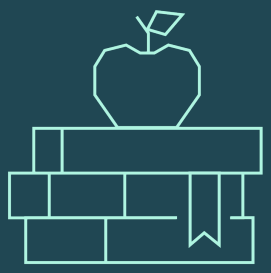
Abnormal

Protecting E-Rate Funds: The Abnormal Solution

Empower K-12 education by ensuring access to a safe and secure digital learning environment with a leading AI-native email security platform.



What is the E-Rate Cybersecurity Pilot Program?

E-Rate, an FCC program, makes telecommunications more affordable for schools and libraries, expanding Wi-Fi access to enhance digital learning for K-12 students. However, increased connectivity also heightens cybersecurity risks.

To combat these threats, the FCC launched the Schools and Libraries Cybersecurity Pilot Program, offering up to $200 million in funding over three years. Eligible institutions receive support for cybersecurity services, including training on competitive bidding, funding applications, and reimbursement processes, to help safeguard their networks and sensitive data.

Increasingly sophisticated attacks are targeting K-12 school systems.

Cyberattacks on K-12 districts are increasing, particularly as criminals target public schools for their perceived weaker defenses and their access to steady government funding.

By exploiting new technologies like generative AI, threat actors can carry out advanced attacks faster and more efficiently than ever before. Socially-engineered threats exploit human vulnerabilities, bypassing traditional security and disrupting essential education services.

To combat increasingly sophisticated attacks, schools must adopt 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.

Abnormal Security's AI-driven approach to email security is the ideal solution for protecting E-Rate funded organizations. By leveraging machine learning, Abnormal can detect and block sophisticated phishing attempts and other email-based threats that traditional security solutions often miss.

This proactive defense not only safeguards the personal information of students and staff but also helps maintain compliance with federal regulations—ensuring that schools and libraries remain eligible for E-Rate funding.

1,981 Schools across the United States impacted by ransomware in 2023.

55% of K-12 data breaches result from security issues at school district vendors.

$350 Million Losses prevented from Abnormal's identification of compromised vendors 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.

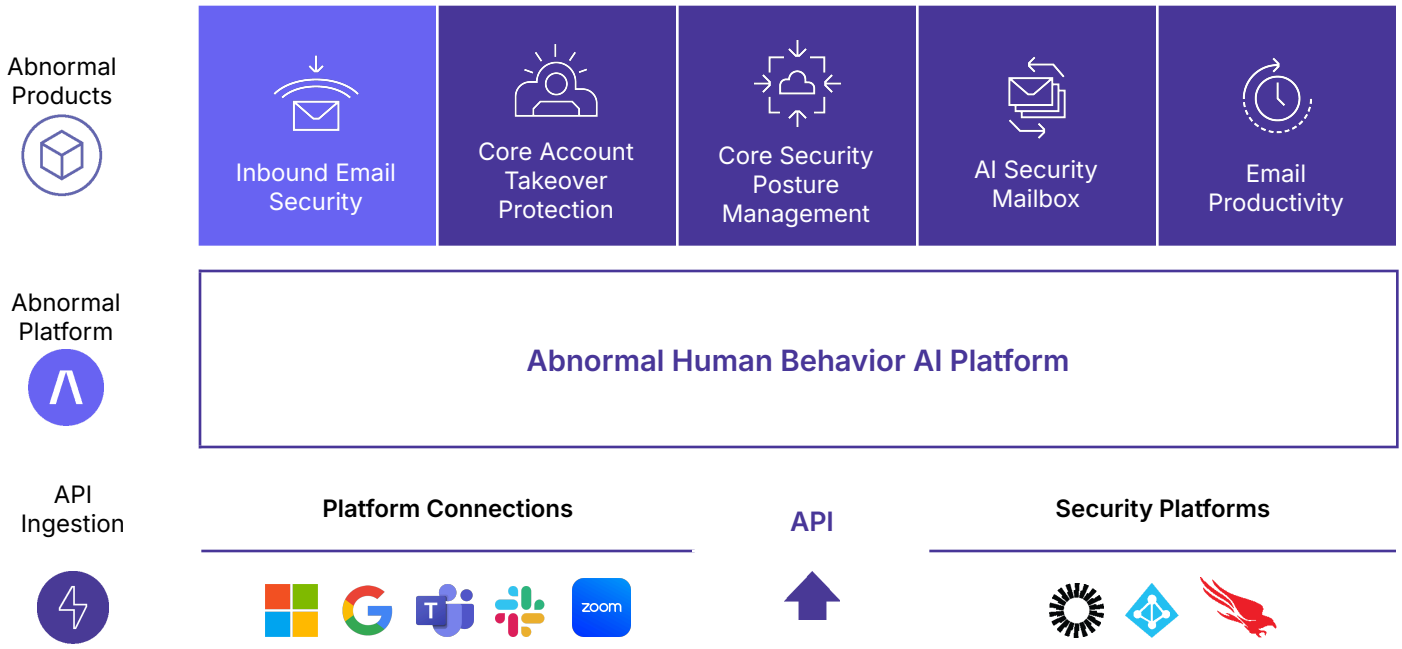
Deploys in minutes. No rules, policies or configuration needed. Abnormal integrates via API in only three clicks.

Enables 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 Enhances Security for E-Rate Funded Schools

As a cloud-native, API-based email security platform, Abnormal offers specialized protection for E-Rate funded schools by leveraging advanced behavioral data science to thwart new and sophisticated attacks that traditional security tools miss. Unlike legacy systems that rely on static rules, Abnormal uses a dynamic approach to accurately detect and automatically neutralize email threats.

Integrating seamlessly with Microsoft 365 and Google Workspace, Abnormal quickly implements its security measures, analyzing thousands of signals from identity, behavior, and content to distinguish between legitimate and malicious messages. By identifying anomalies even within ongoing conversations, Abnormal ensures that E-Rate funded schools can safeguard their faculty, staff, and students from advanced threats that conventional systems fail to detect.



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.

Email security services are expressly named in the Identity Protection and Authentication section of the *Cybersecurity Pilot Program Eligible Services List*, making Abnormal Security an eligible service to purchase as part of the FCC E-Rate Cybersecurity Pilot Program.