ABNORMAL AI

How AI-powered tools can future-proof email security

Behavioral anomaly detection enables agencies to protect their networks from current and emerging email-based threats

John Sourk | Abnormal AI

Email is still the top attack vector for adversaries to breach government systems. Rather than focus on exploiting a single technical vulnerability, attackers target identity, trust and mission workflows. So although humans are every organization's greatest asset, they are also every organization's greatest vulnerability. This is especially true for email, where every end user must act as a security professional while every other IT application is managed by the enterprise.

The introduction of artificial intelligence has allowed threat actors to operate at a speed and scale we haven't seen before, and the technology also allows them to create highly personalized phishing attacks. As a result, email-based threats are becoming harder for users and traditional defenses to detect.

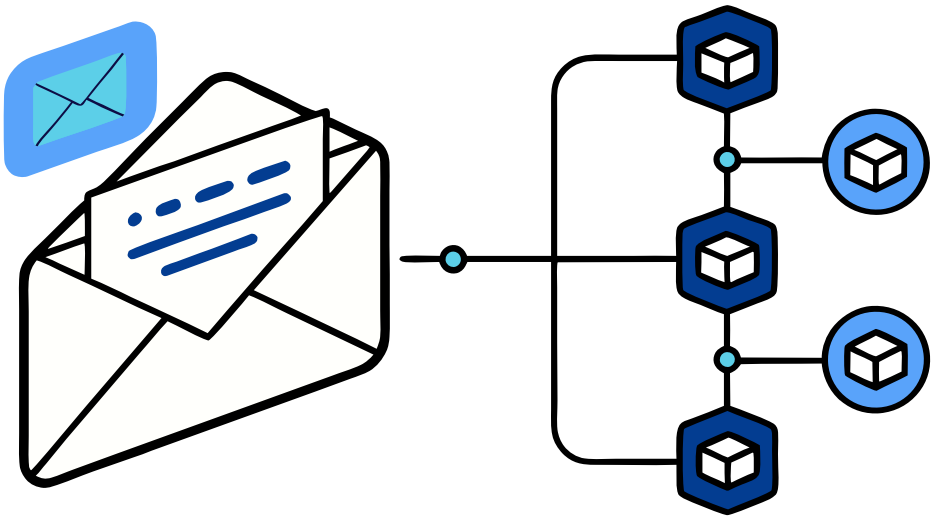
Email is a recurring lever utilized by sophisticated nation-states actors, including the China-based Typhoon clusters. In addition to traditional spear phishing, we've seen a focus on impersonating officials, contractors and trusted partners to gain access and compromise accounts to execute on their missions.

Going beyond traditional signature-based defenses

AI-powered tools give agencies a significant advantage in defending against such attacks as threat actors and adversaries leverage AI for their own purposes. In other words, good AI is required to fight bad AI.

One key way that AI can help agencies block attackers is by analyzing and understanding behavioral data. AI tools can determine a baseline for how users typically behave and then identify behavioral anomalies and potential misuse, which traditional signature-based defenses aren't able to detect. Signatures used to be a critical part of every agency's defensive strategy on the endpoint, but adversaries' tactics outpaced them, requiring a new approach. The result was endpoint detection and response. Similarly, organizations that are relying on signatures to block email-based attacks are not doing enough to stop the modern threat.

Further, AI enables defenders to work at a speed and scale that's not otherwise possible. The technology can identify tens of thousands of signals at machine speed, as opposed to a human analyst sifting through information to find relationships between data points.



Easily identifying and blocking anomalous activities

Abnormal AI's technology helps agencies establish behavioral baselines so they can protect their networks from existing and emerging email threats. That includes understanding how people typically operate, the relationships they have within and outside the organization, and how and where they work. With that

> **Rather than focus on exploiting a single technical vulnerability, attackers target identity, trust and mission workflows."**

information, the technology continually monitors for actions that fall outside those patterns.

Abnormal AI's cloud-native solution is FedRAMP-authorized and aligns with zero trust environments. It integrates with Microsoft 365 and Google Workspace in minutes and quickly begins analyzing data related to identity, behavior and content to differentiate between legitimate messages and those that pose a danger to the agency. Its ability to identify anomalies even in ongoing conversations means it can immediately detect and neutralize threats that legacy systems miss.

Behavioral anomaly detection also reduces false positives, easing the burden on resource-constrained government security teams and allowing analysts to focus on high-impact threats. By correlating contextual signals for individual users with intelligence federated across its customer base, Abnormal AI uniquely detects sophisticated social engineering attacks that evade traditional defenses. When federal agencies can easily identify activities that deviate from established baselines, they strengthen their defense against these high-impact, socially engineered attacks while allowing their employees to continue being productive.

Today, novel threats no longer make headlines. Organizations see them every day—hundreds of them in fact. By eliminating the need to write new rules and signatures each time a new threat arises, Abnormal AI's technology presents the opportunity for federal agencies to simultaneously modernize, reduce costs and improve their security posture. ■

John Sourk *is director of federal sales at Abnormal AI.*