Customer Case Study

Guiding Global Clients Securely Through Mergers, Restructuring, and More

Greenhill & Co. leads its client businesses through major milestones and complex processes: completing mergers and acquisitions, restructuring, raising capital, and obtaining financing. Greenhill's global presence spans North America, Europe, and Asia and serves enterprises across multiple industries, including consumer goods and retail, real estate, energy and infrastructure, finance, healthcare, technology, hospitality, and more.

Advising clients worldwide on multibillion-dollar deals means Greenhill must comply with multiple data security regulations. Greenhill's role also makes it a high-profile target for criminals seeking to steal sensitive data, intercept funds, or commit invoice fraud. "As people within the investment space move from company to company, attackers collect this information, and you'll start getting emails impersonating those users," said CIO/CISO John Shaffer. "We have the same challenge as everyone else, in that users are generally the weakest security link and email is often the way bad things happen."

Despite implementing an advanced security awareness program, Greenhill wanted to prevent employees from confronting email threats in the first place. Shaffer knew that the fewer decisions employees had to make about legitimacy of emails, the more secure the company would be.

To improve security, Greenhill adopted Defender for Office 365 and made gateway changes, but Shaffer's team found that socially-engineered threats were still reaching mailboxes. It was clear that while their existing tools managed basic threats well, Greenhill needed a more strategic line of defense against sophisticated attacks.

Greenhill

Industry
Investment Banking

Headquarters
New York City

Protected Mailboxes
600+

Number of Employees
360+

Financial Firms Face High Risk of Business Email Compromise Every Week

Abnormal data found that financial enterprises have a 60% probability of receiving a BEC attack each week, on average. And over the first six months of 2022, BEC attacks against all sectors increased by 60%.

Since deployment, Abnormal has stopped more than 130 BEC attacks on Greenhill. These emails were designed to trick recipients into paying fraudulent invoices, redirecting payroll deposits, or disclosing sensitive information.

"I don't want realistic-looking email threats reaching employees' inboxes, or even their spam folders where they might be tempted to click on them. Abnormal has stopped threats from getting through."

John Shaffer
CIO/CISO

Customer Case Study

70+

high risk vendor compromises detected.

7,000+

credential phishing emails stopped.

11,000+

name impersonation attacks prevented.

Greenhill Sought a Solution to Keep Advanced Threats Out of Inboxes

Greenhill selected Abnormal because its AI-powered solution provides behavior-based intelligence to detect the advanced spear phishing, name impersonation, and account takeover attacks that Greenhill's other security layers couldn't consistently identify or stop. Implementing Abnormal for a proof of value took just a few minutes because of Abnormal's API-based design. The platform immediately started to monitor Greenhill's email ecosystem to baseline good behavior among senders and recipients, and this monitoring-mode learning process took place invisibly, which addressed one of Shaffer's key concerns.

"When you're dealing with email, which everyone in your company depends on, you can be leery of putting something in place that might affect people's ability to work," he said. "Abnormal didn't affect our mailflow, and the POV showed us the types of things it would catch if the platform were enabled."

Accurate Identification of Executive Impersonation and Supply Chain Attacks

Attacks included CEO impersonation, invoice fraud attempts, and other malicious messages that exploited trusted relationships with individuals and vendors. Abnormal VendorBase™ also identified more than 70 compromised vendor email accounts. "Attackers know how to target an organization, make an invoice look real, and use any kind of insights to fool people, but Abnormal has stopped that," Shaffer said. "It's really accurate. You don't want employees getting emails that come from accounts of someone they trust, but those accounts are actually compromised."

"Also, I don't remember needing to go into the platform and release an email that was stuck in Abnormal. That's not the case with standard systems, where you might need to go into the junk email folder to find something that shouldn't have been in there," stated Shaffer.

The result is more time for other projects. "I don't need to go into the Abnormal Portal every day. It works behind the scenes and makes it easy for us to work on other high-impact projects."

Protects Against Attacks with the Highest Efficacy

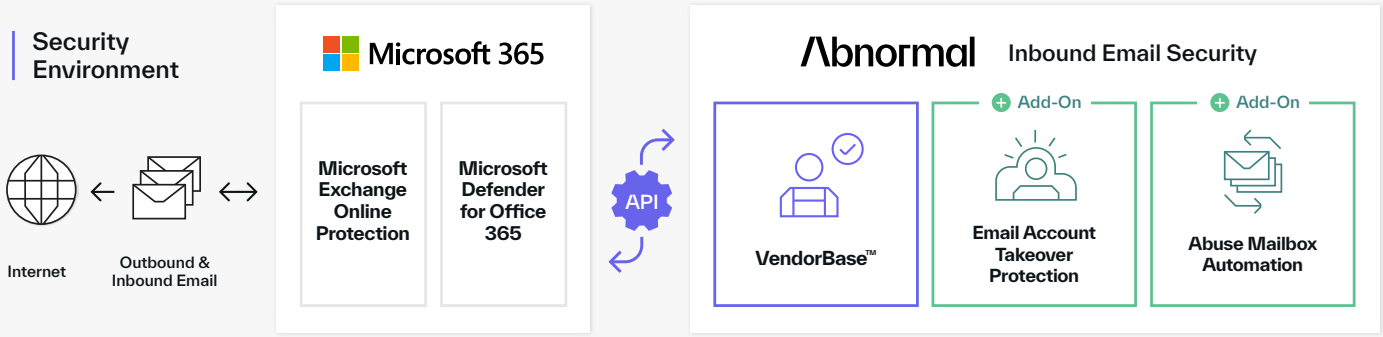
By accurately detecting the socially-engineered attacks that were evading Greenhill's secure email gateway and basic security solutions, Abnormal reduced the company's risk of data privacy incidents and related regulatory penalties.

The high efficacy also freed Greenhill's security team from investigating user reports. It auto-remediates threats from inboxes so the team can focus their attention on other security initiatives.

Zero

Missed attacks in the past 16 months.

Customer Case Study



Accelerated Threat Responses Leaves More Time for Other Security Initiatives

Abnormal detects the widest possible range of email threats and allows Greenhill's security team to work more quickly. "There's not enough time for a person to deal with the malicious emails we receive in a reasonable timeframe and accurate fashion. Abnormal's technology is like that extra person we need, but really fast," Shaffer said. "Email is one thing we don't have to focus on anymore."

Shaffer and his team are working on another way to leverage the value Abnormal provides. They plan to integrate Abnormal with their Revelstoke SOAR to automate and streamline their account takeover response plans.

"Fortunately, we haven't had a situation where someone has been compromised internally. But if we do, we'll be ready with our action plan to minimize the impact on the organization. The Abnormal alert will feed into the SOAR, which will instruct us on how to handle the situation," Shaffer said. "I've talked with Abnormal about how we would respond to a rare case like that, because even if you have a playbook, people still need guidance in the moment."

Confidence Built on Stronger Security and a Trusted Partnership

With Abnormal protecting inboxes, handling responses, and enhancing incident response, Greenhill has a stronger position than ever for safely guiding clients through complex events. "We have a great relationship with Abnormal. They know what I'm looking for and the team has been very responsive," Shaffer said. "I feel really confident in our ability to manage the business email compromise threat, which our firm needed to solve."

Customer Support Tier

Silver

"Abnormal has helped us mitigate risk, maintain compliance, gain efficiencies, and improve our executive experience."

John Shaffer
CIO/CISO

abnormalsecurity.com →