

Adecco Group Secures the World's Largest HR Company with Abnormal AI

A leading workforce solutions provider fortifies email security to stop advanced attacks and automate triage of user-reported messages.

With 3,800 branches across 62 countries, Adecco Group is the world's largest workforce solutions company. It trains more than 750,000 people and helps organizations rethink how work gets done, responsibly and with a human-centric approach to AI. Through its brands—Adecco (staffing and outsourcing), Akkodis (tech and engineering), and LHH (talent development and transition)—the company supports clients around the globe.

Protecting that scale requires security that can scale with it. To safeguard its clients and its brand, Adecco Group needed email security that could keep pace with its global growth.

The Adecco Group Email Security Challenge

Email is one of the main access points for attackers targeting Adecco Group. By exploiting the human layer, the weakest link in any security chain, cybercriminals were able to bypass existing defenses. Addressing this wide attack surface became a top priority for Alex Gomez, VP, Global Head of IT Security, Risk, and Compliance, and his team. Though Microsoft Defender for Office was in place, it intercepted only 15–20% of threats. More than 80% still reached inboxes, shifting the burden of detection to employees. Users could report suspicious messages, but they required manual triage, forcing the global security operations team to limit reviews to 10–15 executives. The broader workforce received no feedback, creating blind spots and limiting opportunities to strengthen security awareness. Adecco Group needed a different approach: AI-native protection that could accurately detect advanced, socially-engineered attacks and automate response across the organization.



THE ADECCO GROUP

Industry
Workforce
Solutions

Headquarters
Zurich, Switzerland

Protected Mailboxes
82,000+

Customer Key Challenges

- 80%+ of threats bypassing existing email defenses.
- Manual triage of user-reported messages limited to 10–15 executives.
- No scalable way to engage users in suspicious emails.

Abnormal Solution

- Deploy API-native cloud email security solution that integrates natively with Microsoft 365, without a gateway or impact to mail flow.
- Detect and remediate advanced attacks autonomously using a behavioral AI approach.
- Automate the triage of user-reported messages and responding to submitted reports.

"I'm a big fan of Abnormal's behavioral approach. We had several cases during the pilot where we experienced attacks that we were able to stop. Those were moments when we said, 'We can see the value and return on investment.'"

Alex Gomez
VP, Global Head of IT Security, Risk and Compliance



Customer Case Study

\$8.7M

Total risk avoidance (USD)

205K

Advanced attacks remediated

6.9K

User reports automatically triaged

The Abnormal AI Solution

Adecco Group deployed Inbound Email Security and AI Security Mailbox at the beginning of 2025. Inbound Email Security (IES) operates behind the scenes, detecting advanced, socially-engineered attacks through behavioral baselining. AI Security Mailbox (AISM) automates the review of user-reported phishing messages while providing personalized, post-submission follow-up. Adecco has also enabled AI agent responses in AISM, which provide users with tailored feedback on their submissions rather than the canned, generic replies delivered by other tools. Recently, Adecco Group added Abnormal's Account Takeover Protection for its subsidiary to protect against internal compromises and attacks.

Why Adecco Group Chose Abnormal

Adecco chose Abnormal's AI-native behavioral protection over rule-based alternatives. IES analyzes behavior, identity, and context to precisely detect anomalies against known-good patterns, following the IES project implementation managed by Martin Sebek on Gomez's team. Adecco now autonomously blocks more than 80% of attacks that bypass MDO and tailors remediation policies across Adecco, Akkodis, and LHH, each with different risk tolerances. With AISM, Gomez and his team have scaled user-reported email triage across the entire organization, addressing user reports in multiple languages, delivering near-instant responses and contextual guidance. Gomez calls it a measurable "cultural shift" that even earned praise from Adecco Group's CEO. "His feedback was, 'You're doing the right things. It's quick and the quality of the interaction with the AI agent is great,'" Gomez recalls.

Securing Innovation Without Slowing Growth

As Adecco Group continues its transformation strategy and expands AI across recruitment, coaching, and engineering services, security must evolve in parallel. Abnormal enables the organization to strengthen its human layer without creating friction. By detecting anomalies through behavior and automating intelligent feedback, Adecco protects its global workforce while empowering innovation at scale.

"We operate three global business units with different risk appetites. With Abnormal, the ability to tailor remediation for each, pair automation with a human-risk approach, and keep a human in the middle was a true aha moment."

Alex Gomez
VP, Global Head of IT Security, Risk and Compliance

Abnormal Products in use:

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

abnormal.ai >