Customer Case Study

Valvoline Inc. Replaces SEG with Autonomous AI to Stop Evolving Threats

Abnormal positions automotive services giant to stay ahead of sophisticated attacks and accelerate their AI initiatives.

Valvoline Inc., a Fortune 1000 company, leads the industry with automotive service innovations that simplify preventive vehicle maintenance. After recently selling its products division, Valvoline's priority is increasing sales at its 1,900+ Instant Oil Change locations across North America. “Our growth focus requires us to modernize our technology and be data-driven,” said Corey Kaemming, Senior Director, Information Security. “From a security standpoint, we have to move fast to keep up with the changing attack tactics.”

The Valvoline Inc. Email Security Challenge

To protect company and customer data, Valvoline used a SEG in conjunction with Microsoft 365’s native security and an API-based solution. Despite using three solutions, email attacks still consistently reached inboxes. “There was a lot of spear phishing and impactful invoice fraud—everything from $5,000 to millions. We put a focus on cybersecurity awareness and training, but humans will always make mistakes,” Kaemming said.

It was clear that Valvoline needed a different cloud email security solution—one that could more effectively detect and stop malicious emails, deploy easily, and automate tasks so Kaemming’s team could spend less time on manual investigation and remediation.

Industry
Retail

Headquarters
Lexington, KY, USA

Employees
10,000+

Protected Mailboxes
9,100+

Customer Key Challenges

- Stop costly and sophisticated attacks evading multiple existing solutions (SEG, M365 and API-solution).
- Optimize security operations to free up valuable SOC resources.
- Overcome reliance on employees to spot and report malicious emails.

Abnormal Solution

- Abnormal AI baselines Valvoline’s human behavior patterns to stop the full spectrum of email attacks.
- AI Security Mailbox acts as a security operations co-worker triaging user reports and enabling SOC team to focus on higher-priority projects.
- Abnormal AI automatically stops attackers from exploiting the human vulnerability of Valvoline employees by precisely identifying inbound email attacks and account takeovers.

“Attackers already use AI for greater impact, so you need solutions that improve as attacks evolve. Abnormal’s been ahead of the behavioral AI game, and as attacks become more refined, Abnormal will be there to help us.”

Waldon Smith
CSIRT Manager

Customer Case Study

$600K
Saved by stopping a recurring invoice fraud attack.

480 hrs
Analyst hours saved per month on email and solution management.

2
SEG and API-solution replaced by Abnormal enabling consolidation.

The Abnormal Security Solution

As a prior customer, Kaemming had first-hand experience with how Abnormal's AI products are highly effective at stopping the full spectrum of email attacks and was confident that Abnormal would be the right solution for Valvoline. The Proof of Value quickly delivered impressive results. "After Abnormal trained on our environment, I saw how high fidelity the alerts were, compared to the other solutions and our own digging," said Waldon Smith, CSIRT Manager. Abnormal's ability to detect malicious QR codes also stood out. "We first implemented Abnormal when QR code attacks were steadily increasing, and Abnormal was on top of it. Our other solution was noticeably behind Abnormal in catching attempted QR code attacks."

Why Valvoline Inc. Chose Abnormal

Abnormal's AI-native detection and automation capabilities have enabled the security team to reallocate their time to other tasks. "The total cost of ownership for our SEG and the other API-based solution was very high because they weren't set-it-and-forget-it tools. We'd had four to five analysts spending 90% of each day on email-related tasks; Abnormal allowed us to get away from that manual work," Kaemming said. The company has since removed its SEG. Additionally, with AI Security Mailbox, users receive quick, personalized replies to their report submissions, improving threat awareness and encouraging ongoing reporting. The Abnormal dashboard also allows the team to identify attack trends, and Abnormal's seamless integration with other tools like Valvoline's SIEM supports cross-platform data utilization.

Accelerating Growth and Security

Kaemming is confident about Valvoline's long-term security posture because he knows Abnormal was designed to evolve with the threat landscape. "When I look at Abnormal, I'm impressed by how long they've been using AI and machine learning and by their record of continuous positive change." Perhaps most importantly, Valvoline employees and VIPs can trust that their inboxes are protected from email threats. "Our goals are to get away from being so reliant on human judgment and leverage AI to be proactive. Abnormal helps us with those goals," said Kaemming.

> "People want to do their jobs without having to worry about being compromised, and Abnormal's behavioral AI stops attacks from reaching our people. My eggs are all in the Abnormal basket. My trust in them is huge."

Corey Kaemming,
Senior Director, Information Security

Abnormal Products in use:

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

abnormalsecurity.com →

Abnormal