Customer Case Study

Softcat Stops Advanced Account Takeover Attacks and Saves Time with Abnormal

AI detects sophisticated threats, streamlines reporting, and improves the employee experience.

Softcat has built its IT services and consulting business upon creating great experiences for both its customers and its employees. “Our belief is that happy employees equate to happy customers,” said Mark Overton, Head of Information Security. Softcat consistently ranks in the mid-90% range for customer satisfaction, and the 30-year-old business is growing quickly—especially in the UK market. To serve its 10,000+ customers, Softcat partners with 3,000 suppliers, offering a single point of purchase for a broad range of technology solutions and services.

The Softcat Email Security Challenge

Softcat protected its email system with Microsoft Exchange Online and a SEG—a combination that worked well initially. However, as the company grew and the nature of email threats changed, Overton became concerned. “We receive a large amount of email for the size of our organisation—around 100,000 inbound emails each day—and we noticed one or two account takeover emails posing as vendors or customers reaching our employees each day. We want our employees to be working in a safe environment. We didn't want key security decisions regarding clicking a link or responding to an email to be left to them if there was a solution to prevent it.”

Softcat

Industry
IT Services & IT Consulting

Headquarters
Marlow, UK

Employees
2,400+

Protected Mailboxes
3,400+

Customer Key Challenges

- Detect advanced account takeover email threats and prevent them from reaching end-user inboxes.
- Free security analysts from responding to user-reported threats in order to focus on higher-value tasks.
- Improve executive and employee productivity by filtering out time-wasting graymail messages.

Abnormal Products

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

“Abnormal understood the problem we were facing and delivered a simple, efficacious solution that complements our existing security controls. Because AI and ML are now so important for modern email security, we have confidence that Abnormal will continue to protect us from new threats.”

Mark Overton
Head of Information Security

Customer Case Study

2,364
Employee and VIP hours saved on graymail in 90 days.

Zero
False positives in 30 days.

10
Hours saved weekly per analyst with automated responses.

Seeking a Simple (Yet Advanced) Security Solution

Overton and his team watched the email security market evolve to address the challenges faced by SEGs as threats became more sophisticated and complex. “When we had our first conversation with Abnormal, they understood the problem we faced with these account takeover attacks bypassing the SEG,” he said.

Still, Overton wanted to be sure Softcat was getting the best possible solution, so they evaluated multiple API-based vendors across the market. Their goal was to find one that would detect advanced account takeover (ATO) attacks without adding work for the security team by requiring intensive management or generating excess false positives.

Why Softcat Chose Abnormal

Because Softcat only looked at API-based vendors, it took just a few minutes to set up the proof of concept for each solution. Abnormal outperformed the other solutions in terms of detecting advanced ATO attacks and avoiding false positives, and Overton said Abnormal offered additional benefits. “We focus on protecting the identity of our users, so that if a malicious email reaches our employees, it should still be hard for an attacker to compromise a user's identity. Abnormal helps us manage the risk of malicious emails spreading from a compromised user—externally or across our organisation."

Abnormal also automates responses to user reports, so the security team has more time to work on other tasks and users don’t have to wait for a response. Additionally, Abnormal’s AI-powered Email Productivity module works seamlessly with Outlook to sort graymail into a promotions folder, saving users time on mailbox maintenance. ”It's been great to get employee feedback about how Abnormal’s graymail functionality has improved their day-to-day experience,” Overton said.

A More Secure and Efficient Email Ecosystem

In seeking a simple solution to their ATO problem, Softcat also found a solution that frees employees from the stress of inbox management and manual threat responses—and more. Said Overton, “Our initial business case was to deal with advanced malicious emails that were reaching our employees and to enhance productivity. With Abnormal, now we also feel much more confident that our organisation's risk of other threats, like business email compromise, is vastly lower as well. That's really reassuring.”

> “We didn't want a solution that would increase the amount of complexity and create a new burden for the security operations team. We also wanted a platform with really high efficacy and minimal false positives. Abnormal ticked those boxes for us and allowed us to bring an effective new layer into our security environment without overcomplicating our business.”
>
> Mark Overton
> Head of Information Security

abnormalsecurity.com →

Abnormal