Customer Case Study

Marmon Holdings, Inc., Secures 120+ Unique Networks with Single Autonomous AI Solution

Global industrial group sought to unify, automate, and strengthen protection from AI-based attacks across all its holdings.

Industry
Manufacturing

Headquarters
Chicago, Illinois, USA

Employees
30,000+

Marmon, a Berkshire Hathaway company, represents the power of strong networks and trust. Based in Chicago, the holding company owns 120+ manufacturing companies that span 11 global industry sectors, managing them using a decentralized model that allows each company to maintain a high level of independence. “This approach allows our companies to stay closer to their customers and to pivot when a market changes,” said Jeff Deakins, Marmon’s Director of Information Security and Infrastructure.

The Marmon Email Security Challenge

The independence of Marmon's companies made it a challenge to enhance, optimize, and future-proof more than 120 unique networks, especially since each had its own security stack. “We have every SEG known to man, but threat actors are targeting manufacturing more with things like ransomware, and we never want to lose factory availability,” Deakins said. “Approximately 50-60% of those attacks are initiated through phishing, but traditional SEGs can’t look at the context of what’s in an email to block them." As a result, analysts were overwhelmed with user-reported emails. "We needed an intelligent, automated control plane across all our environments to provide an effective and consistent security posture.”

Customer Key Challenges

- Apply one AI-based security layer across 120+ security stacks.
- Find and stop behavioral threats missed by SEGs and M365 security tools.
- Save time by automating user-reported email investigation and response.

Abnormal Solution Impact

- Integrated easily and immediately via API to unify visibility, automation, and human behavior AI security across the organization.
- Experienced zero missed attacks and zero false positives in 30 days across all tenants.
- Saved an average of 112 hours of security team time per month with reporting and response automation plus 1,600+ inbox management hours across the organization.

“Increasingly, threat actors will use large language models to increase attack sophistication through things like customized real-time phishing emails based on something like a target’s LinkedIn profile. The only way to combat that social engineering is with a product like Abnormal that uses AI to understand email content and context.”

Jeff Deakins
Director, Information Security and Infrastructure

Customer Case Study

120+
different security stacks protected by Abnormal.

Zero
missed attacks or false positives in 30 days.

112
analyst hours saved per month through automated investigation.

The Abnormal Security Solution

"We wanted consistency in how we filter emails, respond to events, and remediate malicious emails across systems," Deakins said. Abnormal's automation capabilities, human behavior AI, and easy integration made it a candidate. During the proof of concept, Deakins said he was surprised by "the amount of emails that Abnormal identified as malicious that our SEGs were just not able to see."

Abnormal's API design also allows it to monitor internal email communications to prevent the lateral spread of attacks, which SEGs can't do. "These capabilities position us to prevent what's going to happen over the next couple of years with threat actors using AI to do spear phishing on a large scale," he said.

Why Marmon Chose Abnormal

In addition to stopping more attacks than the SEG could, Abnormal's AI Security Mailbox also factored into Marmon's decision, since its help desk team was swamped with user reports. "AI Security Mailbox automates that 100%, so we don't spend any time on it. The user reports it, and if it's malicious, Abnormal just removes it from inboxes," Deakins said. AI Security Mailbox can also provide feedback to users on each of their reports. "The solution can actually point out what in the email is malicious, which is really the ability to coach and drive security awareness," he added.

In addition to saving the security team more than 110 hours a month, Abnormal also saved 1,300+ employee hours and 300 VIP hours in 30 days through AI-based graymail filtration on the 42% of the company's mailboxes for which Email Productivity is already active. During that time, Abnormal missed no attacks and generated no false positives across the entire organization.

More Secure Networks Now and in the Future

Now, Deakins' security team has time for other initiatives, while users have less inbox clutter and more feedback on reports they submit. With Abnormal, Marmon has strengthened its successful model of allowing its companies to maintain their individual networks and security tools, but with a unified layer of future-proof, automated security that understands human behavior. "Abnormal is unique in its ability to understand context. It's easy to administer, and it's easy for our users. Overall, it's a great product," Deakins said.

> "Before Abnormal, we had a reactive security approach. A phishing attack would get through and we would respond. Without a tool like Abnormal, that's the world that you operate in. Now, Abnormal's AI learns and understands our email communications, so we can be proactive."
>
> Jeff Deakins
> Director, Information Security and Infrastructure

Abnormal Products in use:

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

abnormalsecurity.com →

Abnormal