bfore.ai

Case Study

Signify

Saving partners from impersonation scams

PreCrime Brand

Situation

Business Email compromise and impersonation represent the largest cost organizations incur for cybercrime. Losses in excess of $2Bn/year are incurred as a result of this attack method wich is far more common and costly than the more frequently discussed methods such as ransomware or credential stealing.

Regularly Signify's customers and partners would be targeted by impersonation and business email compromise attacks, at times resulting losses of hundreds of thousands of dollars in losses. The security team want to regain control, stop being a victim of cybercrime and start protecting their constituency proactively.

Impact

Signify is the world leader in lighting. They provide professional customers and consumers with quality products, systems and service. Their innovations contribute to a safer, smarter, and more sustainable world.

Signify requested Bfore.Ai to apply PreCrime technology for their brand protection. Aiming to cover their 50 brands to identify emerging threats and stop criminals before anybody became a victim.

TL;DR

- Regularly Signify's customers and partners would be targeted by impersonation and business email compromise attacks

- Signify requested Bfore.Ai to apply PreCrime technology for their brand protection

- Bfore.Ai provides a fully managed Brand Digital Asset protection service

- Over the course of the first 6 months, 41 threat vectors were predicted and proactively taken down. No victims reported.

- Savings of $12M dollars were made through early threat detection avoiding costly commercial gestures & legal proceedings.

About Bfore.Ai

The first truly predictive security solution. We help organizations prevent intrusions and data exfiltration by predicting vectors of future attacks, the information is used in #PreCrime for Network - predictive cyber threat intelligence to upgrade existing security solutions (firewalls, DNS resolvers, anti-phish filters, proxies, etc.) with foresight.

bfore.ai

Key takeaways

50 brands protected across the globe

Up to 72 hours earlier notification compared to existing solutions

95% of countermeasures completed in less than 24 hours

No victims

$12M in estimated ROSI (Return on Security Investment)

<0.05% false positives

How it works

Signify implemented PreCrime via a certified API to their Threat Intelligence Platform. Their advanced security architecture enable the Threat Analysts to push indicators to endpoints (DNS resolvers, firewalls, Web Application Firewalls, etc.) and monitor hits that would indicate an emerging attack.

Bfore.Ai provides a fully managed Brand Digital Asset protection service, by running PreCrime Brand and sending a minimum number of alerts, with near zero false positives, directly to the threat intelligence team.

Network disruption of malicious domains and subsequent takedowns are implemented to stop the attack before it starts.

Customers protected and high savings achieved

Over the course of the first 6 months, 41 threat vectors were predicted and proactively taken down. No victims reported.

Savings of $12M dollars were saved, by avoiding costly commercial gestures, legal proceedings, impact to reputation and optimizing time management from remediation and post-mortem.

PreCrime technology is now helping the Signify Threat Intelligence team keep the organization and their stakeholder secure continuing to identify emerging threats and apply countermeasures to avoid victims.

Bfore.ai the perfect tool to help any Cyber Threat intelligence team to predict the crime before it happens. Superb detection of threat actor's attack infrastructure. But besides detection, bfore.ai, provides the tools to fight the crime with mitigation and take downs of the threat actor's assets

Kobe S. Head of Cyber Threat Intelligence

Contact Us Now

FR +33 7823 62484
sales@bfore.ai
https://bfore.ai

"PreCrime is like weather forecast but for Cybersecurity"

Luigi Lenguito - BforeAi CEO