REA Group Partners With Abnormal AI to Secure Email and Improve Employee Experience

Behavioural AI for REA's M365 and Google email systems protects employees and brokers.

REA Group is a multinational digital business with more than 3,400 people working to change the way the world experiences property. In Australia, REA Group owns and operates Australia's number one address in property, realestate.com.au, and offers end-to-end property experiences across its portfolio of brands that connect buyers and sellers with agents and mortgage brokers. "With multiple brands in Australia, two email platforms, and totally cloud-based operations, we have a different risk profile from other organizations," said Joanna Dalton, Head of Cyber Defence.

REA Group's Email Security Challenge

REA Group was using Microsoft 365's native security tools when it acquired a mortgage brokerage using Google Workspace. "Having different types of users on each platform complicated our email reporting and response, which became very disruptive," said Rob Cumming, Executive Manager, Security. At the same time, advanced BEC and VEC attacks were getting past the platforms' native defenses, requiring more attention from the security team. "We take seriously our role as a custodian of personal information for our consumer customers and broker partners, as well as our lending partners who have specific contractual compliance requirements around data security that we must maintain," Rob Cumming said.

REA Group

Industry
Business Services

Headquarters
Melbourne, VIC, Australia

Protected Mailboxes
11,000+

Customer Key Challenges

- Find an API-based security solution that works with M365 and Google Workspace.
- Improve detection of credential phishing and invoice fraud attacks.
- Reduce the volume of phishing reports the security team must investigate.

Abnormal Solution

- Integrates easily with M365 and Google Workspace and presents data on both systems in a single dashboard for ease of analysis.
- Behavioural AI learns user habits and context in each email system to detect anomalies that indicate fraud and phishing attacks.
- AI Security Mailbox automates email report investigations and responses to save the security team 36 hours per month, on average.

"It's great to have a single pane of glass with both of our email platforms. We can see everything in one place, and Abnormal AI performs extremely well for our M365 and Google tenancies, despite the fact that the user behaviours and threats are markedly different between them."

Joanna Dalton
Head of Cyber Defence

$167K
in vendor fraud attacks detected since integration.

109 hrs
security analyst time saved in 90 days.

Two
email tenants with different user behaviour secured.

The Abnormal AI Solution

Despite the heavy security workload, REA wasn't looking for extra email security, especially not a SEG. "Email gateways are almost like a proxy in front of everything else. Multiple things can go wrong," Rob Cumming said. After three colleagues recommended Abnormal, the REA security team decided to look into it—with reservations. "When people started saying this security tool gets rid of phishing, I was skeptical," said Joanna Dalton, Head of Cyber Defence. "But I talked to friends in the industry who'd already implemented it, and they said to me, 'It's great. We turned it on. We get no phishing, and now we don't have to look at it.' That sounded like something I really wanted to do as well."

Why REA Group Chose Abnormal

CISO Marc Bown liked Abnormal's easy API-based integration with both M365 and Google Workspace. "We turned it on, let it do its thing, and now we occasionally check in, but it doesn't need a lot of maintenance," he said. The team also liked the way Abnormal's human behaviour AI tailors protection to each system to block fraud and phishing while keeping false positive rates low. "We don't want our security to block a customer getting a mortgage or a broker getting clients," Joanna Dalton said.

REA also saves time with Abnormal. The group's security analysts now spend more time on strategic projects like reporting improvements and threat hunting. "We've done some brilliant things this year that we wouldn't have had time for, had we not had Abnormal," Joanna Dalton said. And while the executive team had become adept at spotting and reporting phishing, Abnormal has freed them to focus on other work as well.

Changing the Way REA Group Experiences Security

REA Group employees now have greater phishing awareness because Abnormal automates replies to user reports. REA partners benefit from Abnormal, too. "I've called at least two organizations to let them know our Abnormal dashboard indicated they'd had a business email compromise, so they could look into it," Joanna Dalton said. Marc Bown said Abnormal reinforces REA's property experience leadership. "It's a set-it-and-forget-it win on the defence side, and it's a win on the experience side because it gives our users a more secure and easier email experience."

"This is my third time deploying Abnormal. It's one of our simplest security integrations, and it doesn't need day-to-day maintenance. As a CISO, I want more of that kind of experience. I would love it if more security products were as effective and low-maintenance as Abnormal."

Marc Bown
CISO

Abnormal Products in use:
- Inbound Email Security
- AI Security Mailbox

abnormal.ai