CUSTOMER STORY

SECURING THE NETWORKS OF AN ENERGY OPERATOR_

Data sovereignty was non-negotiable, and this NDR platform meets that requirement perfectly. We now monitor our industrial networks 24/7 without disrupting operations, detecting even the slightest anomaly long before it becomes a threat.

Cybersecurity Director of a regional energy operator

#NDR #ENERGY #INDUSTRIALPROTOCOL #OT #SOVEREIGNTY

> *Our daily challenge is therefore to secure heterogeneous, often legacy and mission-critical systems with limited human resources, while ensuring service continuity and sector-specific compliance.*

01 COULD YOU INTRODUCE YOUR ORGANIZATION AND OUTLINE THE CYBER CHALLENGES SPECIFIC TO YOUR SECTOR?

We are a nationwide energy provider, operating across electricity and gas production as well as distribution, with critical infrastructures spread throughout the country. As such, we face extremely high cybersecurity challenges.

On one hand, growing digitalization (smart grids, industrial IoT, remote site management) creates new entry points for attackers. **On the other hand, our industrial networks** (SCADA, plant automation, sensors and OT protocols) are prime targets for sophisticated malicious actors, including state-sponsored APTs or cybercriminals seeking to cause major disruptions. **A successful cyberattack** could not only interrupt the energy supply, with significant economic and societal impact, but also **damage costly equipment or endanger human safety,** especially at sensitive industrial sites (thermal or nuclear plants, high-voltage substations under maintenance, or railway signaling systems powered in real time).

We are also **bound by strict regulations** (LPM – French Military Programming Law, and more recently NIS2-type directives), **which impose a very high level of protection and control.** Our daily challenge is therefore to secure heterogeneous, often legacy and mission-critical systems with limited human resources, while ensuring service continuity and sector-specific compliance.

Cybersecurity challenges _

Protect

critical infrastructures (electricity networks, industrial systems) against advanced cyber threats (APT, targeted ransomware, sabotage)

Maintain

24/7 availability of OT systems while reinforcing security, without ever interrupting operations.

Meet

strict regulatory requirements (National Cybersecurity Agency of France compliance, NIS2, etc.) and ensure sovereignty of sensitive data.

Detect

sophisticated attacks on segmented networks and specific protocols immediately, often invisible to conventional tools.

Monitor

an extended hybrid IT/OT perimeter with limited human resources, avoiding SOC overload and analyst fatigue.

02 WHAT ARE YOUR MAIN TECHNICAL AND OPERATIONAL CONSTRAINTS WHEN IT COMES TO CYBERSECURITY?

Our constraints are directly linked to the nature of our business and systems. First and foremost, the availability of our industrial systems is critical: **no security solution must interfere with the functioning of our automation equipment, nor introduce latency into the control network.** We therefore need passive, non-intrusive technologies. This is why we use network TAPs to duplicate traffic to NDR probes without ever disrupting production on specific segments.

Secondly, our **sites are geographically distributed, sometimes with limited or isolated network connections.** We needed a system capable of running **autonomously on site**, without reliance on a public cloud. **Data sovereignty** and confidentiality of operational data are non-negotiable: sensitive data (such as the layouts of our electricity grids or information on our industrial clients) cannot leave our infrastructure.

Furthermore, **our IT/OT environments are highly heterogeneous**, mixing modern protocols with very specific industrial ones (Modbus, OPC-UA, S7COM, IEC-104, etc.). The solution must therefore "understand" these OT protocols and adapt to legacy or non-standard devices.

And, like many security teams, **we must do more with less:** the energy sector faces a shortage of OT-specialized cyber talent, and we do not have a SOC of one hundred analysts. **Every irrelevant alert or false positive wastes precious time. We therefore needed a tool that intelligently filters and prioritizes alerts, integrates with our existing processes (ITSM, SOC workflows), and automates as many low-value tasks as possible.** The ultimate goal: significantly strengthen security without increasing operational load, and without requiring a hard-to-staff army of experts.

03 WHY DID YOU CHOOSE TO DEPLOY AN NDR PLATFORM?

It quickly became clear that **securing only our workstations and servers (by EDR/EPP, NGFW or IDS/IPS) was not enough**, particularly in an industrial environment. A large part of advanced attacks transit through, or first manifest themselves on, the network. Yet on industrial automation and OT equipment, it is not always possible to install an agent, and event logs are often minimal or non-existent.

We needed full visibility, across both IT and OT networks, to detect threats before they could impact our systems. **NDR proved essential as it continuously analyses traffic across all our segments (from headquarters to plants and substations), identifying suspicious behaviors from the earliest weak signals.** For example, a compromised machine attempting lateral movement or a new malware communicating externally can be spotted through unusual traffic patterns, even when using encryption or stealth techniques.

In short, NDR closes the "blind spot" between IT and OT: it monitors what we could not see before. This proactive approach allows us to anticipate attacks rather than simply react afterwards. By integrating the NDR solution with our existing cyber ecosystem (SIEM, EDR, etc.), **we are progressively building a unified XDR strategy** based on best-of-breed solutions. This allows us to detect threats earlier and respond more effectively by leveraging the strengths of each specialized technology.

INDUSTRY SECTOR
Regional energy operator

NUMBER OF EMPLOYEES
~2 000

NUMBER OF SUPERVISED SITES
Around thirty critical sites, including power plants, substations, regional control centers, administrative headquarters and sensitive facilities

IT AND INDUSTRIAL ASSETS
Approximately 4,000 workstations and servers distributed across the territory; several hundred OT devices (PLCs, sensors, SCADA systems, high-voltage relays, remote management systems); hybrid

04

HOW DID THE NDR DEPLOYMENT UNFOLD, AND HOW DOES IT INTEGRATE WITHIN YOUR ENVIRONMENT?

Deployment was gradual and carefully managed. We began with a pilot perimeter, one of our power generation plants, to validate the solution's effectiveness and non-disruptiveness in real-world conditions. Concretely, probes were installed on strategic IT and OT network segments, fed by TAPs duplicating traffic in real time. Installation required no downtime: within hours, the sensors were in place and analyzing flows.

Gatewatcher's NDR platform is distinctive in that it can be deployed fully on-premise, perfectly matching our sovereignty requirements. We host the orchestrator and centralised management console in our main datacenter, ensuring that all data remains under our control.

Once the pilot proved successful (with valuable detections emerging in the very first days), we rolled out NDR across all our critical sites: substations, regional control centers, headquarters and sensitive facilities. **Integration** with our ecosystem was seamless.

For instance, NDR aggregates and forwards alerts to our SIEM, and connects via API with our in-house monitoring tools. We also enriched alert information with workstation and user context via Active Directory, easing investigations.

Today, the **COCKPIT** console enables us to manage everything from a single interface: **we can see the status of each probe, ongoing incidents, and zoom into any site or network segment, all in real time.** This unified view is a real asset for our operations, especially with IT and OT teams distributed: each accesses the relevant data through the same collaborative tool, without silos.

> *"This unified view is a real asset for our operations, especially with IT and OT teams distributed: each accesses the relevant data through the same collaborative tool, without silos.*

05

WHICH PLATFORM FEATURES DO YOU USE THE MOST, AND WHY?

We leverage the full breadth of the NDR platform. Detection engines, based on a **multi-vector approach**, are at the heart of the system: **they analyze all flows (including obscure industrial protocols) and trigger alerts whenever behavior deviates from the norm or matches a known attack technique.**
What impressed us most was its ability to detect anomalies even within encrypted traffic or "fileless" attacks, which are notoriously difficult to catch, even with our existing tools.

For detailed traffic analysis, we rely heavily on **DEEP VISIBILITY,** which provides complete insight into **who is communicating with whom, using which protocol, and when.** For example, during investigations, our analysts can instantly trace 30 days of historical metadata and map out all key metrics of an OT device (host activity, latency, TCP/UDP protocols). This is extremely useful for understanding the scope of an incident or identifying lateral movements.

The **integrated Threat Intelligence** (CTI) is also a major asset, enriching NDR alerts.On a daily basis, our SOC team particularly appreciates the **COCKPIT interface, which consolidates alerts into incidents, assigns a risk score, and provides tailored views.** For instance, our IT team filters incidents affecting the office IT environment, while the OT team monitors automation-related alerts, all within the same collaborative platform. We have also begun to use **REFLEX orchestration.** Some response actions are already automated through playbooks: for instance, automatically isolating an infected workstation once NDR flags a critical compromise, or pushing a blocking rule to firewalls when a malicious IP is detected. This automation is still partial (activated for specific scenarios), but it already promises huge time savings in handling recurring threats. We have also begun to use Reflex orchestration. Some response actions are already automated through playbooks:

for instance,

automatically isolating an infected workstation once NDR flags a critical compromise, or pushing a blocking rule to firewalls when a malicious IP is detected. This automation is still partial (activated for specific scenarios), but it already promises huge time savings in handling recurring threats.

06

WHY DID YOU CHOOSE GATEWATCHER TO MEET THESE NEEDS?

After a market study and testing phase, Gatewatcher stood out on several decisive points. First, it is a French vendor, offering a sovereign solution without reliance on infrastructures outside our control. For a sensitive operator like us, this was an extra layer of trust, especially since the solution was designed from the outset in line with ANSSI best practices, **easing our compliance.** Technically, Gatewatcher's NDR proved its value during the pilot: the combination of artificial intelligence, static and dynamic analysis, and its native Threat Intelligence feed enabled detection of threats that other tools had missed.

We particularly valued the platform's 360° view: it covers the entire network, from cloud to plant floor, unlike some competing solutions more focused on traditional IT.

Another decisive factor was **integration flexibility.** Gatewatcher integrates smoothly with our existing systems through open APIs and standard connectors. **Rather than imposing a rigid "black box", they delivered a component that we could integrate into our broader architecture without rethinking everything.**

The platform is also **scalable**: it includes NDR, but also embeds CTI modules and can interoperate with all our existing tools.

By choosing Gatewatcher, we felt we were investing in a long-term partnership rather than just buying a product. The Gatewatcher teams supported us closely during deployment and continue to do so, with a clear understanding of our business needs, particularly around OT. This proximity and sector expertise weighed heavily in the decision.

Finally, it was reassuring to know that Gatewatcher is already deployed by other critical operators in France and Europe (energy, defense, transport, etc.). Seeing the solution perform in comparable environments confirmed to us that it was the right choice to meet our challenges.

07

WHAT CONCRETE BENEFITS HAVE YOU OBSERVED SINCE IMPLEMENTING NDR?

The benefits are numerous. The first, immediate gain was **visibility.** Within days, we uncovered elements we had previously missed: forgotten devices communicating on the network, unexpected flows between substations and servers, or misconfigurations that, though not malicious, posed security risks. Being able to "map out" all our traffic, especially in OT, allowed us to remediate these blind spots very quickly.

In terms of threat detection, the platform has proven effective on several occasions. Shortly after the full rollout, an NDR alert highlighted unusual communication between an office workstation and an industrial control system. This abnormal behavior was instantly categorized as high risk. Investigation revealed an unknown malware attempting to infiltrate the OT network, activity that would have gone unnoticed without NDR.

Overall, our **reaction time** has significantly improved: **we can now move from the first weak signal to handling a compromised machine within minutes, whereas it used to take hours or even days to trace an intrusion.**

Another major benefit concerns SOC workload. **NDR's intelligent alert prioritization has reduced background noise:** our analysts are no longer swamped with hundreds of low-severity alerts. False positives have dropped dramatically (we estimate more than a 30% reduction in some categories). This means the team focuses on genuine threats, an improvement felt directly in operational fatigue. Fewer redundant alerts equals more time for in-depth investigations and proactive threat hunting.

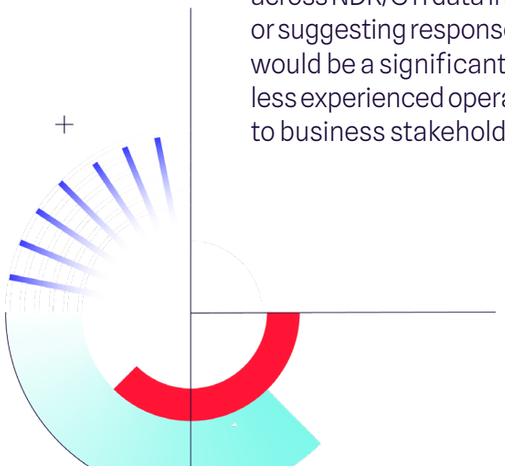
Finally, NDR has **helped us communicate cybersecurity more effectively internally.** Dashboards and reports generated by the platform have enabled us to demonstrate the reality of threats and the effectiveness of our measures to management and business teams. This transparency has strengthened overall trust in our cyber approach, a more intangible but invaluable benefit. Today, cybersecurity is perceived as an asset to the sustainability of our operations, rather than as an opaque cost center.

08

WHAT ARE THE NEXT STEPS TO FURTHER STRENGTHEN YOUR CYBERSECURITY POSTURE?

We want to build on the momentum created by NDR and push further into **reactivity and proactivity**. The next major step, already underway, is the **broader automation of activities via Reflex**. We are working on expanding our automated playbooks to instantly handle routine threats, for instance, isolating an OT segment if a critical behavior is detected, or triggering immediate forensic analysis when an alert is confirmed. The aim is to reduce MTTR even closer to real time, while keeping analysts in control of strategic decisions.

At the same time, we are closely following advances in **AI for cybersecurity. GAIA**, the generative AI-powered cyber assistant, is of particular interest. In the future, we plan to integrate **GAIA into our SOC to support our teams with analysis and decision-making. For example,** GAIA could help analysts by translating complex searches across NDR/CTI data into natural language, summarizing an incident, or suggesting response options based on millions of known IoCs. This would be a significant gain in time and efficiency, especially for our less experienced operators, and would also help present information to business stakeholders in a clear and understandable way.



*Benefits of the NDR Platform_*

Detect threats in real time
across the entire network, before they impact systems.

Monitor all traffic (IT and OT)
for complete visibility and dynamic mapping of communications.

Automatically enrich
alert context using AI and CTI (continuously updated threat indicators).

Prioritize critical incidents
and filter false positives, allowing analysts to focus on what truly matters.

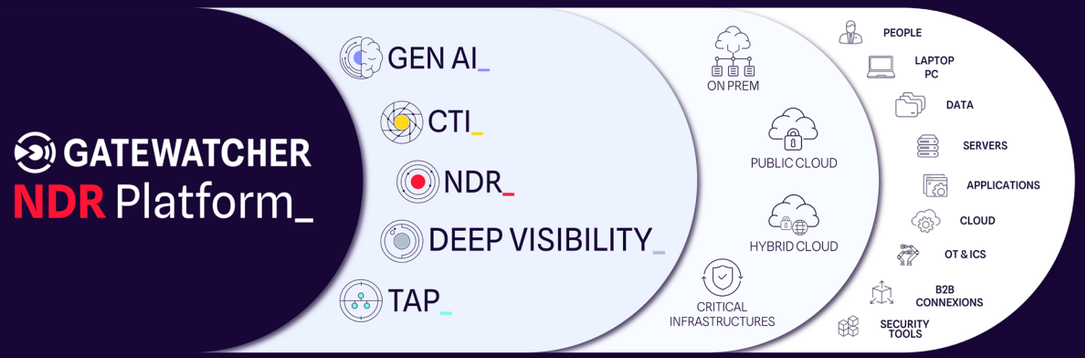
Automate attack response
(host isolation, IP blocking, etc.) to accelerate remediation and reduce response time.

Integrate seamlessly
into the existing ecosystem (SIEM, EDR, firewalls, SOC, etc.) for unified, efficient protection.

*About us_*

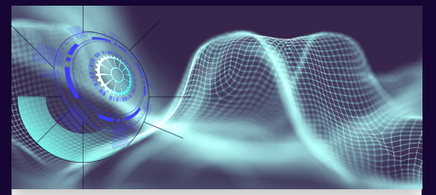
Gatewatcher, a leader in cyber threat detection, has been protecting the networks of businesses and public institutions, including the most critical ones, since 2015. The Gatewatcher NDR Platform (Network Detection and Response) combines artificial intelligence, dynamic and behavioral analytics techniques, 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

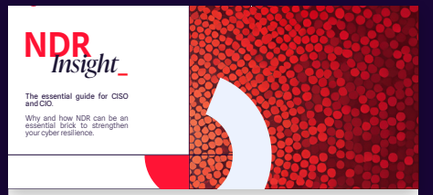


Want to *learn more?* _

[VIDEO]
Easy as NDR : A must have



[USE CASE]
Secure your OT environments



[GUIDE]
NDR insight: Essentials for CISOs, CIOs, an the C-Suite