Abnormal

Fight Bad AI with AI-Native Email Security

To stop AI-generated attacks, security teams need an AI-native email security solution.

Attackers are using generative AI tools like ChatGPTto create hyper-personalized attacks that target the human vulnerability. These attacks are often indistinguishable from human generated content and they are invisible to traditional secure email gateways that can only stop known threats. Organizations need AI-native security tools to detect and block malicious uses of AI.

Abnormal's Human Behavior AI platform is built on an API-based architecture that ingests tens of thousands more behavior signals to deeply understand every identity in the organization. The core AI detection engines analyze and detect abnormalities in email behavior to stop and remediate even the most sophisticated AI-generated content before they reach end-user inboxes.

The Abnormal AI-Native Advantage

Understand User Behavior

Learns the behavior of every identity in the organization by analyzing tens of thousands of contextual signals and creating a risk-aware detection model unique to each organization.

Improve Detection Efficacy

Analyzes behavior signals to detect and remediate the most sophisticated email-based attacks using Human Behavior AI technologies like behavior analysis, social graphing, and natural language processing.

Automate SOC Operations

Applies AI to automate email security with minimal overhead. Human Behavior AI constantly learns to improve detection, and alleviates triage and remediation of labor-intensive tasks like the user-reported email workflow.

91% Of security professionals report experiencing AI-enabled cyberattacks in the past six months

96.9% Of security professionals acknowledge that traditional defenses are ineffective against new and emergent threats.

97.3% Of security professionals believe that AI is important to email defenses.

$4M Saved by the average organization through risk mitigation by implementing Abnormal Security's AI-native email security solution.

Why Abnormal

Holistic Email Protection: Human Behavior AI deeply understands what's normal, detects nuanced threats, and identifies anomalies in communication patterns.

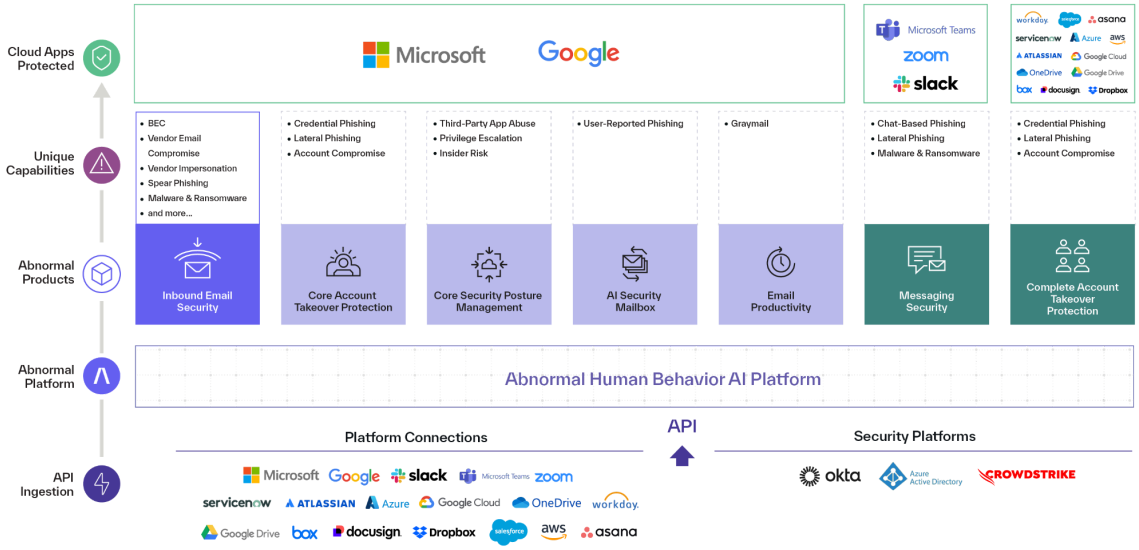
Accelerated AI Automation: Automate security across the cloud-based email platform using advanced AI that understands business context to accurately detect and remediate threats.

Uniform Cross-Platform Defense: Extend multi-layered security measures for consistent protection across communication channels, improving overall security posture and eliminating the need for redundant SEGs.

Abnormal

The Abnormal AI-Native Advantage

The API-based platform ingests 10x more behavior signals that feed the AI detection models to deeply understand what's normal, and automatically detect and remediate known and unknown attacks.



Human Behavior Modeling

Data continuously feeds Abnormal's Human Behavior AI engine to model the behaviors, interactions, and relationships of every employee and vendor associated with an organization. This profound understanding of your unique organizational context forms the basis for future detection and defense.

Behavioral AI Detection

Advanced AI techniques, including computer vision and natural language processing, compare communications patterns against established behavior norms to identify anomalous activity. Continuous monitoring of significant account activities helps extend risk analysis to encompass all aspects of an individual's email account usage behavior.

Multi-Dimensional Defense

Proactive posture management and autonomous account takeover detection across the cloud email environment provide holistic protection and a deep understanding of human behavior. This extends uniform protection beyond Microsoft and Google to other key SaaS applications like Slack, Zoom, Salesforce, and Atlassian.

"Generative AI poses a remarkable threat to email security. Abnormal is uniquely positioned to stay ahead of attackers who are using sophisticated AI to deliver malware and socially-engineered messages to our email inboxes. We're leaning into Abnormal for that expertise."

Karl Mattson, CISO | Noname Security