Customer Case Study

School District Increases Automation and Email Protection with Abnormal

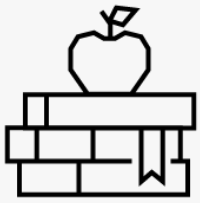
Large K-12 school district enhances automation and improves visibility into attack trends while reducing malicious messages in inboxes.

As a large organization located in a major East Coast metropolis, this K-12 public school district is a prime target for bad actors. Ensuring email attacks never make it to inboxes is among the district's top cybersecurity initiatives, as this helps protect student and staff data by limiting opportunities for individuals to engage with malicious messages.

The K-12 District's Email Security Challenge

In March 2022, the district transitioned all email accounts to Google Workspace, protected by the Cisco Ironport secure email gateway. "We had Google, but we were still using Ironport for email analysis. It didn't really work," said Andrew, Deputy Chief Information Security Officer. Disappointing results and missed attacks prompted the district to remove the SEG.

This meant the district was protected only by the native security within Google Workspace. "With Google's native tools, lots of basic attacks get through," said Andrew. "We were dealing with attacks all the time, many that we had to remediate manually. Visibility into the attacks targeting us was really poor as we only knew what was reported. If Google isn't catching something, there's no ability to know that an attack is occurring." The district knew it needed better protection and greater visibility into its threat environment.



Industry
Education

Location
East Coast, USA

Employees
20,000+

Protected Mailboxes
270,000+

Customer Key Challenges

- Stop the attacks that bypassed native security tools within Google Workspace.
- Limit the number of phishing and vendor compromise attacks landing in student and staff inboxes.
- Increase visibility into the district's attack trends.
- Reduce employee and security team time spent on manual remediation.

Abnormal Products

- Inbound Email Security
- Email Account Takeover Protection
- Abuse Mailbox Automation

"Abnormal gives you a lot of insight into your threat landscape. I now know who my big targets are, who my most vulnerable users are, and I can map my users to their email risk in a way that I never could before."

Andrew, Deputy Chief Information Security Officer

Customer Case Study

3,471
Credential phishing attacks detected and remediated in 90 days.

17,959
Attacks detected over 90 days.

170
Invoice fraud and BEC campaigns stopped over 90 days

The Abnormal Security Solution

Andrew knew another layer of protection was needed and wanted this new tool to seamlessly fit into the district's environment. "I was looking for a platform that hooked into Google's API. That was the most important thing to me. I didn't want to put a piece of hardware in place when we had cloud-native email."

Additionally, Andrew wanted a tool that could offer visibility into the threat environment while also limiting the number of hours his staff spent dealing with email attacks. "I was looking for something that could automate the remediation and research at a basic level so my team could focus on other priorities."

Why the District Chose Abnormal

Andrew discovered Abnormal at a conference and initiated the proof of value process. Through the POV he discovered "Abnormal did what it said it would. It showed a scale of how often we were targeted and how we were targeted, the missing piece we were looking for in a new solution." While Andrew had some insight into their security posture, Abnormal provided a much clearer picture of their threat environment.

Following a massive breach at a fellow school district, Andrew's superiors grew worried about the possibility of seeing their name in similar headlines and recognized the immediate need for a proactive solution—encouraging Andrew to make a quick decision. Based on the POV, Andrew knew Abnormal was right for the job. "We could deploy overnight and immediately reduce our chances of a successful attack." Since implementing, the district's leadership is confident they are protected from seeing their name in similar headlines.

A Relationship Built on Learning

The district and Abnormal have developed a strong relationship since implementation—one that goes beyond Abnormal simply reducing the number of email attacks found in inboxes. Andrew appreciates that Abnormal truly listens to customers when rolling out enhancements and shaping the solution. "I say 'Hey, your products should do this' and Abnormal has responded by developing a number of enhancements, often with my input and ideas included. With most big security companies, that doesn't happen, so I really enjoy getting to help shape the roadmap."

"Abnormal's ease of deployment is incredible and lets you immediately start fixing your problems.

A lot of vendors say their solution is easy to deploy, but often that's not true because each environment has customizations and is unique. But if you have Google or you have Microsoft 365, Abnormal just turns on and it just works, which is great."

Andrew
Deputy Chief Information Security Officer

abnormalsecurity.com →

Abnormal