Customer Case Study

OFX Picks Autonomous AI Leader for Future-Proof Advanced Attack Prevention

Abnormal's behavioural AI helps protect OFX from evolving threats that exploit human behaviour.

OFX is an innovator in global money movement, with operations in nine countries serving enterprise, corporate, and individual clients with transfer, exchange and other services in more than 50 currencies. In an industry where trust and compliance are paramount, OFX works with dozens of regulators worldwide and values the importance of security for itself and its clients.

The OFX Email Security Challenge

OFX used the native security tools in its email system plus a SEG for additional protection. However, increasingly advanced attacks created a need for another layer of incremental threat detection. "As attack strategies quickly evolved, our executives and employees were getting more phishing emails, which was obviously suboptimal," said Santanu Lodh, OFX CISO.

"Security awareness training is critical but it's not enough to comprehensively protect our email system. I wanted to seize the opportunity to add to our current security tools and security awareness training by introducing a behavioural AI solution," he added.

Industry
Financial Services

Headquarters
Sydney, NSW, Australia

Protected Mailboxes
1,000+

Customer Key Challenges

- Identify and stop advanced threats beyond traditional SEG capabilities.
- Spend less time on SEG rules adjustment and email investigation and remediation.
- Eliminate time-consuming false positives that negatively impact the business.

Abnormal Solution

- Behavioural AI detects malicious intent in attack messages that would otherwise reach inboxes.
- Automation frees the security team from manual email investigations and SEG rule updates.
- Easy integration with other solutions provides a more holistic view of security posture.

"Attackers can use generative AI bots to continuously create threat emails. It is not humanly possible to set up rules and policies to address so many potential variations. The only way to tackle AI-generated threats is with behavioural AI protection."

Santanu Lodh
CISO

Customer Case Study

99.9%
reduction in attacks reaching inboxes.

100%
reduction in security team time spent on email analysis.

0.01%
false positives in 180 days.

The Abnormal Security Solution

OFX developed specific criteria for their next possible solution. "We wanted something that would address our existing problem and also be forward-looking. We needed a solution that allowed us to easily configure our security requirements with limited requirements for resources. And we wanted something behaviour-based rather than rules-based to pick up emails that are malicious in intent," Lodh said. "It also needed to have at least a 99.9% efficacy rate."

The security team tested four potential security solutions in parallel for a month, ultimately choosing Abnormal as the option that met those requirements and exceeded them.

Why OFX Chose Abnormal

Lodh puts Abnormal's efficacy rate at 99.9%, while it virtually eliminates false positives. He credits Abnormal's behavioural AI approach for this effectiveness. "The main problem Abnormal solves for us is people's natural tendency to trust communications from their contacts, which attackers can exploit through phishing and account takeovers. Another behavioural challenge is that we continuously hire new staff, and each new person arrives with a unique level of security knowledge. Abnormal helps protect them as they learn OFX's systems and policies."

Abnormal's autonomous AI freed the IT security team from reviewing hundreds of emails a week. And Abnormal integrates easily with other solutions. "Abnormal data gets ingested into our security stack along with telemetry from other sources, to help make it easier to detect anything out of the ordinary," he said

Security that Understands Human Behaviour

Abnormal gives Lodh what he and his team wanted in a security solution: automation, efficacy, and an advanced understanding of sophisticated threats. "Email is the easiest route for threat actors to get into an organisation, and it's easy if you can spoof an email or socially engineer an individual's behaviour. Abnormal AI solves for that and gets smarter every day."

> "We wanted a solution that performs, with the fewest hands on interactions possible. The Abnormal dashboards are intuitive and integration was easy. I'm a big advocate of Abnormal, because it gives us exactly what I wanted. We set it up and it just does its job."

Santanu Lodh
CISO

Abnormal Products in use:

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox
- Email Productivity
- Security Posture Management

abnormalsecurity.com →

Abnormal