Customer Case Study

Landmark Group Transforms Its Email Security Posture with Human Behaviour AI

Leading MENA omnichannel retail group protects its business operations, vendors, and customers by partnering with Abnormal AI.

Industry
Retail

Headquarters
Dubai, U.A.E.

Protected Mailboxes
12,500+

Landmark Group is easy to find in the Middle East, North Africa, India, and Southeast Asia. The private conglomerate owns more than 20 popular retail and hospitality brands, a sizeable omnichannel business, the largest consumer retail loyalty program in the Gulf Cooperation Council countries, and one of the biggest in India. Based in Dubai, the company has digitally transformed its network of 35 distribution centers for optimal agility, resilience, and sustainability.

The Landmark Group Email Security Challenge

Transformation was also a priority for Landmark Head of Privacy and Cyber Security Phil Lea when he arrived two years ago. Landmark's vast supply chain and 55,000 employees were vulnerable to advanced phishing and payment fraud attacks that evaded Landmark's email security tools. Spam reaching inboxes wasted time for end users and SOC analysts. These issues made it challenging to balance risk management with Landmark's growth strategy. "My goal was modernising the security stack with something that would complement our existing protection. It also needed to be scalable to manage risks as we grow by opening new locations and expanding further in Southeast Asia," Lea said.

Customer Key Challenges

- Reduce advanced attacks and spam evading existing email hygiene filters.
- Stop Vendor Email Compromise and invoice fraud attacks before they reach inboxes.
- Automate review, investigation, and remediation tasks to save SOC analysts' time.

Abnormal Solution

- Identifies advanced attacks by using human behaviour AI to evaluate identity, context, and other signals for abnormal activity.
- Improves vendor ecosystem security by detecting and remediating invoice fraud and VEC attacks, even those in progress.
- Saves 1,320 SOC team hours per year by automating threat detection and remediation, plus abuse mailbox investigations and responses.

"Abnormal's human behaviour AI and automation have helped us modernise our security and prepare for the future. Using AI to spot risky behaviour by knowing what 'good' looks like is powerful, and it naturally extends into phishing simulations and security awareness."

Phil Lea
Head of Privacy and Cyber Security

Customer Case Study

US$ 1M
Total VEC attack losses prevented in 12 months

12,000
advanced email attacks stopped per week, on average

240K
AED saved/year via SOC automation and efficiency gains

The Abnormal AI Solution

Lea sought estimates from SEG vendors, but a former colleague recommended Abnormal. “She was very positive about how it helped their business,” he said. Lea was concerned at first about the availability of localised support, but in the end Abnormal’s performance, responsive team, and value proved persuasive. “The solution was on budget, the presales engagement was stellar, and so was the ‘one click’ integration,” Lea said. “Seeing what good and bad behaviour looked like in our email system was invaluable.” Abnormal identified 78 financial fraud attacks during the POV and demonstrated its ability to evaluate messages in multiple languages, including Arabic, without high false positive rates.

Why Landmark Group Chose Abnormal

In the first year, Abnormal’s human behaviour AI detected and stopped supply chain fraud attacks totaling US$ 1M (AED 3.7M) and saved Lea’s team more than 1,320 hours on manual tasks. “The time we've saved is now creating value elsewhere in SecOps,” Lea said. “For example, we’ve increased our velocity around other kinds of security monitoring and device management.”

Abnormal’s dashboard and reporting tools also make it easy for Lea to maintain his role as a self-described “cybersecurity socialist.” “When Abnormal identifies compromised vendors, we share that information with them whenever possible,” he said. “That data supports our collaborative approach to security and helps everyone in the supply chain.” Abnormal also provides data insights that show Lea and his team where they may need to focus additional attention.

A Secure Foundation for Scalable Growth

Abnormal shifted Landmark’s security posture from manual and reactive to AI-automated and proactive. For example, Lea and Landmark now plan to use Abnormal dashboard data to modernise and customise security awareness videos for better employee engagement. “We have regular catch-ups with our customer success manager and we’re excited about future integrations into the platform for even more value,” he said. “AI has transformed our security operations so we can support Landmark's growth, and Abnormal is making that possible.”

> “Abnormal's API-based design saved time from the start. The integration was very quick, all done within Azure with minimal interaction and no need for changes to our routing or SMTP gateways. Abnormal saved us months of integration planning, testing, and change management.”
>
> Phil Lea
> Head of Privacy and Cyber Security

Abnormal Products in use:

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

abnormal.ai >

Abnormal