Customer Case Study

Ingersoll Rand Unlocks the Potential of Behavioral AI Security and Automation

Abnormal replaces the global manufacturer's SEG to protect its connected operational technology products, systems, and customers

Ingersoll Rand makes the equipment other manufacturers use to create their products. With more than 40 brands in its portfolio, Ingersoll Rand's air compressors, power tools, pumps, and material handling equipment serve global customers in industries from aerospace to transportation. More than simply a supplier, the company positions itself as a source of expertise in unlocking its customers' potential with reliable, efficient, and low maintenance solutions.

The Ingersoll Rand Email Security Challenge

Ingersoll Rand provides connected Operational Technology (OT) equipment, so Stuxnet-style attacks are a major concern. Said Noah Davis, VP & Global CISO, "If you can get past the controls, you can create explosions." When Davis joined the company in 2023, advanced email attacks were getting past Microsoft 365's built-in security. He activated an existing contract for a SEG, with increasingly disappointing results as attackers used AI to continuously increase the pace and precision of attacks.

"We were seeing business email compromise, credential phishing, malicious attachments and code, and some polymorphic attacks getting through. Each one required an intensive investigation and response," said Sherri Leach, Deputy CISO.

Industry
Industrial Machinery Manufacturing

Headquarters
Davidson, North Carolina, USA

Protected Mailboxes
32,000+

Customer Key Challenges

- Address escalation in and precision of AI-based attacks getting past the SEG
- Protect customers' connected OT equipment from email-enabled attacks
- Implement more reliable, efficient, and low maintenance security

Abnormal Solution Impact

- Identifies and stops AI-based attacks using human behavior AI
- Prevents threats from exploiting human nature to access wider systems and OT equipment
- Saves time and money across the organization with AI automation and AI-based graymail filtering

"Human behavior is a big issue in cybersecurity. When you're dealing with organizations that include thousands of people, you need a solution that takes that into account and protects less tech-savvy users from themselves. Abnormal's human behavior AI accomplishes this."

Noah Davis
VP & Global CISO

Customer Case Study

$250K
per year saved with AI SOC automation

$50K
prevented losses from a single BEC attack

2,459
employee & VIP hours saved on graymail in 30 days

The Abnormal Security Solution

Davis wanted a zero-maintenance API-based security layer with easy deployment, quick integration, and human behavior AI to detect sophisticated threats that the SEG was missing. “Our strategy is two-pronged. One is to protect our house by improving our security posture against social engineering and known vulnerabilities. Two is continuous improvement, which is why we looked more toward an AI-native email security platform,” he said.

Abnormal offered the opportunity to automate high volume, repetitive tasks so Ingersoll Rand's security analysts could focus on the highest risks. Abnormal also offered easy integration with CrowdStrike, the company's endpoint management solution.

Why Ingersoll Rand Chose Abnormal

Abnormal’s AI-based detection and automation deliver quantifiable value, beyond the SEG displacement. “We save $250,000 yearly as our analysts don’t have to manually investigate and remediate incidents and user-reported emails,” Leach said. Abnormal’s ease of setup met Davis’s expectations. “We protected all of our accounts in under 15 minutes with the native API integration. That speed to value is one of the fastest I've seen.”

Rather than reacting to emails, the SOC team now focuses on work like reverse-engineering polymorphic malware, analyzing user behavior, and adding preventative controls. The team also integrated Abnormal’s Account Takeover Protection with their CrowdStrike environment. “As we see nefarious activity or anomalous activity reports from Abnormal, we pass that data to CrowdStrike, which increases the depth of our defenses,” he said.

A Stronger, More Efficient Security Posture

Davis and Leach are confident in the protection Abnormal provides now, and for the future. “With autonomous AI, you need high trust in the decision-making process and the logic. Abnormal has very high efficacy, and with the amount of data the platform has, the potential insights are almost unlimited,” Davis said. “The better the native AI model gets, the more connections are made that reveal elements of risk, so our SOC team can focus on the highest risk priorities and Abnormal handles the rest.”

> “Abnormal stopped a $50,000 BEC attack—the kind of thing that would have reached inboxes before with a SEG. Threat actors are adding AI and generative AI to make their techniques more convincing, so we needed the capability to respond to AI threats equally, and Abnormal delivers that.
>
> Sherri Leach
> Deputy CISO

Abnormal Products In Use:

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

abnormalsecurity.com →

Abnormal