Boohoo Protects Its Brands and Saves Time and Money with Abnormal

Global fashion group adopts behavioural AI-based approach to address a flood of advanced email attacks, graymail, and spam.

Boohoo manages a portfolio of 13 fashion and beauty brands that design, source, market, and sell to millions of customers around the world through online stores. The company, founded in 2006, uses social media, celebrity brand ambassadors, and pop-culture tie-ins like the Barbie™ X Boohoo line to maintain a high profile. That visibility, plus Boohoo's multiple websites, expansive supply chain, and fast-moving operating model are essential to its success, but they also make the company an appealing target for advanced email attacks.

The Boohoo Email Security Challenge

Even with a traditional SEG in front of Microsoft 365, employees at Boohoo were receiving credential phishing, invoice fraud, and impersonation attacks, which put funds, data, vendor relationships, and brand reputations at risk. Jonny Concannon, Group Information Security Manager, wanted a better solution—one that improved security, integrated easily, and automated threat detection and response.

"The team and I wanted an AI-based approach that would look at what normal is, what abnormal is, and patterns of behaviour across the organisation. We have a big team, but we're a fast-paced organisation, so ease of integration was really important to us. Obviously, integration with Microsoft was a requirement," said Concannon. Tools that could save time on graymail and spam would also help Boohoo keep pace with trends and customer demand, while saving employees time.

boohoo group plc

Industry
Retail Apparel and Fashion

Headquarters
Manchester, UK

Employees
6,100+

Protected Mailboxes
7,800+

Customer Key Challenges

- Detect and remediate advanced credential phishing threats that put the company's data, resources, and operations at risk.

- Identify compromised vendors to prevent financial losses and protect supply chain relationships.

- Free the security team from manual remediation tasks and other employees from filtering through time-wasting graymail and spam.

Abnormal Products

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

"When Abnormal found threats our SEG wasn't detecting, we had to make a change, and Abnormal tying into Microsoft via API was gold for us. Leveraging Microsoft and Abnormal moves us away from the traditional SEG, eliminates that cost, and improves our security."

Jonny Concannon
Group Information Security Manager

Zero

Missed attacks or false positives in 30 days.

40

Security team hours per month saved on manual email tasks.

463

Total employee hours saved on graymail and spam in 90 days.

The Abnormal Security Solution

Abnormal offered the features Concannon wanted, including behavioural AI-based inbound email protection that learns normal email behaviour and detects deviations that can indicate compromise and malicious intent. AI also underpins Abnormal's graymail filtering tool to save time for employees and executives.

Abnormal's auto-remediation capabilities meant Concannon's team of four could spend less time dealing with manual remediation, remediating compromised accounts, and investigating user-reported phishing attacks. Abnormal works with the native email security tools within Microsoft 365 to provide seamless defence in depth. And because Abnormal integrates via API, setting up a proof of concept takes less than an hour, rather than the days or weeks a new SEG would require.

Why Boohoo Chose Abnormal

The proof of concept delivered results within hours. "What surprised me was the volume of advanced attacks that the SEG was missing, like compromised internal email conversations between our HR teams and our CFO. We realised we needed to do something right away. We had also been considering other security solutions, but once we integrated Abnormal so easily and saw that scary data coming through, the decision was made," Concannon said.

Abnormal's dashboard lets Concannon track threat trends, generate reports, and identify threats to use in awareness trainings. "We use it to show what our next steps should be," he said. In addition, the Email Productivity module quickly proved its time-saving value for the customer services team and the C-suite. "Arriving in the morning and not having 20 emails to file or asking us to block senders is obviously a benefit," he said.

Better Security and More Time with Abnormal

Abnormal delivers the security and time savings Concannon sought—catching advanced attacks, avoiding false positives, and identifying high-risk vendor email accounts. Abnormal Inbound Email Security, Email Account Takeover Protection, and Abuse Mailbox Automation save Concannon's team up to 40 hours per month on email security tasks, while Email Productivity saves the company more than 450 hours per quarter on graymail and spam management.

Concannon looks forward to what Boohoo's partnership with Abnormal will deliver next as the business grows and email security needs evolve. "Because Abnormal is API-integrated and AI-native, I think the possibilities are endless."

"The way Abnormal detects vendor email compromise attacks stands out. When a malicious actor took over an ongoing vendor conversation, we could see how Abnormal assessed the change of context, the slight nuances in the way the language shifted, the addition of a file with different bank details, and the fact that the attacker interjected an email address into the CC field. I've never seen these things detected by a traditional SEG."

Jonny Concannon
Group Information Security Manager

abnormalsecurity.com →