



White Paper

IT/OT Cyber Risk: *The Age of Anticipation*



Summary_

1 *Context and new challenges of IT/OT convergence_*

IT-OT convergence: Your greatest strength, your worst vulnerability

P04

Rebound scenarios: When IT opens the door to the enemy

P06

OT vs. IT: When two different approaches collide

P07

The legacy challenge: Securing without interrupting production

P09

You can't protect what you can't see...

P10

Breaking the Decision Deadlock: Converging people, not just systems

P11

2 *Use cases_*

ENERGY: Resilience under digital tension

P12

HEALTHCARE: Safeguarding Patient Care in the digital Hospital Era

P16

INDUSTRY: Securing the connected factory without interrupting production

P20

TRANSPORT & LOGISTICS: Ensuring safe mobility and the flow chain

P24

3 *See, Understand, Anticipate: A new approach to OT cybersecurity_*

Proactivity: The new line of defense

P29

Seeing before impact: The strategic role of NDR

P30

Decision Center: Turning visibility into action

P30

The 4 pillars of an effective IT/OT cybersecurity strategy

P32

Different constraints, a shared imperative for resilience

P33

+

01 CONTEXT AND NEW CHALLENGES OF IT/OT CONVERGENCE





IT-OT Convergence

Your greatest strength, your worst vulnerability

For over a decade, digital transformation has been reshaping operational efficiency, embedding IT deep into the core of OT environments, from production lines to energy grids and hospital technical platforms. That shift has become a major driver of performance.

IT/OT convergence delivers tangible gains across every sector, from sharper predictive maintenance to real-time inventory management and more personalized care. It boosts productivity, streamlines operations, and speeds up the response to the unexpected.

But this convergence breaks a fundamental principle: isolation. By connecting critical assets once protected by physical isolation (the “air gap”), organizations have unknowingly opened a Pandora’s box of cyber risk.

> *A strategic target amid global tensions*

Those risks are amplified by a backdrop of heightened geopolitical tension. Industrial, energy, transport, and healthcare infrastructure have all become high-priority targets.

Attackers are no longer just after data. They are increasingly going after the outright sabotage of operations: paralyzing a transport network, disrupting energy distribution, halting a production line, disabling a hospital's emergency systems. Whatever the method (espionage, sabotage, extortion, or destruction), hitting OT means striking at the heart of national sovereignty: **disrupting the economy, undermining competitiveness, destabilizing essential services, and potentially putting lives at risk.**

> *The Industrialization of Cybercrime*

That risk is compounded by attackers' evolving tradecraft. AI is fueling a new generation of **attacks that are becoming automated, specialized, and faster**. Capabilities once reserved for state-sponsored actors are now gradually being made available to a growing number of attackers.

Faced with this "high-frequency" threat, legacy security tools, already largely blind to industrial protocols, **simply can't keep up.**

> *Regaining Control: A Matter of Operational Survival*

Regaining control is no longer optional. It is an operational imperative. Without granular command of their OT environments, organizations risk a sudden loss of their ability to produce, distribute, deliver critical services, or provide care.

The stake is no longer to protect isolated systems, but to manage the IT/OT network as a whole. Full visibility into what is actually happening is now essential to catch the earliest signs of an attack, detect stealthy threats, and stay ahead of cybercriminals.

In an interconnected IT/OT environment, when the digital layer fails, your entire operational activity can come to a halt.

The number of cyber incidents resulting in a physical disruption of operations tripled between 2021 and 2025.

Source : Gartner

74% of industrial companies admit to having only limited, or no, visibility into activity within their OT network.

Source: SANS Institute report on ICS/OT security



Did you know?

More than 60 % of incidents affecting industrial environments originate in IT systems or in the supply chain (contractors, partners).

Attackers favor these indirect entry points, which are often less protected, to reach their ultimate targets.

Sources : IBM X-Force / Dragos

Rebound scenarios: *When IT opens the door to the enemy*

Contrary to popular belief, OT environments are rarely the initial entry point for an attack; they are the final target. ANSSI, the French national cybersecurity agency, confirms this in its latest threat landscape report: **attackers typically establish a foothold in IT before pivoting into industrial environments.** Entry points are plentiful: user workstations, remote access, compromised credentials, third-party connections during maintenance.

Because these access points remain open to keep the business running, they often fall outside the controls applied to the rest of the IT system. Once inside, attackers map the interconnections and quickly locate the gateways into OT. **From there, compromising a single admin account can be enough, a few hops later, to bring down an entire production line.**

OT vs IT : *When two different approaches collide*

OT environments were built to run in isolation. Their priority is continuity, of production and of service. With limited exposure to the outside world and rarely patched, they relied on closed architectures where isolation itself was the security control.

IT systems, by contrast, were built to exchange data: open, interconnected, and constantly evolving to meet the needs of users and the business.

Their convergence has forced these two philosophies to collide. **By building digital bridges between these environments, organizations have removed the physical boundary that once protected industrial systems.** What used to be two separate worlds is now a shared space, where IT's default openness gets imposed on systems that were not designed to handle it.

Did you know?

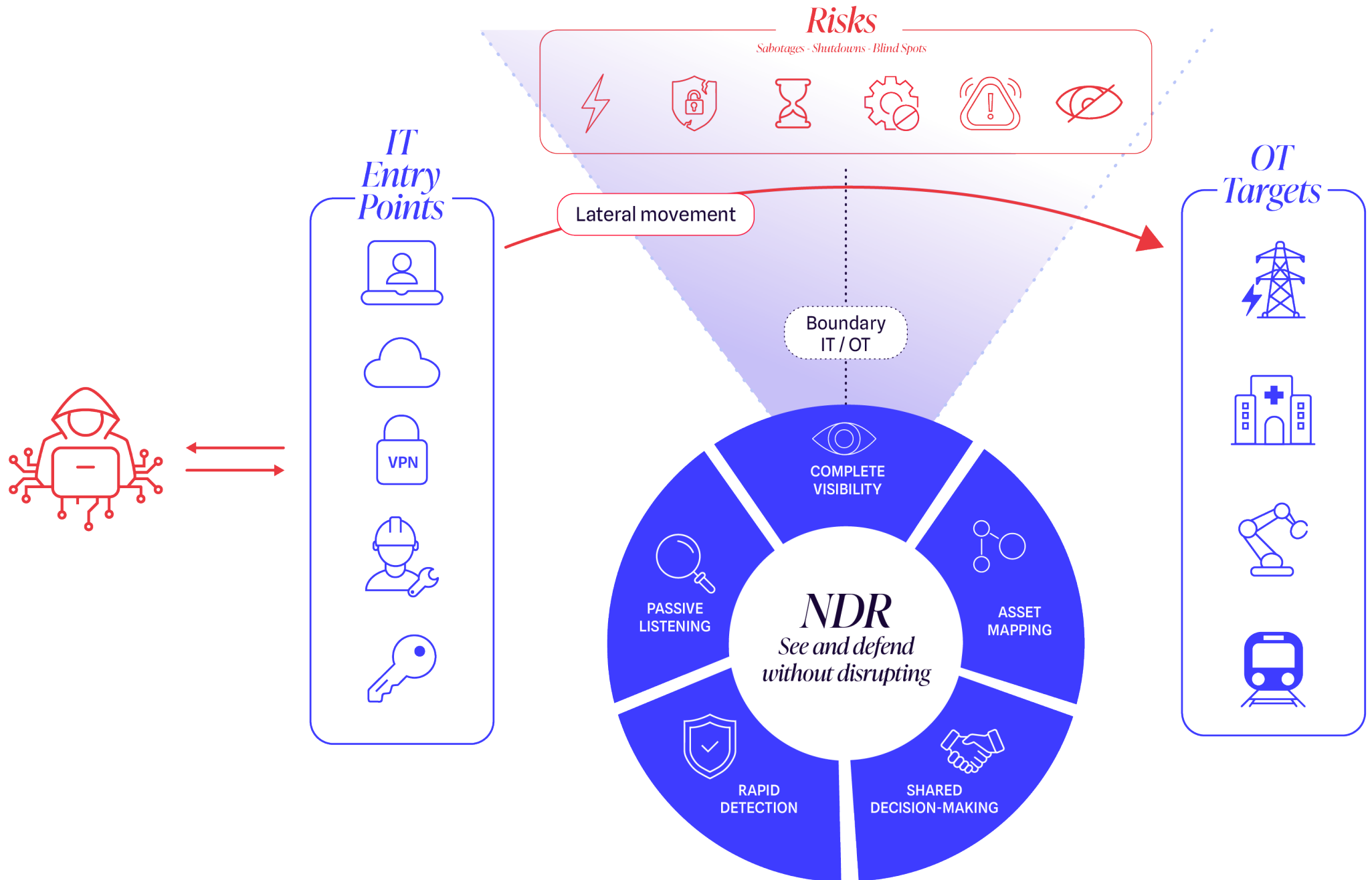


An industrial controller is designed to run for 20 to 30 years, whereas an IT server is typically replaced every 3 to 5 years.

This mismatch creates structural weaknesses: a significant share of industrial environments still relies on legacy systems or protocols that are difficult to secure.

Sources : ANSSI

Diagram of an attack on a converged IT/OT network



The Legacy Challenge:

Securing without interrupting production

OT's stability is its greatest operational strength, but it is also its biggest cyber liability. **Built to run for twenty to thirty years, industrial environments evolve at a pace radically different from IT systems.** Updates are rare, maintenance windows are limited, and every change has to be carefully vetted to avoid any impact on production. In a converging IT/OT world, that glacial pace collides with threats that can evolve, spread, and strike within minutes.

This mismatch in timescales creates a structural tension: **how do you protect critical equipment that is sometimes impossible to patch, reboot, or even scan without risking the business?** In industry, energy, transport, or healthcare, taking a system offline to secure it is generally not an option. Cybersecurity has to adapt to operational constraints, not the other way around.

This is precisely where **Network Detection and Response (NDR) comes into its own.** Unlike security tools that interact directly with equipment and generate their own traffic, **NDR relies on completely passive network monitoring.**

Using traffic-duplication mechanisms (network TAPs, mirror/SPAN ports, or dedicated visibility infrastructure), a copy of all communications is sent to the analysis platform. Industrial equipment keeps running exactly as before while the NDR observes,

decodes, and **analyzes traffic in real time, without ever injecting a single packet onto the production network.**

This approach delivers full visibility into assets, industrial protocols, and IT/OT communications without introducing operational risk. It's especially well suited to environments with a high concentration of "legacy" equipment, where the smallest disruption can trigger a service outage or take down a critical process.

Deployable on-premises as well as in hybrid or cloud architectures, NDR integrates with existing infrastructure without altering how it runs. It delivers advanced detection while meeting the availability requirements of critical environments and aligning with regulatory frameworks such as NIS2 and the IEC 62443 standard.

Did you know?



According to Gartner, **more than 75%** of OT environments contain equipment that cannot be updated without interrupting production.

As a result, many known vulnerabilities remain exploitable for years.

You can't protect *what you can't see...*

In many industrial environments, the challenge no longer stops at detecting an intrusion; it now extends to understanding what is actually happening across the network. **OT traffic runs on specialized industrial protocols that are often opaque to traditional IT security tools**, which struggle to decode them. Interactions between devices are often poorly documented, and some communications entirely escape monitoring.

The result: a significant share of network activity remains hidden, obscuring weak signals or stealthy threats.

In an interconnected environment, a lack of visibility is not just an information gap; it becomes a major risk to business continuity.

Did you know? —



In industrial environments, up to **90 %** of assets are not properly inventoried or monitored in real time.

Without complete visibility, it becomes impossible to accurately identify abnormal flows or behaviors.

Sources : Gartner / Nozomi Networks



More than 60 % of industrial organizations still have IT and OT responsibilities that are siloed, with separate decision-making chains.

Sources : Deloitte / IBM Security

Breaking the Decision Deadlock: *Converging People, not just systems*

IT and OT systems can now talk to each other, but they remain technically distinct, and the organizations running them are all too often trapped in their legacy silos. On one side, IT teams, the guardians of security, prize agility: constant updates, immediate patching, and a priority on confidentiality.

On the other, OT teams, the guardians of production continuity, run entirely on a different logic: uptime above all. For a plant manager, a system that is running is a system you don't touch.

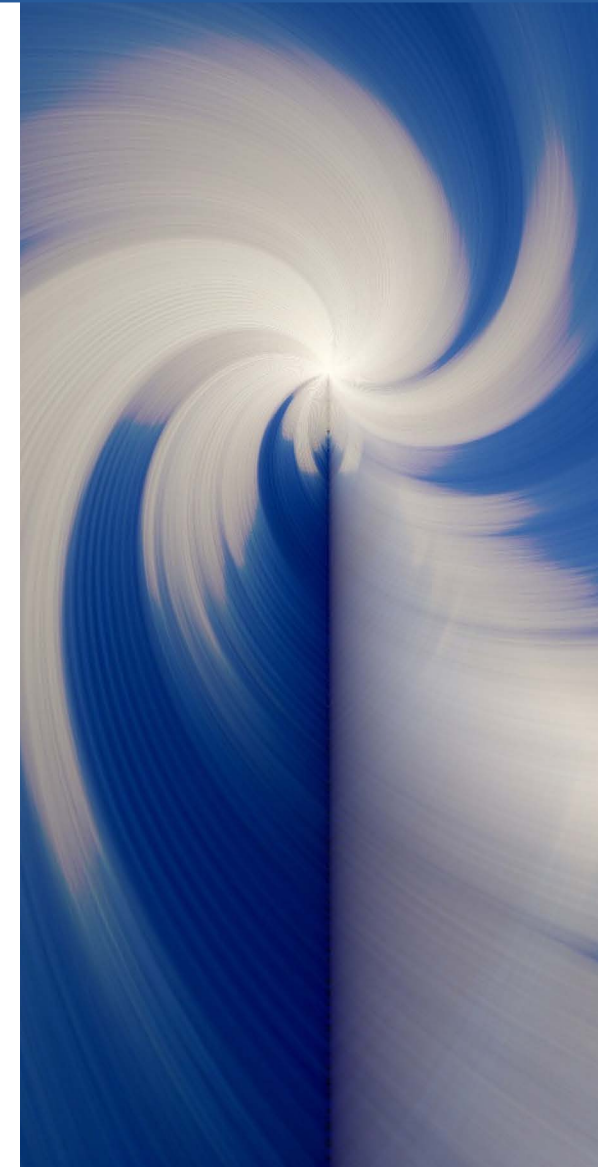
This divergence creates natural tension: **where the cyber expert sees a critical vulnerability that must be patched urgently, the operations team sees a risk of production downtime.**

This clash of perspectives is a serious weak point. During an incident, lines of authority blur: who is authorized to act, at what point, and on what basis? IT teams focus on containing the threat while OT teams focus on preserving continuity, and the two priorities don't always align.

This difference in perception is compounded by a deeper skills gap: IT experts have little expertise in the specifics of industrial environments, and OT experts rarely understand cyber risk. That lack of cross-functional expertise **limits the ability to grasp a situation as a whole and make the right call at the right time.**

In other words, successful convergence also demands deep organizational change, with teams, processes, and responsibilities aligned around a risk they now share. Without that human alignment, even the best technical solutions will keep hitting the same wall: decision paralysis.

Securing OT means breaking down silos, including the human ones, and turning cybersecurity from an IT-imposed constraint into a driver of operational resilience.





02 USE CASES_

+

ENERGY: RESILIENCE UNDER DIGITAL TENSION_

A connected *energy grid*

In the energy sector, IT/OT convergence is no longer just a technical optimization; it's the engine driving the energy transition itself. The rise of smart grids, large-scale integration of distributed renewables, and remote-controlled substations have turned the grid into a living data organism. It's a response to a hard operational requirement: balancing production and consumption in real time across increasingly complex networks. But that hyperconnectivity breaks the historical isolation of industrial systems and opens up an unprecedented attack surface.

Sector-specific protocols, IEC 61850 for substation automation, IEC 104 and DNP3 for remote control, now run across networks interconnected with the corporate information system.

The nature of the primary risk has changed. **A vulnerability introduced through an administrative workstation or a remote maintenance connection can now propagate all the way to protection controllers (IEDs).** For energy operators, the challenge is to protect critical assets whose failure means far more than data loss: a national supply disruption, grid-frequency instability, or irreversible physical damage to high-voltage transformers, the backbone of energy sovereignty.

Recurring attack scenarios



Stealth sabotage via a protection relay

An attacker hijacks a maintenance session to alter the trip thresholds of a protection relay.

Impact: The equipment looks operational, but can no longer protect the grid during an actual surge, potentially triggering a devastating cascading failure.



Dispatch blinding (SCADA hijacking)

False telemetry is injected into the supervision system to simulate a normal load.

Impact: The operator, misled by the falsified readings, misses a critical overload, leading to frequency instability and an uncontrolled load-shedding event.



Ransomware targeting remote-control servers

Attackers encrypt the servers running the control center's human-machine interface (HMI).

Impact: Total loss of remote-control capability across distributed sites, forcing a costly, risky fallback to manual operation.

Regaining control of a borderless network

> Decode the intent behind an industrial command_

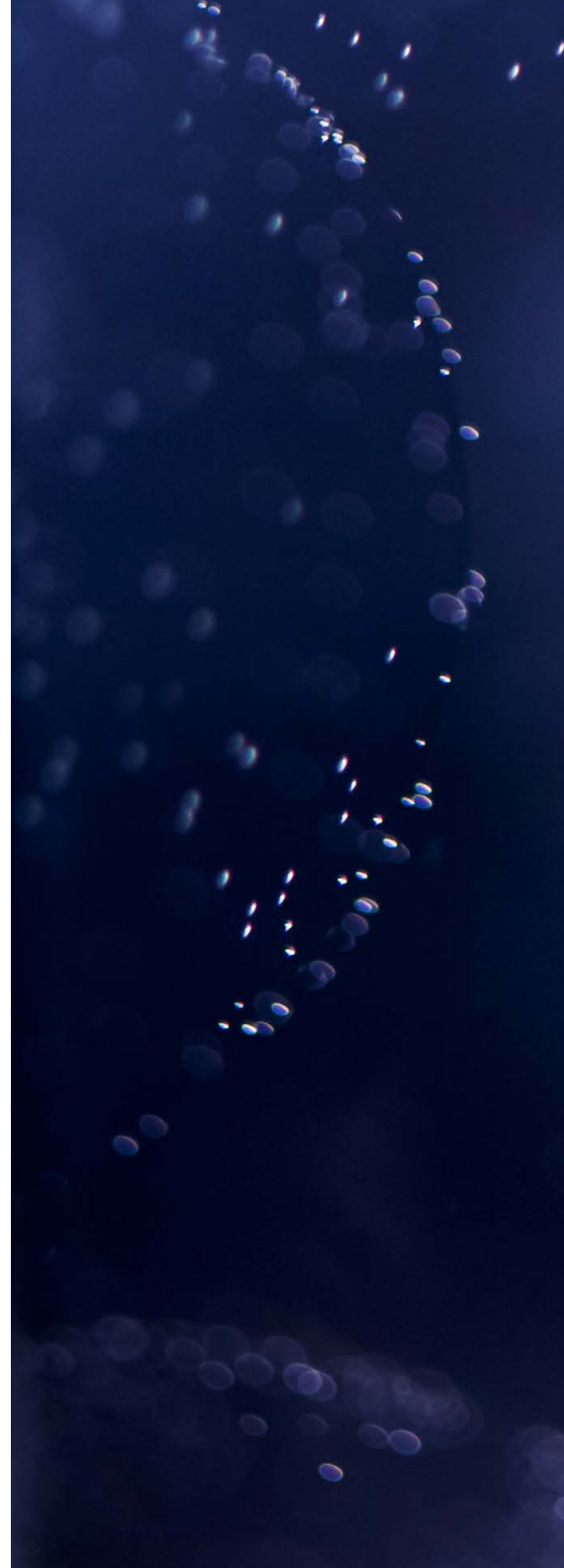
Intrusion detection alone is no longer enough. Security teams need to analyze the semantics of industrial-protocol traffic to tell a legitimate maintenance operation from a stealth sabotage attempt, and flag or block an atypical command before it destabilizes the grid.

> Unify visibility across a scattered infrastructure_

The sector runs on widely dispersed assets, often managed remotely by third parties. Regaining control means continuously mapping the traffic between the IT system, remote-control systems, and field equipment (IEDs), to catch suspicious lateral movement before an aging segment triggers a domino effect.

> Use passive monitoring as a guarantee of stability_

When the production-consumption balance is decided second by second, the security tool itself can never become a source of risk. A passive NDR approach monitors continuously without ever touching critical protection traffic, catching weak signals, easing the load on control-room teams, and reinforcing energy sovereignty along the way.



Gatewatcher's *sector footprint*

Customer references_

Suez, Veolia, RTE, Dunkerque LNG (Groupe Fluxis),
Eau de Paris, Eau du Grand Lyon, Eau de Strasbourg,
and Eau de Bordeaux.

Industrial protocols covered_

IEC 104, DNP3, Modbus, S7, OPC UA, MQTT, ENIP/CIP
(BACnet limited to building management / energy-
efficiency use cases).

> Excluded: DICOM and HL7 (healthcare), Pcom
(generic controllers).

OT equipment / vendors_

Siemens (Siemens Energy), Hitachi Energy (formerly
ABB Power Grids), ABB, Schneider Electric, GE
Vernova, Schweitzer Engineering Laboratories (SEL),
Eaton, Emerson, Honeywell, Rockwell Automation
(Allen-Bradley), SMA, Huawei, SolarEdge, Fronius.



HEALTHCARE: PROTECTING CARE IN THE AGE OF THE DIGITAL HOSPITAL_

Hyperconnected healthcare facilities

Today's healthcare facility has become a hyperconnected ecosystem where the line between the hospital information system (HIS) and the clinical technical platform disappears. Scanners, MRI machines, connected infusion pumps, lab automation, surgical robots: these biomedical devices (IoMT) now communicate continuously over DICOM or HL7. **That convergence streamlines the care pathway and speeds up diagnosis, but it also turns every piece of medical equipment into a potential entry point for an attack.** In a hospital, the threat isn't confined to patient-record confidentiality; it directly threatens the integrity of clinical care itself.

Healthcare is now a top-tier target for attackers running "double extortion" campaigns. The pressure no longer falls on data alone; it falls on the operational survival of the facility, and therefore its ability to deliver care. A paralyzed operating room or an unavailable imaging system is an immediate, critical loss for the patient. **The complexity is compounded by highly heterogeneous equipment fleets that mix the latest cloud applications with critical medical devices running obsolete operating systems that can be neither patched nor isolated without breaking the chain of care.**

As a result, success here depends not on tool performance alone, but on the organization's ability to master the flows created by convergence, so that network openness never becomes the breaking point in patient care.

Recurring attack scenarios



Operating-room paralysis via lateral movement

Ransomware lands via a phishing email on the administrative IT system, then exploits convergence to pivot from console to server to system. A gateway may let the malware progress while providing zero oversight of vital-signs monitoring.

Impact: Patient monitoring drops mid-procedure, forcing a switch to emergency mode with no video or data feed.



Diagnostic integrity tampering (Data Tampering)

An attacker tampers with the metadata of an imaging exam as it moves between the OT network (the scanner) and the IT network (the PACS archiving server).

Impact: A diagnosis is made on a falsified image, or an image gets attributed to the wrong patient, with the network anomaly going completely unnoticed by care staff.



Hijacking of building management systems (BMS)

An attacker breaches the building-management network (HVAC, air pressure) through a poorly secured web gateway.

Impact: Sterility conditions in clean rooms or operating theaters are compromised, taking the technical platform out of service even though the IT system itself is running fine.

Securing care *without hindering it*

> Guarantee continuity of care on an open network_

Cybersecurity is no longer a support function. It's a direct component of patient safety, and downtime is never an option. Managing convergence demands detection that's silent and highly precise.

> Catch drift before it disrupts care_

Weak signals on the network can be the first sign of a threat moving from IT into biomedical OT. Spotting an unusual communication or an abnormal flow is essential. Analysing specialized protocols makes it possible to intercept an attack before equipment malfunctions or is damaged.

> Close the blind spot in the biomedical fleet_

Hospitals have to manage equipment that mixes recent devices with older, unpatched ones. Dynamic asset mapping identifies and monitors every connected device, protecting against vulnerabilities in legacy equipment that can't be isolated or patched.

> Keep oversight transparent for medical teams_

Any security measure that slows access to data or delays a diagnosis directly undermines the responsiveness of care teams. The response to convergence has to be completely non-intrusive.



« Early detection of unusual behavior now allows us to anticipate certain deviations before they affect care services. »

Franck Moussé, CISO - GHT du Cher

Gatewatcher's sector footprint

Customer references_

GHT Réunion, CH St Lô, CH Polynésie française, CHU Nice, GHT Cher, CH Douai, GHT Vaucluse, EFS, and Santé Publique France.

Industrial protocols covered_

DICOM, HL7 (core clinical systems), BACnet and Modbus (building management, critical HVAC, medical gases), MQTT (connected medical devices / IoMT).

> Excluded: DNP3, IEC 104, S7, ENIP/CIP, Pcom (not specific to healthcare).

OT equipment / vendors_

GE HealthCare, Siemens Healthineers, Philips, Canon Medical, Fujifilm Healthcare, Dräger, Medtronic; for HL7 / hospital information systems: Epic, Oracle Health (formerly Cerner); for hospital building management: Siemens, Schneider Electric, Johnson Controls, Honeywell.

“

« With four university hospitals and a very large number of assets to oversee, we needed end-to-end visibility across our IT, OT, and biomedical environments. Gatewatcher's NDR gives us that 360-degree view and makes it easier for our cyber and business teams to work together. The result: tighter control of our attack surface and a stronger incident response capability. »

Stéphane Duchesne, Director of Risk - GHT de La Réunion

“

« With certain biomedical equipment, we don't always have full control. These are vendor-locked, packaged solutions, so we have to find ways to secure them anyway. »

Franck Baibourdian, CISO - CH Avignon & GHT Vaucluse



INDUSTRY: SECURING THE CONNECTED FACTORY WITHOUT STOPPING THE LINE_

Connected industry facing the risk of digital propagation

In manufacturing, IT/OT convergence has become the central pillar of the factory of the future. The Industrial Internet of Things (IIoT), AI, and collaborative robotics are unlocking unprecedented levels of productivity and flexibility. But that agility depends on total, permanent interconnection: **line-side sensors, programmable logic controllers (PLCs), and manufacturing execution systems (MES) are now directly linked to corporate networks and predictive-maintenance cloud platforms.**

This transformation is fueling the rise of Industry 4.0. Predictive maintenance, collaborative robotics, on-site energy management, automated quality control, digital twins: **all of today's industrial intelligence runs on a continuous flow of data between IT systems and OT equipment.** But that hyperconnection also creates a new,

critical dependency. When a digital flow is compromised, it's the physical production line that goes off the rails.

The risk is no longer confined to a single workstation going down. **A compromise can now directly hit production speeds, manufacturing parameters, industrial recipes, or control systems.** In environments where production lines operate on a just-in-time basis and where every minute of downtime results in significant losses, the cyber threat becomes a direct issue of operational continuity and competitiveness.

This exposure is amplified by how heterogeneous the technology mix is: factories run recent, cloud-connected or remotely monitored equipment alongside machines that have been in service for decades, closed systems built to last, now up against threats that evolve at the speed of AI.

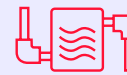
Recurring attack scenarios



Quality sabotage (Data Tampering)

An attacker gets into the OT network and alters a tank's temperature or pressure setpoints over the Modbus protocol.

Impact: Production looks normal, but the finished product is defective or out of spec, leading to massive scrap rates, product recalls, and significant legal exposure.



Industrial ransomware

Attackers encrypt the MES servers or engineering workstations that control the production line's automation.

Impact: Total plant shutdown. Unlike a typical IT incident, recovery is complex, since it can require physically recalibrating every machine on the line.



Intellectual property espionage

Attackers capture robot configuration files or process data as they travel over the network to automation systems.

Impact: A critical leak of trade secrets to competitors, permanently weakening the company's competitive advantage.

Regaining control of the connected shop floor

> Catch operational drift before failure_

In an automated factory, anomalies can be subtle, a changed parameter, an unusual exchange between machines. These weak signals often precede serious incidents. Analyzing industrial-protocol traffic makes it possible to catch them before they hit production.

> Restore end-to-end visibility across fragmented facilities_

Today's plants mix recent technology with older, sometimes non-upgradable equipment. Analyzing traffic flows makes it possible to uncover hidden dependencies, protect legacy equipment, and get ahead of incidents before they spread across the production line.

> Stop an IT incident from becoming an industrial crisis_

With IT/OT convergence, a local incident can take down an entire site. Keeping a flaw in the IT system or a maintenance access point from reaching physical production means monitoring for, and containing, lateral movement before it crosses the IT/OT gateways.

+

Gatewatcher's *sector footprint*

Customer references_

Safran, Arthus Bertrand, Groupe Burger&Cie, France Metal, Sanofi, and Paris La Défense.

Protocoles industriels couverts_

Modbus, S7, ENIP/CIP, OPC UA, MQTT, Pcom.

> Excluded: DICOM and HL7 (healthcare), DNP3 and IEC 104 (energy/utilities SCADA), BACnet (buildings only).

OT equipment / vendors_

Siemens, Rockwell Automation (Allen-Bradley), Schneider Electric (Modicon), Mitsubishi Electric, Omron, Beckhoff, B&R (ABB), ABB, Bosch Rexroth, Phoenix Contact, Unitronics (Pcom), Fanuc, KUKA, Yokogawa, Emerson.



TRANSPORT & LOGISTICS: SECURING MOBILITY AND THE FLOW CHAIN_

Mobility challenged by network porosity

In transport and logistics, IT/OT convergence has become the invisible engine behind operational fluidity. Automated sorting centers, rail signaling, port systems, logistics hubs, traffic supervision, terminal automation: the entire chain now runs on continuous digital exchange between physical infrastructure and information systems.

This transformation answers a hard operational pressure: **move faster, synchronize operations in real time, and absorb ever-larger volumes without disrupting service.** Modern logistics now functions as an interconnected nervous system, where every piece of data immediately drives a physical movement: routing a parcel, positioning a train, opening a gate, controlling an automated conveyor. That fluidity, though, rests heavily on industrial networks and IT/OT interconnections.

Transport infrastructure is no longer a set of isolated systems. It talks to cloud platforms, external contractors, remote-maintenance tools, and central control systems. When IT and OT converge, the attack surface extends from administrative workstations to sorting machines and infrastructure security systems (tunnels, stations, terminals). The major risk is no longer just data theft, but the sabotage of the transportation system itself. **An intrusion that starts with a simple compromised credential can, through lateral movement, paralyze guidance or signaling systems.**

In a world where transport underpins the economy, every hour of downtime isn't just measured in financial penalties. It's measured in systemic disruption to the supply chain, threatening both continuity of trade and user safety.

Recurring attack scenarios



Logistics flow hijacking (Routing Manipulation)

An attacker gets into the OT network of a sorting center and alters routing instructions over the S7 (Siemens) protocol.

Impact: Goods get misrouted or stuck, breaking the supply chain and causing direct losses for end customers.



Blocking of port or rail infrastructure

Ransomware spreads from the management IT system to the supervision servers running automated cranes or signaling.

Impact: Total paralysis of a transport hub. Unlike a typical IT outage, getting back online requires physically inspecting every automated system before operations can safely resume.



Sabotage of safety systems (Building/Technical Management)

An attacker breaches the network managing tunnel ventilation or fire detection through a poorly secured maintenance gateway.

Impact: The infrastructure is forced to close for safety reasons, even though the transport systems themselves are still running fine, triggering regional logistics disruption.

Securing flows that tolerate no interruption

> Detect malicious intent within the operational signal_

Anomalies in an automated facility can be subtle, a changed parameter, an unusual exchange between equipment. These weak signals often precede serious incidents. Analyzing industrial-protocol traffic makes it possible to catch them before they impact operations.

> Secure third-party access and remote maintenance_

Today's infrastructure mixes recent technology with older, sometimes non-upgradable equipment. Analyzing traffic flows makes it possible to uncover hidden dependencies, protect legacy equipment, and get ahead of incidents before they spread across the network.

> Preserve fluidity without adding latency_

With IT/OT convergence, a local incident can affect an entire site. Keeping a flaw in the IT system or a maintenance access point from reaching physical operations means monitoring for, and containing, lateral movement before it crosses the IT/OT gateways.

« Every sensor, every connection is a potential attack surface. »

François Bidondo, CISO - RATP Group

« Modern airport infrastructure relies on the interconnection of numerous IT and OT systems: SCADA, access control, video surveillance, flight operations, baggage-handling equipment, and operational networks. Gatewatcher gives us the visibility we need to understand these interactions, detect threats early, and strengthen the resilience of our operations against an ever-evolving risk landscape. »

Stéphane Fiesque, Deputy Head of IT - Guadeloupe Airport

+

Gatewatcher's *sector footprint*

Customer references_

SNCF, RATP, SAMSIC, Air France, Aéroport de la Guadeloupe, Aéroport de Lyon, IDF Mobilités, APRR et Eurotunnel.

Industrial protocols covered_

Modbus, IEC 104, DNP3, S7, OPC UA, MQTT, ENIP/ CIP (and BACnet for station/airport buildings).

OT equipment / vendors_

Siemens Mobility, ABB, Schneider Electric, Alstom, Yunex Traffic, SWARCO, Kapsch TrafficCom, Wabtec, Rockwell Automation (Allen-Bradley), Honeywell, Johnson Controls.



« Managing a cyber crisis isn't just about detecting a threat. It requires understanding, within hours, which assets are affected and what the operational consequences of each decision will be. Gatewatcher's dynamic mapping gives us real-time visibility across our 600,000 assets and their dependencies, letting our teams make faster, better-informed decisions suited to the demands of critical rail systems. »

José Araujo, , Director of Cybersecurity - SNCF



« The metro, the bus, and the tramway are no longer just physical objects; they are connected objects that must be protected as such. »

François Bidondo, CISO - RATP Group

03

SEE, UNDERSTAND, ANTICIPATE: A NEW APPROACH TO OT CYBERSECURITY_



Proactivity, the new line of defense

IT/OT convergence has fundamentally changed the nature of risk across every sector. Threats no longer target isolated systems; they target hybrid, distributed, interconnected environments where a compromise can now produce immediate physical consequences. Energy networks, hospitals, production lines, logistics platforms, transport infrastructure, sensitive industries: everywhere, digital technology now drives the operations organizations depend on to function.

But visibility alone is no longer enough. To understand a threat in its entirety, **organizations need to correlate signals from multiple sources:** network traffic, security events, asset inventories, threat intelligence (CTI), known vulnerabilities, system logs, and business context. It's that correlation, across sources, **that turns a raw technical alert into a precise read on operational risk.**

This capacity for anticipation rests on **one fundamental prerequisite: visibility into the assets**, communications, dependencies, and abnormal behaviors within converged environments, where recent systems, legacy equipment, remote access, and specialized protocols all coexist. In these complex, converged architectures, the network is the best vantage point there is, capable of revealing what systems are actually doing and how the IT and OT worlds interact.

In this context, **approaches built solely on perimeter defense or after-the-fact incident response show their limits.** The challenge is no longer just to block an attack, but to **understand, early enough, what is actually happening in the traffic between IT and OT systems, so drift can be caught before it hits operations.** Because once an incident becomes visible in production, energy distribution, logistics, or patient care, it's often already too late to act.

The challenge is therefore twofold: detect earlier, decide faster. **Observing traffic, spotting lateral movement, and catching weak signals is only worth something if that information can be put in context, prioritized, and turned into concrete action.** Against attacks that can spread within minutes, **the speed of decision-making matters as much as the quality of the detection.**

In converged environments, shifting from a reactive posture to an anticipatory one isn't just about seeing more. It means turning visibility into understanding, and understanding into the capacity to act. **That chain, see, understand, decide, act, is what forms the real foundation of operational resilience today.**

Seeing Before Impact: the strategic role of NDR_

Built on behavioral network analysis, NDR stands out as one of the few approaches capable of delivering continuous, end-to-end visibility across every flow without disrupting operations.

It notably makes it possible to:

- > *Obtain* a unified view of the actual flows between IT systems and OT equipment
- > *Detect* lateral movement before it reaches critical environments
- > *Identify* abnormal behavior concealed within legitimate traffic
- > *Natively Understand* industrial and proprietary protocols
- > *Monitor* infrastructure without disrupting operations
- > *Correlate* weak signals between IT and OT before any operational impact occurs

Decision Center: *turning visibility into capacity for action_*

NDR forms the foundation of operational knowledge across IT and OT environments. By providing full visibility into network assets, communications, and behaviors, it enables the detection of weak signals and emerging threats. The challenge is no longer getting access to information; **it's interpreting it in its operational context to make the right call at the right time.**

Decision Center, Gatewatcher's agent-based Cyber Decision layer, delivers exactly that by correlating events, risks, dependencies, and business impact to guide action and speed up response.

- > *Advanced Correlation* of IT and OT events
- > *Risk Prioritization* based on sector context
- > *Guided* automated investigation
- > *Recommandation* of actionable decisions suited to the environment
- > *Strengthened coordination* between the SOC, OT teams, and business teams



Beyond understanding, NDR also speeds up response by guiding teams through **incident triage, action prioritization, and orchestrated remediation** tailored to their environment.

Depending on the level of autonomy the organization defines, certain **decisions can be automated** to cut response times, while the most sensitive actions stay subject to human validation.

This approach speeds up the path from detection to action while preserving full governance, with decisions that stay contextualized, explainable, and auditable.

*NDR detects.
Decision Center
accelerates and
orchestrates the response.*

The 4 Pillars of an effective IT/OT cybersecurity strategy

> Regain control of the IT/OT ecosystem

Continuously map every asset, communication, and dependency between IT and OT environments. In hybrid, heterogeneous architectures, only complete, non-intrusive visibility can surface blind spots, critical interconnections, and risky usage patterns without disrupting operations.

> Shrink the gap between Detection and Decision

Automate investigation, correlation, and alert prioritization to speed up operational decision-making. In environments where attacks spread within minutes, the ability to quickly put a threat in context becomes essential to limiting its impact on the business.

SEE EVERYTHING IN CONTEXT

Complete visibility and
real understanding of
assets and flows

DETECT ANOMALIES EARLY

Behavioral detection and weak
signals to anticipate threats

DECIDE QUICKLY AND WELL

Automation and
orchestration for
informed decisions

ACT TOGETHER

IT/OT and business
collaboration to protect what
matters most, the business



> Shift from a reactive posture to an anticipatory one

Adopt behavioral detection capable of analyzing industrial protocols, identifying weak signals, and spotting lateral movement before it reaches critical systems. Against stealthy, evolving threats, anticipation becomes a direct matter of business continuity.

> Bring IT, OT, and business together

Build shared governance between the CISO, OT teams, and operational leadership. IT/OT cybersecurity can no longer be treated as a purely technical topic; it has to be managed according to its potential consequences for production, patient care, logistics, or service continuity.

Different constraints, a shared imperative for resilience

The four sectors covered in this white paper illustrate some of the major challenges of IT/OT convergence, but they're only a glimpse of how diverse these environments really are.

Aerospace, defense, space, specialized industries, optronics, sensitive infrastructure: **every sector has its own operational constraints, proprietary protocols, availability requirements, and sovereignty concerns.**

That diversity demands a cybersecurity approach that can adapt to heterogeneous, sometimes highly constrained environments, where legacy systems, critical infrastructure, and the latest technologies all coexist.

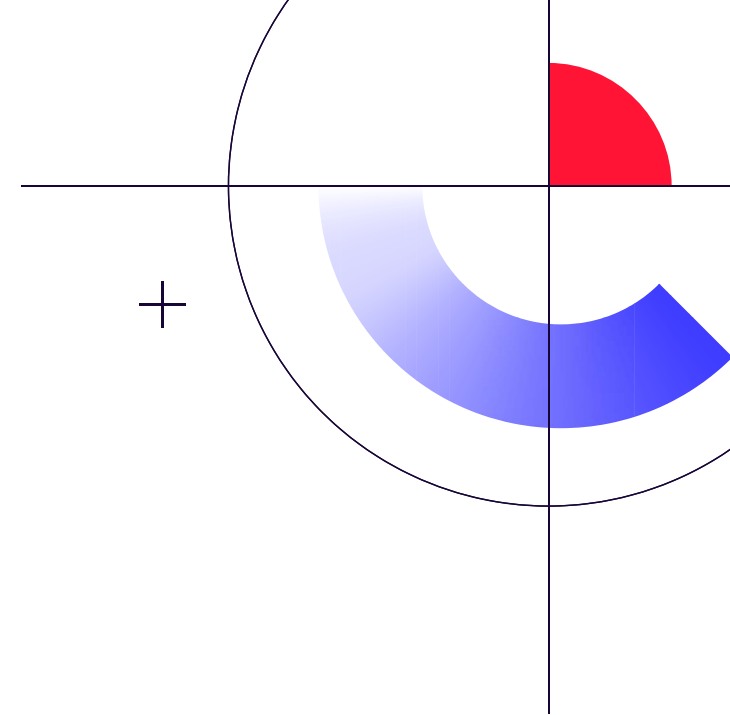
Through its deployments and partnerships, Gatewatcher has built an approach grounded in **native understanding of industrial environments**: broad coverage of OT protocols, passive monitoring suited to constrained infrastructure, the ability to integrate with existing ecosystems, and risk contextualization based on each organization's operational reality.

The experience of clients such as Look Up Space and Lynred illustrates this well: in some sectors, cybersecurity is protecting not just information systems, but critical industrial, technological, and sovereign capabilities.

See earlier, understand faster, decide quickly:

IT/OT convergence demands a cybersecurity approach built on anticipation, not reaction.

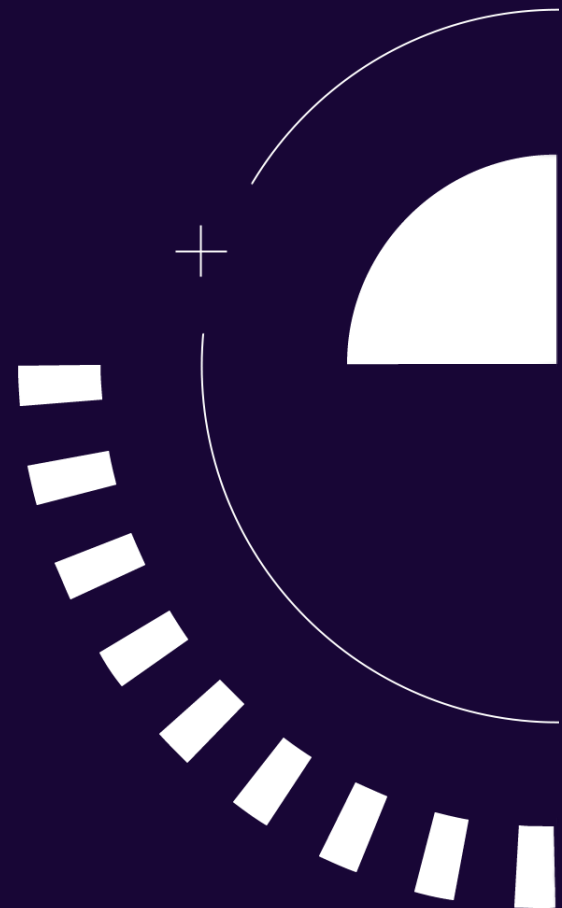
When digital technology drives critical operations, cybersecurity becomes a direct matter of *continuity, operational resilience, and sovereignty*—





About_

A leader in cyber threat detection, Gatewatcher protects the networks of businesses and public-sector organizations around the world, including the most critical ones. The company delivers complete network visibility through an AI-powered NDR platform that analyzes activity across cloud and on-premises environments. Its “Decision Center” turns security signals into actionable, compliant decisions by unifying data from the network, endpoints, cloud, and identity sources, improving SOC efficiency and response times.



✉ contact@gatewatcher.com
 ☎ +33 (0)1 44 51 03 93
 📍 Campus Cyber • Puteaux, France

in GATEWATCHER
 📺 GATEWATCHER Official
 ✕ @GATEW4TCHER

Explore our solutions...

