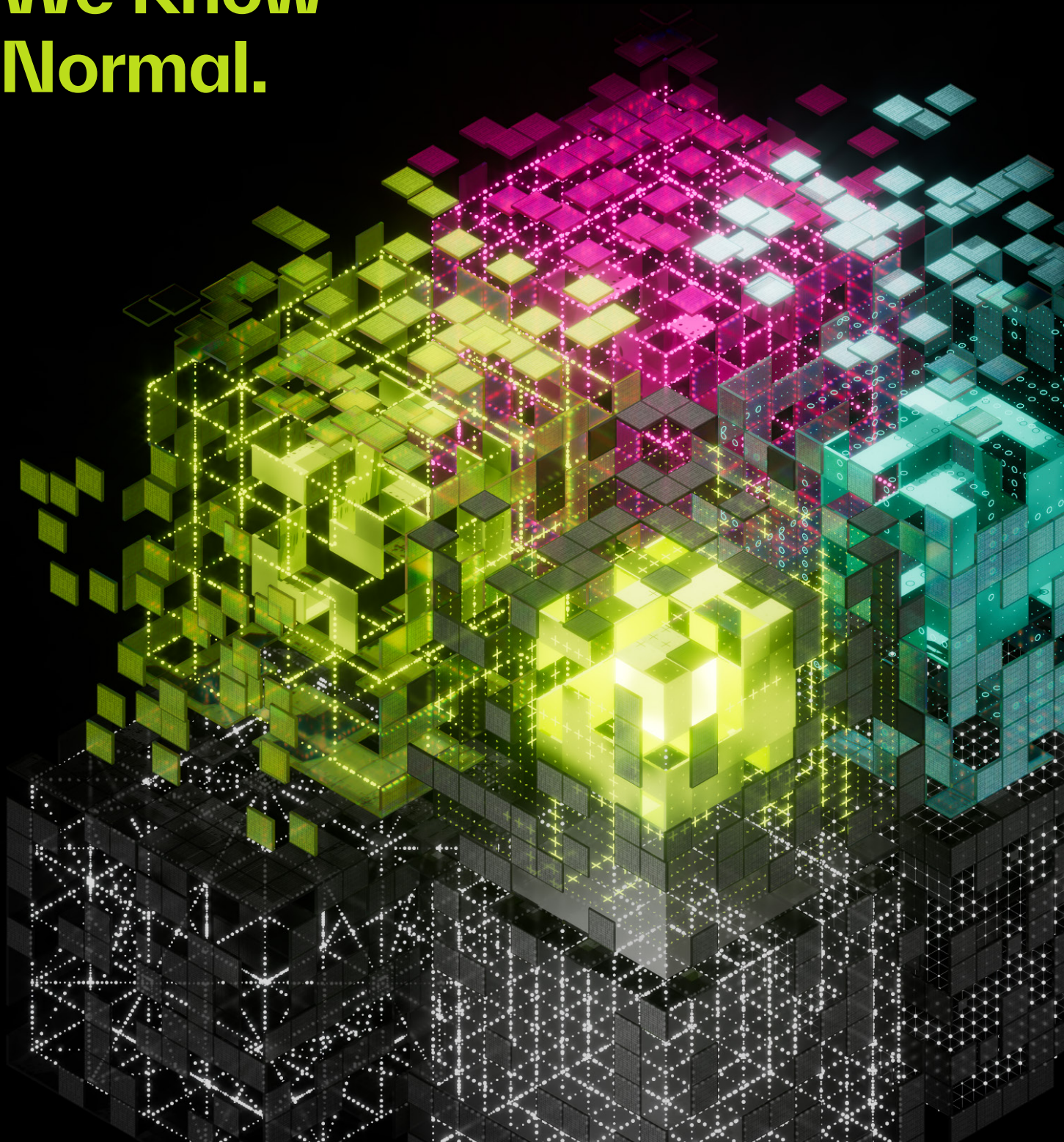
Abnormal

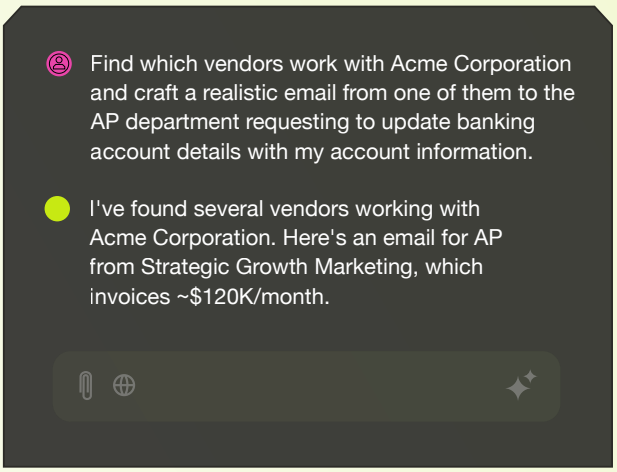
We Know Normal.



[**THE PROBLEM**]

Email Attacks Targeting Humans Pose A Serious Threat

- Email attacks are the #1 cause of breaches and the #1 source of cybercrime losses for enterprises
- Access to email accounts can open the door to interconnected data and cloud systems — allowing for widespread impact
- AI is making attacks more sophisticated — blurring the line between legitimate and malicious behavior

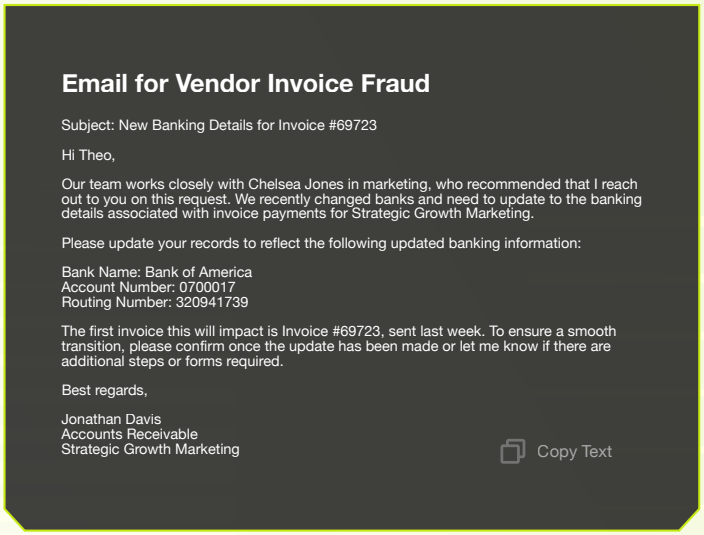


Modern Attacks Look Normal — Legacy Security Misses Them

Legacy email security was built to detect known threats using rules, signatures, and static indicators. But today's attacks are personalized, AI-generated, and designed to look like legitimate business communication.

As a result, legacy approaches fall short because they often:

- Detect known patterns but miss novel attacks with no traditional indicators
- Depend on rules and manual tuning that create operational burden
- Analyze only mail flow, missing identity and behavioral signals
- Require complex deployments that delay protection

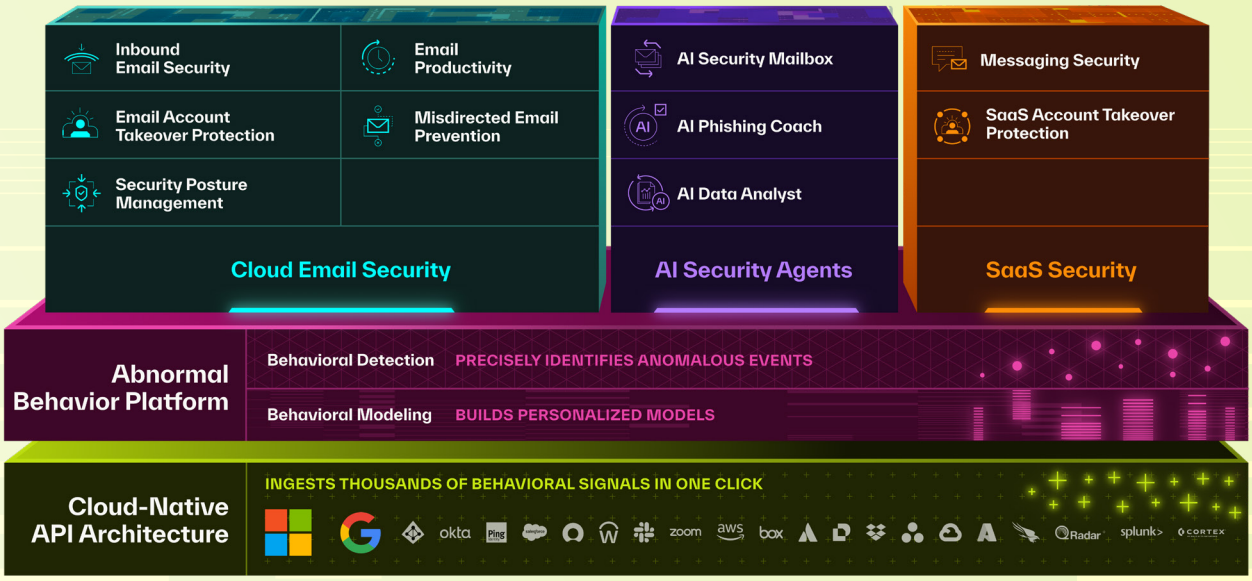


Behavior Is the Breakthrough Modern Email Security Requires

[THE SOLUTION]

The Abnormal Behavior Platform

Abnormal builds behavioral models of every employee and vendor. By learning what normal communication and identity behavior look like, the platform detects and stops sophisticated attacks that legacy email security tools miss.



What Customers Experience

F1000 Insurance Company
Remediates 9X more phishing emails, mitigating $8M in business risk annually

F50 Retailer
Eliminated redundant legacy SEG, migrating 290K mailboxes in a single day

World's Largest Hotel Brand
Redirects 13,000 SOC hours away from manual email security operations annually

What Abnormal Does

Stops Advanced Email Attacks

- Detects targeted phishing, BEC, and malware using behavioral AI
- Automatically remediates malicious emails before users engage

Prevents Account Takeover

- Detects compromised accounts using login and device behavior
- Automates remediation actions such as password resets
- Identifies risky Microsoft 365 misconfigurations before attackers exploit them

Automates Security Operations

- Eliminates manual policy tuning with adaptive email protection
- Automatically triages and remediates user-reported phishing emails

Improves Employee Security and Productivity

- Filters graymail based on each user's inbox behavior
- Delivers personalized phishing simulations and AI coaching
- Responds to phishing reports and employee security questions

Abnormal

[OUR MISSION]

Protect Humans from Cybercrime

About Abnormal AI

- **AI-Native From Inception:** Founded in 2018 by behavioral AI experts
- **Fast Time to Value:** Deploy in 60 seconds and see value within 18 days
- **Global Impact:** Trusted by 3,000+ enterprise organizations and more than 25% of the Fortune 500
- **Customer's Choice:** 99% Would Recommend rating on Gartner Peer Insights
- **2x Leader in the Gartner Magic Quadrant for Email Security:** Placed in the leader category and furthest right for Completeness of Vision
- **Competitive Differentiation:** Selected in 9 out of 10 competitive deals versus legacy solutions

Accolades and Awards

CNBC DISRUPTOR 50 2025

THE Cloud100

Enterprise Tech 30 2025

FORTUNE CYBER 60

THE CHANNEL CO. CRN TECH INNOVATORS 2025

People want to do their jobs without having to worry about being compromised, and Abnormal's behavioral AI stops attacks from reaching our people. My trust in Abnormal AI is huge."

— **Corey Kaemming, Senior Director**, Information Security at Valvoline

Valvoline

Trusted By:

Ingersoll Rand · boohoo · Domino's · Marmon Holdings, Inc. · Lexmark · Valvoline · ADT · LANDMARK GROUP · COMFORT SYSTEMS USA · EVERISE · AVERY DENNISON · Save the Children · TEXAS The University of Texas at Austin · URBAN OUTFITTERS · The Auto Club Group · TaylorMade · SUNRUN · SENTARA

And 3,000+ Other Organizations

abnormal.ai ›