CUSTOMER STORY

INVESTMENT BANK_

“

The NDR has become our fine-mesh safety net: it catches what other solutions miss. In an environment where a single second of latency can cost millions, this level of visibility is vital.

Cybersecurity Director, Investment and Corporate Bank

#INVESTMENTBANK #CYBERRESILIENCE #NDR

> “ *Beyond client data, it’s our trading algorithms, transactional platforms, and real-time data flows that must be protected.*

01

CAN YOU INTRODUCE YOUR ORGANIZATION AND EXPLAIN THE CYBERSECURITY CHALLENGES SPECIFIC TO THE INVESTMENT BANKING SECTOR?

We are a major banking group operating in market activities, asset management, and private banking. In this context, our exposure to cyber threats is constant and ever-evolving. We face targeted and often sophisticated attacks, combining spear phishing, stealthy lateral movements, and complex attack chains. Being interconnected with market infrastructures, international counterparties, and critical systems such as SWIFT significantly increases systemic risk. **Beyond client data, it’s our trading algorithms, transactional platforms, and real-time data flows that must be protected.** We also need to maintain a **high level of compliance** (PCI DSS, DORA, EBA, GDPR, etc.) without ever impacting **operational performance.** Our mission is to ensure that cybersecurity is never a barrier to our investment strategy.

02

WHAT WERE YOUR CYBERSECURITY OBJECTIVES BEFORE DEPLOYING THE NDR SOLUTION?

Our priority was to enhance visibility across the most critical segments of the network including interbank flows, trading environments, and sensitive authentication layers. We wanted **to detect abnormal behaviors earlier, even when traffic was encrypted or segmented.** EDR and SIEM solutions were no longer sufficient: too much noise, too many blind spots, and an excessive workload for our teams. We needed a passive yet comprehensive solution, **capable of identifying weak signals without disrupting operations.** Finally, **we wanted to automate simple responses while keeping full control over critical decisions**.

Cybersecurity challenges _

Protect
critical interbank flows and sensitive transactional data

Monitor
segmented and encrypted environments without impacting performance

Reduce
SOC operational load amid growing alert volume and variability

Meet
regulatory requirements (DORA, PCI DSS, NIS2)

Oversee
multiple entities with different criticality levels

03

WHY DID YOU CHOOSE AN NDR APPROACH, AND WHAT GAPS DID THIS TECHNOLOGY FILL?

The NDR technology complemented our existing XDR architecture. Unlike EDR, which focuses solely on endpoints, NDR analyzes all network flows including those between systems and external communications. In a sensitive environment, this ability to detect lateral movements, internal scans, or abnormal behavior is essential.

We first deployed the Gatewatcher **Trackwatch** detection probe on our most critical segments, particularly those linked to payment systems, due to its ANSSI qualification and compliance with LPM requirements. In parallel, we implemented **the Gatewatcher NDR Platform** to extend visibility to our less critical environments (office IT, printers, HR, etc.), while maintaining unified supervision.

This dual approach allows us to manage each zone according to its level of criticality while maintaining a global, consolidated view.

04

WHAT CRITERIA DROVE YOUR CHOICE OF GATEWATCHER OVER OTHER SOLUTIONS?

Beyond the sovereignty aspect, which remains a prerequisite for our critical environments, what truly convinced us about Gatewatcher was the depth of its **multi-vector detection engine,** combined with an **interface that is both clear and easy to use.** The platform **enables immediate alert triage** while still allowing deep **investigation** when context requires it. This two-level approach, **simplicity in day-to-day use and strong analytical power,** fits our operational requirements perfectly.

The management intuitive interface also stood out for **multi-entity management,** which is a key need in a group where each subsidiary has its own scope and responsibilities. Finally, Reflex allowed us to orchestrate **simple remediation scenarios that interoperate with our existing security and network equipment**. The NDR platform integrated into our current stack without adding unnecessary complexity. Lastly, because Trackwatch is ANSSI-qualified, it fully met our **regulatory obligations** for sensitive environments. This qualification comes with **comprehensive hardening** across every layer, hardware, system, and application, ensuring integrity, confidentiality, and resilience against threats, including zero-day attacks. This level of security provides essential peace of mind in such highly critical contexts.

HEADQUARTERS
PARIS
FRANCE

INDUSTRY
Investment banking, capital markets, structured finance, services for large enterprises

ESTIMATED SIZE
~10,000–15,000 EMPLOYEES DEDICATED TO “INVESTMENT & MARKETS” LINES (EXCLUDING RETAIL BANKING)

MONITORED SCOPE
20+ sites, including headquarters, data centers, trading floors, and critical platforms. Segmented, hybrid networks with SWIFT and SEPA interconnections, private cloud, and regulated zones.

IT FOOTPRINT
Around 20,000 workstations and servers, with monitoring across business-critical systems, payment systems, interbank flows, and office environments.

05

HOW DID THE SOLUTION INTEGRATION GO IN YOUR COMPLEX ENVIRONMENT?

The integration was carried out in several phases. We started with our critical environments, deploying physical appliances in our sensitive zones. Gatewatcher's non-intrusive approach enabled deployment **with no downtime and no impact on sensitive applications.** The platform offers two distinct modes: an **on-premises deployment,** which is essential for segments subject to strong regulatory constraints, and a cloud version better suited to administrative or hybrid environments. This flexibility allowed us to tailor the setup to our risk landscape. Native connectors made it possible to quickly integrate the platform with our SIEM and other solutions. Within the first few weeks, we saw a clear improvement in network visibility and a reduction in our response time. **Gatewatcher's support was also instrumental: rule tuning, playbook creation, and coaching for our SOC analysts... That made adoption and configuration significantly easier.**

> *Gatewatcher's non-intrusive approach enabled deployment with no downtime and no impact on sensitive applications.*

06

WHAT TANGIBLE BENEFITS HAVE YOU OBSERVED SINCE IMPLEMENTING THE SOLUTION?

We have **significantly reduced both our mean time to detect and our mean time to remediate.** Where it previously took us several hours to qualify an alert, it now takes only a few minutes. **Behavioral detection has enabled us to identify network reconnaissance attempts that would have gone unnoticed by other tools.**

The NDR provides us with a global view of our environment, while ensuring precise segmentation for each entity within the group. **Analysts' cognitive load has been reduced thanks to intelligent alert triage.** In addition, the ability to trigger **automated actions** saves us valuable time when dealing with recurring incidents. Our analysts can now focus on what truly matters and remain fully **in control of decision-making.**

07

WHAT ROLE DOES NDR PLAY IN YOUR CYBER GOVERNANCE STRATEGY?

NDR isn't a standalone tool for us: it's a strategic component of our cyber governance. It provides precise metrics on network behavior, anomalies, and exposure surfaces. **These indicators feed into our steering committees and directly influence our prioritization and decision-making.** Having **a sovereign platform that can be segmented by entity while still being managed centrally** is fundamental for us. It allows us to standardize security policies across the group while preserving a degree of local autonomy. **NDR also helps us demonstrate the value of our security approach to executive leadership by making risks visible, measurable, and easy to understand.**

*NDR benefits_*

> *Full, non-intrusive visibility*
across all traffic flows (north/south & east/west), including encrypted traffic

> *Enhanced behavior-based detection,*
enriched by AI

> *Smart alert prioritization and contextualization*

> *Seamless integration*
with the existing SOC ecosystem

> *Entity-level segmentation and unified monitoring*

> *Reduced MTTD and MTTR*
through automation

> *Easier compliance*
without sacrificing operational performance

08

HOW DO YOU ENSURE RAPID RESPONSE WHEN A THREAT IS IDENTIFIED?

We combine several levers: advanced real-time detection through Gatewatcher's NDR Platform, contextual enrichment powered by CTI, and automated response scenarios. For example, if a suspicious internal scan is detected on an office IT segment, a playbook is automatically triggered: the workstation is isolated, the SOC is notified, and a ticket is automatically created for the relevant team. All of this happens without immediate human intervention, with post-action review and validation afterward. This approach allows us to respond very quickly while still staying in control. **We've secured several potential attack vectors without impacting our SLAs.**

09

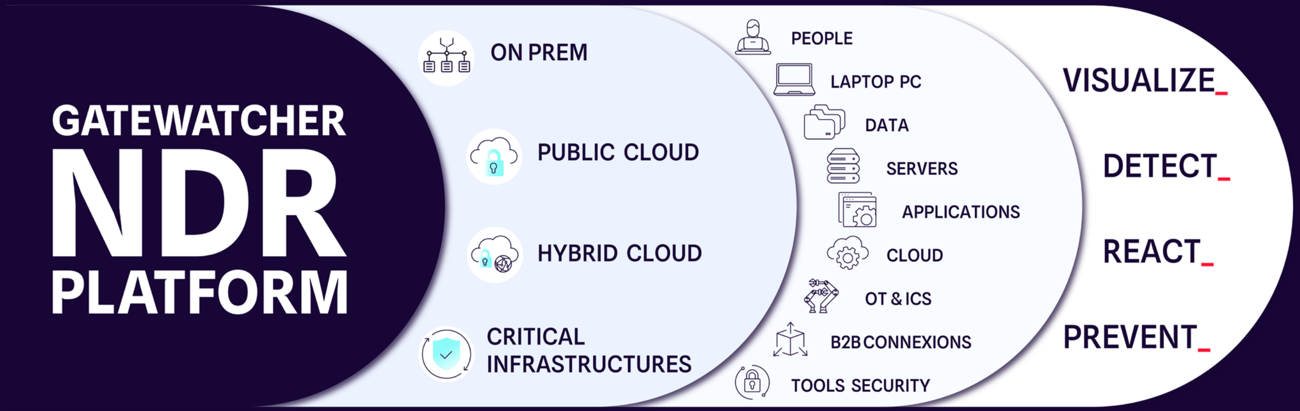
WHAT ARE YOUR NEXT CYBERSECURITY CHALLENGES, AND HOW IS GATEWATCHER HELPING YOU PREPARE?

We're planning a gradual expansion of monitoring to additional scopes: more of our cloud environments, certain offshore environments, and other entities across the group. The NDR's decentralized-but-orchestrated model is a real advantage: each subsidiary gets its own dedicated view, while we maintain a consolidated, group-wide picture. We're also working **to strengthen automated response,** especially for recurring incidents, by developing new playbooks.

*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).



GATEWATCHER NDR PLATFORM

ON PREM

PUBLIC CLOUD

HYBRID CLOUD

CRITICAL INFRASTRUCTURES

PEOPLE

LAPTOP PC

DATA

SERVERS

APPLICATIONS

CLOUD

OT & ICS

B2B CONNEXIONS

TOOLS SECURITY

VISUALIZE_

DETECT_

REACT_

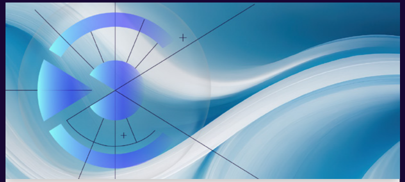
PREVENT_

Want to *learn more* ?_

[VIDEO]
Easy as NDR:
What is the R of NDR?

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

[GUIDE]
Discover our latest NDR Insight guide.



[USE CASE]
Improve my detection time (MTTD).

Contact-us