Customer Case Study

Human Behavior AI Security Fits TaylorMade's Passion for High-Performance Golf

Abnormal's holistic email protection lets TaylorMade's people trust their email and focus on the brand's core mission.

TaylorMade is a globally recognized manufacturer and retailer of high-performance golf equipment, golf balls, accessories, footwear, and apparel. As a company of golfers creating products for golfers, TaylorMade has built its brand on technical innovation. Their passion is helping golfers at all levels and life stages enjoy the game—whether they're kids learning to putt, recreational golfers, top amateurs, or elite professionals like those that TaylorMade partners with and sponsors.

The TaylorMade Email Security Challenge

TaylorMade's security team protects intellectual property, the supply chain, and customer data worldwide. "Social engineering through email phishing is a major threat," said TJ Lingenfelter, Associate Director, Head of Information Security and Compliance.

Despite security awareness training and the use of Microsoft 365's native email security tools, attacks were still reaching inboxes, which consumed the security team's time, eroded user trust, and raised the risk of data exposure. "We dealt with phishing-based account takeovers weekly," said Colin Self, Sr. Engineer, Information Security and Compliance. "We were concerned that if our MFA failed, it could be serious. We needed a better first line of defense."

TaylorMade®

Industry
Sporting Goods Manufacturing

Headquarters
Carlsbad, CA, USA

Protected Mailboxes
5,500+

Customer Key Challenges

- Eliminate email security gaps to detect and block advanced phishing attacks.
- Reduce SOC time spent on account takeover response and remediation.
- Achieve fast security improvements with no major engineering commitment.

Abnormal Solution

- Leverages human behavior AI to identify advanced credential phishing attacks by evaluating messages in context.
- Autoremediates attacks to prevent end users from engaging with phishing attacks that could lead to account takeovers.
- Deploys quickly via API-based integration and rapidly learns the email ecosystem's behavioral characteristics.

> "We didn't go with a SEG because we're a company of innovators and we wanted security that wasn't built on old technology. Abnormal understands today's world and the future of email security, where AI is a factor and our users' challenges keep changing."

TJ Lingenfelter
Associate Director, Head of Information Security and Compliance

Customer Case Study

365
analyst hours saved by AI Security Mailbox each quarter.

90%+
reduction in account takeover attacks.

100%
user-reported threats and spam auto remediated.

The Abnormal Security Solution

Lingenfelter and his team wanted to stop threats quickly and spend less time managing email, as this would allow them to ramp up other initiatives. They ruled out adding a SEG because it would require a considerable resource investment with no guarantee of efficacy. “We had already spent so much time setting up security in Microsoft. We didn't want to start over and risk ending up back where we were a year ago,” he said.

They also decided AI and machine learning capabilities were a requirement. "There's never a phishing email that comes in that’s exactly the same as the last, so dynamic anomaly detection was quite important," said Nathan Kelly, Sr. Engineer, Information Security and Compliance. After several competitive POVs, Abnormal's API-based solution stood out as the clear winner.

Why TaylorMade Chose Abnormal

Abnormal's AI and automation lightened the security team's email workload fast. "My engineers were able to immediately take on other projects instead of spending their time reacting to email attacks. They now also spend fewer hours on post-attack discussions with end users because attacks aren’t getting through," Lingenfelter said.

In addition, AI Security Mailbox enables end users to trust their inboxes. "With previous vendors, our users questioned the responses they received because they were often inaccurate or inconsistent. Now we get real-time, accurate responses," Kelly said.

Self said Abnormal detects attacks that other solutions would struggle with. “Abnormal has stopped quite a few targeted attacks that used multiple complex redirects to get to the initial phishing page because Abnormal focuses on the abnormal signals of the semantics of the message,” he said.

Abnormal Frees TaylorMade to Focus on Golf

Lingenfelter was impressed with how fast Abnormal improved TaylorMade’s email security. “Getting results that quickly was exactly what we wanted,” he said. Moreover, his team has confidence in Abnormal’s strength as a partner. “Whatever the next threat is, we trust Abnormal to get in front of it,” Kelly said.

Abnormal also gives TaylorMade’s people more time for the passion that drives their work. “We can spend less time on email security and more time on the range and the course,” Self said. “Better email security, better golf.”

> “We're seeing AI used to better craft social engineering and malware attacks, which are introduced through email. Abnormal understands the way AI is being used as a threat, and they know how to use AI for better mitigation and better responses. If you don't have that ability, you're way behind now.”
>
> TJ Lingenfelter
> Associate Director, Head of Information Security and Compliance

Abnormal Products in use:

- Inbound Email Security
- AI Security Mailbox

abnormalsecurity.com →

Abnormal