust for the Communities It Serves

Sentara Healthcare practices its mission to “improve health every day” for patients at 12 Virginia and North Carolina hospitals and for the more than 950,000 community members insured through Sentara Health Plans. The 134-year-old system has nearly 30,000 employees, including more than 1,300 physicians and advanced practice clinicians that provide a full range of services at 300+ sites of care. Sentara’s commitment to care delivery and employee experience have earned it multiple IBM Watson Health “Top 15 Health Systems” and Forbes “Best Employer” awards in recent years.

Sentara’s dedication to community health includes a focus on safety and security. “Healthcare in general is part of the country’s critical infrastructure,” said Chad Spiers, Director of Cybersecurity. “We're targeted from a ransomware perspective pretty heavily, as most health systems are. We'd been successful with our previous mail system, but spoofing emails were still getting through—especially messages from threat actors posing as vendors requesting payment or requesting wire transfers.”

“At the same time, we were migrating to cloud services because cloud-native, AI-driven, and API-based tools deliver more benefits and require less employee time than traditional perimeter security tools,” Spiers said. But after a number of spear phishing attempts, Sentara started looking for cloud-based solutions to augment its IronPort and Microsoft 365 security layers.

SENTARA®

Industry
Healthcare

Headquarters
Norfolk, Virginia

Protected Mailboxes
48,000+

Number of Employees
30,000

Financial Supply Chain Attacks Increase

Business email compromise (BEC) attacks are evolving as attackers shift from executive impersonation to vendor impersonation scams that can lead to legitimate or fake invoice payments being routed to criminal accounts. These impersonation attacks now comprise over half of all BEC attacks seen by Abnormal.

In the first eight months of using Abnormal, Sentara avoided more than 700 advanced BEC attacks that bypassed other email security layers.

> “Vendors say their integration will be easy and seamless, but we’ve found that there are usually issues. It was refreshing to see Abnormal actually deliver on that integration promise.”

Mike Freeman
Cybersecurity Manager

60+

IT team hours saved per month.

140+

compromised vendors identified.

Zero

missed attacks in the first eight months.

Adopting a Cloud-Based, AI-Driven Approach to Threat Detection

Spiers said Abnormal started demonstrating value immediately. “We knew there was going to be significant value for Sentara. Within a day of starting the proof of value, Abnormal provided us with very promising data.” In addition to identifying credential phishing attacks, Abnormal was soon uncovering vendor email compromise and executive impersonation attacks that had bypassed Sentara’s other email security layers.

“You can only go so far with signature-based detection, although that first layer of defense knocks out 90% of the threats. With Abnormal as our second layer, we can block attacks that are more targeted toward Sentara, such as social engineering invoice emails that are difficult to catch. Abnormal catches, reports, and auto-remediates them.”

Spiers added that Abnormal also accelerates detection. “Abnormal quickly acts on malicious emails because it’s all API-based, versus PowerShell scripts. It’s not another hop in the email thread, so there are fewer potential points of delivery failure.”

Freeing Resources for Additional Security Initiatives

Before Abnormal, Sentara’s cybersecurity interns dealt with a huge volume of spam that bypassed the existing filters. “We had a small army of interns to remediate more than 100 spam tickets each week, and we ran into some challenges removing email from various mailboxes in time,” said Mike Freeman, Cybersecurity Manager. “There was a lot of time spent contacting users and figuring out how to delete emails from inboxes.”

Upon integration, Abnormal started detecting and auto-remediating spam, so the interns could focus on other tasks. Once Sentara integrated Abnormal with Siemplify, a cloud-native SOAR solution, automated responses to threat reports were handled faster and results reached users sooner. “We’ve heard feedback from our users that report potential spam, and they appreciate the timely feedback that Abnormal delivers,” Freeman said.

That faster response time reinforces Sentara’s security culture. “When you don’t get a response to your reports, you might stop sending them in,” Spiers said. “So Abnormal’s fast responses were a big factor in our decision.”

Automates SOC Operations

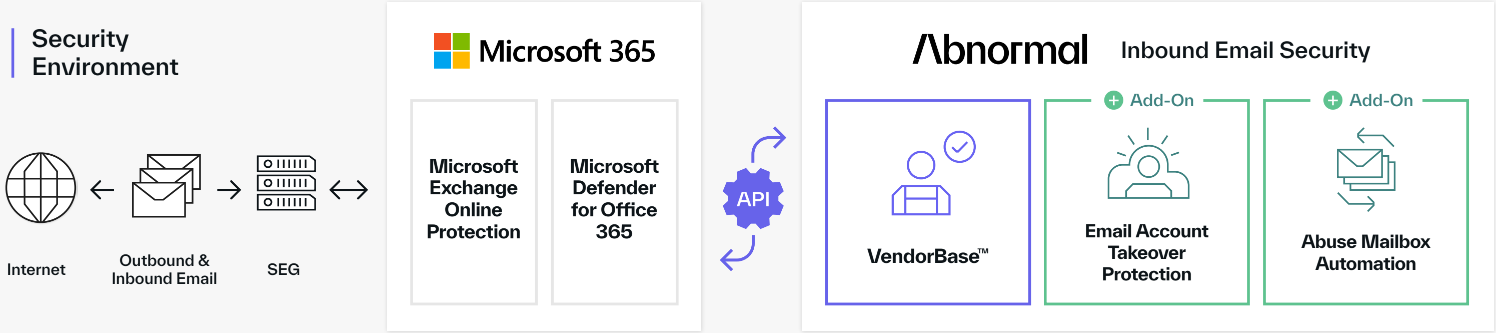
Before Abnormal, Sentara’s IT interns conducted more than 100 spam investigations each week, pulling their focus away from other security projects. Meanwhile, employee-reported threats required days to get a response.

Abnormal blocks spam and works with Sentara’s SOAR solution to quickly investigate threat reports, remediate any threats found, and send the results to the user while it’s still fresh in their mind.

31,448

spam emails auto-remediated by Abnormal over the past 90 days.

Customer Case Study



Behavior-Based Solution Enables a More Robust Security Program

After implementing Abnormal, Sentara realized multiple benefits, starting with a dramatic reduction in threats reaching employee inboxes. Abnormal VendorBase™ has also identified more than 140 Sentara vendors with compromised email accounts, which strengthens Sentara's protection from vendor email compromise and supply chain fraud.

With Abnormal's spam and graymail filters activated and auto-remediation enabled, Sentara's SOC team is freed from spam investigation. "That enables us to strengthen our security posture by having our interns and analysts work on projects like threat hunting and uncovering other indicators of compromise," Spiers said.

The shift away from manual spam-fighting also lets Sentara offer a better employee experience and maintain its talent pipeline—critical considerations in a field where demand outpaces supply. "Offering that variety of projects, not just spam investigations, helps us to develop cyber talent. We cultivate a lot of talent from our intern program to hire because in cybersecurity there's always more work than people available."

Finally, the Abnormal dashboard provides insights for trend identification and examples of real attack emails to use in Sentara's anti-phishing training. "Being able to see who's the most impersonated, for example, helps us raise awareness across the organization up to the executive level," Freeman said.

Sentara Strengthens Its Security Posture, Employee Experience, and Talent Pipeline

With reduced inbox threats, better employee email experiences, and more time to cultivate cybersecurity talent, Spiers sees multiple benefits to working with Abnormal.

"Sentara is an early adopter for multiple layers of email security, but I think it will become more common," Spiers said. "People don't understand yet how easy it is to plug in Abnormal and receive the value that an API-based security layer provides, but when they do, more people will shift that way."

Customer Support Tier

Platinum

"Abnormal has delivered on their promises to save us time and better protect our email ecosystem.
It's so easy to implement, and we never want to turn it off. "

Chad Spiers
Director of Cybersecurity

abnormalsecurity.com →

Abnormal