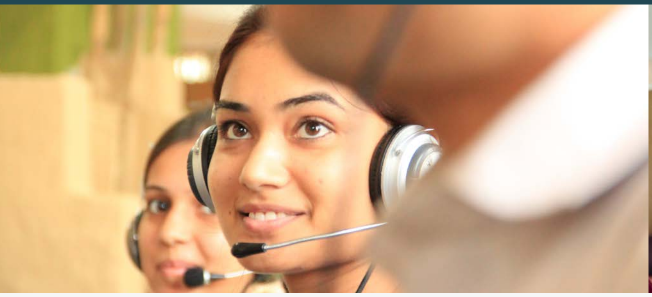
Customer Case Study



Scaling Up Securely, Everise Leverages Globally Dispersed Workforce to Deliver New Client Solutions

Everise has been revolutionizing customer experiences since 2016. Combining technologies like AI and robotic process automation (RPA) with a focus on people, Everise provides innovative customer and technical support services to enterprises and high-growth companies in healthcare, technology, travel, logistics, and other industries in the Americas, Europe, and Asia. While Everise helps its clients reduce costs, protect their brands, and moderate their content, it also cultivates an internal culture that routinely wins awards for technology innovation, leadership, and employee experience.

By 2020, Everise had 4,500 employees in the United States, Guatemala, Ireland, Japan, Malaysia, and the Philippines, who are now working remotely. Our employees all work in contact centers, and during COVID we needed to rapidly shift our staff to a home-based model. Since we had improved our infrastructure in 2019, we were able to let our people take their PCs home to work," said Bill Loss, Everise VP for IT Engineering and Technology Services.

By mid-2021, Everise had more than 11,000 employees to meet new demand for outsourced services. But the shift to remote work brought new email security risks. "Our people are good at what they do, but they're not email security specialists, and attackers know that. That's why ransomware, social engineering, and email attackers go after the human 'soft targets'—to get results."

Industry

Business Process Outsourcing and Technology

Location

Austin, Texas

Protected Mailboxes

15,000+

Credential Phishing Attacks Surged, Targeted Everise

As businesses pivoted in the pandemic era, so did cybercriminals. In the US in 2020, phishing was the most common internet crime reported to the FBI, with more than 240,000 documented victims. And credential phishing attacks continue to rise sharply, from 66% of advanced attacks in Q4 2020 to over 73% in Q2 2021. Targeted phishing messages use deadline pressure and impersonation in ways that evade off-the-shelf security solutions. In the year since deployment, Abnormal AI-based anomaly detection has stopped thousands of these phishing attacks across more than 15,000 Everise inboxes.

> "Abnormal protects our executives from individually targeted attack emails that our first line of defense can't catch. Our accounts payable team is safer and more efficient, too. Abnormal stops sophisticated malicious emails before our people ever see them."

Bill Loss
VP for IT Engineering and Technology Services

100%

reduction in employee time spent on remediation.

90%

of all threats are credential phishing attacks.

670%

decrease in business email compromise attacks.

Everise Sought New Protection to Excel at Employee and Customer Experience

As Everise worked to quickly extend its on-premises security practices to executive and employee home offices, they also had to contend with a rising tide of email attacks that were tailored to get past their existing security, including email security tools in Office 365 and employees' security awareness training. "We started to see a large increase in the number of BEC attacks and social engineering attacks, primarily targeting senior leadership. We saw emails impersonating clients with fraudulent invoices seeking payment. Credential phishing emails impersonated our CEO and service providers like DocuSign," said Amy Grisham, Director of IT Governance and Compliance. "We needed to stop these threats and to confidently recognize those emails coming from legitimate senders."

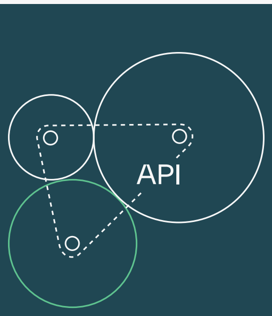
And it wasn't only front-line employees struggling to sort threats from safe messages. "It quickly became apparent, that more employees meant more targets. That was a lightbulb moment that made it clear we needed to focus more heavily on email security to prevent compromise that could damage our revenue, our employee experience, and the quality of the customer experience we deliver."

Seeing the Email Threat Landscape Clearly

With their Abnormal risk assessment, they saw hundreds of email attacks in company inboxes. This trend would mean thousands of attacks were slipping through each year, each with the potential to cause financial losses and brand damage.

One surprising and disturbing finding: "We learned there are bad actors out there that know who works for our accounts payable team. They would send our AP team members very specific, personalized emails that look like legitimate invoices, but these attack emails actually included a payload in the invoice attachment to install malware, or they may be trying to get a fake invoice paid under false pretenses. If we stop those before it even gets to them, their day gets a lot easier."

"Seeing the things that got past our initial security made us realize that we needed a better solution. Abnormal caught the more insidious threats and showed us we were getting many more financial-compromise emails than we had realized," Loss said.



Integrates Insights and Reporting

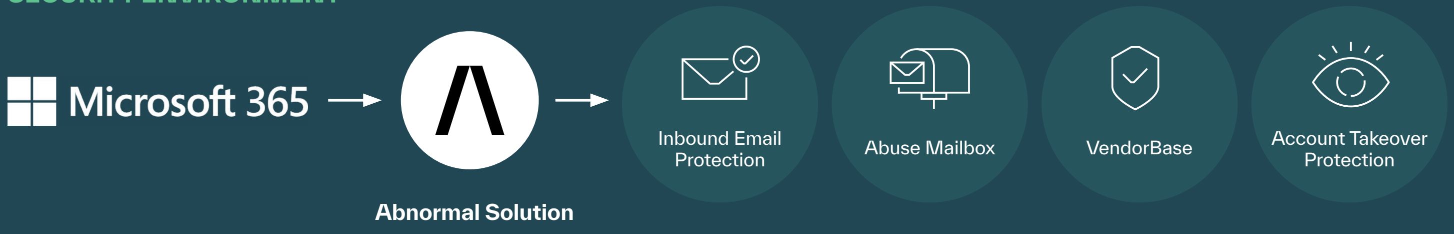
While Abnormal protects Everise from email attacks, it also makes it easy for the company leaders to see the results—both in real-time and through historical data. By accessing the Abnormal dashboard, it can see exactly which threats and trends they're protected against, which enhances their security insights and helps them understand the ROI on Abnormal.

15

hours saved per SOC team member each week.

Customer Case Study

SECURITY ENVIRONMENT



Microsoft 365 → Abnormal Solution → Inbound Email Protection, Abuse Mailbox, VendorBase, Account Takeover Protection

Number of Employees

13,000+ throughout the United States, Guatemala, Ireland, Japan, Malaysia, the Philippines, and Singpore

Customer Support Tier

Gold

Everise Saves Time with Abnormal AI and ML Precise Detection

Abnormal saves Everise considerable time by eliminating the need to manually remediate email attacks and takes the pressure off to evaluate emails for threats. Everise relies on Abnormal's behavioral AI-based detection engine to recognize legitimate senders and requests. Because Abnormal functions as a trusted partner to analyze emails, it can confidently respond to incoming messages faster and provide the best possible customer experience without delay.

Additionally, Abnormal gives Everise real-time visibility into email threats. "We have weekly leadership reviews with seven-day reports on the number of attacks Abnormal has stopped, trends over the past week, top impersonations in the environment, and top recipients of phishing attacks. Grisham said. "The Abnormal dashboards give more information than some other tools, like what our system is looking at, where users are logging in, their behavior and operating systems. We can dig down into the data in a way we can't with a lot of other tools."

Abnormal also makes it easy for employees to take an active role in threat prevention without overloading the SOC team. "Employees can report suspicious emails, following which Abnormal's Abuse Mailbox automatically investigates and determines whether they are safe, malicious, or spam. If malicious, Abnormal automatically removes the emails from all inboxes."

Abnormal Frees Everise to Deliver Exceptional Customer Experiences

Because of Abnormal, Everise is free to concentrate on delivering award-winning customer experiences—and to brainstorm more ways in which they can leverage Abnormal solutions to optimize their security. "Abnormal has been a great partner to work with," Grisham said. "They go above and beyond in supporting their clients." That dedication, plus the superior Abnormal technology, lets Everise focus on supporting its clients and growing its business.

> "The integration was one of the easiest we've ever done. Turn it on, let it run, and see the results. You quickly realize Abnormal's value to the organization."
>
> **Amy Grisham**
> Director of IT Governance and Compliance

ABNORMALSECURITY.COM →