CUSTOMER STORY

GHT 84

GHT VAUCLUSE, A FRENCH REGIONAL HOSPITAL NETWORK

> In environments where IT and OT converge, as it is often the case in many industries, one of the key challenges is securing all critical infrastructures. NDR complements our existing protections by offering cross-network visibility, allowing us to detect weak signals and anomalies that often go unnoticed with other tools.

FRANCK BAIBOURDIAN, CISO
Avignon University Hospital & Vaucluse Hospital Group

#NDR #HEALTH #BIOMED #SHADOWIT

01

COULD YOU INTRODUCE YOURSELF, AS WELL AS THE VAUCLUSE HOSPITAL GROUP (GHT), AND EXPLAIN THE CONTEXT IN WHICH YOU WORK AS THE CISO?

The GHT encompasses about ten healthcare facilities, soon to be eleven, spread across the Vaucluse department. We manage approximately 2,500 beds, 6,200 employees, and our information systems include 4,200 workstations and 650 servers. As the CISO, I coordinate security efforts with the IT managers of each facility. While they remain autonomous, I work closely with them to define and implement cybersecurity best practices. We operate in a **complex environment**, where **the diversity of IT systems and the operational needs of healthcare professionals** must be balanced with **security and regulatory requirements**.

*Cyber challenges_*

Ensure
uninterrupted patient care

Detect
threats early

Implement
a solution that is interoperable with existing tools

Protect
our equipment against supply chain attacks

Guarantee
compliance with regulations (NIS2)

Franck Baibourdian_

CISO - Avignon University Hospital & Vaucluse Hospital Group

02

WHAT ARE THE SPECIFIC AND UNIQUE CYBERSECURITY CHALLENGES YOU FACE AS A HEALTHCARE ORGANIZATION?

Our top priority as a healthcare provider is **to ensure uninterrupted patient care**. This means our systems must be up and **running at all times** because even a brief disruption could have serious consequences. The challenge lies in balancing robust security measures with the need for healthcare professionals to work seamlessly without overly restrictive technology constraints.

What sets us apart as a GHT is that each facility has its own IT department led by a local IT manager. These managers are my key partners in addressing security, and together we implement action plans and follow through on recommended measures. The challenge is to maintain a unified approach to cybersecurity while adapting solutions to the unique needs of each site. Additionally, our systems grow more complex as we integrate with external entities, like private clinics or other hospitals. We need to secure these connections without disrupting the flow of patient care.

03

WHAT ARE THE MAIN TECHNICAL AND OPERATIONAL CHALLENGES YOU FACE IN CYBERSECURITY, ESPECIALLY IN A HOSPITAL ENVIRONMENT?

Hospitals are incredibly diverse environments, almost like small cities. We have over 150 different professions, all reliant on IT systems, with a wide variety of technologies in use. Some systems are modern and secure, while others, like **biomedical equipment, are much older and often run on outdated, less secure protocols**. On top of that, we work with numerous **external providers** who access our systems remotely for maintenance, introducing additional risks.

This **diversity** makes cybersecurity particularly challenging, as every component in our ecosystem has a different level of maturity and security. Adding to the complexity, we must also navigate **budget constraints and regulatory requirements**, such as compliance with the NIS2 directive. This requires careful planning to align our cybersecurity priorities with the resources we have available.

04

WHAT LED TO YOUR DECISION TO IMPLEMENT AN NDR SOLUTION, AND HOW DOES IT INTEGRATE WITH YOUR OTHER SECURITY TOOLS?

In environments where IT and OT converge, as is often the case in many industries, one of the key challenges is securing all critical infrastructures. Traditional solutions like EDR remain essential but don't provide full coverage for all network interactions. With **the growing attack surface, the increasing sophistication of threats, and the complexity of infrastructures, comprehensive monitoring has become indispensable**.

This is why we chose to adopt an NDR solution. It complements our existing protections by offering **cross-network visibility, allowing us to detect weak signals and anomalies that often go unnoticed with other tools**. This is especially critical for devices like biomedical equipment, which can't always be secured using traditional solutions. With NDR, we can continuously monitor these communications, significantly enhancing our ability to respond quickly to threats.

> “
>
> *With NDR, we can continuously monitor all network communications, significantly enhancing our ability to respond quickly to threats.*

HEAD OFFICE
Henri Duffaut Hospital
in Avignon

BUSINESS SECTOR
Health

6 200
employees

11
sites in France

2 500
beds

4 200
workstations

650
servers

SPECIALITIES
Emergency care, intensive care, maternity (levels 1 & 2), and EMS services

05

WHAT ARE THE MAIN CHALLENGES IN SECURING BIOMEDICAL DEVICES AND OTHER EQUIPMENT YOU CAN'T DIRECTLY CONTROL?

Biomedical devices present a unique challenge because they are often outdated and rely on closed or proprietary systems, making it impossible to install security solutions like EDR. In this context, **NDR plays a critical role by monitoring the network traffic around these devices and identifying any suspicious activity.**

By layering security measures such as network segmentation and access control, we can quickly detect and respond to any intrusion attempts or misuse, even if we can't directly intervene on the device itself. This multi-layered approach allows us to mitigate risks effectively while maintaining operational continuity.

06

WHAT WERE YOUR MAIN GOALS WHEN IMPLEMENTING THE NDR SOLUTION, AND HOW DID YOU MEASURE THE SUCCESS OF ITS INTEGRATION?

We had two main goals when implementing the NDR solution.

> The first was to **ensure seamless collaboration between our external team, the SOC** (Security Operations Center), **and our internal teams**. The NDR needed to integrate smoothly into the SOC so alerts could be handled in real-time. At the same time, it was crucial for our internal operational teams to fully adopt the solution, enabling them to respond quickly to incidents without relying solely on the SOC, with clearly defined roles and responsibilities for everyone involved.

> The second key objective was **alert relevance**. One of the most critical success criteria was minimizing false positives. Any solution that generates too many irrelevant alerts quickly becomes ineffective. We focused on fine-tuning the alerts to ensure they were both precise and actionable. By achieving these two goals, we were able to rapidly enhance the efficiency and responsiveness of our security system.

07

WHAT WERE THE MAIN CRITERIA FOR SELECTING GATEWATCHER'S SOLUTION, AND HOW DID IT STAND OUT FROM OTHERS ON THE MARKET?

What truly set Gatewatcher apart from other market solutions was its **ease of use and feature richness**. The interface is highly intuitive and allows for advanced customization of dashboards, which is crucial for our teams. For example, the integration with Kibana and Elasticsearch offers exceptional **flexibility in how we analyze and visualize data**.

As the CISO, I value having a comprehensive view of network activity while enabling my technical teams to drill down into details, even to the level of individual data packets. This level of granularity allows us to conduct highly precise investigations into potential incidents, making Gatewatcher a significant asset for our cybersecurity strategy.

“

By layering security measures such as network segmentation and access control, we can quickly detect and respond to any intrusion attempts or misuse

08

WHAT ADVICE WOULD YOU GIVE TO ANY ORGANIZATION CONSIDERING DEPLOYING AN NDR SOLUTION IN A HOSPITAL ENVIRONMENT?

I would recommend taking a step-by-step approach, starting with **monitoring the most critical networks**, such as those handling essential infrastructure or patient data exchanges. It's crucial **not to rush into trying to monitor everything at once**, as this can lead to an overwhelming number of alerts that are difficult to manage.

Close collaboration with the SOC and Gatewatcher teams is essential to clearly define roles and ensure only relevant alerts are escalated. Lastly, it's important to remember that good network hygiene and crisis preparedness are just as vital as the technology itself. Cybersecurity is a collective effort, and collaboration between institutions is key to effectively addressing threats.

IN PRACTICE_

Managing ***Shadow IT*** with NDR

In a hospital environment, Shadow IT poses significant security risks, creating unsecured and potentially vulnerable entry points into the network. This often involves connected biomedical devices or remote maintenance tools. Additionally, there are more universal risks tied to employees using personal devices, which are often not identified by IT teams. The open nature of a hospital further amplifies intrusion risks, as it allows for potentially unsecured external connections.

NDR helps us address these challenges by providing comprehensive network monitoring across all devices and applications. It offers real-time inventory and mapping of assets, users, and usage (IT, OT, IoT, VM, Cloud). While not replacing other solutions, it detects unauthorized devices and enables us to quickly secure these overlooked elements.

Controlling ***Network Access*** with NDR

One of NDR's key strengths is its ability to act quickly on the network by disabling switches or blocking suspicious access. This speed is critical in hospital settings, where some older, proprietary biomedical devices cannot be secured using traditional solutions.

Despite their vulnerabilities, these devices remain connected, creating potential security gaps. NDR allows us to monitor these devices in real time and, in the event of abnormal behavior, immediately cut off their network access. This ability to segment and isolate critical devices enhances our security without requiring direct intervention on the devices themselves.

> *NDR helps us address these challenges by providing comprehensive network monitoring across all devices and applications. It offers real-time inventory and mapping of assets, users, and usage (IT, OT, IoT, VM, Cloud).*

Want to *learn more ?_*

Contact us today ⟶

BENEFITS_

Agility and modularity
of the solution – Ideal for sectors with stringent requirements like healthcare

Enhanced visibility
into interconnections and network communications

Full control
of data that remains your property

Advanced detection and targeted response
to all types of threats, including the most sophisticated

IT/OT synergy
for comprehensive threat visibility, including healthcare protocols (DICOM, HL7, IHE)

Compliance
with the NIS 2 directive to strengthen cybersecurity in the healthcare sector

*Easy as_*

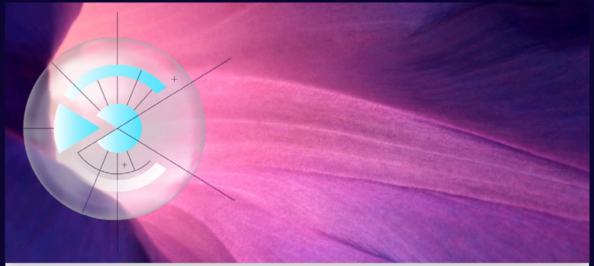
NDR_ CTI_ TAP_ GEN AI_ DEEP VISIBILITY_

Want to *learn more?*_

VIDEO • WEBINAR
ADVANCED PERSISTENT THREATS
HOW NDR CAN BETTER PROTECT YOUR INFRASTRUCTURE?
Adrian Jones
Country Manager UK

[WEBINAR]
Advanced Persistent Threats: How NDR can better protect your health infrastructure?

[BLOG ARTICLE]
Healthcare and Cybersecurity – How to protect hospitals with NDR technologies?



[USE CASE]
Anticipate intrusions into the healthcare environment.