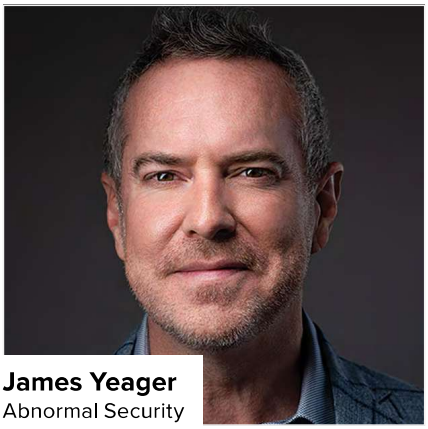
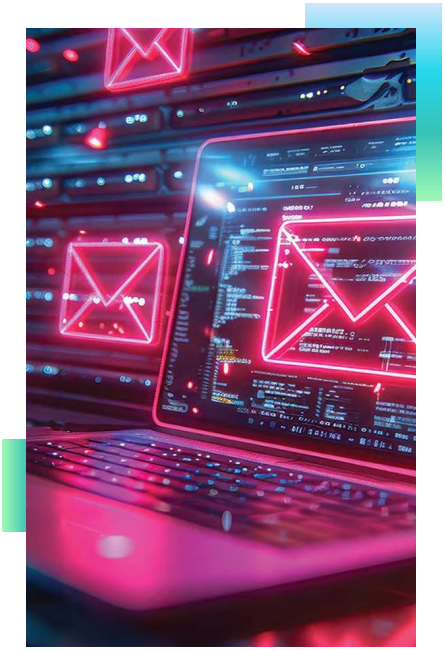
ABNORMAL SECURITY

Pervasive email-based attacks call for comprehensive security solutions

Phishing and other email-based attacks are pervasive and extremely costly for government agencies. A solution powered by artificial intelligence and fueled by automation is the only way to keep up with the volume and sophisticated nature of these threats.



James Yeager
Abnormal Security



Email-based attacks have been behind some of the most prolific breaches government organizations have faced over the last two decades. In fact, per the most recent FBI Internet Crime Complaint Center (IC3) report, phishing attacks have been the most reported types of cyberattacks for the last five years.

These attacks remain prominent because often organizations underestimate bad actors. Adversaries are determined, well-resourced, and have unfettered access to an extensive set of tools that enrich their capabilities. Because of this, organizations find themselves at a disadvantage, often neglecting to upgrade their own tools effectively in order to meet the pace and skillset of the adversary.

Moreover, bad actors now have new tools at their disposal, like generative AI, which can allow cybercriminals to create perfectly written and highly convincing email attacks at scale, improving their ability to evade both human and technology-based defenses.

And, in today's highly interconnected cloud computing world, bad actors typically only need to access just one component of a victim's cloud infrastructure to gain entry to an entire enterprise. Bad actors no longer even need to access an agency employee's account. Compromising a third-party contractor's account is often more than enough to gain a foothold, providing the adversary with the opportunity to move freely as they gain additional access to end users and their applications. This tactic, which has proven to be low-hanging fruit for the adversary community, continues to create an immeasurable amount of exposure and risk for government agencies and the contractors operating on their networks.

This all translates to a considerable and systemic challenge for government agencies, which are overmatched by threat actors when it comes to both pure human capacity and technology limitations.

Comprehensive Solutions

What agencies need are comprehensive, multi-dimensional solutions that can handle the full spectrum of email-based cyberattacks. Unfortunately, most legacy solutions, such as Secure Email Gateways (SEGs), focus on inbound attack activity. These solutions act as a proxy, sitting between the sender and the receiver and rely exclusively upon known security artifacts and heuristics to render a pass/fail judgment about whether an email should pass through to a receiver's inbox. As today's threat actors are becoming increasingly sophisticated in their attacks – often omitting known indicators of

compromise entirely – and without any attack signals to detect, SEGs are put on the backfoot.

At Abnormal Security, we have a fundamentally different approach. First, our API-based architecture allows us to get away from the sins of the legacy in-line engineering that fails customers today. It also allows us to deploy across a production environment in a matter of minutes, delivering immediate operational value to our customers.

Second, we leverage human behavioral AI to gain a deep understanding of every employee within an organization based on communication patterns, sign-in events, and thousands of other attributes. Against these behavioral baselines, autonomous AI models enable Abnormal to precisely detect anomalous activity and stop never-before-seen attacks with superhuman speed and accuracy. Our philosophy is to understand and protect humans better than humans.

As we go forward, Abnormal Security intends to become much more than a dominating force in the email security market. Our platform will drive extensible value for our customers across the broader cloud application ecosystem – not just for email, but also for SaaS and collaboration tools like Slack, Microsoft Teams, and Zoom, as well as for identity and cloud infrastructure applications.

Abnormal is strongly positioned to protect organizations across industries — including government agencies — against email-based attacks. But email is just the beginning of our journey to deliver fully AI-automated cybersecurity. ■

***James Yeager** is vice president of public sector for Abnormal Security.*

"GOVERNMENT DEPARTMENTS AND AGENCIES NEED COMPREHENSIVE, MULTI-DIMENSIONAL SOLUTIONS THAT CAN HANDLE THE FULL SPECTRUM OF EMAIL-BASED CYBERATTACKS."