CUSTOMER STORY

STRENGTHENING CYBERSECURITY IN THE EDUCATION SECTOR_

“

With a limited IT budget, we are forced to make tough choices. But a single attack could cost us far more than prevention.

Director of cybersecurity & data protection officer at a higher education institution

#NDR #EDUCATION #BUDGETOPTIMIZATION

01

WHAT ARE THE MAIN CYBERSECURITY CHALLENGES IN THE EDUCATION SECTOR?

Cybersecurity in education goes far beyond securing computers. **The education sector has become a prime target for cybercriminals**, with a sharp increase in attacks over the past three years. **Our institution manages thousands of student records, financial data, and a complex digital infrastructure** ranging from **school management systems to online learning platforms.** With such a fragmented ecosystem, securing every entry point is a major challenge.

Protecting student and staff data is our top priority. Our online learning platforms, grading systems, and administrative portals process massive volumes of sensitive personal information: not just transcripts or registration files, but also medical and accessibility support plans, bank details for tuition fees and grants, disciplinary records, counselling notes, or scanned IDs used for online examinations. All of this makes us an attractive target for cybercriminals. A single breach would not only have financial consequences, but also severely **damage trust among families and the reputation of the institution.**

Beyond digital risks, **library management systems, external partnerships, and distributed infrastructures** add another layer of complexity. From **securing campus network access to preventing unauthorized intrusions,** we must constantly adapt to evolving threats to keep our operations safe.

02

HOW DO BUDGET CONSTRAINTS IMPACT YOUR CYBERSECURITY?

Our institution faces a cruel paradox: growing security needs, but with a stagnant (or barely increasing) IT budget. Unlike large corporations with dedicated teams, the education sector allocates on average around 6.6% of its IT budget to cybersecurity, far below the 10% recommended, at a time when cyberattacks have surged by more than 100%. **This forces us to make tough choices between renewing teaching equipment and reinforcing cybersecurity.**

This financial reality leaves us dangerously exposed. **For years, we prioritized "visible and urgent spending" over strengthening the network,** less visible, but vital. Cybercriminals know this, which is why education has become an easy target. A cyberattack on our student management systems could paralyze teaching and compromise exam data, with remediation costs equaling **several months of our IT budget.**

*Cyber challenges_*

Protect
intellectual property against industrial and state-sponsored espionage

Detect
and manage advanced threats (APTs, ransomware, targeted attacks)

Maintain
a high level of cybersecurity with limited resources

Ensure
sovereignty and control over sensitive data

Guarantee
an agile and evolving security posture

03

HOW IS YOUR NETWORK ARCHITECTURE STRUCTURED?

Our network is segmented between a **teaching network** (students, teachers, learning platforms) and **an administrative network** (sensitive data, internal management). This separation reduces risk, but the multiplication of digital tools, remote connections and cross-usage has complicated our security.

Previously, we relied on multiple tools that did not communicate with each other, leaving us **without an overall view and only partial detection.** Deploying Gatewatcher's NDR platform has changed everything: we now benefit from complete, **centralized visibility of network traffic,** without modifying our infrastructure. For larger or multi-site institutions, these challenges are even more critical in our sector.

This allows us to quickly **identify abnormal behaviors, protect all our environments (campus, cloud, external tools), and reduce pressure on our IT team.** The solution integrated naturally into our systems, **strengthening security without adding management complexity or disrupting daily operations.**

04

WHY DID YOU DECIDE TO IMPLEMENT AN NDR SOLUTION?

When assessing our cybersecurity posture, **we identified the network as our main blind spot.** Our existing solutions were effective at protecting user devices, servers, and applications. However, network activity remained largely invisible. **Without real-time anomaly detection, we were still vulnerable to stealthy threats moving within our infrastructure.**

For an educational institution, security must be fast, transparent, and seamlessly integrated into our environment. **Implementing an NDR solution met this requirement by reinforcing visibility without disrupting daily operations.**

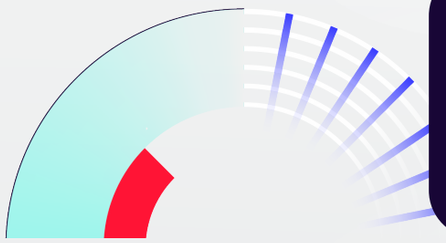
05

WHY DID YOU CHOOSE GATEWATCHER AS YOUR NDR PROVIDER?

What convinced us about Gatewatcher was their agility and **ability to adapt to our specific challenges.** Instead of imposing a rigid framework, they offered a modular solution, tailored to our real vulnerabilities and capable of evolving alongside our environment.

The approach is granular: we can adjust features according to our operational needs and priorities, maximizing value.

As a result, cost becomes not a constraint but an advantage, proportional to usage, making the solution accessible while delivering performance levels equal to, or even higher than, far more expensive NDR solutions.



> *We must constantly adapt to evolving threats to keep our operations safe.*

SECTOR
Education

STAFF

> 4 000
staff

> 25 000
students

> 80
research laboratories

USER PROFILES
Students, teachers, administrative staff, parents, external contributors, academic partners

DIGITAL EXPOSURE
40 platforms (specialized resources, course management, student portals, etc.) and more than 15,000 connected devices (desktops, tablets, Wi-Fi hotspots, IoT for building management, etc.)

06

HOW DOES GATEWATCHER USE ARTIFICIAL INTELLIGENCE TO BETTER PROTECT YOUR INSTITUTION?

GAIA, Gatewatcher's cyber assistant, truly helps and relieves the burden on IT teams. We use it to analyze data from multiple sources, cross it with all our implemented solution documentations, enabling teams to quickly and clearly understand detected incidents. This simplifies decision-making and clarifies remediation protocols.

This intelligent assistance transforms the complexity of alerts into actionable insights, reinforcing incident reporting while freeing SOC analysts from repetitive tasks. GAIA optimizes detection, understanding, and investigation of cyberthreats, while integrating seamlessly with existing institutional tools.

> *What convinced us about Gatewatcher was their agility and ability to adapt to our specific challenges. Instead of imposing a rigid framework, they offered a modular solution, tailored to our real vulnerabilities and capable of evolving alongside our environment.*

07

HOW WOULD YOU DEFINE SUCCESS WITH GATEWATCHER'S NDR?

Our priority was clear and intelligent visibility, being able to distinguish real threats from background noise, which is a challenge when IT teams are small.

Gatewatcher's NDR platform has become essential, particularly in managing Shadow IT, which is widespread in education: laboratories running autonomous systems, classes using specific teaching tools, or administrative services deploying non-centralized platforms. While often useful, these practices can create hidden doors for cyberattacks, invisible to traditional protection measures.

With Gatewatcher's NDR, we have significantly improved our detection and response times. At the first sign of weak signals, our team receives alerts enriched with contextual data (attack type, device affected, potential vector). Gatewatcher's CTI provides a real advantage by sharing threat intelligence specific to education, helping us react quickly and effectively. This contextual knowledge allows us to anticipate recurring attack campaigns in our sector and adapt our defenses accordingly.

In addition, the Reflex solution automates incident response, reducing workload for our teams. We estimate a 30–50% time saving in incident qualification, as analysts immediately access key information. Ultimately, Gatewatcher enables us to secure our educational environment in a simple, transparent way, tailored to our real needs.

Key benefits_

Ensure
continuous and granular monitoring of all infrastructures to anticipate and neutralize cyberthreats.

Manage
critical periods (exams, enrolments) proactively to ensure uninterrupted teaching continuity.

Map
all connected devices in real time and detect unauthorized usage or Shadow IT.

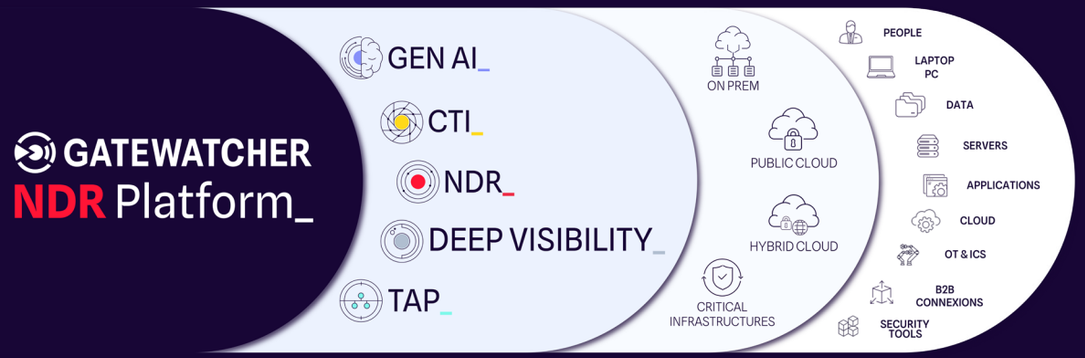
Centralized
alerts intelligently into a single dashboard for faster response and effective threat prioritization.

Identify
alerts intelligently into a single dashboard for faster response and effective threat prioritization.

*About us_*

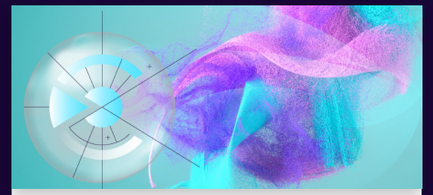
Gatewatcher, a leader in cyber threat detection, has been protecting the networks of businesses and public institutions, including the most critical ones, since 2015. The Gatewatcher NDR Platform (Network Detection and Response) combines artificial intelligence, dynamic and behavioral analytics techniques,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

[GUIDE]
Ransomware practical guide



[USE CASE]
Uncover weaknesses in my system

[ARTICLE]
How are EDR and NDR complementary ?