Customer Case Study

Protecting Sustainable Community Development with Human Behaviour AI

Berkeley Group uses Abnormal's AI and automation to protect its reputation and business relationships from advanced email attacks.

Industry
Housing and Community Development

Headquarters
Cobham, Surrey, UK

Protected Mailboxes
2,800+

Berkeley Group creates stronger communities and healthier ecosystems by building homes, neighbourhoods, and commercial spaces in London, Birmingham, and the South of England. The company's unique approach transforms brownfield spaces into vibrant areas featuring high-quality houses or high rises and walkable green space. With a total of 89 development sites, a global team, and a large network of contractors and subcontractors, Berkeley Group has a vast business ecosystem to protect.

The Berkeley Group Email Security Challenge

Like many construction businesses, Berkeley Group was a target of phishing and business email compromise attacks. “Attackers wanted credentials and cash, so we saw lots of impersonations of our executive team," said Ash Hughes, Head of Security.

In addition to Microsoft 365’s native email security tools and a secure email gateway (SEG), the company focused on security awareness training and education. “We relied a lot on end users to report suspicious emails,” he added. “But when a user followed a compromised link, we had to respond manually to protect our data. We also needed to prevent reputational and financial damage if attackers hijacked an email chain or divert payments,” Hughes said.

Customer Key Challenges

- Stop credential phishing and BEC attacks from reaching users' inboxes.
- Reduce reliance on user reports to detect missed attacks.
- Use AI automation to give the SOC more time to manage complex cases.

Abnormal Solution

- Identifies targeted, sophisticated phishing attacks by using human behaviour AI that detects hard-to-spot indicators of fraud.
- Automates user reporting functions with AI so the security team can focus on higher risk events and other projects.
- Allows end users to trust the content of their inbox, spend less time reporting, and get faster reporting feedback.

“The context Abnormal provides—the way it tags indicators within an email, and the threat intelligence on who has interacted with the email—is so valuable. Having all that information at a glance in the Abnormal portal delivers huge efficiencies for our security team.”

Ash Hughes
Head of Security

Customer Case Study

5
Minutes required to set up the Abnormal POV.

18.9%
of attacks stopped in 90 days were text-based.

366
SOC hours saved in first 4 months on user email reports.

The Abnormal Security Solution

“We had a SEG and Microsoft, but we still had an influx of phishing attacks,” Hughes said. He learned about Abnormal's human behaviour AI approach at an event for security professionals. In addition to stopping attacks, Hughes knew that the ideal solution would make Berkeley Group’s small in-house security team more efficient. “Most SOC teams have about 45 security tools, but we needed to get the most value from three or four primary tools,” Hughes said. “We booked a half-hour call to set up our Abnormal POV. It only took five minutes, so my team got 25 minutes back right away. Within a week, Abnormal was using content and context to detect attacks we never caught with our previous tools.”

Why Berkeley Group Chose Abnormal

Abnormal detection of shifts in email behaviour has improved Berkeley Group’s security posture. “Before, we might get an alert or user report hours after the email arrived,” Hughes said. “Now we don’t have to race to investigate because Abnormal blocks risky emails from users' mailboxes, and if the platform does miss something, it auto-remediates all similar emails by pulling them from inboxes.”

The platform’s API architecture was a huge selling point for Hughes and his team. “I didn’t need to add new hardware or change our email flow. Abnormal integrated with Microsoft seamlessly, and we control that connection so we know where that data endpoint is,” he said. In addition, Abnormal’s autonomous AI enabled analysts to focus on other issues, while end users can focus on their work, knowing they can trust the messages in their inboxes.

A Sustainable Security Partnership

In addition to better email security and more efficiency, Berkeley Group now has a security partner that’s invested in helping them reach their goals as needs and threats evolve. “From day one, the Abnormal team was interested in building a relationship and understanding how they could make our experience better, including offering to make feature requests to meet our needs,” Hughes said. “The platform’s performance and ease of use, and the Abnormal team’s responsiveness set Abnormal apart from other email security providers.”

> "Whether it's QR code attacks, new malicious URL strategies, or new ways of phishing our end users, the speed with which Abnormal has detected emerging and evolving threats to keep them out of inboxes has been fantastic."
>
> Ash Hughes
> Head of Security

Abnormal Products in use:

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

abnormalsecurity.com →

Abnormal

© 2024 Abnormal Security Corporation. All rights reserved. v2.0