Customer Success Story

Fortune 200 Asset Management Company Protects Customer Wealth from Email Threats

As a leader in insurance and asset management, this Fortune 200 company recognizes that its security must protect its employees and customers from cyber attacks. Customers place their trust and their assets in the control of this company, so the security team built a robust solution reducing risk, gaining visibility, and securing user identity—the new perimeter.

After experiencing thousands of credential phishing attacks and a number of successful account takeovers, where threat actors would gain access to employee email accounts, this insurance company knew they needed additional protection for their Microsoft 365 environment. Despite having a secure email gateway and other additional protections, they were still uncomfortable with the number of advanced email attacks bypassing their security infrastructure.

They chose Abnormal Security due to the visibility it provided into their email environment, the number of advanced email threats it detected, and the number of compromised accounts it remediated. With this added layer of security, this company is better protected from business email compromise and account takeovers, ensuring that they—and their customers—remain safe from cyber attacks.

> “High efficacy is important to us. We need to protect our employees and clients from all angles. We had multiple layers of email security, but it wasn’t enough... **we needed Abnormal to catch what others missed.**

Vice President,
VP Cyber Security

Industry
Insurance and Asset Management

Location
United States

Protected Mailboxes
20,800+

CHALLENGES

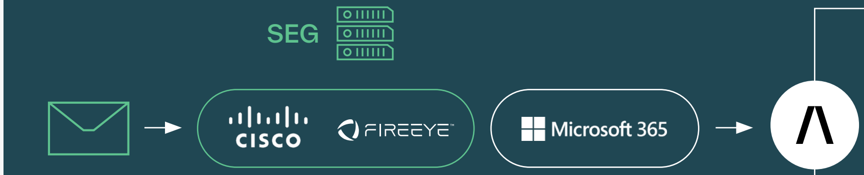
- Missed attacks by Cisco ESA (IronPort) and FireEye
- Multiple compromised accounts that were circumvented by multi-factor authentication
- Received numerous BEC attacks impersonating executives
- Wanted an additional layer of protection to prevent employees from falling victim to social engineering attacks

BUSINESS IMPACT

- Gained immediate visibility into the types of attacks, key recipients, attacker strategy, and attacker origin
- Stopped over 3,500 credential phishing attacks and 190 unique business email compromise campaigns within last 90 days
- Implemented within 15 minutes and found one compromised account within the first day

Zero High efficacy with **zero compromised accounts** in past 2 years

SECURITY ENVIRONMENT



Attacks Prevented by Abnormal Missed by Cisco, FireEye, and Microsoft 365 in the Past 90 Days

Phishing	BEC	Malware	Account Takeover	Fraud
3,507	193	136	220	802

Abnormal abnormalsecurity.com