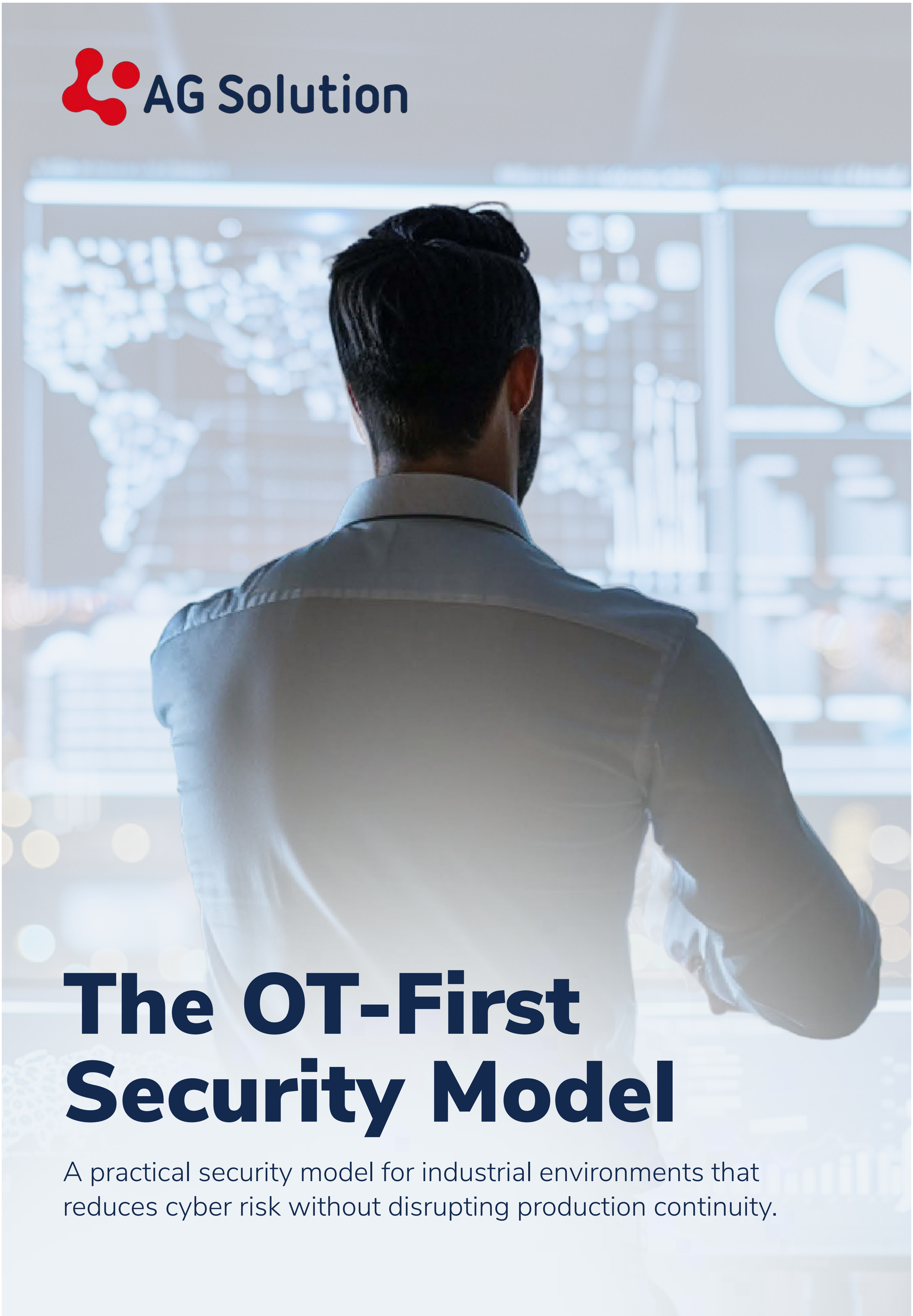
AG Solution



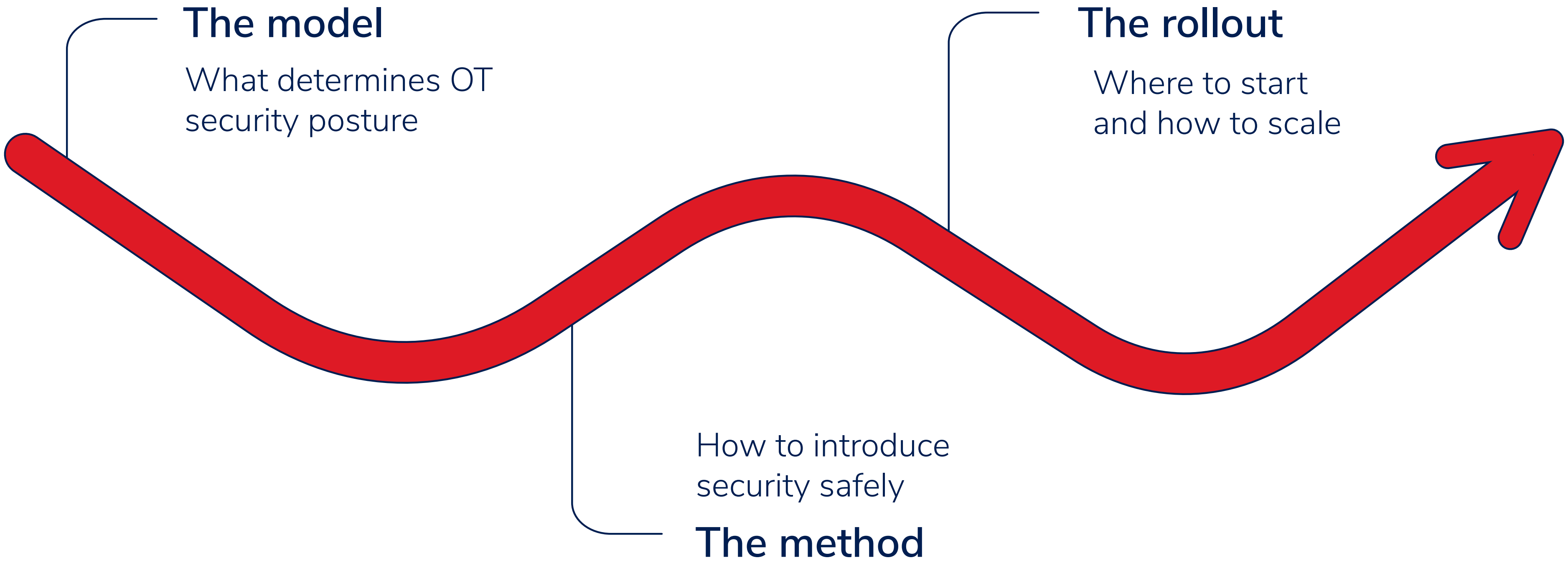
The OT-First Security Model

A practical security model for industrial environments that reduces cyber risk without disrupting production continuity.

01

Executive Summary

Implementing the OT-First Security Model



The model

What determines OT security posture

The method

How to introduce security safely

The rollout

Where to start and how to scale

Manufacturers are operating increasingly connected OT environments without the visibility or control required to manage cyber risk safely. As a result, security actions themselves often become a source of operational disruption. Cyber incidents, regulatory pressure, and vendor-driven complexity are exposing a widening gap between traditional security models and the realities of industrial operations.

The OT-First Security Model is designed to address that gap. It is a production-aware approach built specifically for operational technology, focused on the factors that actually determine security outcomes in industrial environments. The model is grounded in four core capabilities and supported by a low-risk implementation pattern that reflects how manufacturing systems behave in practice. Its objective is to reduce exposure, limit blast radius, and protect operational continuity while meeting regulatory expectations such as NIS2 and IEC 62443.

WHAT THE OT-FIRST SECURITY MODEL DELIVERS:

- **Visibility:** Eliminate hidden assets, undocumented connections, and blind spots that typically surface only after an incident.
- **Segmentation:** Contain incidents locally instead of allowing them to spread across lines or sites.
- **Access Control:** Ensure vendors and internal teams access only what they need, only when they need it.
- **Governance:** Establish consistent, auditable controls aligned with evolving regulatory and management accountability.

What differentiates this model is not only what it includes, but how it is applied. OT-first security acknowledges two realities that are often understated in industrial environments: visibility can introduce risk before it creates control, and change is the highest-risk moment in production systems. To manage this, the model follows a structured rollout pattern — **pilot** → **greenfield** → **brownfield** → **quick wins** — designed to reduce risk, build confidence, and demonstrate value before broader scaling.
The result is practical resilience. Organizations gain fewer unknown exposures, a lower risk of downtime, clearer accountability, and more predictable compliance across complex, multi-site environments.

WHO THIS PAPER IS FOR:

This paper is written for CISOs, plant managers, and OT leaders responsible for production continuity, cyber risk reduction, and regulatory accountability.

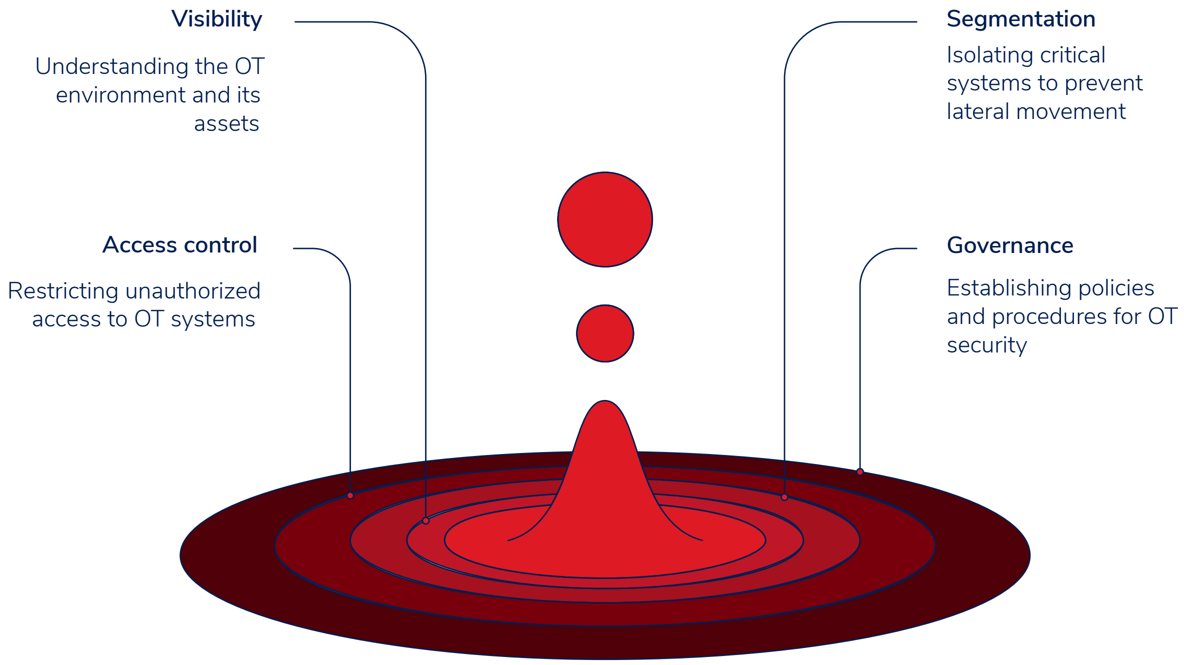
The sections that follow examine the challenges shaping OT security today, outline the foundations of the OT-First Security Model, and explain how it can be introduced safely in real manufacturing environments.

While the four foundations described here define what most directly shapes OT security posture, they are not intended as an exhaustive checklist. The depth, sequencing, and supporting controls depend on each organization's maturity, governance model, and operational constraints.

HOW THE ELEMENTS OF THIS PAPER FIT TOGETHER

The OT-First Security Model brings together three elements that work in sequence:

- **The Model** defines what determines OT security posture through four foundational capabilities: visibility, segmentation, access control, and governance.
- **The Method** explains how these capabilities are introduced safely, using phased progression that prioritizes low-risk visibility, controlled insight, and continuous monitoring.
- **The Rollout** describes where to start and how to scale in real environments — beginning with pilots, embedding security into greenfield projects, adapting to brownfield constraints, and reinforcing progress through targeted quick wins.


Visibility
Understanding the OT environment and its assets
Segmentation
Isolating critical systems to prevent lateral movement
Access control
Restricting unauthorized access to OT systems
Governance
Establishing policies and procedures for OT security

02

Current State: The Manufacturing Security Challenge

The data reflects this shift. In 2024, 31% of organizations reported six or more OT intrusions, nearly three times the figure from the previous year. These incidents were not benign: more than half resulted in productivity losses, over forty percent involved exposure of critical data, and nearly half affected physical safety or process integrity. In manufacturing contexts, this means cyber risk is operational risk.

Limited visibility remains a central problem. Only a small fraction of organizations have a complete, current view of their OT environments. Most plants operate with partial inventories, outdated diagrams, and undocumented integrations. Without a reliable baseline of assets and network behavior, security teams cannot detect anomalies, assess exposure, or demonstrate compliance. Decisions about risk and control are often made without a clear picture of how production systems actually operate.

At the same time, regulatory expectations are tightening. Frameworks such as NIS2 and related resilience requirements are expanding accountability beyond IT, placing responsibility squarely at the management level. Organizations are expected to demonstrate consistent governance, documented controls, and clear ownership across sites and operations. Non-compliance increasingly carries financial, legal, and personal accountability consequences for leadership.

Many manufacturers also underestimate the level of expertise required to implement OT security safely. Building and sustaining visibility, segmentation, access governance, and monitoring demands a mix of process knowledge, controls engineering, OT networking, and cybersecurity skills. Few internal teams cover all of these disciplines. Relying on a single “OT security specialist” is rarely sufficient, particularly in complex or legacy-heavy environments.

Talent shortages compound the problem. A majority of organizations report difficulty finding or retaining specialized OT cybersecurity expertise. In practice, this slows implementation, increases reliance on ad-hoc decisions, and raises the risk of misconfiguration during discovery, segmentation, or change.

Even segmentation—one of the most effective controls—remains unevenly applied. Many plants still operate flat or partially segmented OT networks. In these environments, a localized intrusion can move laterally across systems, turning a contained issue into a plant-wide disruption. Where segmentation exists, it is often misaligned with actual production flows or has degraded over time as environments changed.

Taken together, these conditions create sustained pressure:

- OT systems are more connected and more exposed.
- Visibility into real environments remains limited.
- Regulations demand stronger governance and accountability.
- Expertise gaps slow progress and increase risk.
- Vendor and supply-chain access multiplies exposure.

What manufacturers need is not more technology, but a structured, production-aware approach that brings clarity, predictability, and operational alignment to OT security—without destabilizing the systems that keep plants running.

03

The Four Foundations of the OT-First Security Model

The OT-First Security Model is built around four capabilities that most directly determine whether OT security efforts succeed or fail in manufacturing environments. These foundations are not meant to cover every control or activity involved in cybersecurity. Rather, they define the conditions that make additional controls effective instead of disruptive.

Without these foundations in place, adding tools or controls typically increases complexity without meaningfully reducing operational risk.

Effective OT security does not begin with technology. It begins with management intent. The success of this model depends on explicit leadership support: clear prioritization, sustained funding, and the authority to apply security consistently, even when it competes with short-term operational efficiency. In practice, that support is often built progressively, as visibility improves and the realities of the environment become harder to ignore.

When leadership backing is weak or ambiguous, OT security initiatives rarely fail for technical reasons. They stall because decisions are deferred, controls are applied inconsistently, or security is repeatedly deprioritized in favor of keeping production moving. The four foundations below define what a viable OT security posture requires, but their impact is determined by how clearly leadership enables their implementation.

3.1 VISIBILITY: ESTABLISHING A FACTUAL BASELINE

Visibility comes first because nothing else works without it. In most plants, the documented view of the OT environment is years—or decades—out of date. Equipment has been added, modified, bypassed, or replaced without documentation. Vendors have made changes on the fly. Network diagrams rarely reflect what is actually running on the shop floor.

Establishing visibility in OT environments must be done carefully. Many systems cannot tolerate intrusive scanning or generic discovery tools. A single misstep can interrupt a running process. While AI-assisted discovery is improving, it still cannot reliably interpret the thousands of logic instructions inside PLCs or understand how those instructions interact across a production line without expert validation.

A reliable visibility baseline typically includes:

- A complete view of operational assets, including unmanaged devices introduced over time
- Communication paths between systems, not just asset lists
- Critical dependencies that could trigger cascading failures if altered
- “Shadow OT”: equipment or connections installed without central oversight

Accurate measurement also prevents false confidence. Many security failures stem from incorrect assumptions about how systems interact or from trusting diagrams that no longer reflect reality.

Visibility is not a one-time exercise. OT environments change continuously—vendors connect remotely, equipment is modified, and small adjustments accumulate. Without ongoing visibility, blind spots return quickly.

3.2 SEGMENTATION: CONTAINING WHAT YOU CANNOT PREVENT

Segmentation turns visibility into control. When designed and maintained correctly, it limits how far an incident can spread and keeps localized problems from becoming plant-wide disruptions.

Most organizations recognize its value, yet implementation quality varies widely. Some plants have segmentation on paper but operate flat networks in practice. Others rely on configurations that no longer align with the physical or logical layout of production.

Effective OT segmentation does not attempt to firewall every device. It focuses on:

- Grouping systems based on how they actually function together
- Restricting only the communication that needs to be restricted
- Aligning rules with production flow rather than theoretical models
- Allowing operators and maintenance teams to work without constant friction

When segmentation reflects production logic, it improves both security and operability. Changes can be isolated to specific zones without creating unintended impact across the line—a practical benefit that is often overlooked in security planning.

3.3 ACCESS CONTROL: MANAGING WHO TOUCHES WHAT—AND WHEN

Access control is where many OT incidents begin, and where many manufacturers still struggle. Plants rely on a mix of internal staff, contractors, machine builders, and service partners, many of whom require remote access. Without structure, this quickly becomes a patchwork of shared credentials, ad-hoc VPNs, unmanaged remote tools, and portable media.

A mature OT access model clearly separates:

ONSITE ACCESS

Operators and technicians need to work efficiently, but access should match responsibility. This typically includes role-based permissions, credential hygiene, least-privilege enforcement, and physical access boundaries around critical equipment.

REMOTE ACCESS

Remote vendor access is often unavoidable, but it must be controlled. Effective practices include:

- Secure jump hosts or remote-access gateways
- Full session logging and monitoring
- Time-bound or task-specific access
- Clear approval and ownership for vendor connections
- Strong controls around removable media, which remains a common infection vector

When access is governed properly, plants maintain operational flexibility without sacrificing accountability or control.

3.4 GOVERNANCE: KEEPING SECURITY CONSISTENT OVER TIME

Governance is where intent becomes reality. Many organizations have capable engineers and appropriate tools but still struggle to sustain OT security because priorities are unclear, mandates are weak, or security consistently loses to production pressure.

Effective governance requires explicit executive ownership. Leadership must define acceptable risk, allocate funding, and grant OT security teams the authority to intervene when controls are bypassed or shortcuts emerge. Without this backing, policies exist on paper while practices diverge across sites, vendors, and projects.

Strong OT governance establishes a single source of truth:

- Clear expectations aligned with regulatory and accountability requirements
- Defined responsibilities across IT, OT, and operations
- Processes for approving changes and handling incidents
- Security requirements for vendors and partners
- A rhythm of continuous improvement as environments evolve

Governance also determines timing. When security expectations are built into new projects and vendor engagements, controls are easier to apply and far less disruptive. When security is added after systems are live, it is costlier, harder to enforce, and more likely to be scaled back under pressure.

Finally, governance extends beyond process. Human behavior remains a major factor in OT incidents. Training, awareness, and realistic controls require sustained executive support. Without it, even well-designed programs erode over time.

These four foundations define what effective OT security must include. Implementing them, however, requires confronting realities that most manufacturers only discover once security work begins. Some challenges are predictable. Others remain hidden until visibility improves.

04

Hidden Realities of OT Security

On paper, OT security often appears straightforward: map the environment, segment the network, control access, and establish governance. In real plants, the gap between theory and practice is wide. The realities below are rarely addressed in traditional security models, yet they determine whether OT security efforts stabilize operations—or create new risk.

These observations are drawn from day-to-day work inside active industrial environments. They reflect how OT systems actually behave under production pressure, not how they are assumed to behave in frameworks or reference architectures.

4.1 COMPLEXITY AND LEGACY CONSTRAINTS

4.1.1 LEGACY LOGIC IS DEEPLY COMPLEX—AND OFTEN UNREADABLE

Many PLCs have been running unchanged logic for years, sometimes decades. Code has been extended, patched, and repurposed as equipment was modified or lines were expanded. In some cases, the original integrators are long gone. In others, logic has been adjusted repeatedly to keep production running, with limited documentation.

There is no automated tool that can reliably interpret all dependencies or predict how a change will behave once deployed across a brownfield environment. AI can assist with anomaly detection, but it cannot replace human understanding of process logic, safety interlocks, or timing constraints.

Claims of fully automated logic analysis rarely hold up in complex, real-world OT environments without extensive validation by people who understand the process.

4.1.2 BROWNFIELD PLANTS HIDE “SHADOW OT” EVERYWHERE

In most manufacturing sites, OT evolves organically:

- A contractor installs a switch to solve a temporary issue
- A machine builder adds remote access for maintenance
- A supervisor connects a device “just for diagnostics”
- Equipment is replaced without updating diagrams

Over time, these changes accumulate quietly. The result is a patchwork of devices and connections that never appear in official documentation.

Shadow OT is not an exception. It is the norm. And in many plants, it becomes visible only once security work begins.

4.1.3 AI CAN ASSIST— BUT IT CANNOT REPLACE EXPERIENCE

AI-based monitoring and anomaly detection can add value as environments grow more complex. But AI does not understand process context. It cannot infer why a pattern exists, whether it is tied to a specific product run, or how it behaves under abnormal conditions.

AI is a tool, not a strategy. In OT environments, human judgment, process knowledge, and familiarity with a plant’s operational history remain essential.

These realities explain why OT security cannot rely on generic IT methods or automated tooling alone. A viable approach must account for legacy constraints and build control incrementally.

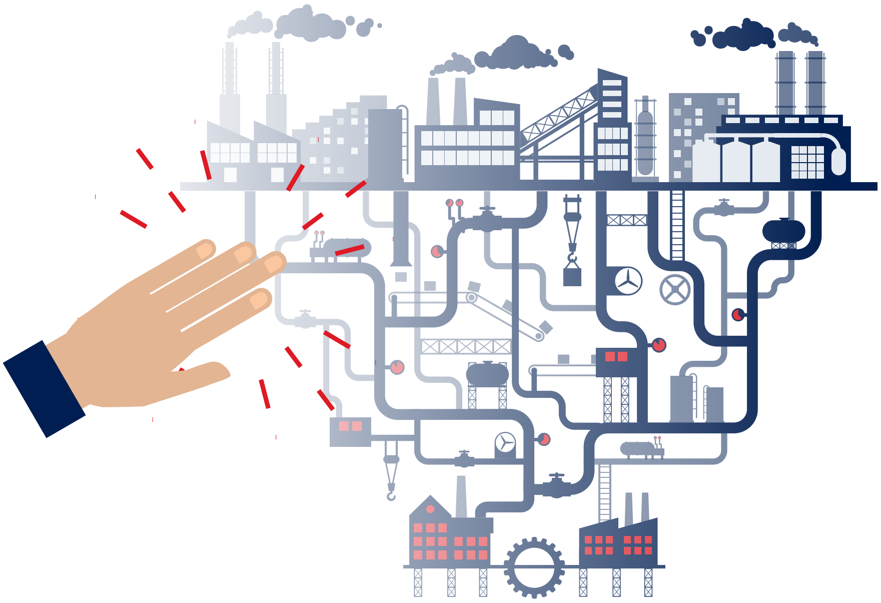
4.1.4 EXPERTISE REQUIREMENTS ARE HIGHER THAN MOST ORGANIZATIONS EXPECT

Implementing OT security safely requires more than a single specialist. It demands coordinated expertise across automation, controls, networking, cybersecurity, safety, and operations. Many organizations underestimate this and attempt to centralize responsibility in a small team or individual.

In practice, this increases the risk of sequencing errors, misconfigured controls, and disruption during discovery or segmentation. The ongoing shortage of experienced OT security professionals makes it difficult for manufacturers to staff these programs internally, which is one reason many initiatives stall or progress slowly.

Security Actions Can Create Hidden Risks in OT Environments.

Complexity and legacy
Unreadable logic,
shadow OT



High-risk operational moments
Visibility creates risk,
change is dangerous

Limits, vendor behavior
Tooling and vendor risk

4.2 TOOLING AND VENDOR-DRIVEN RISK

4.2.1 TOOLING HAS LIMITS—AND SOMETIMES BECOMES PART OF THE PROBLEM

Vendors often promote “plug-and-play” OT visibility or automated segmentation. In real plants, tools must contend with legacy networks, unsupported protocols, and equipment that cannot tolerate intrusive monitoring.

Some discovery tools generate traffic patterns that older devices misinterpret. Some detection platforms struggle with industrial protocols or overwhelm teams with false positives. Others require architectural changes that plants are not ready to absorb.

Tools matter. But in OT environments, they are effective only when applied with process understanding and careful sequencing.

Many of these tools are also expensive and designed for structured assessments rather than continuous internal use. Most plants cannot justify owning them for occasional discovery work, which is why manufacturers often rely on external expertise to perform deep visibility assessments safely.

4.2.2 VENDOR BEHAVIOR SHAPES THE SECURITY POSTURE MORE THAN MOST REALIZE

Manufacturers depend on machine builders, integrators, and service providers who require onsite or remote access. Each partner brings its own practices, tools, and assumptions. Some operate with strong security discipline. Others do not.

Without clear governance, vendors effectively define the security model themselves—often unintentionally. This leads to wide variation across plants, even within the same organization, and introduces risk that is difficult to see until something breaks.

4.3 HIGH-RISK OPERATIONAL MOMENTS

4.3.1 VISIBILITY CREATES RISK BEFORE IT CREATES CONTROL

Visibility is often described as a low-risk first step. In practice, gaining visibility means interacting with networks whose behavior is not fully understood. A poorly chosen discovery method, a misconfigured switch, or a device that reacts unpredictably under load can interrupt production.

Plants cannot pause operations for discovery. Every action must be planned, timed, and validated with the assumption that continuity comes first. Visibility in OT therefore requires a deliberate, low-impact approach—not the automated scanning techniques common in IT.

4.3.2 CHANGE IS THE MOST DANGEROUS MOMENT IN OT

Small changes can have outsized consequences. Updating a switch, modifying a firewall rule, replacing a PLC, or introducing a new remote access path can trigger issues that only appear under load or during specific operating states.

This is why OT teams are often reluctant to touch stable systems, even when security improvements are necessary.

In production environments, “working” does not always mean “safe.” But stability is non-negotiable. Security initiatives that ignore this reality quickly lose trust.

4.3.3

ASSETS ASSUMED TO BE ISOLATED OFTEN ARE NOT

During assessments, it is common to find equipment believed to be isolated but still reachable through undocumented links, leftover connections, or vendor-installed access paths. These assets create silent risk because the organization assumes they are protected when they are not.

Such connections often surface only after traffic is observed over time or when proper measurement tools are applied. In one brownfield assessment, a packaging-line PLC assumed to be isolated was reachable through an old vendor VPN appliance left online after commissioning. The connection was undocumented, unknown to plant staff, and effectively bypassed existing perimeter controls.

These hidden realities explain why OT security initiatives fail even when intentions are sound. They also explain why a production-aware, OT-first approach is necessary—one that respects legacy constraints, sequences change carefully, and treats security as an operational discipline rather than a technical overlay.

05

Building the OT-First Security Model

(METHODOLOGY & APPROACH)

Turning the four foundations into a working OT security posture requires a method that reflects how industrial environments actually operate. Plants cannot absorb large, disruptive changes. They cannot afford to act on untested assumptions. And they cannot rely on tools alone to interpret years—often decades—of technical decisions embedded in equipment, logic, and network architecture.

For these reasons, the OT-First Security Model follows a phased, controlled approach. It moves deliberately from understanding to action, sequencing changes to limit operational risk, surface hidden conditions early, and allow decisions to be made based on observed behavior rather than assumptions.

5.1 PHASE 1: ESTABLISH A LOW-RISK VISIBILITY BASELINE

The first step is to understand the environment without destabilizing it. Phase 1 avoids intrusive discovery and focuses instead on building a factual baseline through observation, validation, and controlled verification. The priority is safety, not completeness.

This phase typically includes:

- Reviewing existing documentation and comparing it to observed reality
- Identifying areas where safe, low-impact observation is possible
- Using non-intrusive methods to observe traffic and system relationships
- Documenting what is known, what is uncertain, and what is missing

This work often surfaces issues that were previously invisible: devices added over time, undocumented vendor access, obsolete firmware, or systems operating outside expected configurations. The objective is not to achieve full visibility in one step, but to create a baseline that teams can trust before introducing any form of active discovery.

5.2

PHASE 2: DEEPEN INSIGHT WITH TOOL-ASSISTED DISCOVERY—CAREFULLY

Once a stable baseline exists, targeted tooling can be introduced to deepen insight. Unlike IT environments, where broad automated scans are routine, OT systems require precision and restraint. Tools are selected and configured incrementally, with each step validated against operational behavior.

This phase enables teams to:

- Identify previously unknown assets
- Understand communication patterns across zones and subnets
- Detect vulnerabilities tied to firmware or protocol use
- Observe how systems behave under normal operating load

Control is the defining principle. The goal is to expand understanding without interrupting production or triggering unexpected behavior in legacy devices.

5.3

PHASE 3: PREPARE THE ENVIRONMENT FOR CONTINUOUS MONITORING

Continuous monitoring becomes viable only after the environment is sufficiently understood and stabilized. At this stage, monitoring platforms can observe changes over time without interfering with operations, shifting security from episodic assessment to sustained oversight.

Continuous monitoring allows teams to:

- Detect newly introduced devices or connections
- Identify deviations from established baselines
- Track exposure as systems evolve
- Receive early warning signals before issues affect production

This marks the transition from reactive security to proactive operational risk management.

ALL PHASES

ALL PHASES IN ONE GRAPH

01

PHASE 1: LOW-RISK VISIBILITY BASELINE

Manual observation and documentation to create a safe, factual baseline

02

PHASE 2: CAREFULLY INTRODUCED TOOLING

Incremental deployment of targeted tools to deepen insight and map vulnerabilities

03

PHASE 3: CONTINUOUS MONITORING

Implementation of sensors and platforms for ongoing, proactive security

5.4 A MODEL DESIGNED FOR OT—NOT REPURPOSED FROM IT

Traditional IT security frameworks assume frequent change, built-in redundancy, and rapid failover. OT environments do not. In manufacturing, even small changes can affect safety, throughput, or quality.

The OT-First Security Model is designed around operational consequences, not theoretical completeness. Each phase prioritizes continuity, respects legacy constraints, and sequences change to reduce risk. Automation and AI are introduced only after the environment is understood and controlled—not as substitutes for judgment during early discovery or segmentation.

The model consistently prioritizes:

- Operational continuity
- Process stability
- Respect for legacy equipment
- Low-impact change sequencing
- Vendor coordination
- Alignment with management accountability

Avoiding premature automation is intentional. Rules engines and AI-based tools are valuable once control exists, but they cannot replace the human judgment required when visibility is limited and the cost of error is high.

5.5 DEFINING WHAT "GOOD" LOOKS LIKE

One of the strengths of this methodology is clarity. When visibility, segmentation, access control, and governance are introduced in a deliberate sequence, organizations can define what a healthy OT security posture actually means for their environment.

In practice, a healthy posture includes:

- A validated asset inventory that reflects the real environment
- Segmentation aligned with production logic and operational flow
- Governed access for internal teams and external vendors
- Predictable change processes with clear ownership
- Monitoring that detects risk before it affects operations
- A measurable reduction in unknown exposure over time

This definition becomes the reference point for audits, regulatory discussions, and investment decisions.
With the methodology established, the next challenge is execution. The way security is introduced matters as much as the controls themselves. Pilot areas must be chosen carefully. Greenfield projects require a different approach than brownfield sites. And early, visible progress is essential for building organizational confidence.

06

IMPLEMENTATION STRATEGY

Implementation Strategy:

PILOT → GREENFIELD → BROWNFIELD → QUICK WINS

Implementing OT security is not a linear rollout of controls. In industrial environments, change itself introduces risk. For that reason, the OT-First Security Model defines four implementation principles—pilot, greenfield, brownfield, and quick wins—that reflect how security can be introduced progressively without destabilizing production.

This sequence is not a maturity model. It is a practical way to align security improvements with operational reality, reducing risk while building confidence and momentum.

WHAT TYPICALLY CHANGES EARLY WHEN THE OT-FIRST SECURITY MODEL IS APPLIED

While every environment is different, organizations that apply the OT-First Security Model in a structured way tend to see similar early shifts:

- Clearer understanding of what is actually connected, communicating, and exposed
- Reduced uncertainty during changes, as dependencies become visible and documented
- Fewer high-risk access paths, especially unmanaged remote connections
- Clearer ownership and decision-making across IT, OT, and operations
- Greater confidence to proceed with pilots, upgrades, or segmentation without disrupting production

These outcomes do not signal completion. They indicate that a stable foundation is in place—one that allows security to improve without introducing new operational risk.

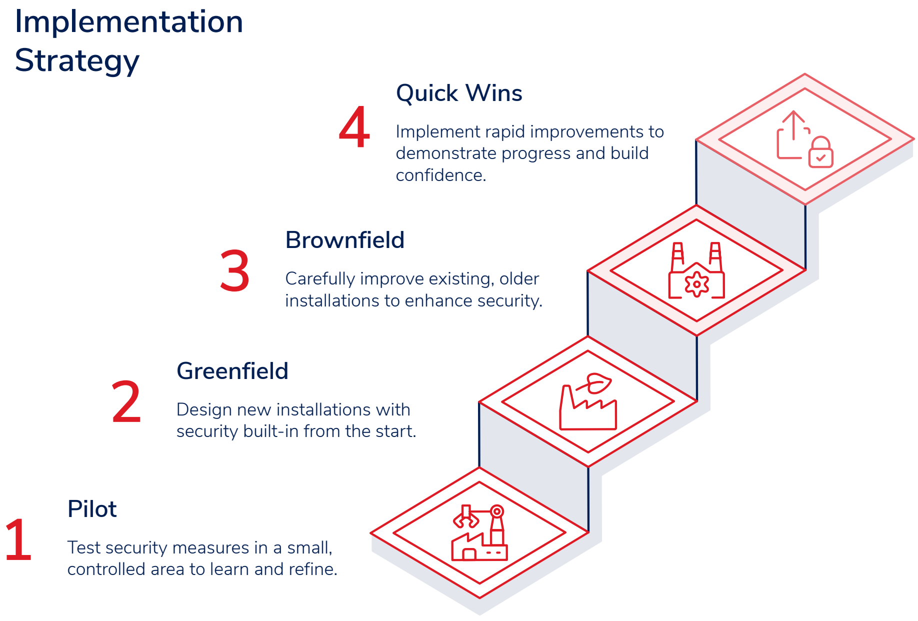
6.1 START WITH A PILOT: CONTAINED, CONTROLLED,AND MEASURABLE

A pilot creates a low-risk environment to validate the OT-First Security Model in practice. It allows teams to test assumptions, expose hidden dependencies early, and demonstrate value before scaling.
The initial pilot should not target the most complex or critical part of the plant. It needs clear boundaries and enough diversity to reflect real conditions without putting core production at risk.

Strong pilot candidates often include:

- A standalone production line
- A support system such as utilities, packaging, or wastewater
- An area with known visibility gaps but manageable operational impact
- A location with limited or stable vendor involvement

A pilot validates more than technical controls. It tests how discovery behaves in real conditions, how segmentation affects communication, how access changes daily routines, and how governance functions across teams. It also surfaces issues no diagram or tool can predict—unofficial connections, undocumented logic, vendor-specific behavior, or dependencies that only appear under load.
A well-executed pilot becomes the reference point for subsequent rollouts.



Implementation Strategy

4 Quick Wins

Implement rapid improvements to demonstrate progress and build confidence.

3 Brownfield

Carefully improve existing, older installations to enhance security.

2 Greenfield

Design new installations with security built-in from the start.

1 Pilot

Test security measures in a small, controlled area to learn and refine.

6.2

APPLY THE MODEL TO GREENFIELD PROJECTS: BUILD SECURITY BEFORE COMPLEXITY APPEARS

Greenfield projects offer a rare opportunity to embed security before legacy constraints take hold. Applying the OT-First model early reduces future retrofit costs, limits technical debt, and simplifies compliance.

In greenfield environments, architecture, segmentation, access control, and governance can be aligned from the start—before variations in equipment, integrators, and vendor practices introduce complexity.

Key advantages include:

- Clean network design without inherited constraints
- Segmentation aligned with intended production flow
- Access rules defined before vendors begin work
- Well-documented environments shared across teams
- Faster alignment with regulatory and governance expectations

Greenfield work also helps organizations refine internal standards and templates that can later be adapted to existing sites.

6.3

BRING THE MODEL INTO BROWNFIELD PLANTS: WHERE THE REAL WORK HAPPENS

Brownfield environments carry the highest exposure and the least visibility. They are also where the greatest risk reduction can be achieved—if changes are sequenced carefully.

Most OT security challenges emerge in brownfield plants. These environments reflect years of incremental change: equipment upgrades, vendor interventions, workarounds, and undocumented fixes. Even within a single facility, no two areas behave the same way.

Applying the OT-First model in brownfield settings requires:

- A slower, observation-first approach
- Discovery methods suited to older equipment
- Realistic expectations about hidden assets and undocumented connections
- Close coordination with OT teams who understand how systems behave
- A change rhythm aligned with production and maintenance windows

Brownfield work frequently reveals:

- Forgotten or repurposed devices
- Networks that evolved without design
- Controllers running outdated firmware tied to critical sequences
- Remote access paths created years earlier and never removed
- Integrator-specific practices that vary across sites

These environments cannot be reshaped quickly. The strategy must prioritize changes that deliver meaningful risk reduction with minimal operational impact, one controlled step at a time.

6.4 DEMONSTRATE QUICK WINS: PROVING VALUE EARLY AND OFTEN

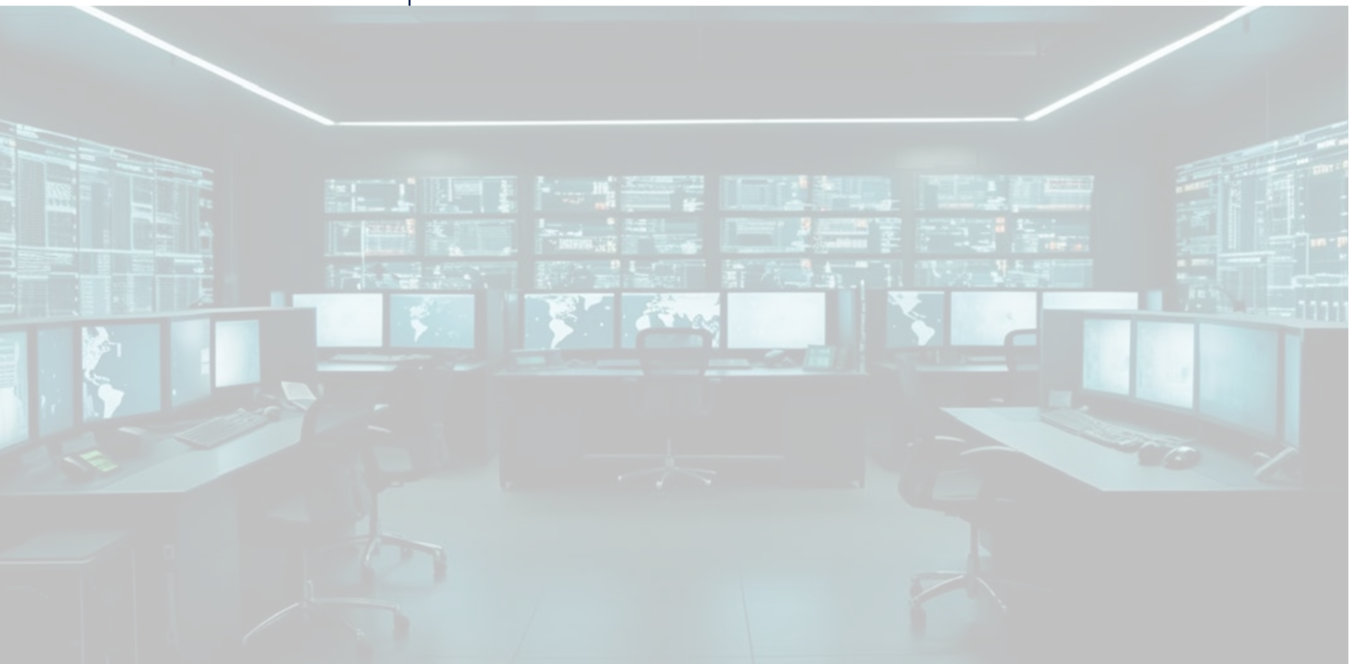
Quick wins show progress in weeks rather than years. They build trust with OT teams, justify investment, and demonstrate that security can support operations instead of complicating them.

Typical quick wins include:

- Removing unused or unmanaged remote access accounts
- Restricting high-risk communication paths
- Documenting previously unknown assets
- Updating firmware on non-critical equipment
- Applying segmentation rules to a single zone with measurable impact
- Standardizing access roles for internal teams and vendors

Quick wins do not replace long-term work. They reinforce confidence while more complex phases progress in parallel.

With the implementation strategy defined, the next step is to show how the OT-First approach translates into measurable outcomes in real environments—how visibility, segmentation, access control, and governance come together to reduce risk and strengthen operational resilience.



07

USE CASE

Use Case:

SECURING BROWNFIELD OT WITHOUT DISRUPTING PRODUCTION

The following example is a composite, anonymized case drawn from multiple industrial engagements. It reflects conditions commonly encountered in brownfield manufacturing environments and illustrates how the OT-First Security Model is applied in practice.

CHALLENGE

A large, multi-site food manufacturing organization engaged support to improve the security of its factory systems. Many of its plants operated under strict production and quality constraints, relied heavily on legacy equipment, and carried technical debt accumulated over years of incremental change.

Network documentation was incomplete. No one could reliably explain which systems needed to communicate with which, or why. Applying intrusive discovery or rule-by-rule firewalling was considered too risky. The overriding concern was avoiding any action that could disrupt production while restoring control over the environment.

APPROACH

The work began by reducing obvious exposure first. Known backdoors and unmanaged remote access paths were closed, lowering immediate risk without altering core production behavior.

From there, visibility was introduced carefully. Instead of relying on assumptions or outdated diagrams, controlled firewall-based observation was used to monitor actual traffic flows. This allowed teams to see how systems communicated in practice, under real operating conditions.

Observed traffic was captured and consolidated into structured views using targeted scripts. The majority of communication flows could be explained, documented, and justified based on function and process context. For the

remaining cases, local OT teams were involved to validate purpose and necessity before any changes were considered.
Once a trusted baseline was established, firewall rules were progressively tightened to permit only verified communication paths. This reduced exposure significantly while preserving operational continuity.

Remote access was then restructured using monitored, time-bound connections. Vendors and specialists retained the access they needed to perform their work, while accountability and control were restored.

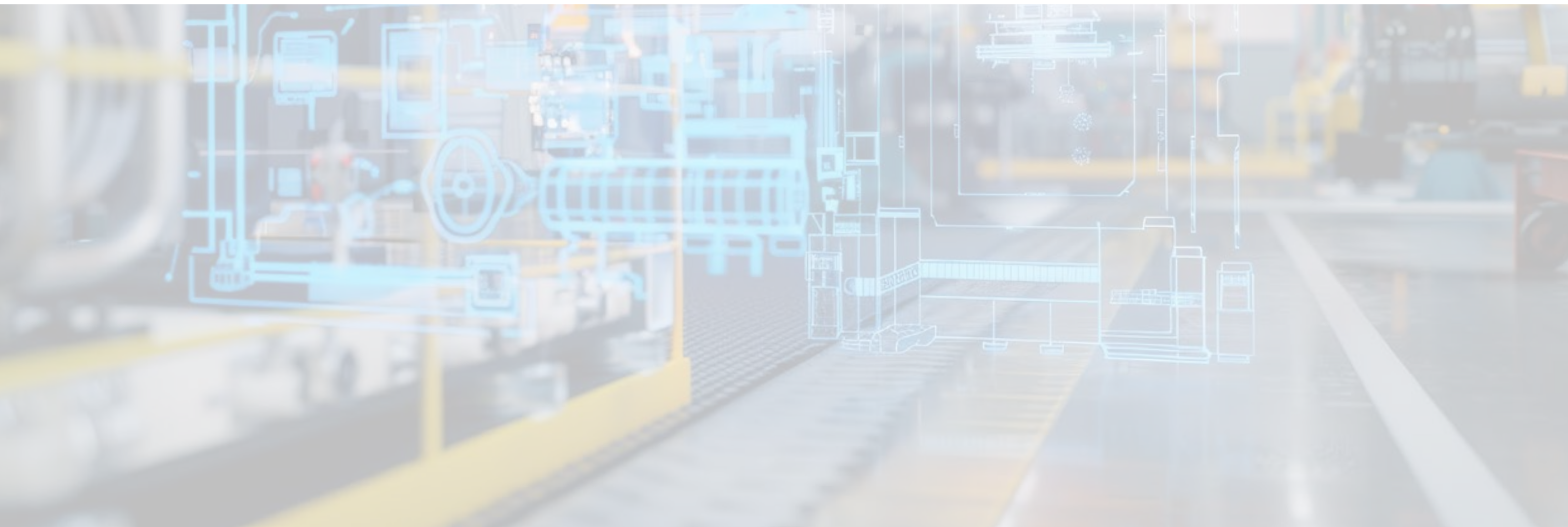
RESULTS

Beyond improved security, plants reported operational benefits over time. Increased visibility and clearer governance reduced trial-and-error during changes, improved preparation for maintenance and upgrades, and contributed to more stable operations.

In several sites, teams noted fewer disruptions during modifications and a smoother coordination between security, IT, and operations. These improvements emerged not from additional tooling, but from better understanding, sequencing, and control.

What This Example Demonstrates

This case illustrates how complex brownfield environments can be broken into manageable steps. By sequencing visibility, containment, access control, and governance carefully, organizations can reduce exposure, protect stability, and build confidence—without disrupting production.



08

Conclusion & Next Steps

Manufacturers are operating in a security environment shaped by growing connectivity, tighter regulatory expectations, and deeply complex operational realities. Legacy infrastructure, widespread vendor access, undocumented change, and limited tolerance for disruption make it difficult to manage OT risk using generic, IT-driven security models.

The OT-First Security Model provides a structured way through that complexity. It starts with visibility, applies segmentation and access control deliberately, and stabilizes the environment through governance aligned with management accountability. The strength of the model is not any single control. It is the sequence.

Visibility without segmentation leaves organizations aware of risk but unable to contain it. Segmentation without access control still allows uncontrolled movement. Governance without monitoring quickly falls out of date as environments change.

Applied together—and in the right order—these foundations allow manufacturers to reduce exposure without destabilizing operations. That balance is essential in production environments where change itself is often the highest risk.

The methodology described in this paper reflects conditions found in real plants: legacy equipment with limited tolerance for disruption, complex PLC logic that resists automation, the persistence of shadow OT, and the operational consequences of even minor changes. These realities demand a deliberate, experience-led approach rather than a tool-centric or compliance-only response.

For most organizations, the next step is not a sweeping security program. It is choosing a safe place to begin—a pilot area, a greenfield opportunity, or a brownfield line where visibility gaps or access risks are already known. From there, the model scales naturally: site by site, zone by zone, reinforced through quick wins and measurable progress.

The OT-First Security Model is not a theoretical framework. It reflects how security is introduced, tested, and sustained in active industrial environments. With clear sequencing, disciplined governance, and leadership ownership, manufacturers can reduce risk, protect production continuity, and meet accountability expectations without introducing new operational instability.

AG Solution continues to support organizations applying this model in real manufacturing environments, helping teams balance security and production while building long-term operational resilience.

About AG Solution

AG Solution is a consulting and engineering partner focused on OT-first modernization and cybersecurity for industrial operations. With teams across Europe and the United States, we work with manufacturers to strengthen production environments where reliability, safety, and continuity cannot be compromised.

Our work centers on securing and modernizing operational technology in real plants, not theoretical architectures. We support manufacturers in applying OT-first security through structured visibility assessments, production-aligned segmentation, governed access models, and vendor-aware governance frameworks. These approaches are designed to reduce cyber risk without introducing new operational risk.

AG Solution's experience spans both OT cybersecurity and broader industrial modernization, including automation, manufacturing execution systems, data and AI initiatives, and large-scale transformation programs. We work across regulated and process-intensive industries such as pharmaceuticals, food and beverage, chemicals, energy, and other batch- and process-driven environments.

Whether supporting a new greenfield facility, stabilizing a complex brownfield site, or scaling OT security across multiple plants, our teams operate with a clear principle: security must work with production, not against it. Our approach is shaped by years of field experience inside operating plants, where sequencing, restraint, and operational awareness determine success far more than tools or frameworks.

REFERENCES

ENISA (2024). *European Union Agency for Cybersecurity — NIS2, Cybersecurity Act, and Related OT/ICS Guidance.*

Fortinet (2024). *2024 State of Operational Technology and Cybersecurity Report.*

KPMG (2024). *Annual Control Systems Cybersecurity Report 2024.*

AG Solution

OT-first advisory and execution for secure, resilient industrial operations.

Contact us

Antwerp – Paris - Barcelona – Madrid – London - Lyon – Lille –
Rotterdam - Cologne – Geneva Almeria - Porto - Tarragona - Krakow –
Zaporizhzhia - New York - Houston