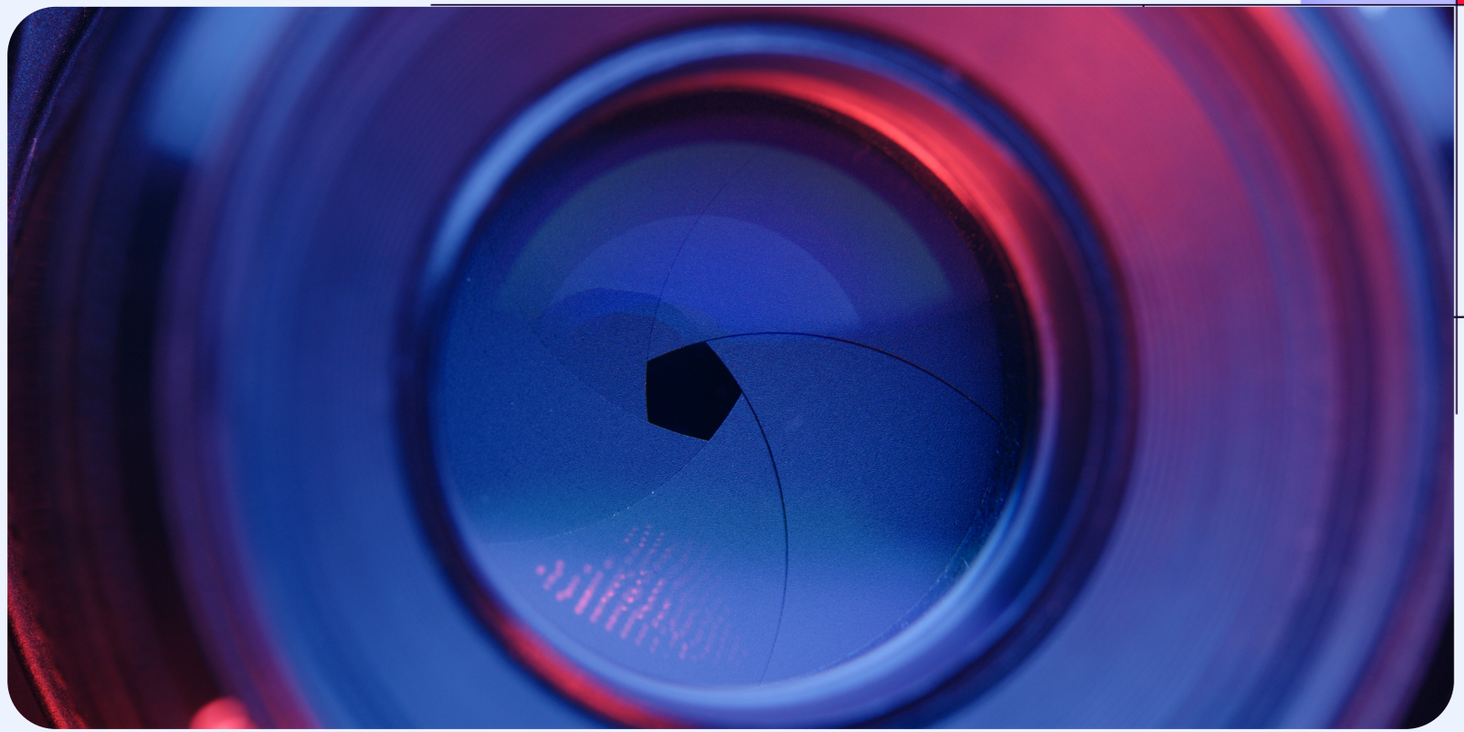
CUSTOMER STORY

LYNRED



“

In less than two days, the machines were installed, and the flows were visible. The NDR, aligned with our ISMS, provided us with complete visibility. This approach allowed us to detect relevant elements as early as the first week.

Bertrand FRÉMONT
CISO LYNRED

#NDR #DEFENSE #AEROSPACE #INDUSTRY

Bertrand FRÉMONT_
CISO LYNRED

About

LYNRED and its subsidiary US-based LYNRED USA are global leaders in designing and manufacturing high quality infrared technologies for aerospace, defense and commercial markets. Their vast portfolio of infrared detectors covers the entire electromagnetic spectrum from near to very far infrared. The Group's products are at the center of multiple military programs and applications. Its IR detectors are the key component of many top brands in commercial, civilian and military thermal imaging equipment sold across Europe, Asia and North America. The organization is the leading European manufacturer for IR detectors deployed in space.

Cyber challenges_

Detect and secure
critical industrial and defense networks against advanced cyber threats

Manage
limited cybersecurity resources while ensuring comprehensive protection

Integrate
EDR and NDR solutions for unified threat detection and response

Adapt
to evolving cyber threats with a scalable and resilient security strategy

Unify
cybersecurity across a fragmented environment for seamless protection

01

CAN YOU EXPLAIN THE CYBERSECURITY CONTEXT IN WHICH YOU OPERATE?

LYNRED is equally co-owned by Safran and Thales but we were completely independent in the choice of our cybersecurity technical solutions for this project.

Our company is employing over 1,000 employees and is running its operations 24x7. Considering our size and the critical nature of our sector, **we must optimize our resources and we need to avoid multiplying different solutions for every specific issue.**

Additionally, **LYNRED operates across two major sites**, in Grenoble and the Paris region, adding further complexity to our infrastructure management. Therefore, we chose a unified approach to better meet our needs while considering our infrastructure.

> *It was therefore crucial to add a layer of network visibility to monitor activities that escape the EDR's perimeter, especially on industrial systems (IS).*

02

WHAT DOES THE CYBER RISK LOOK LIKE, AND WHAT TRADITIONAL METHODS DO YOU USE TO MITIGATE IT?

The main risk we face today concerns **cryptographic attacks**, which we have identified as the primary threat. Alongside this observation, we have launched a comprehensive initiative to reduce these risks, addressing our systems architecture, organization, and the tools we use. Like many industrial companies, we are strengthening our security posture. We are gradually **moving away from traditional antivirus solutions,** which have become insufficient against new threats, to adopt more robust solutions better suited to evolving cyberattacks.

03

WHAT SOLUTIONS HAVE YOU CHOSEN, AND WHAT IS THE STATUS OF THEIR DEPLOYMENT?

We decided to approach our three projects—architecture, organization, and tooling—in an integrated manner. The idea is to **combine several complementary solutions:** EDR for individual protection, NDR for large-scale protection, a managed SOC for 24x7 continuous monitoring, and a CSIRT for emergencies or business continuity planning (BCP).

Our choice was based on several factors:

> **Trust in the technology,** with the key question of whether the solution would ruly meet our specific needs.

> **Our ability to manage it internally,** or whether it would eventually need to become a managed service.

> **The financial aspect,** even though, in this case, the allocated budget was relatively similar for the different options.

We opted for the Sentinel One EDR, Gatewatcher NDR, and managed SOC with Synetis.

04

WHY DID YOU CHOOSE TO INVEST IN AN NDR SOLUTION?

While EDR is an effective solution, an industrial environment like LYNRED's imposes constraints that do not always allow its deployment, particularly on certain specific systems. It was therefore crucial to add a layer of network visibility to monitor activities that escape the EDR's perimeter, especially on industrial systems (IS).

EDR is deployed where we have complete control of the system, particularly on servers and workstations, but in OT environments, where we do not have this control, NDR becomes essential. **NDR allows us to capture all network traffic,** regardless of the nature of the equipment involved, complementing the coverage offered by EDR. Together, these two solutions provide **comprehensive protection tailored to the diversity of our systems.**

Discover our technological alliances

HEAD OFFICE
Veurey-Voroize, France

BUSINESS SECTOR
Semiconductor Manufacturing

> 1,000
employees

MARKETS SERVED
defense, space, security & surveillance, industry, consumer, smart building and automotive

05

AFTER OPTING FOR AN NDR SOLUTION, WHY DID YOU CHOOSE GATEWATCHER?

As part of our request for proposals, we conducted an in-depth analysis of the various solutions available on the market. We participated in workshops and demonstrations with several vendors, including international competitors.
At the end of this process, **we chose what we considered the best-performing solution that met our detection and security needs.**

We also had **several detection objectives:** monitoring North/South traffic, such as data exfiltration between the Internet and the DMZ, and collecting East/West traffic, especially on our industrial networks.

What convinced us about Gatewatcher was the **modularity of the solution:** it can be deployed on-premises, in SaaS mode, or a hybrid of both, depending on the needs. This flexibility is crucial, especially in a context where our infrastructure is spread between Grenoble and Paris. Gatewatcher precisely allows the combination of physical probes and virtual machines in a virtualized infrastructure.

Another essential aspect for us was **interoperability.** We wanted solutions that were fully integrated into our existing ecosystem, capable of communicating with each other, rather than isolated systems. Additionally, the solution is comprehensive and quite easy to handle.

06

CAN YOU TELL US ABOUT THE SOLUTION DEPLOYMENT AND THE MAIN CHALLENGES ENCOUNTERED?

The deployment, although quick once the locations and interconnections were defined, requires special attention because «the devil is in the details». Each network flow must be carefully considered, involving close collaboration with the network team and Gatewatcher. This is not a project that can be carried out alone.

Once this preparatory phase was completed, everything moved very quickly: in less than two days, the machines were installed, and the flows were visible. The NDR, aligned with our ISMS, provided us with complete visibility. This approach allowed us to detect relevant elements as early as the first week.

Concrete use cases_

> Phishing attempt thwarted through DNS query analysis:

We quickly foiled a phishing attempt by **identifying a malicious domain through a simple DNS query.** Gatewatcher detected this suspicious activity by analyzing queries to potentially dangerous servers. Although the process initially generated many alerts, these quickly proved crucial in enhancing our security. Thanks to this analysis, **we blocked the threat before it reached the intended user's mailbox.**

> Mitigation of a critical vulnerability on IP telephony:

We identified an attempt to exploit a vulnerability on our IP telephony platform, thanks to the visibility provided by NDR on North/South flows. By analyzing incoming and outgoing data, the **NDR detected that one of the platforms was not up to date with a security patch.** This detection allowed us to act quickly by fixing the flaw and taking proactive measures, such as blacklisting malicious sources trying to exploit this vulnerability.

07

WHY DID YOU CHOOSE TO COLLABORATE WITH AN MSSP TO OPERATE YOUR NDR?

As a mid-sized company with a dedicated cybersecurity team, it was essential for us to make the most of our NDR solution. **There is nothing worse than deploying a solution without fully leveraging its benefits.** In order to optimize cost and efficiency for a 24x7 monitoring, we chose to outsource this part with Synetis' support while keeping control over the consoles. That said, our decision to use a MSSP meets our specific needs. The Gatewatcher solution is intuitive and easy enough to handle to be operated internally by companies with the necessary resources.

One of our main challenges was being able **to react quickly,** even if a threat, such as data exfiltration, occurred on a Friday evening. It is not enough to rely solely on the NDR; you must trigger the appropriate alerts, act on the information system, and contact the CSIRT if necessary. Since our internal teams did not have the required skills for such responsiveness, we opted for this hybrid solution while maintaining the ability to conduct our analyses.

Our model is based on a tripartite collaboration: LYNRED, Synetis as managed SOC, and Gatewatcher for NDR solution operation.

08

YOU DEPLOYED BOTH AN NDR AND AN EDR SIMULTANEOUSLY. WHY NOT CONSIDER XDR SOLUTIONS?

The XDR approach is sometimes used for marketing purposes. We do not see the benefit of choosing a single solution that claims to do everything, **as such solutions generally do not excel in all areas.** Our goal is still to streamline the tools we use. If we end up with a different console for every issue, it will not be optimal for us or the managed services we work with.

In my opinion, **these are still distinct solutions today.** NDR and EDR aim to protect the company but do not apply to the same types of assets and do not operate at the same level. Therefore, it is not necessary, at this stage, to attempt to merge all these technologies into a single solution.

Key benefits_

Detect
advanced threats across IT and OT

Monitor
network traffic for hidden risks

Accelerate
threat response and mitigation

Enhance
cybersecurity resilience in industrial environments

Integrate
seamlessly with EDR and SOC

> *A key strength of the solution was its reactivity and near-instantaneous response. In just 3 hours, thanks to our managed service, we identified the attack, blocked the sources, and launched the necessary updates.*

ABOUT US

A leader in the detection of cyber threats, Gatewatcher has been protecting critical networks of companies and public institutions worldwide since 2015. Our Network Detection and Response (NDR) and Cyber Threats Intelligence (CTI) solutions, analyze the vulnerabilities, quickly detect and respond to cyber-attacks. Thanks to AI converging with dynamic analysis techniques, Gatewatcher delivers a real-time 360-degree view of threats, covering both cloud and on-premise infrastructures.

Contact us

GATEWATCHER
NDR Platform_

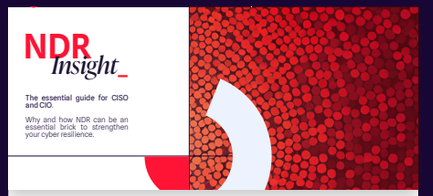
GEN AI_
CTI_
NDR_
DEEP VISIBILITY_
TAP_

Gatewatcher NDR platform offers cyber-threat mapping and behavioral analysis to ensure enhanced detection of targeted attacks, even in the case of encrypted data flow. It combines machine learning with static and dynamic analysis.

Want to *learn more?_*

[CUSTOMER STORY]
Discover our customer story with KNDS European defense industry holding company

[USE CASE]
Strengthen my EDR



[GUIDE]
NDR Insight: The essential for CISO, CIO and C-Level