CUSTOMER STORY

CAISSE DES DÉPÔTS

“

Whether it is protecting the funds entrusted to us or the integrity of French citizens’ personal data, our priority is to secure information flows that have immense strategic value.

Christophe Cavrot, Director of Security, Architecture and Technology Strategy

CDC Informatique **– Caisse des Dépôts Group**

#PUBLICFINANCE #PUBLIC #PRIVATE #NDR #ECONOMY #VISIBILITY

CHRISTOPHE CAVROT_

Director of Security, Architecture
and Technology Strategy
CDC Informatique – Caisse des Dépôts Group

01 CAN YOU INTRODUCE THE CAISSE DES DÉPÔTS AND THE MISSIONS THAT DEFINE YOUR WORK?

Caisse des Dépôts is a public-sector group and a long-term investor. Its core mission is to serve the public interest and support the country's economic development, in support of policies implemented by the State and local authorities.

The Group's activities are structured around five strategic pillars that affect the daily lives of millions of French citizens:

> **Protection of regulated savings:** The institution guarantees the security of deposits for more than 50 million savers (Livret A, LDDS – Sustainable and Solidarity Development Savings Account, LEP – Popular Savings Account). These funds are then converted into very long-term loans to finance large-scale national projects.

> **Financing of social housing:** As the leading financier of the sector in France, the Group covers more than 70% of financing needs for the construction of new social housing.

> **Role as a trusted third party:** Caisse des Dépôts manages public mandates and private funds protected by law (notaries' funds, escrow deposits). It also acts as banker for Social Security and various institutions.

> **Support throughout citizens' life paths:** Through pension management and free digital services such as Mon Compte Formation (My Training Account) or Mon Parcours Handicap (My Disability Pathway), the institution supports citizens at every stage of their lives. It also operates specific services such as Ciclade.fr (a platform to search for dormant accounts).

> **Support for economic development:** Via Banque des Territoires or Bpifrance (the French public investment bank), the Group is a major investor supporting the growth of companies and start-ups throughout the country.

*Cyber Challenges_*

Secure
Critical financial flows and sensitive data supporting public-interest missions

Detect
Threats in complex, segmented, and regulated environments without impacting performance

Optimize
SOC operations in the face of growing alert volumes and increasing threat sophistication

Comply
with strict cybersecurity and regulatory requirements (GDPR, NIS2 – Network and Information Security Directive 2, LPM – French Military Programming Law)

Govern
a diverse ecosystem of entities with varying levels of criticality and security constraints

> *"The challenge is no longer just about protecting entry points and final targets, but about controlling everything that flows between the two. NDR turns our network into a source of active intelligence to neutralize attacks at their earliest signs.*

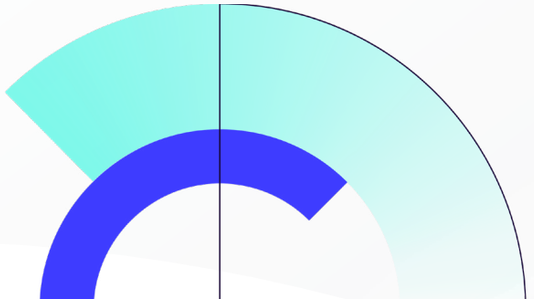
02

IN LIGHT OF YOUR MISSIONS, WHAT ARE THE MAIN CYBERSECURITY CHALLENGES THE INSTITUTION MUST ADDRESS?

Given the diversity and sensitivity of Caisse des Dépôts' missions, security challenges crystallize around two major, closely intertwined axes.

On the one hand, the institution must protect itself as a leading financial organization, which exposes it to threats directly targeting its assets. The challenge is therefore to guard against classic fraud attempts as well as sophisticated attacks aimed at diverting funds or manipulating financial transactions. Maintaining a robust level of security is a sine qua non condition for institutional trust.

On the other hand, **the value and security of citizen data are an absolute priority, as the Group processes massive volumes of information relating to pensioners, training applicants, and French savers.** These datasets, considered high quality due to their up-to-date and comprehensive nature, represent prime targets for malicious actors seeking to resell them or use them as a basis for planning more complex cyberattacks.



> *"The integration of artificial intelligence, and more specifically generative AI, into the Gatewatcher solution makes it possible to go beyond traditional detection and deliver truly augmented, agile, and predictive analysis.*

03

WHAT TOOLS DID YOU PREVIOUSLY HAVE IN PLACE, AND HOW WAS YOUR NETWORK MONITORED AND SECURED?

Before Gatewatcher, our environment already relied on a traditional security baseline, including endpoint and server protection, monitoring tools and a SIEM (Security Information and Event Management), as well as solutions dedicated to cloud and network security. These tools fulfilled their role and enabled us to detect and respond to certain threats, but their effectiveness was limited to incidents that had already been triggered.
In practice, they often intervened too late, once an attack had already begun, and sometimes even after the attacker had already gained access to systems.

Despite these measures, **blind spots remained,** particularly in terms of **full network visibility** and **proactive detection of abnormal or malicious behavior.** These gaps represented a strategic risk: some threats could quietly evolve within our infrastructure without being detected, jeopardizing the overall security of the institution.

HEADQUARTERS
Paris, FRANCE

INDUSTRY
France's leading public financial group, long-term investor, public-interest missions, financial services for the State, local authorities, and strategic sectors

~350 000 EMPLOYEES
across the Group (several thousand in IT, digital, and security functions)

IT ESTATE
> Tens of thousands of workstations and servers
> Highly heterogeneous information systems covering critical infrastructures, financial applications, interbank and institutional flows, and office environments

MONITORED SCOPE:
> Multi-entity, multi-site environment including headquarters, data centers, subsidiaries, and regulated platforms
> Critical financial flows, inter-company exchanges, private and hybrid cloud environments

04 WHAT ULTIMATELY CONVINCED THE INSTITUTION TO ADOPT AN NDR PLATFORM?

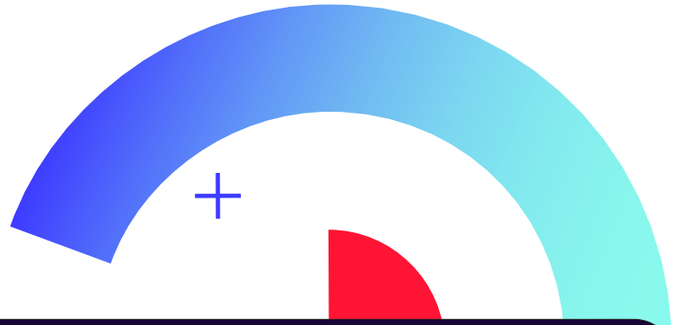
The review of our existing setup highlighted a need for increased visibility. Historically, security efforts focused on two specific endpoints: the perimeter, protected by firewalls or WAFs (Web Application Firewalls), and the workstation, secured by EDR (Endpoint Detection and Response) and antivirus solutions. However, the space between these two pillars, that is, all traffic flowing between servers, workstations, and the perimeter, remained complex to monitor accurately.

Faced with increasingly sophisticated threats, traditional tools, often too static, were reaching their limits. Adopting an NDR (Network Detection and Response) solution became essential to address three major strategic expectations.

First, it was about **filling the network blind spot** by deploying a solution capable of dynamically and continuously analyzing traffic, where traditional tools provided only partial visibility.

Second, the platform needed to **facilitate decision-making by providing a better understanding of internal traffic,** enabling earlier identification of abnormal behavior and much more agile remediation actions.

Finally, the fundamental objective was **to move from reactive defense to active prevention.** With NDR, the institution can now act upstream: instead of intervening once an attack has already reached its final target, it can detect threats in transit and intercept them before they cause damage.



> *The real advantage is playing the move ahead rather than reacting after the fact. On a workstation or server, when an alert triggers, the attacker is already present and the system may already be damaged. With network analysis, remediation happens upstream, before the attack even reaches its target.*

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

The choice of Gatewatcher emerged naturally following a rigorous tender process, as the solution aligns closely with the DNA of Caisse des Dépôts and its digital resilience strategy. As a public institution, relying on a European player with a strong French footprint is a key sovereignty argument that reinforces trust in our infrastructures. Beyond this political dimension, it was **the partnership proximity** that made the difference compared to major US vendors. **Having a partner capable of understanding our concrete needs and allowing us to influence the technological roadmap is a major strategic advantage; we are not just a number, but an active stakeholder co-evolving with the solution.**

This trust is further reinforced by **market recognition,** notably from **Gartner, which positions Gatewatcher as a "Visionary."** For an institution like ours, which relies on international benchmarks to guide its strategy, this validation is **a crucial credibility factor.**

Finally, **the integration of artificial intelligence, and more specifically generative AI, into the Gatewatcher solution goes beyond traditional detection to deliver truly augmented, agile, and predictive analysis.** These innovation efforts fit perfectly with our next-generation SOC (Security Operations Center) approach, where technology supports human expertise in addressing evolving threats.

06

WHICH PLATFORM CAPABILITIES DO YOU USE MOST, AND HOW DO THEY INTEGRATE WITH YOUR ECOSYSTEM?

The strength of the Gatewatcher solution lies in its **comprehensiveness,** providing **a deep network analysis layer that complements our existing tools by covering the entire intrusion chain, or kill chain.** On a daily basis, our teams leverage this capability for **multi-engine analysis** and **real-time traffic inspection.** Beyond local antivirus engines, which form a first foundational layer, we rely heavily on rigorous metadata analysis. This approach enables us to detect weak signals and advanced techniques by monitoring critical elements such as PowerShell commands traversing the network, beaconing related to C2 (Command and Control) servers, and various tunneling techniques.

This well-structured feature set covers all attack phases, from reconnaissance to exfiltration and persistence. We leverage anomaly detection capabilities (NBA – Network Behavior Analytics) and malicious domain identification (DGA – Domain Generation Algorithm), including shellcode and ransomware detection, whether in reconnaissance or execution phases. By eliminating our former blind spots, Gatewatcher's integration into our ecosystem supports a fundamental strategic shift: acting directly on the network flow rather than waiting for the impact on the host.

The real advantage is playing the move ahead rather than reacting after the fact. On a workstation or server, when an alert triggers, the attacker is already present and the system may already be damaged. With network analysis, remediation happens upstream, before the attack even reaches its target.

> *"An augmented analyst is one who can focus on expertise and added value. By entrusting the automatic processing of background noise to the platform's AI, we reduce operational fatigue and increase our responsiveness to real threats.*

07

HOW DID THE DEPLOYMENT UNFOLD, AND WHAT LESSONS DID YOU LEARN FROM THE IMPLEMENTATION PHASE?

The deployment proceeded very smoothly, following a controlled timeline despite starting during the summer period.

Two major phases can be identified. First, **a rapid two-month technical commissioning phase** covering the entire chain from procurement to physical installation of the equipment. Once the appliances were in place, activation itself was extremely fast, delivering the first usable analysis reports within just a few days. This was followed by a four-month **targeted optimization** phase. Rather than being overwhelmed by a massive flow of alerts at startup, the approach prioritized features. The platform's granularity enabled **progressive tuning,** first isolating functions without false positives before refining more complex network analyses.

This implementation phase also delivered major insights and unexpected added value in terms of IT hygiene. **What initially appeared to be false positives during tuning turned out to be a powerful audit tool, highlighting servers generating abnormal or illegitimate traffic.** Thanks to this granular visibility, the institution carried out genuine network cleanup by correcting server configurations that would otherwise have remained hidden. This turned a simple technical deployment into a critical digital sanitation operation.

One of the major benefits of this phase was the tool's ability to surface abnormal network behaviors on our own servers. It wasn't just a configuration phase; it was a real cleanup and remediation effort for our information system.

08

WHAT TANGIBLE RESULTS DO YOU SEE TODAY IN TERMS OF RESPONSIVENESS AND SECURITY OPERATIONS MANAGEMENT?

Gatewatcher's integration marked a decisive step toward what we call an "augmented SOC," with benefits measured across three essential pillars of cyber defense effectiveness.

The first, and one of the most important, is **combating analyst fatigue.** Level 1 teams often spend considerable time on repetitive tasks that inevitably lead to weariness and, by extension, a higher risk of human error. By automating the processing of a large portion of low-value alerts, the solution significantly reduces background noise.

This efficiency gain enables a second strategic pillar: **refocusing on high-value missions**. By freeing analysts from routine tasks, we give them time for what truly requires their expertise—deep investigations, decision-making, and security tuning. This time is reinvested in creating new alerts to anticipate emerging threats rather than merely reacting to them.

Finally, this transformation relies on **a consolidated investigative view** that was previously lacking. While we had EDR logs from endpoints and firewall flows, we lacked fine-grained visibility into what was actually traversing the network. Today, network analysis correlates all this information, delivering a comprehensive view of the attack process and genuine peace of mind for teams. They now have a complete and detailed understanding of the intrusion chain, enabling faster and more accurate responses.

An augmented analyst is one who can focus on expertise and added value. By entrusting the automatic processing of background noise to the platform's AI, we reduce operational fatigue and increase our responsiveness to real threats.

09

CAN YOU SHARE A NOTABLE EXAMPLE WHERE THE NDR PLATFORM PREVENTED AN INCIDENT OR IMPROVED SERVICE QUALITY?

Beyond preventing a single isolated incident, the platform's contribution lies in a genuine shift in analytical posture. **NDR has filled what could be called the "missing link" in our visibility.**

Today, the tool allows us to anticipate alerts and obtain a complete view of incidents. Where we previously had to juggle firewall flows and EDR data without a direct connection, we now benefit from fine-grained analysis of traffic reaching servers or workstations. **This correlation gives us a full understanding of the attack process.**

Another key benefit relates to the evolution toward an "augmented SOC." The tool learns from our environment, which is a real breakthrough enabled by AI. This reduces analyst fatigue by automating background noise processing, allowing us to focus on high-value alerts.

Finally, the solution supports compliance **with our most stringent regulatory requirements,** whether DORA (Digital Operational Resilience Act), GDPR (General Data Protection Regulation), banking regulations, or the French Pacte Law. It is a cornerstone of our strategy to secure all our business lines: Banque des Territoires, social policies, asset management, and strategic shareholdings.

NDR benefits_

Complete, non-intrusive visibility
across all flows (North–South and East–West), including encrypted traffic

AI-enhanced behavioral detection

Alert prioritization and contextualization
with intelligence

Seamless integration
with the existing SOC ecosystem

Entity-based segmentation
and unified supervision

Reduced MTTD and MTTR
through automation

Simplified compliance
without loss of operational performance

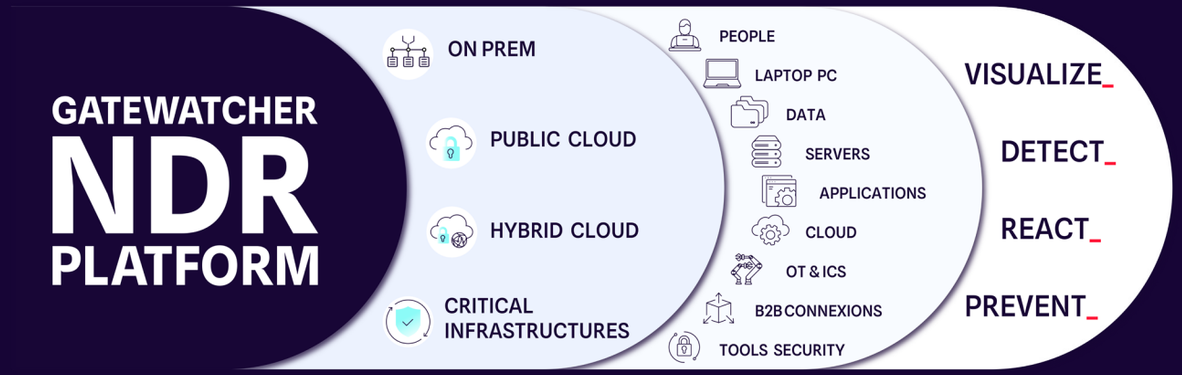
Decision-support capabilities

GATEWATCHER

*ABOUT_*

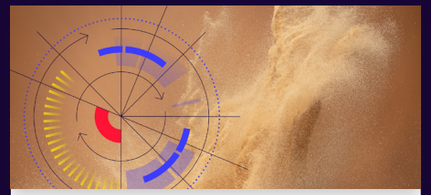
A leader in cyber threat detection, Gatewatcher has been protecting the networks of enterprises and public institutions, including the most critical, since 2015. By combining AI with dynamic analysis techniques, Gatewatcher's NDR platform supports SOC decision-making through contextualized analysis and 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)

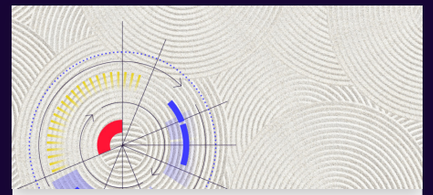


Want to *learn more?_*

[PODCAST]
At the Heart of Public Finance:
When Cybersecurity Supports the Economy



[USE CASE]
Increase SOC effectiveness



[USE CASE]
Improve your response time (MTTR) to security incidents

Contact us