CUSTOMER STORY

Look Up

“

Sovereignty and information control are critical, and this solution addressed that challenge perfectly. It enabled us to implement a sovereign hybrid model, where the orchestrator handles most event processing while preserving internal control.

Yohann BAUZIL
CISO at Look Up

#NDR #STARTUP #SOVEREIGNTY

Yohann Bauzil_
CISO at Look Up

About Look Up

Look Up is a pioneering company specialized in space surveillance and the security of orbital operations. Its mission is to ensure the sustainable use of space by developing advanced solutions that enhance space traffic management and protect critical infrastructure. Committed to making space safer and more accessible, Look Up supports both public and private players in gaining control over their orbital assets.

Cyber challenges_

Protecting
intellectual property from industrial espionage

Detecting
and managing advanced threats (APTs, ransomware, targeted attacks)

Maintaining
a high level of cybersecurity with limited resources

Ensuring
sovereignty and control over sensitive data

Establishing
an agile and scalable security posture

01 CAN YOU INTRODUCE LOOK UP AND THE CYBERSECURITY CHALLENGES YOU FACE?

The space industry is facing growing challenges: the increasing number of satellites, the proliferation of debris, and emerging threats all contribute to the rising vulnerability of infrastructure. At the same time, we operate in a rapidly evolving tech sector. We must **balance innovation and fast development with the protection of our strategic assets - all while optimizing our resources.**

In this context, cybersecurity becomes a strategic priority. Beyond protecting innovation and sensitive data, it's essential to maintain a strong security posture without sacrificing agility. Our goal is to reach a level of protection on par with large enterprises - using resources scaled to our size. We view cybersecurity not as a constraint, but as a growth enabler, **driven by a pragmatic, scalable, and efficient approach.**

> *NDR emerged as the most suitable solution. It offers a global view of traffic across PCs, servers, cameras, Wi-Fi, shadow IT, and more, allowing us to detect suspicious behavior at the earliest warning signs.*

02

WHAT ARE THE SPECIFIC CYBER RISKS THAT CONCERN YOU MOST?

Growing companies face numerous and evolving threats. These go beyond common cyberattacks and include risks specific to our industry and business model. Protecting intellectual property from industrial espionage is a top priority. Likewise, detecting and managing advanced threats - such as APTs, ransomware, and targeted attacks - remains a major concern. More than a technical issue, **cybersecurity is a key trust factor for our partners and a vital element in ensuring our long-term success.**

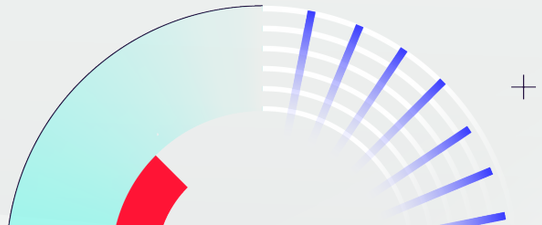
03

WHAT ARE YOUR MAIN TECHNICAL AND OPERATIONAL CYBERSECURITY CONSTRAINTS?

Like many startups, we need to strike a **balance between efficiency and resource optimization.** Ensuring advanced security without a full-time dedicated team requires strategic choices. Our top priority is having **real-time visibility** into our infrastructure to detect suspicious activity early. This monitoring capability must be paired with enough **responsiveness** to investigate incidents quickly, without causing operational overload.

Finally, interoperability also plays a crucial role: any solution we adopt must integrate seamlessly with our existing tools to ensure smooth and effective management.

To meet these challenges, we opted for an **XDR approach** - combining **NDR, EDR, and a security orchestrator.**



04

WHY DID YOU CHOOSE TO IMPLEMENT AN NDR SOLUTION?

We quickly realized that protecting endpoints alone wasn't enough. **Modern attacks often move through the network,** making comprehensive visibility essential to detect threats before they impact systems.

NDR emerged as the most suitable solution. It offers a global view of traffic across PCs, servers, cameras, Wi-Fi, shadow IT, and more, allowing us to detect suspicious behavior at the earliest warning signs. **With its real-time mapping, trace analysis, and investigation capabilities,** we can trace attacks back to their source, understand the attack pattern, and refine reporting.

This strengthens the monitoring of critical communications, boosts incident response times, and minimizes operational impact by delivering actionable insights. The next step will be integrating **Reflex®** to enhance automation and remediation.

HEADQUARTERS
Toulouse, France

INDUSTRY
Aerospace & Defense services

EMPLOYEES
< 50

FOUNDED
2022

GROWTH
Among the largest seed rounds in Europe and strategic partnerships with major institutional and private players within just 2 years

05

WHAT WERE YOUR KEY GOALS WHEN DEPLOYING THE NDR SOLUTION?

Our objective was clear: strengthen our security posture without compromising agility. **We needed a solution that could scale with us, adapting to our evolving needs without adding unnecessary complexity.**

Continuous network monitoring was essential to detect emerging threats before they became critical. But detection alone wasn't enough. We also needed the ability **to quickly assess and prioritize incidents so that we wouldn't waste resources on low-relevance alerts.** Lastly, automating part of the remediation process was crucial to streamline incident management and boost efficiency.

> *We also needed the ability to quickly assess and prioritize incidents so that we wouldn't waste resources on low-relevance alerts.*

06

WHY DID YOU CHOOSE GATEWATCHER TO MEET THESE GOALS?

Before making a decision, we explored several options. We were looking for a partner that could meet our requirements without sacrificing agility. What immediately stood out about Gatewatcher was the **ability to implement a non-cloud-native approach,** allowing us to retain full control over our sensitive data.

In our industry, sovereignty and control over information are paramount, and this solution perfectly matched that need. It enabled us to implement a sovereign **hybrid model, where the orchestrator manages most event** processing while maintaining **internal oversight.**

Beyond integration, modularity was a key factor. As a startup, we evolve quickly—and our cybersecurity must keep up. **Gatewatcher's flexibility allows us to adapt protection levels based on our needs, without unnecessary overhead.**

Finally, the prospect of advanced automation through future Reflex integration confirmed our decision. Optimizing incident response and reducing response time are strategic levers that will help us scale more efficiently over the long term.

Key benefits_

Detect
threats in real time before they impact systems

Deploy
a flexible, hybrid (non-cloud-native) solution ensuring data sovereignty and control

Monitor
all network traffic for complete visibility

Prioritize
alerts and delegate handling to the orchestrator while retaining control over critical threats

Analyze
suspicious behavior through detailed network mapping

Improve
incident response time through automation

*ABOUT US_*

Gatewatcher, a leader in cyber threat detection, has been protecting the networks of businesses and public institutions, including the most critical ones, since 2015. The Gatewatcher NDR Platform (Network Detection and Response) combines artificial intelligence, dynamic and behavioral analytics techniques, and contextualized Cyber Threat Intelligence (CTI). This enables unified, comprehensive visibility, real-time detection and mapping of systems, and an automated, prioritized response to attacks. Deployed across cloud, on-premise, or sensitive infrastructures, and compatible with IT, OT, and IoT environments, it secures all critical assets while streamlining operations through its integrated AI assistant. Gatewatcher combines technological power with operational peace of mind to align cybersecurity with your business objectives.

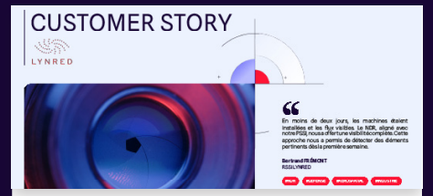
Contact-us

GATEWATCHER
NDR Platform_

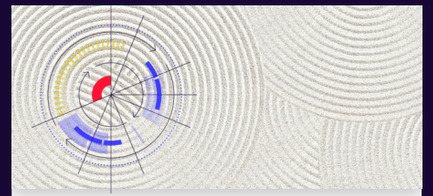
- GEN AI_
- CTI_
- NDR_
- DEEP VISIBILITY_
- TAP_

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.

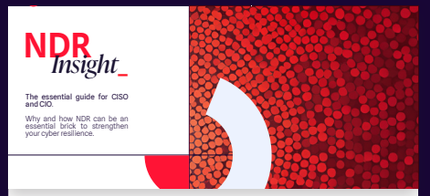
Want to *learn more?_*



[CUSTOMER TESTIMONIAL LYNRED]
Discover our customer story with Lynred



[USE CASE]
Improve Your MTTR



[GUIDE]
Guide: NDR Essentials for CISOs, CIOs, and the C-Suite