Customer Case Study

Stanmore Resources Transforms Its Security Operations with Human Behaviour AI

Major Australian metallurgical coal supplier replaces its SEG with Abnormal AI to stop advanced threats and protect operations.

Stanmore Resources mines specialised coal for global steel production, with operations at three major sites in Australia. To deliver 13+ million tonnes of metallurgical coal per year, Stanmore runs an advanced technology ecosystem to meet the needs of its miners, corporate staffers, and suppliers. Stanmore's entrepreneurial culture allows the organization to manage large-scale remote operations and strategic technology partnerships alongside community relationships and sustainability initiatives.

The Stanmore Resources Email Security Challenge

Stanmore used a Mimecast SEG with its Microsoft 365 email system, but the SEG struggled to detect advanced and AI-driven attacks such as executive impersonation, business email compromise (BEC), phishing, extortion, and account takeover attempts.

“A successful attack could have cost hundreds of millions of dollars through operational disruption,” said Rob Luhrs, Head of Technology. The Technology team spent much of its time triaging alerts, analysing threats, identifying false positives, remediating attacks, and tuning the SEG instead of working on strategic projects. Email users had a poor experience, and despite extensive awareness training, some engaged with attacks that reached their inboxes.

stanmore

Industry
Mining and Minerals

Headquarters
Brisbane, Queensland, Australia

Protected Mailboxes
1,900+

Customer Key Challenges

- Replace underperforming SEG with a solution to detect AI-driven threats.
- Implement automation to relieve the Technology team of email security tasks.
- Identify a scalable, API-based solution compatible with Microsoft 365.

Abnormal Solution

- Stopped advanced inbound email attacks using behavioural AI data from across company platforms to identify anomalous behaviour.
- Automated threat detection and remediation so Technology teams can focus elsewhere, and users don't find attacks in their inboxes.
- Integrated in a few steps with Microsoft 365 for scalability and fast time-to-value without operational disruptions.

> “AI Security Mailbox shows the interactive nature of Abnormal. When users report an email, they get a report back straight away. That means a lot to our users, and it’s effective education. With Abnormal automatically assessing and interacting with users who report suspicious emails, security efficiency is enhanced and, uniquely for a security solution, so is the user experience.”
>
> Rob Luhrs
> Head of Technology

Customer Case Study

80%
less time spent on email threats and responses.

$500K
saved by detecting a single BEC attack.

200+
average additional attacks detected per month.

The Abnormal AI Solution

Stanmore's leaders wanted to replace the SEG with a solution that could detect AI-enabled attacks, integrate easily with M365, and automate time-consuming email security tasks. Abnormal's human behaviour-based threat detection and automation was promising, but the team worried that integration would be a headache.

"Everyone on our team has been burned by a vendor who said, 'just plug and play'," said Peter Hamilton, Principal, Cyber Security. "But the Abnormal POV really was easy to set up without disrupting our busy program and it demonstrated value so quickly." Among the missed threats found by Abnormal was an executive impersonation attack that could have cost Stanmore $500,000.

Why Stanmore Resources Chose Abnormal

"We're very happy with the combination of M365 and Abnormal," Peter Hamilton said. "We have a better technical defence now with an added safety net of behavioural defence that complements the Microsoft ecosystem." The team is also pleased with the Abnormal dashboard's clarity. "The nontechnical language in the summary is helpful when we report upwards: 'fraud attempt, extortion, phishing attempt,'" Peter Hamilton said. "It makes it clearer to everyone the return on security investment that we're getting from this security solution."

Abnormal's behavioural AI detects an average of 200 more attacks per month than the SEG did, making Stanmore's operations more secure. At the same time, Abnormal's automation has reduced the Technology team's email-related workload by 80% while giving users faster responses to their reports and giving the team better visibility into threats.

Stronger Security, Built to Evolve as Threats Do

Stanmore's security leaders now worry less about email-related security risks, and the Technology team is focused on strategic security initiatives. Users trust the contents of their inbox and get informative feedback immediately when they have a question about a message. "By reducing our risk exposure, Abnormal also helps us with compliance," Rob Luhrs said. "Abnormal has quickly become essential for protecting our complex mining communications against advanced threats like FraudGPT and other AI-based attacks, so we're better prepared for the future."

> "Before Abnormal, we had several advanced invoice attacks detected at the last minute by our legal or financial teams rather than by our SEG. Abnormal's human behaviour AI now catches these attacks before users see them, so our data, finances, and operations are less at risk."
>
> Peter Hamilton
> Principal, Cyber Security

Abnormal Products in use:

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

abnormal.ai ❯

Abnormal