Customer Case Study

BSI Raises Its Security Standards With Behavioural AI Threat Detection

Global performance consultancy trusts Abnormal AI to detect advanced threats and protect critical infrastructure clients.

BSI serves over 77,000 global clients with deep expertise in standards development, certification, training, and assessment to help them become safer and more sustainable. BSI's clients come from industries such as healthcare, construction, food and retail, supply chain, energy, government, manufacturing, transportation, and technology. Originally the British Standards Institute, BSI is also the UK National Standards Body, representing the country in ISO, IEC, and other major standards entities.

The BSI Email Security Challenge

BSI has a goal of zero security incidents to maintain trust with its high-profile and critical infrastructure clients. "Almost all the clients we work with are regulated," said Mike Pitman, CISO. "We have to provide security that supports their regulatory requirements." Protecting intellectual property is another top concern. "If we're doing a medical evaluation of a client's new heart valve design, that IP data is potentially worth hundreds of millions in revenue," he added. BSI used Microsoft 365's native email security tools, but spear phishing, business email compromise (BEC), and vendor email compromise (VEC) attacks were reaching inboxes, raising risk and generating extra work for SOC analysts.

The Abnormal AI Solution

"We wanted an API-based solution that would complement Microsoft's email security with anomaly checking," said Michael Smithers, Head of Security Operations. A serendipitous meeting with Abnormal AI

bsi

Industry
Professional Services

Headquarters
London, UK

Protected Mailboxes
6,000+

Customer Key Challenges

- Supplement native M365 security to stop spear phishing, BEC, and VEC attacks.
- Protect sensitive client data to support their regulatory compliance.
- Find more time for security analysts to work on strategic projects.

Abnormal Solution

- Behavioural AI detects anomalies and autoremediates advanced phishing, email compromise, and account takeover attacks.
- Account takeover protection analyzes sender and recipient behaviour and identity data to detect and lock down hijacked accounts.
- Automated remediation and reporting tools significantly reduce malicious link clicks and email reports, saving 10+ SOC team hours per week.

> "I've been through SEG implementations at other organizations, so I know the pain of setting them up and the burden of operating them. Abnormal's API-based design didn't require us to redesign anything to deploy, so we can simply make the most of our existing M365 setup."

Mike Pitman
CISO

90%
fewer malicious URL clicks by email end users.

40%
fewer user-reported emails.

10+
SOC team hours/week saved on email investigations.

at an event was intriguing but also generated healthy skepticism. “Abnormal made some strong claims around success rates,” Pitman said, “but we were a bit cynical because we see similar claims all the time.” Smithers noted that Abnormal’s design seemed to complement rather than disrupt BSI’s Microsoft stack, which led to BSI running a proof of value with Abnormal. “The wild claims turned out to be true," Pitman said. “It definitely discovered things that M365’s native security tools missed.”

Why BSI Chose Abnormal

Abnormal’s integration and performance quickly impressed the team. "Of all the deployments I've done, Abnormal was the easiest,” said Brian Brady, Security Operations Team Lead. “And the account takeover tool has detected compromises before other security systems have.”

Smithers agreed. “We didn’t realize how much Abnormal would help us. Traditional SEGs miss advanced social engineering attacks, but Abnormal blocks them so we don’t need to run an automation or the reset playbook and require users to reset their password.”

The result is less time spent on email threat response and more confidence for BSI’s experts and clients. “Before, if an attack got through while we were at a customer site, we could lose access to everything. That wasted time and didn’t inspire customer trust,” Pitman said. “With Abnormal, that doesn’t happen.”

Stronger Security Now and More Sustainable Security for the Future

Pitman and his team are confident that Abnormal’s AI-native approach to human behaviour gives BSI a security advantage. “I think it comes down to sentiment analysis. That’s a difficult thing to develop and evolve, so it’s the differentiator for social engineering detection,” Pitman said. He also thinks Abnormal’s evolving AI-based solutions can protect BSI as security needs change. “Attacks may get so advanced that we have to verify ourselves on team chats and video calls. The ability to integrate Abnormal there will be a game-changer.”

> “Abnormal offers a more graceful way to detect and remediate malicious emails and other advanced attacks. Unlike a traditional SEG, Abnormal improves our safety and maintains our risk-averse posture while also minimizing business disruptions and saving our security analysts time.”
>
> Michael Smithers
> Head of Security Operations

Abnormal Products in use:

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

abnormal.ai ›

Abnormal