Customer Case Study

Global 500 Financial Organization Moves to “Digital Everything” to Enhance Customer Experience and Email Security

Industry

Financial Services

Location

Canada

Protected Mailboxes

34,000+

As a leading Global 500 financial services company, the organization is responsible for nearly a trillion dollars in asset management, investor interests, and a global workforce. Its insurance, investment, financial advisory, and asset management services are trusted by customers across Canada, the United States, Asia, and Europe. With millions of customers, it’s important to this financial organization to protect their wealth, reduce their risk, and help them to reach their goals and live more rewarding, healthier lives.

To maintain this trust and continue to foster growth, the organization is transforming its global business operations to deliver “digital everything.” This requires a fresh look at each line of business and its supporting technologies, people, and functions to identify opportunities to reorganize, replatform, and accelerate their rate of digital change to become quicker and more competitive.

During this transformation, the security operations team has a critical role in protecting assets, processes, and people. The team knew that even though the organization wasn’t having to deal with successful email attacks yet, they should keep looking for ways to enhance protection for their more than 34,000 inboxes worldwide. “Email is the most vulnerable area we have, because it requires humans to decide quickly whether or not to click a link or open an attachment. Blocking malicious emails before they reach a human is key,” said the company’s Director of Threat Intelligence.

Advanced Supply Chain Threats and Fraud Avoided

Attacks via third-party vendors increased 156% against companies between July 2020 and June 2021. Cybercriminals now exploit the vendor-customer email channel to impersonate trusted vendors and commit invoice fraud, billing account update fraud, and RFQ scams against vendors’ clients. Upon integration, Abnormal found compromised accounts within 70+ of the organization’s vendors, closing a gap that could have led to costly attacks.

> “As we move into a ‘digital everything’ world, protecting our customers and employees is the top priority. We’re moving faster and becoming more competitive, and we need to ensure that our security can keep pace. Abnormal makes that happen.”

AVP of Security Operations

$14M

in supply chain compromise attacks prevented.

77

compromised vendors found in the first 90 days.

11K

attacks bypassing the secure email gateway each month.

The organization's proactive mindset led it to Abnormal. Rather than wait for an attack to succeed, "we took the next step in our email security evolution," said the Associate VP of Security Operations.

Revealing and Stopping Thousands More Email Attacks

Abnormal quickly uncovered a volume of email threats the organization hadn't expected—more than 70 compromised vendors and more than 11,000 advanced email attacks per month bypassing the company's secure email gateway. "We were fortunate that we did not have any problems, because Abnormal showed us that we had been interacting with compromised vendors and that thousands of attacks were bypassing our other two layers."

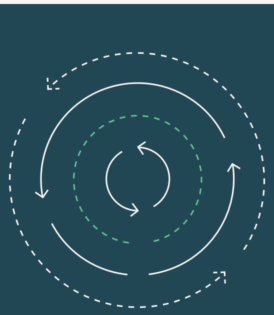
Abnormal is the organization's final line of defense against advanced email threats and those that matter most, with IronPort dedicated to anti-spam, FireEye detecting advanced threat malware, and Abnormal providing protection against business email compromise and other socially-engineered attacks that the other two layers aren't able to detect.

As one of the organization's security engineers explained, "Abnormal is catching things that our other two security platforms should've caught. It's like this big wall of safety that complements and exceeds what the other tools are doing."

Behavior-Based Protection Against Supply Chain Compromise

The fact that so many attacks were slipping through at an organization with two layers of email security already in place shows how sophisticated these threats have become. These attacks impersonate trusted vendors and avoid the known bad signals that other email security solutions are built to identify, like malicious payloads and suspicious links. Abnormal takes a different approach, using machine learning and natural language processing to separate known good email behaviors from those that signal fraud.

Before the company implemented Abnormal, these next-generation attacks were getting through, particularly when they were delivered as text-only emails designed to elicit responses regarding payment data or sensitive account information. "Plain-text business email compromise attacks were getting through. The tools ahead of Abnormal are looking for a file or signature, but Abnormal is really understanding the context with next-generation, next-level machine learning. That's what is different and it's why Abnormal is catching these attacks, despite being the last line of defense," said one security engineer.



Highest-Precision Protection Against All Attacks

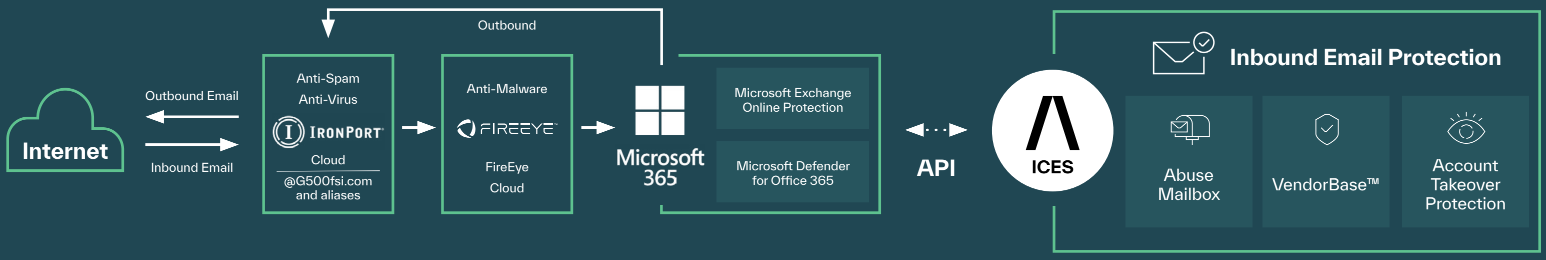
Abnormal uses ML and NLP to learn what the organization's good email behavior looks like, then reviews messages against more than 45,000 signals to detect anomalies that deviate from the good-behavior baseline. Abnormal's combination of advanced technology and extensive signal data prevented more than 75,000 advanced email attacks on the organization during its first year.

75K+

attacks prevented in the first year with Abnormal.

Customer Case Study

SECURITY ENVIRONMENT



Number of Employees

40,000+ globally dispersed throughout Canada, the United States, China, India, Ireland, the United Kingdom, and Southeast Asia

Customer Support Tier

Platinum

Avoiding $14 Million in Fraud Losses and Saving Time with Abnormal

When Abnormal was first implemented in read-only mode to understand the depth of the issue, the platform's comparison of vendor emails to its proprietary VendorBase™ immediately detected fraudulent vendor interactions. In many cases, these emails were originating from compromised vendor accounts, and the organization had no way of knowing that the emails contained false payment information designed to steal funds or account data. Within the first six months, Abnormal detected 77 of these attacks through VendorBase, saving the organization an estimated $14 million in losses.

"Abnormal is seeing attacks that are mutating and that are more targeted or crafted, where other security solutions are only able to see something if it's been detected elsewhere first. The entire platform is proactive, and it has really opened my eyes to what was actually reaching our user inboxes," said one of the company's security engineers working with Abnormal. Now, the security team can see email threats accurately and they spend less time addressing them, thanks to Abnormal's automatic remediation features.

Abnormal Provides Proactive Email Security for a Global Brand Transformation

Abnormal's advanced email fraud detection and proactive remediation capabilities are an ideal fit for an organization with a strong cybersecurity culture and a commitment to data privacy. Thanks to the company's ongoing testing that led them to Abnormal, the security team is now confident they can stop the most dangerous attacks.

That allows the team to focus on securing the organization's transformation initiatives and maintain the trust the company has built with millions of worldwide customers over its long life. As the Director of Security Engineering put it, "Part of the ROI on Abnormal from a security perspective is the return on our good name, because we're not in the news because of a breach."

> "Abnormal autoremediates our largest threats. It's immediate and proactive rather than reactive. Everyone that we show it to inside the organization is blown away."
>
> AVP of Security Operations

ABNORMALSECURITY.COM →