Customer Case Study

Coats Optimizes Its Extensive Supply Chain Security, Protecting Customers and Vendors

Coats is the global leader in industrial thread manufacturing, with more than 17,000 employees producing enough fiber daily to stretch to the sun and back four times. The 250-year-old company has stayed at the forefront of textile innovation as demand evolved from sewing thread to healthcare PPE and carbon-composite fibers for aerospace manufacturing. Coats leverages new technologies and market expertise to develop products for customers in the apparel, luggage, footwear, home and recreation, personal protection, transportation, telecommunications, and energy industries.

During 2020, Coats—like many enterprises—faced an increase in advanced email attacks year over year. Coats had invested in Microsoft Defender for Office 365 which was effective in blocking common email attacks by leveraging rules and policies, and threat intelligence. However, for advanced attacks they needed a solution like Abnormal Security that leverages a behavioral approach to detect and block never-seen-before attacks with high efficacy.

“We were also finding messages in quarantine that didn’t belong there, and we didn’t understand why they were quarantined. The overall result was more risky messages getting through, more good messages stuck in quarantine, and more time assessing why our controls weren’t stopping potentially illegitimate messages and trying to fine-tune our safelist,” said Benjamin Corll, VP of Cyber Security and Data Protection. The result was time and attention diverted from innovation and other security priorities.

COATS

Industry
Manufacturing

Protected Mailboxes
11,000

Location
Global HQ:
London, UK

North America HQ:
Charlotte, NC

Weekly Account Takeover Risk Rises with Company Size

Abnormal 2021 data showed a strong relationship between company size and ATO risk, with companies the size of Coats facing a 30% weekly probability of at least one compromised account.

Upon implementation, Abnormal identified 766 attacks that had reached Coats inboxes in the preceding month. In the first nine months, Abnormal Integrated Cloud Email Security prevented 7,790 attacks, primarily name impersonation phishing attempts, from Coats’ 11,000 mailboxes.

> “Abnormal keeps our users from receiving advanced threat emails in their inbox, eliminating the risk of engaging in fraud or compromised messages. Abnormal automatically reduces our threat exposure and shrinks our attack surface.”

Helge Brummer
VP of Global Technology & Operations

50

high-risk and medium-risk vendor email accounts identified.

97%

decrease in daily unsafe user engagements.

Ø

accounts compromised in the past year.

Finding a Defense-in-Depth Solution for the Microsoft 365 Environment

“We chose Microsoft 365 to reduce our on-premises overhead, increase email system uptime, and meet executives’ needs for familiar email tools,” said Albert Carreon, Head of Global Architecture. “Microsoft Defender and Exchange Online Protection handle the basic blocking and tackling on email security to filter out messages that are known to be bad.”

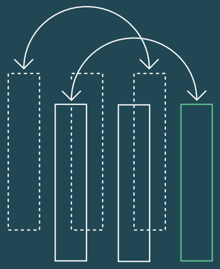
The challenge was stopping email attacks designed without malicious links or attachments to evade basic safeguards. The number of phishing, and business email compromise messages getting through left Coats vulnerable to attacks that could cause extensive damage. Coats knew it needed to layer another solution onto its Microsoft controls. “We looked at traditional secure email gateways (SEGs), but their protections were similar to what Microsoft was doing,” Corll said.

“We needed a powerful, modern, behavior-based solution that was designed to work seamlessly with Microsoft. Abnormal Security’s Integrated Cloud Email Security (ICES) platform was the right choice. ICES uses ML and AI to evaluate behavior and content.” Corll said. **“Since we turned on ICES in the past year, we have not experienced a single compromised account.”**

Securing Email Communication Across a Vast Supply Chain

Coats operates in 55 countries, supplying more than 1,ØØØ customers who make items ranging from jeans, luggage, and mattresses to firefighter gear, fiber optic cables, vehicle airbags, and smartphones. Because Coats and its customers have such complex supply chains, Coats Digital developed its own agile, sustainable supply chain solution for fashion manufacturers and brands. Preventing supply chain compromise is a critical component of maintaining security and trust across the Coats ecosystem.

Upon implementation, Abnormal’s AI-driven VendorBase identified Coats’ 7,Ø99 vendors and evaluated their messages for potential compromise, based on each vendor’s legitimacy, history of compromise, and history of impersonation attempts at Coats and across all Abnormal customers. The behavioral analysis within VendorBase found 3Ø vendors at high risk, another 2Ø at medium risk, and 33 attacks from legitimate vendor and partner accounts. Based on the results, “Abnormal showed that it’s a robust defense-in-depth solution with unparalleled vendor analysis,” Corll said.



Automates SOC Operations

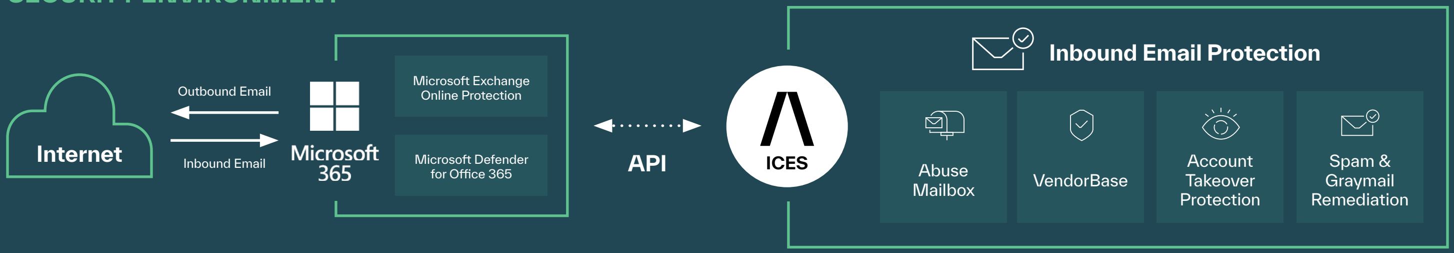
In addition to stopping advanced email threats, Abnormal speeds up the removal of internal messages sent by accident using the search and respond feature. The Coats SOC team also leverages Abuse Mailbox to save time and automatically triage emails with greater accuracy, saving up to 9Ø minutes per message.

3Ø

hours per week saved on inbox investigations and errant message retrieval.

Customer Case Study

SECURITY ENVIRONMENT



Internet

Outbound Email

Inbound Email

Microsoft 365

Microsoft Exchange Online Protection

Microsoft Defender for Office 365

API

ICES

Inbound Email Protection

Abuse Mailbox

VendorBase

Account Takeover Protection

Spam & Graymail Remediation

Number of Employees

17,000+ globally dispersed across Europe, Africa, Southeast Asia, and the Americas

Customer Support Tier

Silver

Coats Saves Time and Maintains Focus with Abnormal ICES Precise Detection

With the Abnormal Integrated Cloud Email Security platform, Coats avoided the need for multiple, potentially incompatible, products to enhance their Microsoft email security. ICES is the only email security platform that deploys precise detection against advanced email attacks, streamlines email security architecture, reduces security team overhead, all while maintaining Microsoft 365's native security features.

ICES also creates a more efficient inbox user experience. The ICES promotions folder separates marketing messages from spam, so it's less risky for users to check their promotions. If they move a promotion email to their main folder, Abnormal remembers that choice. “At first you look every day. Now, I'm looking maybe once a week. Overall, my productivity has changed for the better,” said Helge Brummer, VP of Global Technology & Operations.

Remediating email sent by mistake is more efficient, too. “Minutes matter when a managing director is sweating bullets because a message went to the wrong recipients.” Instead of 30 to 90 minutes, Corll and his team now remediate them in two minutes from the Abnormal console.

Coats Vendors and Customers are Better Protected with Abnormal ICES

With Abnormal ICES layered over Microsoft Defender, Coats employees are free to focus on continuing the company's 250-year tradition of innovation, rather than sorting through emails and trying to assess the risks. Coats vendors and customers are also better protected because Abnormal ICES has reduced by 97% the number of engagements Coats employees have with potentially unsafe messages.

Working with Abnormal also frees the Coats security team to focus on other priorities. “The Abnormal customer support team is phenomenal,” Corll said. “They are very responsive and great about explaining new features in the pipeline–giving us reliable dates on when those will be available.”

> “Abnormal is context- and behavior-based, so it complements Defender well. Defender is effective in blocking spam, graymail and generic phishing attacks while Abnormal blocks sophisticated advanced attacks with high efficacy. The combined solution creates a true layered defense that protects against all types of email attacks.”
>
> **Benjamin Corll**
> VP of Cyber Security and Data Protection

ABNORMALSECURITY.COM →