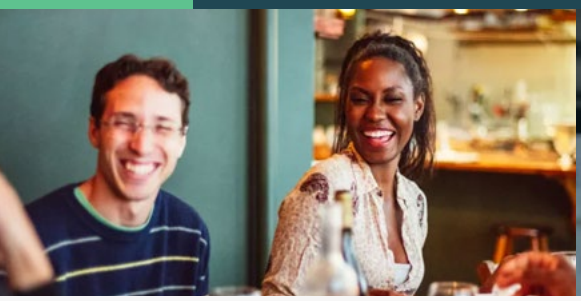
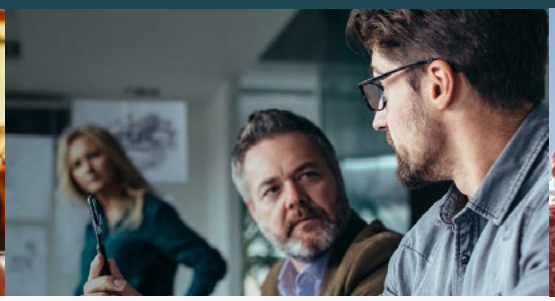
Customer Case Study


Connecting the World Through Technology and Hospitality

Choice Hotels aims to connect the world through the power of hospitality. As one of the world's largest lodging franchisors, the company is known for its 7,100 hotels under multiple brand names across upscale, boutique, and economy properties. Connecting that ecosystem and its customers requires modern security for a vast and always-growing email attack surface.

Although Choice doesn't operate the locations, the company is responsible for protecting the data of 50 million loyalty members and other guests, according to Jason Stead. Stead is the CISO of Choice Hotels and a director on the board of RH-ISAC, the retail and hospitality cybersecurity group.

"Hospitality is a highly targeted industry because hotels have troves of guest data that is of interest to nation-state actors and financially-motivated criminals," Stead said. In fact, the industry culture seems tailor-made for social engineering. "Hospitality is welcoming and helpful. That's exactly what phishers are looking for—people willing to do whatever it takes to provide great service." And unfortunately, attackers don't stop with frontline employees either. "Last year, several of our top leaders were continually targeted. The attacks required time and effort from my operations team to remediate those situations," explained Stead.

Even with two secure email gateways deployed, advanced threats were appearing in inboxes. In many of these cases, cybercriminals exploited more than 120 of the company's vendors to attempt phishing and invoice and payroll fraud.

CHOICE HOTELS®

Industry
Hospitality

Location
Rockport, MD

Protected Mailboxes
3,650+

Number of Employees
1,800+

BEC Threatens Hospitality Brands

Business email compromise attacks impersonate executives, clients, vendors, or coworkers to bypass legacy tools and reach inboxes. The RH-ISAC 2021 CISO Benchmark Report Summary found that nearly 25% of its members faced risks related to phishing, BEC, malware, and other email threats.

Abnormal protects Choice Hotels from these advanced email threats to their data, operations, and reputation.

"We employed two SEG solutions in sequence, and that still wasn't solving our email security problems. Abnormal frees us from inbox cleanup, so we can proactively identify and address other security threats before they become problems."

Jason Stead
CISO

Customer Case Study

36%

reduction in IT response efforts to email threats during peak season.

120+

compromised vendors detected by Abnormal VendorBase™.

97

attacks stopped by Abnormal on average each day.

Choice Hotels Needed to Stop Advanced Email Threats Bypassing Their SEGs

Stead hoped Abnormal could prevent what the company's SEGs and people couldn't catch. "We train our people to identify these threats and to respond," Stead said. "But not everybody will consistently follow through. Frankly, it's easy for anybody to fall victim to these scams."

Integrating Abnormal with Microsoft 365 was simple. "We set up an account in less than five minutes and walked out of the proof of value (POV) meeting with the tools to manage and own the solution," said Jason Simpson, Vice President, Engineering. The Abnormal behavioral AI-based detection engine started delivering results soon after the POV began.

"It was great," Stead added. "The Abnormal team alerted us when our leaders or employees were about to fall victim to an advanced email threat so we could proactively prevent it. Even though we were still in monitor-only mode, their direct support allowed us to mitigate those attacks in real time."

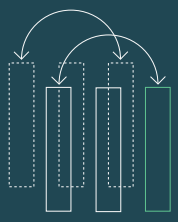
Rapid Results in Detecting BEC, Phishing, and Supply Chain Fraud

Among the threats Abnormal quickly detected was a BEC email urging an employee to purchase gift cards for them, a common ploy in these attacks. "An employee had engaged with that bad actor via that email," Stead said. "We were able to stop the employee before they went to the store to buy the gift cards and send the information to the bad actor."

Abnormal's AI-driven behavioral benchmarking also detects phishing and vendor email compromise attacks that appear to come from trusted senders. "Abnormal detected potential wire fraud emails reaching our people who process wire transfers, so we were able to prevent those transactions," Stead said.

Stead recognized that one attack that Abnormal detected was likely targeting other hotel chains, too. **"We were able to share that intelligence with one of our competitors to help them identify and mitigate it before something bad happened,"** he said.

By working in the background, quickly detecting threats, and enabling intelligence sharing, "Abnormal delivered the fastest POV time-to-value, by far, that I've ever seen," said Simpson.



Automates SOC Operations

Abnormal freed Choice Hotels' SOC team from time-consuming manual threat review by providing fully automated email triage, remediation, and reporting of all autodetected and user-reported threats in one interface.

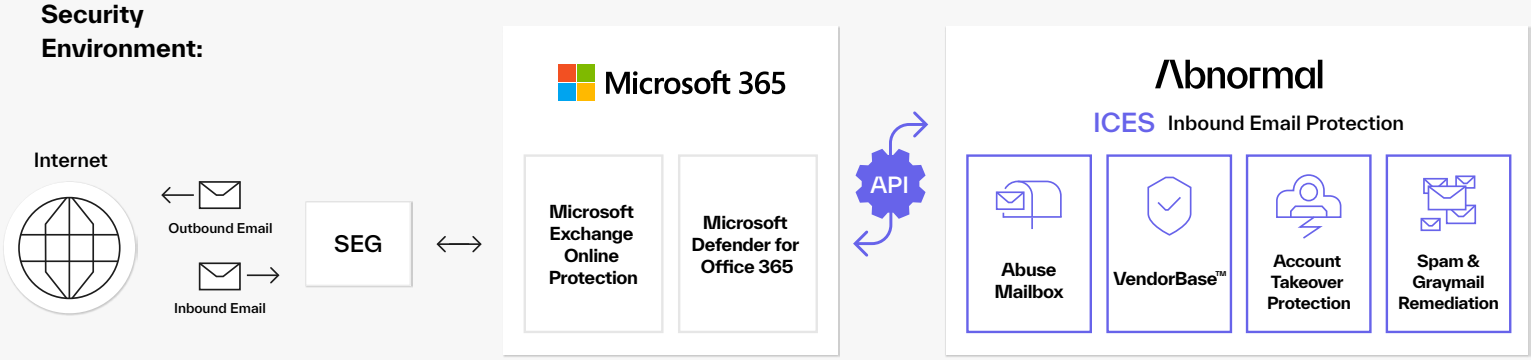
The search and respond functionality allows for rapid containment of missed attacks and misdirected emails, so analysts can focus on detecting and preventing other security threats.

100%

of reported malicious phishing emails were auto-remediated by Abnormal.

Customer Case Study

Security Environment:



More Time and Resources for Proactive Security Management and Education

Because Abnormal is simple to maintain, the Choice Hotels team spends minimal time tuning the product. Its AI and ML features automatically adjust against the baseline of known good activity. "The result is that there have been no issues with Abnormal," Stead said. There's also time saved on awkward conversations when a phishing email appears to come from a franchisee, vendor, or customer. "In the past, we would have to contact them to evaluate where it came from, but now those emails never land in the inbox," Stead said.

In its first year, Abnormal reduced SOC response efforts by 36% from March through May during the company's busiest season for email activity and threats. "That freed my team to spend more time on threat intelligence gathering and threat hunting," Stead said.

They also have more resources for awareness training. Abnormal's dashboard provides real social engineering attacks they can analyze and use for education. "Abnormal gives us a robust suite of phishing examples that we can use to train our employees, and it's not just about training them for their corporate world, but also for their home lives," Stead said.

"Overall, Abnormal has been so effective that we're moving toward eliminating at least one of our secure email gateway solutions," Stead added.

Abnormal Helps Choice Hotels Strengthen Internal and Industry Email Security

With Abnormal automatically handling advanced email threats, Choice Hotels uses the time it previously spent on reactive security responses to proactively identify threats, provide more realistic awareness training, and fortify the hospitality cybersecurity space.

"Our goal is to create enough friction so that threat actors go somewhere else," Stead said. "What we're doing now, especially with Abnormal and RH-ISAC, is banding together to uplift the entire industry."

Customer Support Tier

Gold

"During our peak threat season, we experienced a 36% reduction in response efforts to email threats that make it past our SEGs. Because of Abnormal, our busiest months this year have required less response work than our quietest months last year."

Jason Stead
CISO

abnormalsecurity.com →

Abnormal © 2022 Abnormal Security Corporation. All rights reserved.