CASE STUDY

tenable.ad

# How the pharmaceutical leader Sanofi successfully protects its global Active Directory infrastructures

## Worldwide critical infrastructures

- Industry: Pharmaceutical
- Location: Worldwide
- Revenue 2017: 35,055M €

SANOFI

Sanofi is a global and leading pharmaceutical company committed to improving healthcare access. From prevention to treatment, Sanofi transforms scientific innovation into healthcare solutions in fields such as human vaccines, infectious diseases, and diabetes. The company's massive R&D investments have further established its leadership. The pharmaceutical group has greatly increased its presence abroad, especially in emerging countries. Today, it counts more than 100,000 employees in 100 countries and 87 manufacturing sites in 38 countries.

## Challenges

More people and locations have led to a more complex environment, representing a bigger attack surface. With its numerous facilities worldwide, what is the probability of one end user's endpoint becoming compromised? Through a basic phishing campaign, this is almost child's play for an attacker to get into the company and explore the entire network using only native Active Directory commands.

### Benefits

- Bird's-eye view of the company's infrastructure security
- Harmless to critical infrastructures such as production chains
- Continuously refined remediation and improvement plans

### KPIs

- 1 centralized Tenable.ad console for the entire perimeter
- 25+ domains in 10+ forests
- 360,000 protected users spread over 170 countries

### Stakeholders at Sanofi

- 1 Security Manager
- 2 Security Engineers
- 2 Active Directory Architects

### Tenable dedicated team

- 2 Senior AD Security Engineers
- 1 Technical Account Manager
- 1 Customer Success Manager

On top of that, Sanofi is subject to strong legal regulations on its production chain. For instance, concerns about the doses of a vaccine are enough for legal measures to force Sanofi to withdraw from the market the entire production of vaccines, inflicting millions of dollars in losses. Since facilities are more and more interconnected, adequate security measures must be taken.

As the security backbone of the Information System, Active Directory was one of the central components being used to monitor and protect these production environments. The challenges for Sanofi were to find the right solution able to protect its worldwide perimeter and to consolidate the security of these Active Directory environments.

## Solutions

The CISO's team identified Tenable.ad as the most effective way to tackle Active Directory risks at their root, instead of dealing with the aftermath.

One of Sanofi's main goals was to clarify the different sets of policies, configurations, and data within the group to detect inconsistencies, vulnerabilities, and/or malicious behaviors. The Tenable.ad platform manages multiple infrastructures and allows Sanofi to have a global view of all these security parameters at a glance through a unique console. Delegation rights, password policies, authentication protocols, GPOs, and other critical functions are now perfectly managed and controlled by Sanofi's teams. The size and constant evolution of the AD perimeter is no longer a security risk.

Sanofi increased its security boundaries even further by elaborating a global security roadmap plan thanks to Tenable.ad's recommendations. Tenable.ad's in-depth threat scores enabled Sanofi to define the best course of action for achieving a state-of-the-art Active Directory infrastructure.

## Result

### Worldwide Active Directory infrastructure coverage

The Tenable.ad deployment was completed in a flash. Without having to install an agent or requiring administrative rights,

### Integration plan insights

- 6 months to fully monitor every Sanofi domain
- Zero risk on production IT operations
- Intensive training sessions with internal and external Sanofi teams

monitoring was smoothly implemented over the whole AD perimeter – including the numerous entities and international subsidiaries of the pharmaceutical group. The implementation of the solution was completely transparent to the 360,000 AD user accounts and had no impact on the day-to-day activities of Sanofi's employees. Using unrivaled Tenable.ad Indicators of Exposure, Sanofi was able to identify and tackle major security risks within its corporate environment. Since then, the company has prevented all security regressions on its infrastructures using Tenable.ad's real-time monitoring.

## Continuous protection of highly critical assets

R&D data is a strategic target for crime organizations, rogue states, and competitive players. Preventing sensitive data leaks by enforcing strong security boundaries on the core system securing user access is key to ensuring strong market positions in the pharmaceutical industry.

Sanofi chose Tenable.ad for its ability to go beyond the classical event log correlation approach to consider the entire risk spectrum. This way, Sanofi was given all the necessary tools to successfully tackle ever-evolving and ever-increasing attack vectors. By interfacing Tenable.ad's real-time capabilities to its SIEM infrastructures, Sanofi was able to immediately react to any new attack vector and protect its infrastructure before damage could been done.

## Adaptable to fit modern corporate environments

Tenable and its certified partner network provide not only the most advanced product for Active Directory security, but also a complete solution adaptable to any corporate environment. By listening carefully to Sanofi's issues and specificities, Tenable's certified partner gained a deep understanding of Sanofi's business so they could design tailor-made propositions. Finally, Sanofi's engineers were given access to Tenable's Users Community, where they had the opportunity to share intelligence and best practices with security peers.

"BY DEPLOYING TENABLE.AD ON OUR GLOBAL PERIMETER, WE GAVE STAKEHOLDERS MUCH-NEEDED VISIBILITY OF CORPORATE CYBERSECURITY RISKS."

– Jean-Yves Poichotte
Global Head of Cyber Security