CybelAngel

CUSTOMER CASE STUDY

Signify Secures Data Leak Protecting Intellectual Property

CybelAngel prevents Intellectual Property theft by illuminating exposed project files.

WWW.CYBELANGEL.COM

> CybelAngel made a lot of noise in the company. Stakeholders would ask where did I find this? What provider am I using? CybelAngel's name and finding connected devices came up again and again.

Kobe Shwartz,
Head of Cyber Threat Intelligence and Analysis

Executive Summary

ABOUT SIGNIFY

Signify is a global leader in lighting for professionals, consumers, and the Internet of Things. Signify has a large international presence with 38,000 employees in 70 countries. Known internationally for their marque brands like Phillips, Color Kinetics, and Interact, Signify has sales of €2.6 billion.

With applications ranging from commercial, residential, and agricultural, Signify partners with a wide range of third parties across the globe. Signify has invested heavily in innovative technologies such as IoT applications such as their Li-Fi, energy-efficient lighting, and 3D printed luminaries contribute to a safer, smarter more sustainable world.

Within a highly competitive market pushing technological boundaries, the loss or theft of intellectual property would have a major impact on revenue and product development. Signify depends on Kobe Shwartz and the cyber threat intelligence department to prevent these losses when and where ever they appear.

CHALLENGES

A key cyber threat Kobe Shwartz handles is leaks from employees and Signify employs tens of thousands of people. Employees tend to keep emails, documents, and project files from their everyday work. There are a multitude of reasons as to why; reflex, they are proud of their work, trying to keep organized or to be later used as a template, and so on.

These files are squirreled away on USB drives, personal servers, or cloud drives like GDrive, far beyond a cybersecurity team's awareness or control. While there is no malicious intent from employees, there will be harm done. Documents living outside of a company's control are leaks, these leaks become breaches in due time.

Kobe Shwartz, Head of Cyber Threat Intelligence and Analysis at Signify, was facing just this issue when a former employee archived hundreds of design documents onto an unprotected personal server.

> One alert stood above the rest. A former employee removed project files from us and another brand. It doubled the risk and severity as not just one company but two were affected.
>
> Kobe Shwartz,
> Head of Cyber Threat Intelligence and Analysis

These documents contained new designs that if leaked could've damaged Signify and other brands' competitive position and control of innovative technologies. **"The documents uploaded were highly sensitive. Immediately, Legal and Privacy stakeholders were called in. The potential compliance and legal ramifications could have been severe. With the info from CybelAngel we could take action immediately,"** explained Kobe Shwartz.

Solution: Data Breach Prevention

CybelAngel continuously scans the web for exposed documents on unprotected servers, connected devices, or other digital repositories beyond an enterprise's awareness or control.

Our Machine Learning allows us to sift through billions of records to reduce that number to dozens that our cyber experts analyze, removing false positives to separate the signal from the noise for clients.

"We started with a small team and couldn't handle all the alerts. CybelAngel could process the alerts, digest them, and send us specific incident reports with no false positives." - Kobe Shwartz related. With reliable alerts, Kobe and his team could focus their efforts where they could do the most good.

In addition to confirmed alerts, CybelAngel provides critical context that is key to remediating leaks. CybelAngel incident reports include detailed information, in some cases the name of the person leaking, companies involved, file paths, and examples of documents from the leak.

"The incident reports are detailed, it makes them easy to handle. Every alert 2 and up was sent to a stakeholder and the specifics included made issues simple to be handled." Kobe Shwartz recounted. The context in CybelAngel alerts helped to identify the leaker, pinpoint the vulnerability and empower Kobe and Signify to take action removing the project files from the personal server.

> "When we at Signify use CybelAngel, it's about finding data leaks that nobody was aware of."
>
> Kobe Shwartz,
> Head of Cyber Threat
> Intelligence and Analysis

CybelAngel's digital risk protection solution has become a part of an ongoing training program. Having real-world and personal examples has added to the effectiveness of the data resilience officer and their programs. **"CybelAngel is different. It helps us cover attack surfaces and areas that no one else does. This increases our coverage and has become a key part of our threat intelligence program,"** describes Kobe Shwartz.

RESULTS

- Millions of dollars in potential legal actions and privacy violations were prevented in the first month
- Major reduction in incident response time from actionable contextualized incident reports
- Increased Visibility - CybelAngel located multiple unsecured connected devices unknown to IT
- Real-world examples of prevented breaches help the Data Reliance Officer develop training programs