Customer Case Study

Technologent Implements a Future-Proof Solution for Advanced Email Security

Global technology solutions provider implements API-based alternative to two SEGs that failed to detect sophisticated attacks.

Technologent is committed to helping its enterprise customers move their businesses forward through cutting edge technology and support services. The women-owned company serves Fortune 1000 companies worldwide through its 14 offices with an array of solutions including hybrid cloud and infrastructure transformation, data management, digital automation, cybersecurity, and more—all with the goal of helping their customers become more "agile, modern, and compliant."

The Technologent Email Security Challenge

Despite Technologent's technology expertise, sophisticated phishing and business email compromise attacks were reaching the company's inboxes due to the limitations of their email security providers' threat detection capabilities. These attacks often targeted executives and reached their inboxes because they contained no traditional indicators of compromise like malicious links or attachments.

The small security team handled the resulting manual investigations and remediation in addition to their other responsibilities. "We leveraged the native capabilities of Office 365 and it wasn't enough. We deployed a traditional SEG that fell short, and then added a second SEG with similar results. We quickly found that traditional email gateways are simply not enough," said Jon Mendoza, CISO. To solve the problem, he looked for an API-based solution that uses AI to detect sophisticated attacks.

Technologent®

Industry
IT Services and IT Consulting

Headquarters
Irvine, CA

Employees
700+

Protected Mailboxes
1,800+

Customer Key Challenges

- Prevent advanced text-based BEC and phishing attacks from reaching executive and employee inboxes.
- Reduce security team time spent repeatedly fine-tuning two SEGs in an attempt to stop attacks without quarantining good emails.
- Detect and prevent vendor email compromise attacks to protect relationships with Fortune 1000 clients.

Abnormal Products

- Inbound Email Security
- Email Account Takeover Protection
- Abuse Mailbox Automation
- Email Productivity

"Even with two SEGs, I was getting calls from the CEO on Saturday nights, asking 'Why am I getting these emails?' With Abnormal stopping advanced attacks, I don't get those calls anymore, and email attacks don't come up in our management meetings."

Jon Mendoza
CISO

Customer Case Study

4.2K+
Advanced attacks prevented within 6 months.

77
High-risk vendors detected since implementation.

Zero
Missed attacks or false positives within 30 days.

The Abnormal Security Solution

Mendoza wanted an effective solution that was easy to deploy. He also wanted one that would relieve the security team of the ongoing need to adjust SEG email rules, which often created unintended disruptions. "It was very important that a solution not just meet our requirements today, but also in the future," he said.

Abnormal works seamlessly with Microsoft 365 to provide AI-driven cloud email security, account takeover protection, and spam and graymail detection with automatic threat remediation and automated reporting. Because Abnormal quickly learns what's normal in the ecosystem, it detects advanced BEC, vendor fraud, and phishing attacks that other solutions miss.

Why Technologent Chose Abnormal

The Abnormal proof of value quickly delivered results. "On the second day, Abnormal called about a malicious email and the indicators they saw. Both of our SEGs had let it go through. Abnormal saved us a lot of money, because the message was something that an account manager would respond to quickly if it landed in their inbox," Mendoza said.

Abnormal also confirmed Mendoza's concerns about lateral email security. "I thought messages from internal user to internal user weren't really being protected by the SEGs. In fact, we found that area was left wide open." Now, Abnormal protects Technologent from the internal spread of malicious emails, in addition to external attacks. "Abnormal's reporting shows us how many threats we no longer have to respond to manually, which is great, but what's more important to me is the fact that those threats no longer reach our users' inboxes."

A Future-Proof Solution for Advanced Email Security

Today, Technologent's security team is free to focus on other tasks. Employees and VIPs no longer find phishing and BEC attacks in their inboxes. Mendoza has more visibility into the company's email threat landscape through Abnormal dashboards, and he's confident that Abnormal will keep pace with Technologent's needs as the threat landscape changes. "Abnormal has been a magnificent partner, facilitating great interactions and giving us the support that we need."

> "The bad guys are innovating, so we have to be at the forefront of security to mitigate our risks and prevent these advanced attacks. Abnormal is the first platform that lives up to the promise of AI and ML for threat detection. And because Abnormal is API-based, when Microsoft pivots, Abnormal can pivot alongside it seamlessly and easily. This model is where the market is headed."
>
> Jon Mendoza
> CISO

abnormalsecurity.com →

Abnormal