Customer Case Study

Mace Reinforces Trust, Builds Efficiency with Behavioural AI-Based Email Security

Abnormal helps leader in global construction save time, prevent data and monetary losses, and strengthen relationships.

Mace is a leading commercial construction and consultancy firm with operations on five continents and some of the world's best-known buildings in its portfolio. In addition to iconic construction like Battersea Power Station and the Shard, Mace creates airport, military, retail, university, and expo properties. The company also provides consulting services aligned with its mission to create "a more connected, resilient and sustainable world."

The Mace Email Security Challenge

Two trends presented growing security challenges for Mace. The first was the increase in advanced email threats that evaded the firm's signature-based defence solutions. Kirit Marvania, Digital Operations Director, said that a wave of vendor email compromise attacks highlighted the need for additional protection. "Microsoft 365 covers a lot of bases. But it doesn't necessarily have the speciality to address threats that come from trusted sources like vendors."

The second trend was a shift in security mindset. "Historically, construction hasn't been the most cyber secure industry, because in this space assets have always been bricks, mortar, and construction equipment," said Kaushik Bagchi, Head of Digital Security. "But the kind of high value, high visibility projects we do involve a lot of highly confidential data, so we have pushed to improve our cybersecurity."

mace

Industry
Construction

Headquarters
London, UK

Employees
7,200+

Protected Mailboxes
32,000+

Customer Key Challenges

- Prevent advanced vendor email compromise attacks from reaching inboxes, where users were interacting with them.
- Protect sensitive data regarding clients and high-profile projects to maintain trust and GDPR compliance.
- Enable security team to focus on key projects by reducing time spent on manual email attack remediation.

Abnormal Products

- Inbound Email Security
- Email Account Takeover Protection

"You can't rely on traditional secure email gateways anymore, because the threat environment has changed from signature-based to behavioural and language-based. Abnormal looks at each threat as a whole, including the language and the intent, and that approach sets it apart."

Kaushik Bagchi
Head of Digital Security

Customer Case Study

160
Hours of security team time saved in one month.

113
High-risk vendors identified on integration.

Zero
Missed attacks or false positives in 30 days.

The Abnormal Security Solution

Vendor email compromise was a major problem for Mace. “Our vendors were being compromised and then used as attack vectors. Our users trusted where the emails were coming from and so their guard was down, and over time there were more and more of these attacks,” Bagchi said. “We needed another layer of defence, and it needed to be smarter than those threat actors.” A Mace partner recommended that they try Abnormal, which uses behavioural and language-based AI to identify deviations from normal email content and intent, even from trusted senders.

Why Mace Chose Abnormal

Abnormal quickly proved its value to Mace. “During the trial, Abnormal picked up on business email compromise and invoice fraud coming in that put hundreds of thousands of pounds at risk. We saw that Abnormal caught these things and would automatically mitigate them,” Bagchi said. “It's not just the monetary value we would have lost, but also potentially millions of pounds in GDPR reporting costs and penalties. So the proof of Abnormal’s value was that it's a fraction of the cost of a successful attack and it provides ease of mind because it is so effective.”

In addition to Abnormal’s advanced AI and ML algorithms designed to stop attacks, its API integration with Microsoft also appealed to Mace. “The process of identifying and mitigating malicious emails is seamless. We don't have to do anything apart from look at the dashboard and see how many attacks have been caught,” he added.

A Stronger Security Foundation with Abnormal

Mace now has a dedicated partner in preventing costly advanced email attacks. “The entire Abnormal customer success team is quick to respond, effective, and knowledgeable,” Bagchi said.

Abnormal’s findings also serve as a resource the Mace security team uses to strengthen security across the supply chain. “When we find a compromised vendor, we can reach out through our supply chain team and contact them,” Marvania said. With shareable security intelligence from Abnormal, Mace has one more way to build a more connected, resilient, and sustainable world.

> “We were being hit by a multitude of invoice fraud attempts. Some came from genuine suppliers who had compromised mailboxes, and that business email compromise was spreading into other organisations. Nearly 30% of our security resources went to dealing with these sorts of threats, plus time spent by operations, legal, and data protection staff. With Abnormal preventing those attacks from reaching inboxes, we saved time equal to a full-time employee in a month.”
>
> Kirit Marvania
> Digital Operations Director

abnormalsecurity.com →

Abnormal