CybelAngel

CUSTOMER CASE STUDY

Sanofi Secures Attack Surface With The Help Of CybelAngel

How the global leader in healthcare prevents hundreds of data leaks from turning into major breaches across complex supply chains

“With CybelAngel, we establish a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can’t, by design, take control of their security.”

Jean-Yves Poichotte

Global Head of IS Security, Sanofi

Executive Summary

CHALLENGES

Sanofi is a global leader in healthcare across seven major therapeutic areas from cardiovascular to vaccines. The company was founded in 1973 and now employs over 100,000 people across more than 100 countries. It relies on 73 manufacturing sites operating in 32 different locations.

The COVID crisis has shed a dire light on the structural vulnerabilities and daunting attractiveness of global pharmaceutical supply chains for hackers. The end-to-end health pharmaceutical supply chain has become the target of an increasing number of cyber-attacks, both from state-affiliated and criminal organizations.

“Protecting Sanofi is great, explains Jean-Yves Poichotte, but it is not enough because we are not alone.” Indeed, almost half of Sanofi’s operations are in fact delegated to third parties. “Each time we open our organization, explained Jean-Yves Poichotte, it is a new opportunity for the hackers to penetrate our infrastructure, and to steal some information. The others are my weak point. So **our posture is to say that if we can’t protect, we have to detect and to react fast** in order to prevent the damages.

SOLUTION

With CybelAngel, Sanofi can anticipate risks across geographically-scattered operations, and react before exposure turns into devastating security breaches.

Jean-Yves Poichotte explains: “With CybelAngel’s digital risk protection solution, we have established a new border of detection outside of our architecture, encompassing the world of our partners and suppliers, where we can’t, by any type of action, take control of their security.”

RESULTS

120+ third-party-related breaches are prevented each year

Increased visibility over blindspots into vendors’ IT infrastructure

Incident response down to hours instead of days thanks to zero-false positives, real-time alerting, detailed and actionable incident reports

Robust, ongoing vendor risk assessment program

Watch the full interview