Abnormal

Fortifying Cal-Secure: The Abnormal Advantage

Safeguard Golden State entities and their communications with the leading AI-native email security platform.

What is Cal-Secure?

Cal-Secure was created in response to the escalating and increasingly sophisticated cyber threats that pose significant risks to California's State Entities and critical infrastructure.

Recognizing the potential for severe economic, operational, and reputational damage from cyber attacks, Cal-Secure aims to establish a robust cybersecurity framework that proactively identifies, mitigates, and responds to these evolving threats—ensuring the safety and security of California's digital assets.

Increasingly sophisticated attacks are targeting California entities.

By exploiting new technologies like generative AI, threat actors can carry out advanced attacks faster and more efficiently than ever before. Socially-engineered threats prey on the human vulnerability to bypass traditional security measures, leading to severe disruptions in governmental operations and public services.

The evolving nature of these attacks necessitates a proactive and multifaceted cybersecurity approach, leveraging advanced technologies like artificial intelligence and machine learning to detect and mitigate potential risks in real time.

Abnormal provides the solution.

Through the power of AI, Abnormal stops attacks that target human behavior—reinstating trust in digital communications for Californians and empowering security teams to do more.

The Abnormal platform baselines known good behavior across employees and vendors by analyzing every email from every identity using thousands of contextual signals. By understanding known behavior, Abnormal can detect malicious activity that may indicate an attack.

This approach builds risk-aware detection models to stop all types of inbound email attacks, automatically constructing searchable knowledge engines with detailed profiles of the organization's employees and vendors and continuously monitoring their risk levels.

$2.9 Billion	Lost to business email compromise (BEC) attacks in 2023.
74	Percentage of data breaches that involve the human element.
$350 Million	The amount of losses from compromised vendors prevented by Abnormal in 2023.

The Abnormal Advantage at a Glance

Provides full spectrum protection. Blocks the malicious and unwanted emails that bypass other solutions, including never-before-seen attacks that do not contain traditional indicators of compromise.

Stops account takeovers. Detects internal and external compromised accounts and automatically remediates them.

Increases efficiency. Improves employee and executive productivity with adaptive protection.

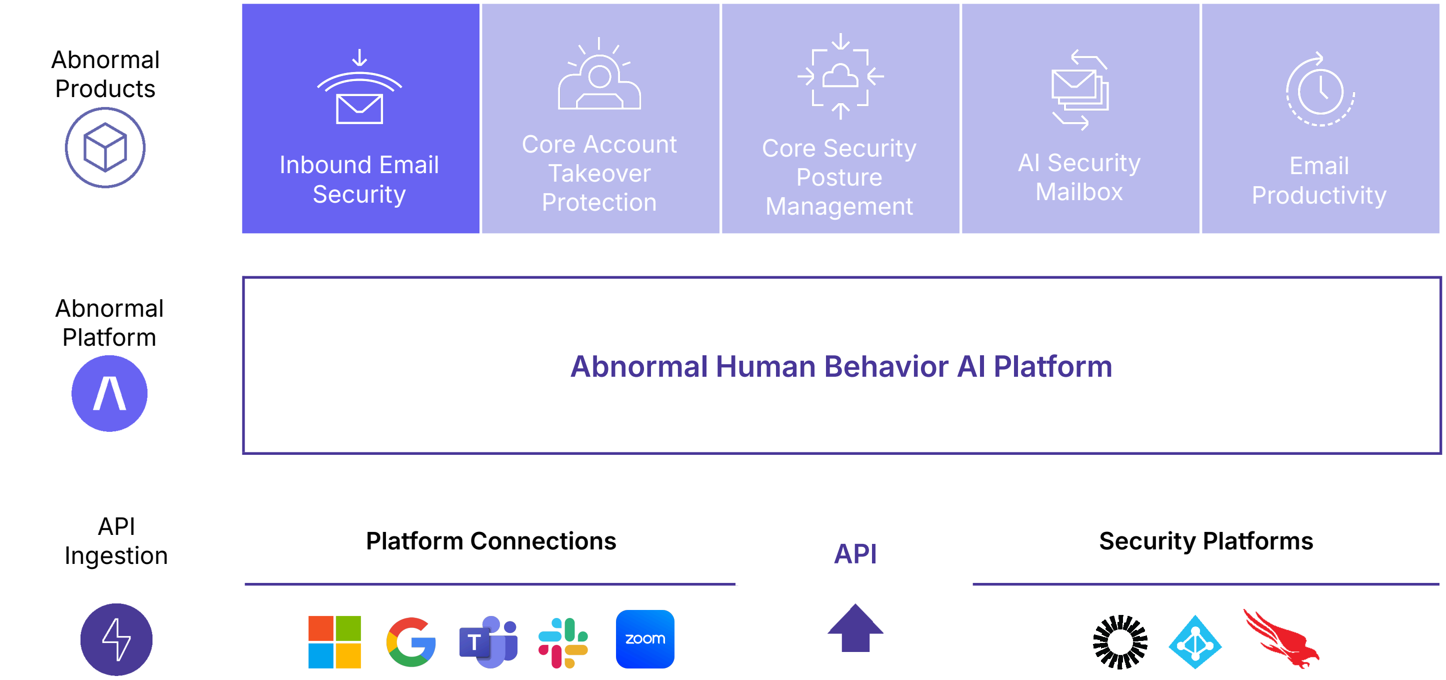
Deploys in minutes. No rules, policies or configuration needed. Abnormal integrates via API in only three clicks.

Provides multi-platform protection. Expands detection and remediation capabilities beyond email to business-critical applications including Workday, Salesforce, Slack, Zoom, AWS, and dozens of others.

Abnormal Alignment With Cal-Secure

As a cloud-native, API-based email security platform, Abnormal leverages advanced behavioral data science to stop never-before-seen attacks that evade traditional security tools. Unlike legacy email security solutions that rely on static rules and policies, Abnormal uses a fundamentally different approach to precisely detect and automatically remediate email threats.

In order to align with Cal-Secure, California's innovative cybersecurity strategy, Abnormal's technology is instrumental in safeguarding State Government email systems against sophisticated cyber threats—ensuring robust protection and compliance with the State's stringent security standards.



Abnormal Products

Inbound Email Security

Core Account Takeover Protection

Core Security Posture Management

AI Security Mailbox

Email Productivity

Abnormal Platform

Abnormal Human Behavior AI Platform

API Ingestion

Platform Connections

API

Security Platforms

The Abnormal Human Behavior AI Platform protects cloud email with the following email products:

Inbound Email Security:
Stops sophisticated socially-engineered email attacks, like business email compromise and vendor fraud, with higher efficacy by leveraging human behavior AI.

Core Account Takeover Protection:
Detects, disables, and remediates compromised accounts across email accounts.

Core Security Posture Management:
Continuously discovers and mitigates permission and configuration risks across your cloud email.

AI Security Mailbox:
Automatically investigates user-reported emails, remediates any related messages when needed, and responds to users with conversational AI for real-time security training content.

Email Productivity:
Filters time-wasting emails from employee inboxes with an adaptive and policy-free approach.

Abnormal

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

abnormalsecurity.com →