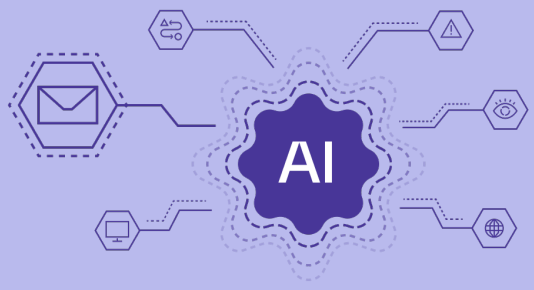
Abnormal

Fighting Bad AI with AI-Native Email Security

Attackers are exploiting generative AI to create highly sophisticated email attacks at scale. To stop them, security leaders need an AI-native email security solution.



Attackers are now using generative AI tools like ChatGPT to create content that is often distinguishable from human-generated content. By doing so, they can bypass traditional security measures that rely on detecting known threat signatures. Now, the AI arms race is on as organizations begin to realize that "good" AI is necessary to detect and block "bad" AI.

Abnormal's API-based architecture continuously feeds its AI models organization-specific signals and telemetry from internal data sources to create behavioral profiles for every identity in the organization. It then deploys its AI core detection capabilities to analyze and detect abnormalities in email behavior and remediate malicious activity before threats 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

Architecturally built to meet the critical capabilities required to detect and remediate the most sophisticated email-based attacks with technology such as behavioral analysis, social graphing, and natural language processing.

Automate SOC Operations

Applies AI to automate the monitoring, triage, and remediation of labor-intensive tasks including 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

Protect more. Detects the full spectrum of attacks, including costly business email compromise, vendor fraud, malware, and more.

Spend less. Eliminates costs of redundant software, including secure email gateways, and fully automates email security operations.

Secure the future. Provides a single, extensible platform to stop emerging email attacks, including account takeovers, attacks emanating from third-party apps, collaboration application abuse, and more.

Abnormal AI Engine

The Abnormal platform ingests, analyzes, and cross-correlates signals to detect and remediate novel malicious attacks, resulting in 4x fewer attacks.

Behavioral Modeling

Continuously and automatically trains AI models by creating complex profiles of employees, domains, IPs, devices, vendors, and applications with data across email and email-like applications to analyze risk and block even the most sophisticated attacks.

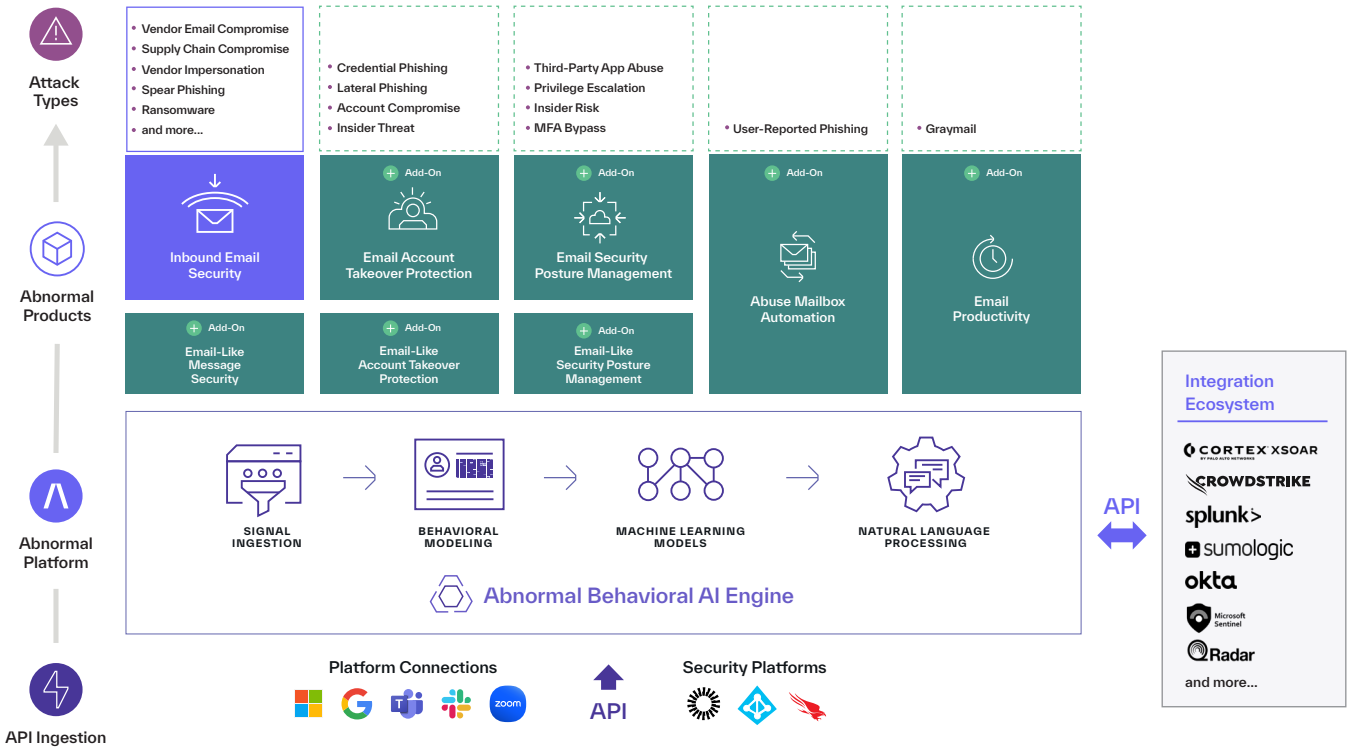
Natural Language Processing & Understanding

Uses a suite of neural network and large language models to compare profiles to raw data and detect fraudulent topics and tone and sentiment, including urgency and formality, within email content.

Social Graphing

Builds a graph of interactions between entities both within and outside of the organization to better detect deviations from normal communication patterns.

> "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



See Abnormal in Action. **Request a Demo.**

abnormalsecurity.com →