Customer Case Study

Agriculture and Consumer Company Improves Overall Security by Replacing a SEG with Abnormal

AI-based threat detection, automated remediation, and resource savings enable better, more cost-effective security.

This leading company knows how to build value across a diversified business ecosystem. The company produces several well-known consumer brands, but the company's scope extends far beyond a single category. Their operations include regenerative organic certified farms; farming and milling in several countries; sustainable consumer packaging and renewable energy production from crop waste.

The Company Email Security Challenge

The company continuously improves its security by following the NIST and MITRE ATT&CK frameworks. "We're always looking at new technology, because legacy ways aren't always the best anymore," said the CISO. One example was the company's secure email gateway. Installed in front of Microsoft 365, a traditional SEG was failing to catch hijacked conversations and other advanced attacks. As a result, the company used time-consuming backstop procedures to prevent business email compromise attacks like payroll diversion and invoice fraud.

"Any request to update payment data went to an IT team that would spend 3-4 hours validating its legitimacy. If there was an incident, the security team would spend at least 20 hours resolving it. The SEG's cost and questions about whether it was furthering our NIST and MITRE goals prompted us to look at other options," said the CISO.

Industry
Agriculture & Forestry

Headquarters
USA

Employees
10,000+

Customer Key Challenges

- Replace a traditional SEG that wasn't stopping advanced threats, especially BEC attacks like payroll diversion and invoice fraud.
- Reduce the time spent by security analysts on manually investigating and remediating user-reported emails and threats.
- Find a solution that would work well with Microsoft 365 and support the company's progress toward security framework goals.

Abnormal Products

- Inbound Email Security
- Account Takeover Protection
- AI Security Mailbox

> "Abnormal saves us time, improves our security, and eliminates our need for a SEG. Switching to Abnormal allowed us to reallocate 60% of our former SEG budget to buy additional solutions to address our other security needs."
>
> CISO

32

Security analyst hours saved per month on user-reported email investigations.

Zero

Missed attacks or false positives in 30 days.

60%

Cost savings with Abnormal compared to the SEG.

A POV That Delivered on Its Promises

The CISO decided to run an Abnormal POV, though he was initially skeptical of claims about Abnormal's ease of deployment. "They said it would take 15 minutes to set up and 24-48 hours to start seeing results—and it did. It also hooked into our environment in the backend, so we avoided the DNS and routing changes that can bring down mail systems during POV setups."

Abnormal quickly started catching attacks that the SEG and Microsoft 365 had missed. One was an intrusion into an ongoing conversation with a vendor by an attacker using a lookalike domain. "After reviewing the results and getting reviews from other Abnormal users, there was no reason to keep using our SEG," said the CISO. "Abnormal caught every single attack that sought to change account details, and much more."

Freeing Up Security Resources with Abnormal

The CISO saw that adopting Abnormal would allow the company to deprecate the SEG, which the company did within a week of activating Abnormal. "We were able to reduce our SEG budget by 60% and use that money to buy other security solutions."

In addition to stopping more attacks, Abnormal's automation features save the company more than 30 hours a month that a security analyst used to spend investigating and responding to user-reported phishing emails. Now, the analyst has time for more challenging projects and professional growth. "Before, that was a manual process and a nightmare, and 99% of the time the messages were spam but not malicious. Abnormal allows the team to work more efficiently, and end users have noticed fewer questionable messages reaching their inboxes."

Creating Value Through Stronger Security

Further, Abnormal's dashboard and reporting tools help the CISO easily notify executives when they're being targeted, add email data to the monthly security scorecard, and report to the Board of Directors. By saving the company time and money, Abnormal helps the company pursue its security framework goals while protecting against advanced email threats—and show that ROI.

The CISO believes any security leader who's worried about the evolving nature of email attacks should consider Abnormal. "Try it and see for yourself. It only takes 15 minutes to set up, and you'll be surprised by what's getting through your current solutions."

> "The SEG is dying. Generative AI makes it easier and faster than ever to craft realistic-looking email attacks, even without coding skills or the resources of state sponsorship—and it's going to get worse before it gets better. If we don't have something innovative pushing the boundaries and stopping these attacks, we're going to fall behind. Abnormal's AI engine gives us an advantage against new threats that SEGs can't provide."
>
> CISO

abnormalsecurity.com →

Abnormal