CUSTOMER STORY

SAMSIC
FACILITY MANAGEMENT

“Gatewatcher NDR helps strengthen SOC capabilities, reduce reliance on service providers, improve the detection of advanced threats, and enable a faster and more effective response.

DAVID LY - Technical Cybersecurity Manager at Samsic Facility Management – Samsic

#NDR #SOC #REACTIVITY

DAVID LY_

Technical Cybersecurity Manager at Samsic Facility Management – Samsic

01

CAN YOU PRESENT SAMSIC FACILITY MANAGEMENT AND THE BUSINESS CHALLENGES THAT MAKE SERVICE CONTINUITY CRITICAL ON A DAILY BASIS?

Samsic Facility Management is a major player **in outsourced facilities management,** delivering tailored solutions designed to optimize costs, improve efficiency, and ensure a working environment adapted to companies' needs. Its offering ranges from single-service contracts (such as cleaning or security) to multi-service facility management, as well as full outsourcing of general services. The objective is to allow organizations to focus on their core business while benefiting from a high-performance, secure working environment that complies with hygiene and environmental standards.

Service continuity is based on the ability to anticipate and manage incidents (system failures, natural disasters, fires, etc.). Samsic Facility Management implements emergency plans and conducts regular simulations to ensure business resilience and maintain operational continuity in the event of a crisis.

02

WHAT SECURITY TOOLS AND PROCESSES DID YOU HAVE IN PLACE, AND WHAT WERE THEIR LIMITATIONS IN TERMS OF OPERATIONAL EFFECTIVENESS?

We had a set of traditional security tools in place: firewalls, EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), and monitoring solutions. These solutions provided a first line of defense. However, they had significant limitations in terms of operational effectiveness: they offered only partial visibility into network traffic, generated a high volume of alerts that were difficult to prioritize, and did not allow for accurate detection of sophisticated or dormant threats circulating at the network level.

In this context, **deploying the Gatewatcher NDR solution became essential**. It provides **complete, real-time visibility into network flows,** enables **the detection of abnormal behaviors** and multi-vector attacks from their earliest weak signals, and significantly strengthens teams' ability **to investigate, correlate, and respond effectively.**

Gatewatcher NDR therefore integrates as a critical building block to close the blind spots left by existing solutions and to raise the overall level of cybersecurity.

*Cyber challenges_*

Strengthen
the overall understanding of what is truly happening across IT and cloud environments

Reduce
risks and the SOC's operational workload in the face of the increasing volume and diversity of alerts

Automate
alert qualification and prioritization

Support decision-making
by determining what matters, what does not, and what requires action—based on all network signals

Improve
the group's overall resilience against advanced threats

03 WHAT ARE YOUR MAIN TECHNICAL AND OPERATIONAL CONSTRAINTS IN TERMS OF CYBERSECURITY?

Training of SOC analysts and continuous skills development: Teams must be regularly trained to keep pace with the rapid evolution of threats. The shortage of expert resources and the difficulty of maintaining a high level of specialization represent a major constraint.

User awareness: Despite ongoing awareness initiatives, the human factor remains one of the primary risk vectors. Ensuring constant and consistent vigilance across the organization continues to be an operational challenge.

Dependence on external service providers: Part of the security operations and monitoring relies on third-party providers, which can result in reduced direct control, delays in incident response, and coordination constraints.

Heterogeneity and complexity of infrastructures: The coexistence of on-premises environments and heterogeneous network architectures makes it difficult to standardize tools, correlate data, and implement unified monitoring.

These constraints reinforce the need for solutions that deliver full visibility, more accurate detection, and reduced operational burden.

In the face of increasing infrastructure complexity, operational overload, and lack of visibility, **Gatewatcher NDR strengthens SOC capabilities, reduces dependence on service providers, improves the detection of advanced threats, and enables a faster and more effective response.**

04 WHAT CONVINCED YOU TO ADOPT AN NDR PLATFORM, AND WHAT ROLE DID YOU EXPECT IT TO PLAY WITHIN YOUR SECURITY STACK?

What convinced us to adopt the Gatewatcher NDR solution was primarily its ability to provide **continuous monitoring of network traffic** and to identify, in real time, abnormal or malicious behaviors, **whether zero-day threats, stealthy attacks, lateral movements, or unusual activities that are difficult to detect with traditional solutions.**

By delivering complete and unified network visibility, NDR technology addresses a critical detection blind spot and **strengthens the overall understanding of what is truly happening across our IT and cloud environments.**

We expected this solution to seamlessly complement our existing security stack by **integrating naturally with our SIEM, EDR, and firewall tools.** The objective was clear: significantly reduce risk, detect threats earlier, respond faster, and improve the group's overall resilience against advanced threats. Today, the solution has established itself as a strategic component of our cyber defense, providing enhanced precision, visibility, and action capabilities to our teams.

INDUSTRY
Business services (cleaning, security, reception, technical services, maintenance, logistics, etc.)

HEADQUARTERS
Cesson-Sévigné, France

136 000
employees

640
agencies

+27
countries

05

WHY DID YOU CHOOSE GATEWATCHER OVER ALTERNATIVES, AND WHAT MADE THE DIFFERENCE FOR YOUR TEAMS?

We chose Gatewatcher among the market alternatives for several strong reasons that immediately made a difference for our teams.

First and foremost, its French expertise and sovereign positioning were essential criteria. **Working with a European player that fully controls its technological development provided the transparency and level of trust required to strengthen our cybersecurity posture.**

Gatewatcher also stood out for the strength of its advanced detection capabilities and the automation of its analyses. **Through a unique combination of Artificial Intelligence (AI), Machine Learning (ML), and static and dynamic analysis, the platform detects the most sophisticated threats while automating alert qualification and prioritization.** This has significantly improved our teams' efficiency and responsiveness.

Another key factor was its seamless integration and interoperability with our existing environment, enabling a straightforward deployment with minimal operational constraints.

Finally, a decisive point: **Gatewatcher is currently the only European NDR vendor recognized in the Gartner Magic Quadrant as a Visionary. This international recognition confirms the technological maturity, innovation capacity, and credibility of Gatewatcher's positioning alongside global market leaders.** Added to this is a **high-quality support and guidance experience,** characterized by close collaboration, availability, and a deep understanding of our challenges.

It is this unique combination of sovereignty, globally recognized innovation, advanced detection, ease of integration, and exemplary support that made Gatewatcher the obvious choice for our teams.

> “ *Gatewatcher NDR therefore integrates as an essential building block to address the blind spots left by existing solutions and to raise the overall level of security.*

06

WHICH GATEWATCHER SOLUTIONS DID YOU CHOOSE, AND HOW DO THEY INTEGRATE INTO YOUR ECOSYSTEM (SECURITY TOOLS, SIEM/SOAR, CLOUD, MSP/MSSP)?

We chose to adopt the complete Gatewatcher solution suite, consisting of Gatewatcher NDR, Gatewatcher REFLEX, and Gatewatcher COCKPIT, which acts as the NDR management and orchestration layer. This combination allows us to cover the entire threat detection and response lifecycle while significantly strengthening our operational efficiency.

Gatewatcher NDR provides us with unified and continuous visibility across all our network traffic, eliminating silos between IT and cloud environments.

Gatewatcher REFLEX plays a key role in automation: **it enables us to automatically send notifications for critical alerts and, when necessary, immediately isolate the affected machines.**

The integration of these solutions with our existing security tools (SIEM, EDR, firewalls, MSP/MSSP services) was seamless. This interoperability strengthens the overall coherence of our security posture, reduces technological silos, and enables **advanced automation of our response processes.**

The result is consolidated visibility, enhanced detection capabilities, and faster, more reliable incident response, supporting a more resilient cyber defense.

07

HOW DID THE DEPLOYMENT UNFOLD (PRIORITIES, SCALING, ADOPTION), AND WHAT DID YOU LEARN ALONG THE WAY?

The deployment of Gatewatcher NDR was carried out in a smooth and progressive manner, in parallel with our previous NDR solution, Darktrace. From the very first hours, data ingestion was immediate, without requiring any prior learning phase, which allowed us to gain **instant operational visibility.**

False positive management proved to be particularly straightforward. As Gatewatcher NDR demonstrated a strong understanding of our traffic and environments, we were able to quickly fine-tune detection rules and reach a highly satisfactory level of relevance from the outset.

Scaling was achieved naturally, supported by a flexible architecture and effective interoperability with our existing tools. The teams adopted the solution rapidly, thanks in particular to the platform's ergonomics and the high quality of the information provided.

We would also like to highlight the excellence of the Gatewatcher engineer who supported us throughout the project. His expertise, availability, and deep understanding of our needs were decisive factors in ensuring a fast, controlled, and smooth deployment. It is this unique combination of sovereignty, globally recognized innovation, advanced detection capabilities, seamless integration, and exemplary support that made Gatewatcher the obvious choice for our teams.

This deployment confirmed that operational efficiency does not depend solely on technology, but also on the quality of support and the ease of adoption.

> “
>
> *It is the unique combination of sovereignty, globally recognized innovation, advanced detection, seamless integration, and exemplary support that made Gatewatcher the obvious choice for our teams.*

08

WHAT CONCRETE RESULTS ARE YOU OBSERVING TODAY (RESPONSIVENESS, INVESTIGATIONS, OPERATIONAL PEACE OF MIND, TRACKED INDICATORS)?

Since the deployment of Gatewatcher NDR, we have observed concrete and immediately measurable results across our entire detection and response chain.

Automatic alert correlation and full event traceability now give us **a much more precise and contextualized view of incidents.** This improvement also translates into more **reliable, better structured, and more actionable reporting for both operational teams and decision-makers.**

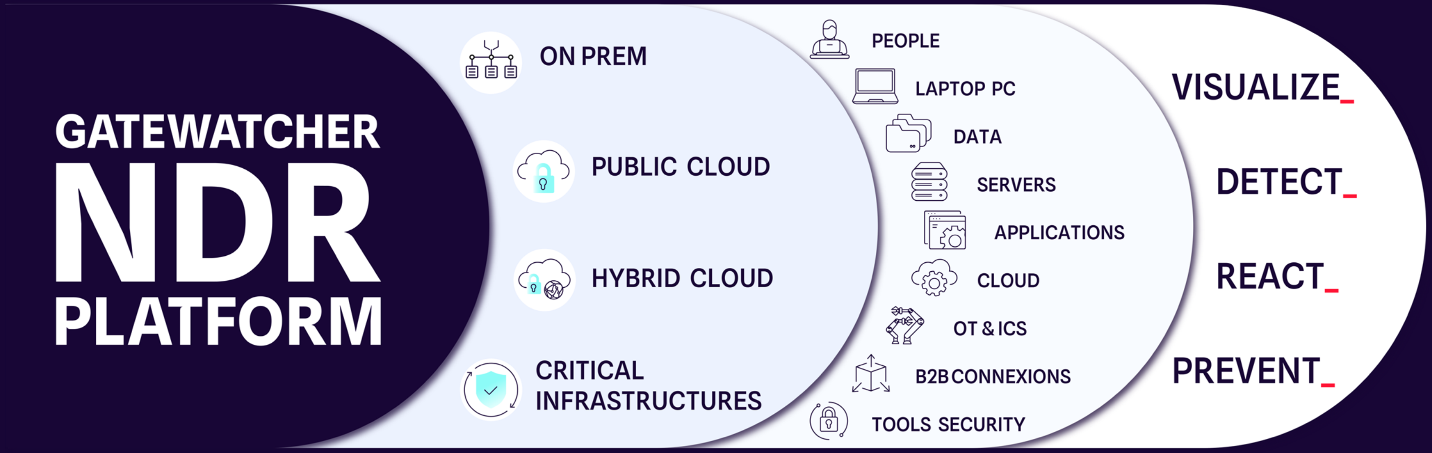
One of the major benefits is **the significant reduction in false positives,** which frees up analyst time and allows teams to focus on truly critical alerts.

We are also seeing **a clear reduction in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).** Thanks to the quality of the information provided and cross-flow correlation, investigations are faster, more effective, and carried out with greater confidence. Overall, the platform strengthens our responsiveness, improves the quality of investigations, and brings real operational peace of mind, supported by performance indicators that are now more precise and more reliable.

*About*_

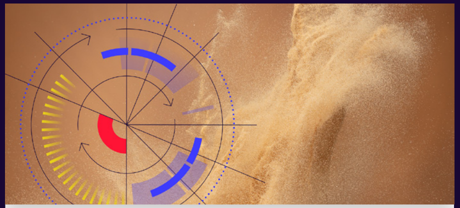
A leader in cyber threat detection, Gatewatcher has been protecting the networks of enterprises and public institutions, including the most critical, since 2015. By combining AI with dynamic analysis techniques, Gatewatcher's NDR platform supports SOC decision-making through contextualized analysis and alert triage. It enables autonomous, tailored responses to each identified threat by delivering complete visibility into network activity, across cloud and on-premises environments. Compatible with IT, OT, and IoT environments, it secures all critical assets while simplifying operations. Gatewatcher combines technological power with operational peace of mind, aligning cybersecurity with business objectives.

Gatewatcher has been recognized as a Visionary in the 2025 Gartner® Magic Quadrant™ for Network Detection and Response (NDR).

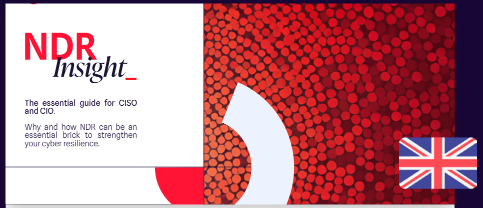


Want to *learn more?*_

[VIDEO]
Easy as NDR | What is a corporate network asset inventory?



[USE CASE]
Increasing SOC effectiveness


NDR
Insight_
The essential guide for CISO and CIO.
Why and how NDR can be an essential brick to strengthen your cyber resilience.

[GUIDE]
The essential guide for CISO and CIO

Contact us