Customer Case Study

MIPS Prevents Gaps in Security Coverage with Abnormal AI

Medical Indemnity Protection Society (MIPS) quickly improved members' healthcare data security with human behaviour AI.

As a member-owned, not-for-profit medical / professional indemnity insurer, MIPS is committed to protecting and empowering healthcare professionals across Australia. MIPS provides government-mandated indemnity cover to doctors and dentists, ensuring they have the protection needed to practice with confidence. Beyond insurance, MIPS offers its members expert legal advice, professional guidance, and access to accredited continuing professional development resources.

The MIPS Email Security Challenge

MIPS must comply with strict regulations to protect member and patient data. "Regulation can bring challenges," said Lucian Burns, CISO, "but we take our role as custodians of our members' information seriously."

MIPS had tried many strategies to protect users from spear phishing and advanced attacks. When the traditional secure email gateway proved too resource-intensive—and Microsoft's native tools failed to stop AI-powered threats—MIPS tried a competing AI-based solution, which failed to provide relief from false positives. As contract renewal time for that solution approached, MIPS sought an upleveled AI option, with 30 days to find, test, and implement a better choice, if one existed.

mips

Industry
Insurance

Headquarters
Melbourne, Victoria, Australia

Protected Mailboxes
250+

Customer Key Challenges

- Quickly find and deploy a stronger solution for email phishing attacks.
- Maintain compliance with stringent and evolving privacy regulations.
- Reduce false positives and boost productivity for a small security team.

Abnormal Solution

- API-based design and optimised onboarding allowed MIPS to integrate, test, and implement Abnormal AI in less than 30 days.
- Easily accessible Abnormal AI documentation made it simple for MIPS to deliver required proof of data-privacy compliance to regulators.
- Human behaviour AI sharply reduced false positives without allowing attacks, so the SOC team could work on more strategic tasks.

"Our previous solution generated many false positives and increased our small team's workload. With Abnormal, we've seen a dramatic drop in false positives, so our team can focus more on improving our cyber resilience and assurance over our controls and supply chain."

Lucian Burns
CISO

Customer Case Study

20+
SOC hours saved per month on email investigations.

<30
days required for integration, POV, and onboarding.

Zero
hurdles to obtaining vendor security assurance.

The Abnormal AI Solution

Abnormal AI's API-based design and optimized onboarding allowed MIPS to integrate, test, and implement it in less than 30 days. "Abnormal was one of the best onboarding experiences we've had," Burns said. "I granted access through Microsoft 365, Abnormal set itself up, learned all about us, and started protecting." MIPS was impressed with Abnormal's focus on human behaviour. "AI isn't distracted by the desire to please, fear of loss, exhaustion, or complacency," Burns said. Abnormal's ease of integration also aligned with MIPS' desire to focus the security team on higher value work. Abnormal's accessible security documentation simplified third-party risk governance for MIPS as well.

Why MIPS Chose Abnormal

Abnormal's human behaviour AI sharply reduced false positives and attacks. As a result, the security team can work on more strategic tasks, and end users can work more efficiently with fewer microinterruptions caused by questionable emails. Abnormal integrated easily with an existing SAT application to enhance MIPS' existing phishing awareness training with immediate Abnormal feedback on user reported threats. "Keeping users informed on the threats they discover is a great mechanism to build a security culture," Burns said. Integrating Abnormal with the SIEM was also simple.

The main reason for selecting Abnormal, though, was trust. "A major data breach can threaten the existence of an organisation," Burns said. "Abnormal is reliable, when Abnormal and Microsoft Defender are in conflict on an email, we trust Abnormal."

A Prescription for Stronger Security and Trust

Abnormal's human behaviour AI gave MIPS the confidence to move forward quickly, and it helps MIPS feel better prepared for attackers using AI in precisely targeted and timed email attacks. "AI-based security is essential now, and Abnormal diligently keeps an eye on things for us," Burns said. Abnormal's customer support maintains their trust, too. "Our support experience has been best in class," Burns said. "Add to that the increased benefit with regard to security, features, and functionality, and the bottom line is Abnormal is a clear winner."

> "A reputation for data protection is key to an organisation like MIPS, and a transparent, responsible security program is crucial to maintain that reputation. The strong security of Abnormal AI, with its own dedicated AI engine, gives us peace of mind."
>
> Lucian Burns
> CISO

Abnormal Products in use:

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

abnormal.ai ›

Abnormal