Customer Case Study

Avery Dennison Automates Email Investigation and Response, Enhances BEC Prevention

Materials science and digital identification leader saves time and protects vendor relationships with Abnormal for Google Workspace.

Avery Dennison provides classic labels for clients across more than a dozen industries, as well as smart packaging and RFID-enabled labels for better visibility and safety in retail, logistics, and food production. The Fortune 500 company also manufactures specialized adhesive products for the construction, electronics, auto, and medical industries. The company's 36,000+ employees operate in more than 50 countries across six continents.

Avery Dennison's Email Security Challenge

With so many employees, plus thousands of vendors and customers, the security team has a major task in preventing advanced attacks and minimizing mail flow interruptions. "Protecting our adhesive and RFID product intellectual property is critical, and producing at the volume we do requires 100% uptime," said Jeremy Smith, VP and Information Security Officer, who manages security operations with a team of six.

Google Workspace provided the cloud email functionality the company needed, but there were security challenges. "Our vendors were being compromised and sending us phishing messages from those accounts. Overall, Google does a decent job of hygiene, but they didn't have much context about past messages to detect these external threats," Smith said.

AVERY DENNISON

Industry Manufacturing	**Headquarters** Mentor, Ohio, USA
Employees 36,000+	**Protected Mailboxes** 30,000+

Customer Key Challenges

- Free up security team time spent on manual email attack investigation and remediation.
- Stop phishing and BEC attacks that were bypassing native Google security.
- Reduce supply chain risks from correspondence with compromised vendors and customers.
- Identify an API-based security solution optimized for Google Workspace mail flow and reporting.

Abnormal Products

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

> "Investigation and remediation were very time-consuming for our team. Abnormal automated our manual processes and provided more efficacy at the same time. That allows us to focus our security resources in other places."
>
> Jeremy Smith
> VP and Information Security Officer

40
Security team hours saved each week.

358
BEC attacks detected and prevented within 90 days.

330
High-risk vendors identified.

The Abnormal Security Solution

"When we first started looking, Abnormal's API-based approach really interested us. Abnormal also offered automation capabilities that could reduce the amount of manual work we had to do on investigations and remediation," Smith said.

The Abnormal proof of value was quick to set up and to deliver results. "We provided the API key to our Google Workspace environments, and Abnormal quickly started learning. We gave it a week or two to go back through our email logs and analyze that traffic. Abnormal was able to find a number of compromised vendors that were sending us messages. We could see instantly what Google was not able to detect and what Abnormal could."

Why Avery Dennison Chose Abnormal

The ability to detect compromised vendors is critical for stronger security and relationships. "When Abnormal detects a vendor compromise, we contact those vendors and let them know. It happens fairly often because they tend not to have the same level of security controls as a Fortune 500 company like Avery Dennison," Smith said.

The team now has enough time to do this because Abnormal has automated many of the tasks they used to do manually, starting with an integrated phishing reporting button in every employee's Gmail inbox. "Before Abnormal, when we analyzed a message and determined that it was malicious, we had to login to our other security tools to put blocks in place. Then we had to search for and remediate each instance of the message in our email system. It was very time-consuming, but with Abnormal, there's no longer a need for our security team to manually manage those emails," Smith said.

Abnormal Enhances Security and Efficiency

With email security on autopilot, Smith's security team has gained 40 hours back each week to focus on more strategic projects. "Having that time allows the incident response team to work on things like better tuning our SIEM, better detection capabilities across the organization, and better efficacy across all of our tooling." Smith also said the Abnormal customer response team has helped Avery Dennison to easily make minor tweaks as needed. "Working with Abnormal has been a great partnership from the start."

> "Abnormal recently detected an attack in which a compromised vendor was receiving messages from an Avery Dennison impostor account. They were about to pay a fake $200K invoice.
>
> Abnormal helped us save our vendor $200K, which showed them how our use of Abnormal adds value for them, too. We also got positive feedback for having a well-defined incident response process and an organized instant response team."
>
> Jeremy Smith
> VP and Information Security Officer

abnormalsecurity.com →

Abnormal