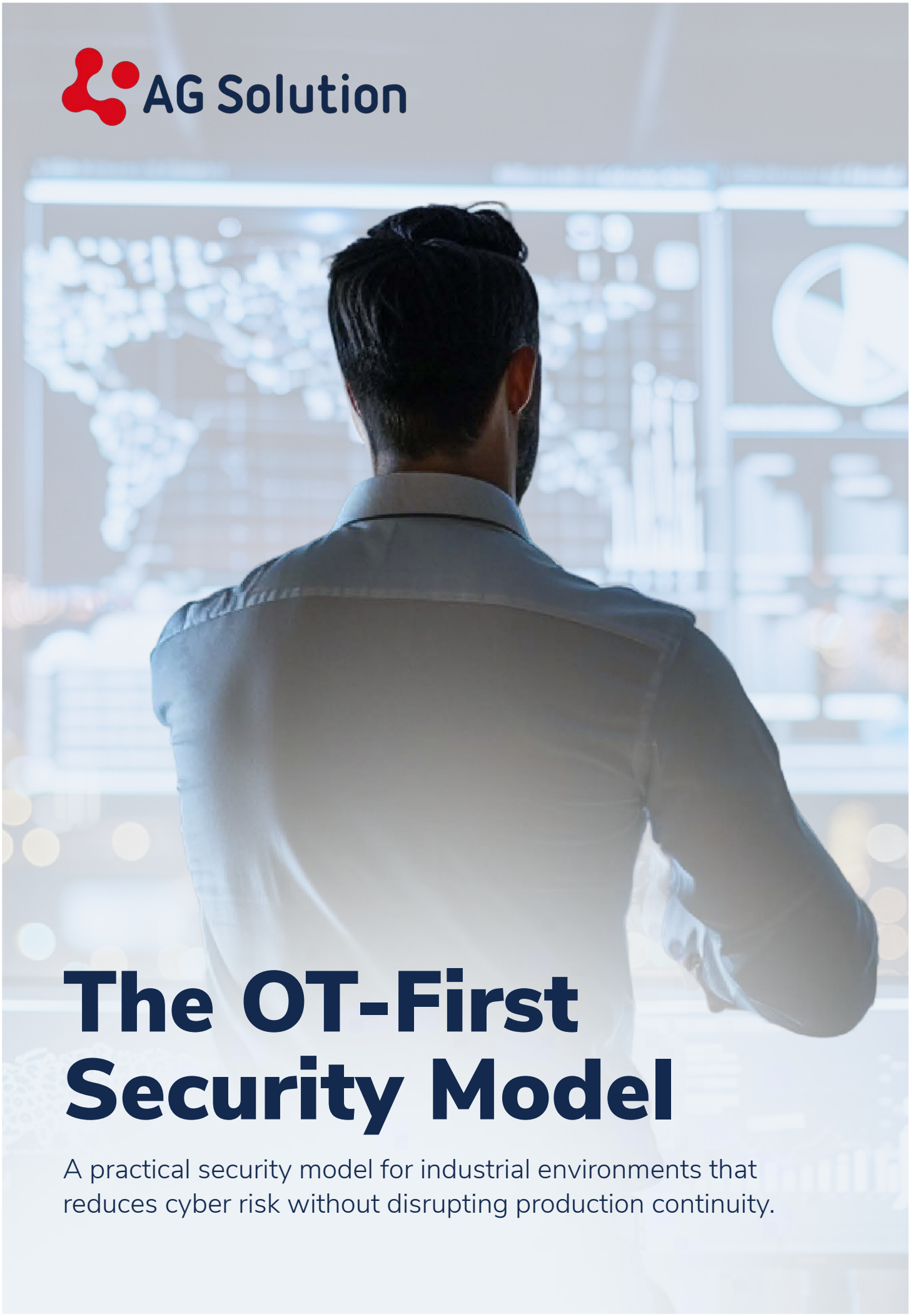
AG Solution



The OT-First Security Model

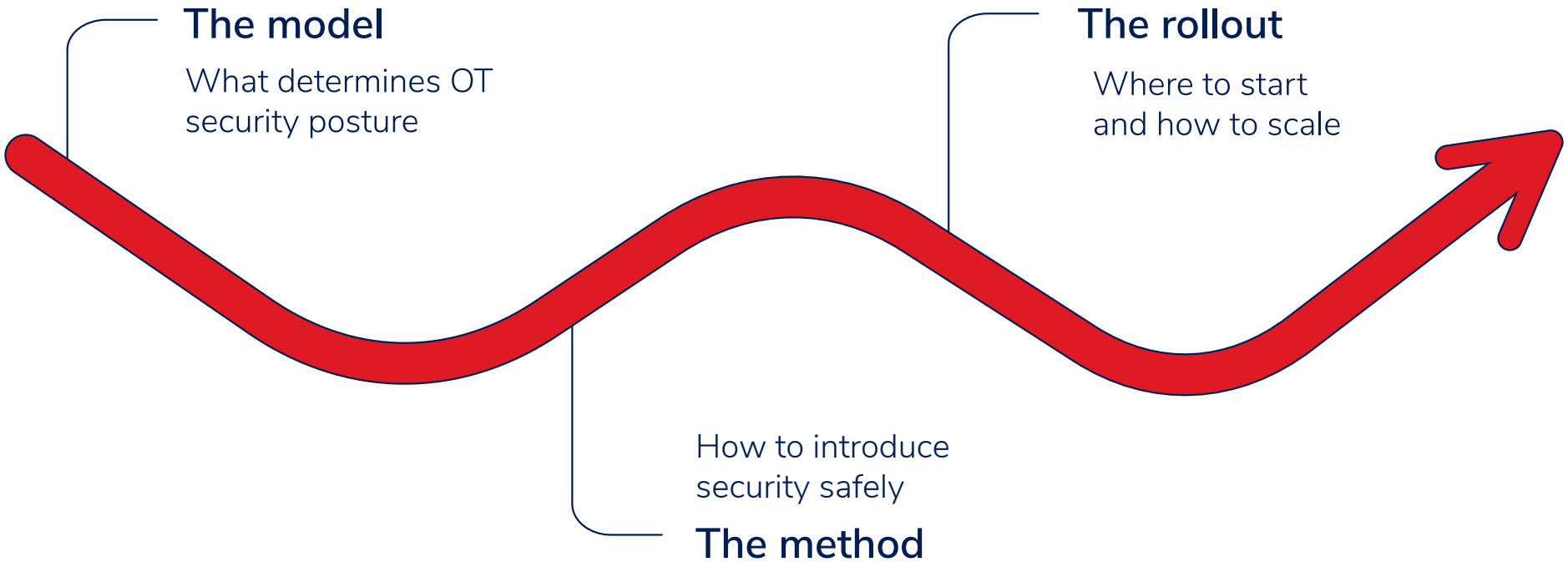
A practical security model for industrial environments that reduces cyber risk without disrupting production continuity.

01

EXECUTIVE SUMMARY

Executive Summary

Implementing the OT-First Security Model



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 critical gap between traditional security models and the realities of industrial operations.

The OT-First Security Model addresses this gap. It is a production-aware approach designed specifically for operational technology, built around four primary capabilities that determine the security posture of industrial environments, and supported by a proven, low-risk implementation pattern. The model focuses on reducing exposure, limiting blast radius, and maintaining operational continuity while meeting regulatory obligations such as NIS2 and IEC 62443.

WHAT THE OT-FIRST SECURITY MODEL DELIVERS:

- **Visibility:** No more hidden assets, undocumented connections, or blind spots that surface only after an incident.
- **Segmentation:** Security incidents remain contained instead of spreading plant-wide.
- **Access Control:** Vendors and internal teams access only what they need, only when they need it.
- **Governance:** Consistent, auditable controls aligned with evolving regulatory requirements.

What makes this model distinct is not only what it includes, but how it is applied. The OT-First approach recognizes two rarely stated truths of industrial security: **visibility can introduce risk before it creates control**, and **change is the most dangerous moment in OT environments**. To manage this reality, the model incorporates a structured rollout pattern: **pilot → greenfield → brownfield → quick wins**, that reduces risk, builds confidence, and allows value to be demonstrated before broader scaling. The outcome is practical resilience: fewer unknown exposures, reduced risk of downtime, greater transparency in accountability, and predictable compliance across complex industrial environments.

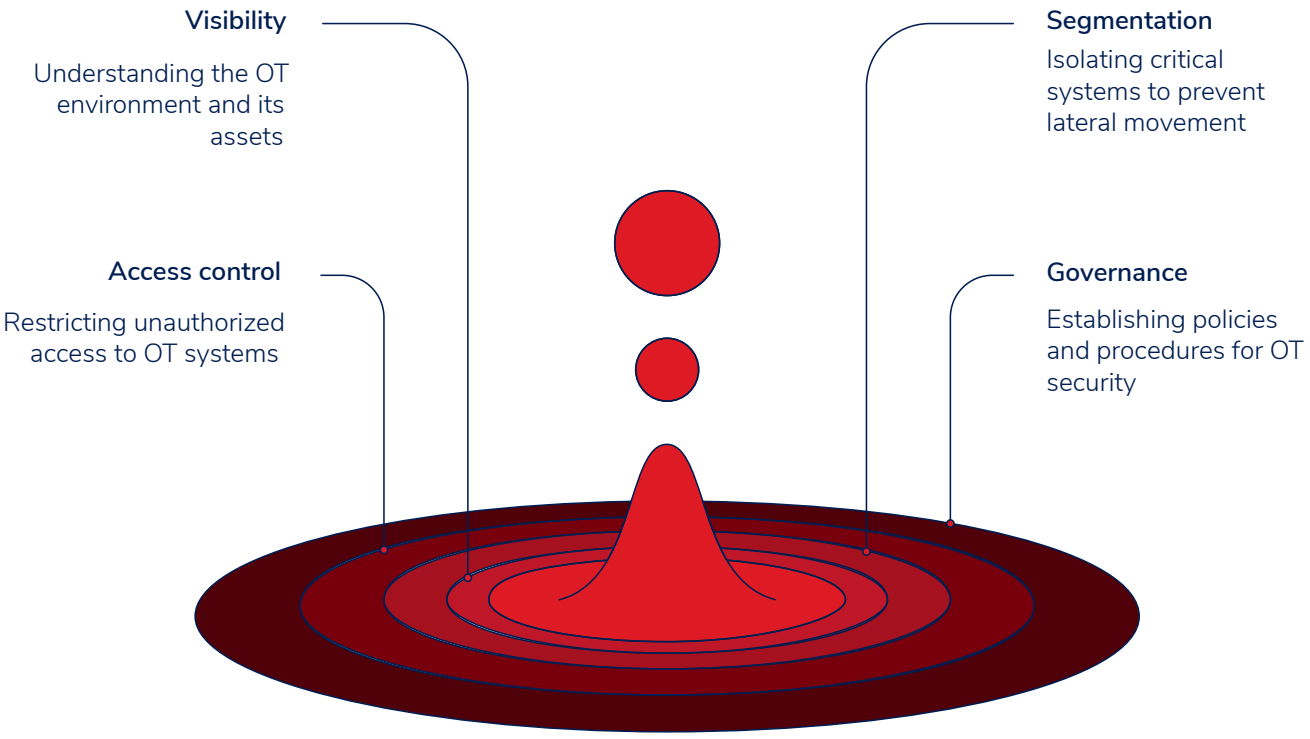
WHO THIS PAPER IS FOR:

CISOs, plant managers, and OT leaders responsible for production continuity, cyber risk reduction, and NIS2 alignment. The sections that follow detail the challenges facing OT security today, the foundations of the OT-First Security Model, and how it can be implemented safely in real manufacturing environments. While these four foundations define what most directly shapes OT security posture, they are not intended as an exhaustive list of all measures involved; the depth, sequencing, and supporting controls depend on each organization's maturity, governance, and operational context.

HOW THE ELEMENTS OF THIS PAPER FIT TOGETHER

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

- The Model defines what determines OT security posture: the four foundational capabilities (visibility, segmentation, access control, and governance).
- The Method explains how these foundations are introduced safely, through a phased approach 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 in greenfield projects, adapting to brownfield constraints, and reinforcing progress through targeted quick wins.



02

Current State: The Manufacturing Security Challenge

Manufacturers today operate in an environment where operational technology has become both indispensable and increasingly exposed. As production systems integrate with cloud platforms, enterprise IT networks, vendors, and remote support, they inherit the same threat landscape as corporate environments, but with far higher stakes.

The numbers reflect this shift. In 2024, **31% of organizations reported six or more OT** intrusions, nearly triple the figure from the previous year (Fortinet, 2024). These incidents are not isolated: **55% resulted in productivity losses**, **43% led to critical data exposure, and 48% affected physical safety or process integrity** (Fortinet, 2024). In operational environments, this means cyber incidents translate directly into risk of downtime, quality deviations, and safety exposure, not just IT recovery efforts.

A major contributor is **limited visibility.** Only **5% of organizations have complete visibility into their OT environments, leaving** most plants operating with incomplete inventories, outdated diagrams, and undocumented integrations (Fortinet, 2024). Without a reliable baseline of assets and network traffic, security teams cannot detect anomalies, assess risk, or validate compliance. As a result, security and compliance decisions are often made without reliable evidence of how production systems actually behave.

Regulatory expectations are also intensifying. The **NIS2 Directive,** the Cybersecurity Act, and related **EU and industry resilience requirements** are expanding obligations across critical sectors, requiring consistent governance, documented controls, and clear accountability (ENISA, 2024). Non-compliance increasingly carries financial and legal consequences, including significant penalties and increased management accountability.

Most organizations also struggle with the level of expertise required to implement OT security correctly. Building visibility, segmentation, access governance, and monitoring typically demands a combination of process understanding, controls engineering knowledge, OT networking experience, and cybersecurity expertise. Few internal teams have all these capabilities, and relying on a single "OT specialist" is rarely enough. With **70% of companies citing a shortage of specialized OT cybersecurity talent** (KPMG, 2024), expertise has become a significant barrier to achieving a stable OT security posture. In practice, this slows implementation, increases reliance on ad-hoc decisions, and raises the risk of misconfigured controls during discovery and change.

Even segmentation, one of the most effective measures, remains inconsistently deployed. While adoption has grown, **40% of organizations still operate with flat or partially segmented OT networks**, leaving them vulnerable to lateral movement during an intrusion (Fortinet, 2024). This significantly increases the likelihood that a localized incident will escalate into a plant-wide disruption.

In combination, these trends create a high-pressure environment:

- OT systems are more connected and therefore more exposed.
- Most manufacturers lack full visibility of their environments.
- Regulations demand stronger and more consistent controls.
- Talent shortages slow implementation and response
- Supply-chain access multiplies operational risk.

Manufacturers need a structured approach that brings clarity, predictability, and operational alignment to OT security.

03

THE FOUR FOUNDATIONS OF THE OT-FIRST SECURITY MODEL

The Four Foundations of the OT-First Security Model

The OT-First Security Model is structured around four primary capabilities that shape the OT security posture of manufacturing environments. These foundations are not intended to represent every activity or control involved in OT cybersecurity, but they are the elements that most directly determine whether security efforts succeed or fail in practice.

Other supporting measures, tools, and services play an important role in a complete OT security program. However, without these four foundations in place, additional controls tend to increase complexity without materially reducing operational risk. Securing an industrial environment begins before technology is selected or controls are deployed. It begins with management intent. This model's effectiveness depends on explicit executive support: clear prioritization, balanced funding, and organizational mandate to apply security consistently, even when it competes with short-term operational efficiency. In practice, this support often needs to be built progressively as visibility increases and operational realities become clearer.

Without this support, OT security initiatives rarely fail due to technical issues. They fail because decisions are deferred, controls are inconsistently applied, or improvements are perpetually deprioritized in favor of running lean. The four foundations described below define what an effective OT security posture must include, but their impact is determined by how decisively leadership enables their implementation.

3.1

VISIBILITY: ESTABLISHING A FACTUAL BASELINE

Visibility is the first step because nothing else works without it. Nevertheless, in most plants, the “map” of the OT environment is decades out of date. Equipment has been added, replaced, bypassed, or modified without being documented; vendors have made changes on the fly; and network diagrams rarely reflect the current state of the shop floor.

Establishing visibility must be done carefully. Many environments cannot tolerate intrusive scanning or generic discovery tools. A single misstep can disrupt a running process. Moreover, although AI-based discovery tools are improving, they typically cannot unpack the thousands of logic instructions inside PLCs or reliably interpret how those instructions interact across a production line without expert validation.

A reliable visibility baseline usually includes:

- A complete view of operational assets, including unmanaged devices that have slipped into use over time.
- Communication paths between systems, not just the systems themselves.
- Critical dependencies that could cause cascading issues if altered.
- Any “shadow OT”, equipment, or connections that were installed without central oversight.

Proper measurement also reduces the risk of misinterpreting the environment. A surprising number of security failures stem from incorrect assumptions about how systems interact, or from trusting outdated diagrams that no longer reflect the plant’s reality.

It is crucial to treat visibility as an ongoing practice rather than a project milestone. Environments shift. Vendors connect remotely. Small changes add up. Without continuous visibility, blind spots return quickly.

3.2 SEGMENTATION: CONTAINING WHAT YOU CANNOT PREVENT

Segmentation takes the visibility baseline and turns it into control. When done well, it limits the spread of an intrusion and ensures that a problem in one area doesn’t ripple across an entire plant.

The industry knows its value: 60% of organizations now segment their OT networks (Fortinet, 2024), but implementation quality varies widely. Some plants have a segmented diagram on paper but operate a flat network in practice. Others rely on outdated configurations that no longer align with the environment's physical or logical layout.

Effective segmentation doesn’t try to firewall every sensor or device. Instead, it focuses on:

- Grouping systems based on how they actually function together.
- Restricting only the communication that genuinely needs restricting.
- Applying rules that align with production flow, not theoretical models.
- Ensuring operators and maintenance teams can work without constant friction.

When designed around production logic, segmentation strengthens security while preserving operational flexibility. When a change is needed, it can be isolated to one zone without risking unintended impact across the line, a practical benefit often overlooked in security discussions.

3.3

ACCESS CONTROL: MANAGING WHO TOUCHES WHAT... AND WHEN

Access control is where most breaches begin, and where many manufacturers still struggle. OT teams work with a mix of internal staff, external contractors, machine builders, and service partners, many of whom require remote access. Without structure, this becomes a sprawling patchwork of credentials, shared accounts, ad-hoc VPN rules, and USB-based updates. A mature OT access model distinguishes clearly between:

ONSITE ACCESS

Operators and technicians must be able to work efficiently, but access levels should match their responsibilities. This typically involves role-based permissions, credential hygiene, enforced least privilege, and physical access boundaries around critical equipment.

REMOTE ACCESS

Remote vendor access is unavoidable (and in many cases essential), but it must be tightly controlled. This means:

- Secure jump hosts (remote-access gateways).
- Logging of every session.
- Temporary or time-bound access where possible.
- Vendor access that is approved, monitored, and limited to the specific systems they support.
- Strong controls around removable media, which remains a common infection vector.

When remote access is governed correctly, plants gain the best of both worlds: expertise when needed and security when not.

3.4

GOVERNANCE: KEEPING SECURITY CONSISTENT OVER TIME

Governance is where management intent becomes operational reality. Many organizations have capable engineers and well-chosen tools, yet still struggle to sustain OT security because priorities are unclear, mandates are weak, or security competes unsuccessfully with production pressure.

Effective OT governance requires explicit executive ownership. It depends on leadership making deliberate decisions about acceptable risk, funding levels, and the authority of OT security teams to intervene when controls are bypassed or shortcuts emerge. Without this backing, policies exist on paper, but practices diverge across sites, vendors, and projects.

Strong OT governance creates a single source of truth:

- Policies and expectations tied to regulations such as NIS2, IEC 62443, and the Cybersecurity Act (ENISA, 2024).
- A clear division of responsibilities across IT, OT, and production teams.
- Processes for approving changes, updating configurations, and handling incidents.
- Requirements that vendors and partners must follow to connect to the environment.
- A rhythm of continuous improvement as systems, teams, and technologies evolve.

Governance also determines whether security is applied proactively or too late. When security expectations are embedded into new designs, projects, and vendor engagements ("security at the gate"), controls are easier to implement and far less disruptive. When security is added after systems are already live, it is costlier, harder to enforce, and more likely to be scaled back under operational pressure.

Finally, governance extends beyond processes and documentation. Security awareness across the organization, from engineers to operators to contractors, is essential. A significant share of incidents originates from human behavior: phishing, credential misuse, or unsafe workarounds. Executive support for awareness programs, training, and realistic controls is therefore not optional; it is a core element of sustaining any OT security posture.

These four foundations are essential, but implementing them requires facing the realities that most manufacturers only discover after they begin. Some of these challenges are predictable; others remain invisible until visibility work starts.

Hidden Realities of OT Security

Most OT security discussions look straightforward on paper: map the environment, segment the network, control access, and establish governance. However, anyone who has worked inside a real plant knows that the gap between theory and practice is vast. The realities below are rarely addressed in traditional security models, yet they determine the success (or failure) of every OT security program.

These insights come directly from what AG Solution teams encounter in daily industrial projects across Europe and the U.S. They reflect the practical constraints of real OT environments, not idealized frameworks.

4.1

COMPLEXITY AND LEGACY CONSTRAINTS

4.1.1

LEGACY LOGIC IS DEEPLY COMPLEX AND OFTEN UNREADABLE

Many PLCs have been running the same logic for years, sometimes decades. Some were programmed by integrators who are no longer in business. Others contain thousands of ladder instructions woven into sequences that evolved as equipment was expanded or modified.

There is no automated tool that can reliably interpret every dependency or predict how a change will behave once deployed across most brownfield OT environments. AI models can support anomaly detection, but they cannot replace human understanding of process logic, safety interlocks, or timing constraints.

As a result, claims of fully automated logic assessment rarely hold up in complex, real-world OT environments without extensive human validation.

4.1.2 BROWNFIELD PLANTS HIDE "SHADOW OT" EVERYWHERE

In brownfield plants (most manufacturing sites today), OT evolves organically:

- A contractor installs a switch to solve a temporary need.
- A machine builder adds a remote-access module for maintenance.
- A line supervisor connects a device "just for diagnostics."
- Equipment is replaced without updating diagrams.

These additions accumulate quietly over the years. The result is a patchwork of devices and connections that do not appear in any official documentation.

"Shadow OT" is not an exception; it is the norm, and it often becomes visible only when security work begins.

4.1.3 AI CAN ASSIST, BUT IT CANNOT REPLACE EXPERIENCE

AI-driven anomaly detection has value, especially as environments grow. However, AI cannot infer process context, understand the consequences of an instruction change, or recognize when a "normal" pattern is tied to a specific product run or seasonal production cycle.

AI is a tool, not a strategy. Human judgment, process understanding, and knowledge of the plant's history remain essential.

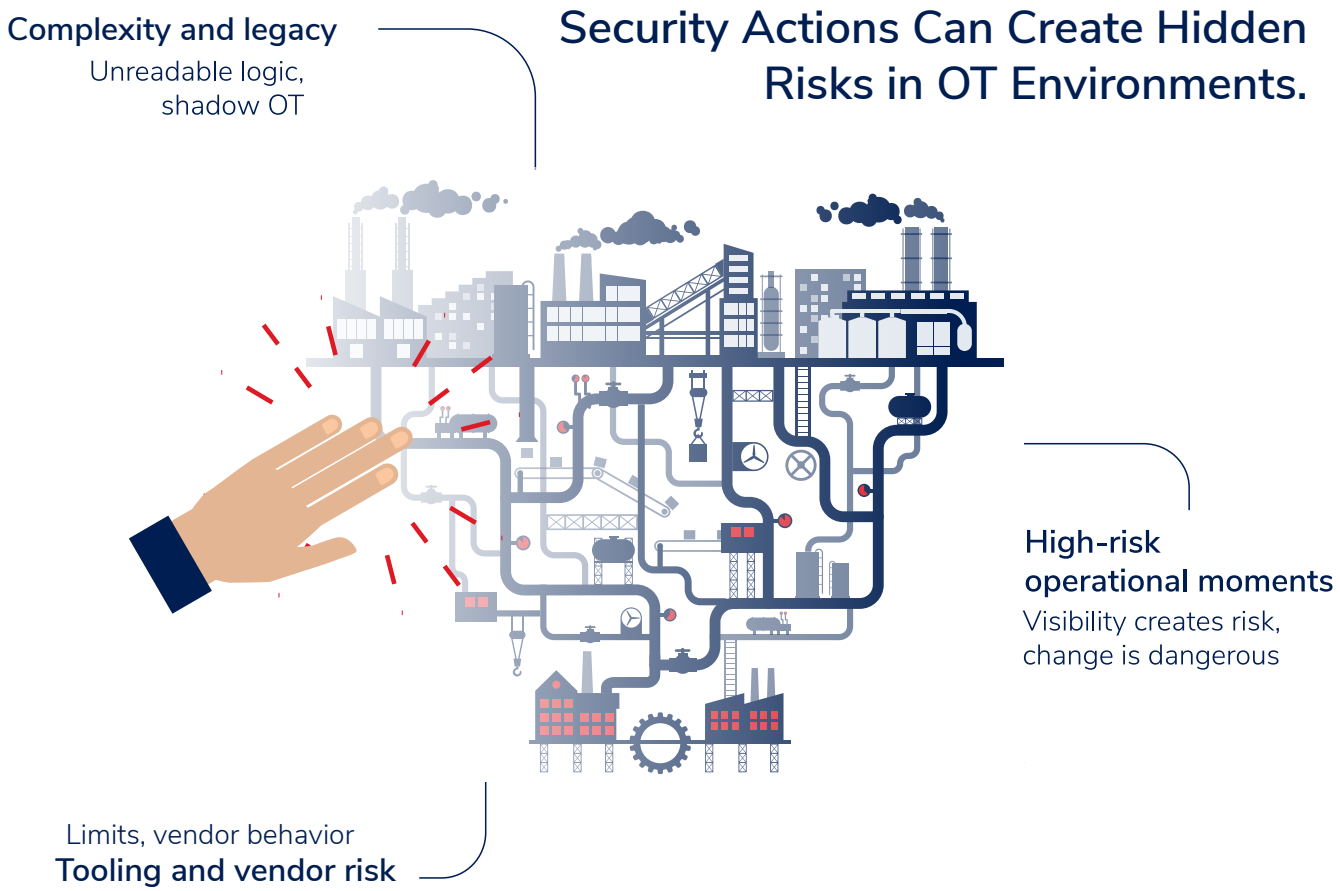
These realities explain why OT security cannot be approached with generic IT methods or automated tooling alone. Manufacturers need a model that acknowledges the constraints of real operations and builds control step by step.

4.1.4

EXPERTISE REQUIREMENTS ARE HIGHER THAN MOST ORGANIZATIONS EXPECT

Implementing an OT security model requires more than one skilled engineer. It demands a mix of disciplines: automation engineering, controls, networking, cybersecurity, and operational experience. Many organizations underestimate this and attempt to centralize responsibility in a single role or small team.

In practice, this increases the risk of sequencing mistakes, misconfigured controls, and disruptions during discovery or segmentation. The industry continues to face a lack of specialized OT security professionals, making it difficult for manufacturers to staff these programs internally (KPMG, 2024). This is one of the reasons many initiatives stall or progress more slowly than planned.



4.2 TOOLING AND VENDOR-DRIVEN RISK

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

Vendors frequently advertise “plug-and-play OT visibility” or “automated microsegmentation.” In real plants, tooling must adapt to legacy networks, unsupported protocols, and equipment that cannot tolerate intrusive monitoring. Specific discovery tools introduce traffic bursts that older devices misinterpret. Some IDS/IPS solutions struggle with industrial protocols or generate false positives that overwhelm teams. Other solutions require architectural changes that plants are not ready for.

The right tools matter, but in OT environments, they are effective only when applied with process understanding and careful sequencing.

Many of these specialized tools are expensive and designed for structured assessment work. Most factories cannot justify purchasing them for internal use, especially for occasional or one-off discovery efforts. This is why organizations typically depend on external expertise to perform deep visibility assessments safely and at scale.

4.2.2 VENDOR BEHAVIOR SHAPES THE SECURITY POSTURE MORE THAN MOST REALIZE

Manufacturers often depend on machine builders, automation partners, or maintenance providers who connect remotely or onsite. Each partner brings its own methods, software versions, and expectations. Some follow strong security practices; others rely on outdated or inconsistent approaches.

This creates wide variations across plants, even within the same company. If clear policies do not govern vendors, they effectively define the security model themselves, sometimes unintentionally.

4.3 HIGH-RISK OPERATIONAL MOMENTS

4.3.1 VISIBILITY CREATES RISK BEFORE IT CREATES CONTROL

The industry often positions visibility as a low-risk first step. In reality, gaining visibility means touching a network whose behavior is not fully understood. A poorly chosen discovery method, a misconfigured switch port, or a device that reacts unpredictably under load can interrupt a running process.

Plants cannot “pause production for discovery.” Every action must be tested, timed, and executed with the understanding that continuity comes first. As a result, visibility in OT requires a deliberate, low-impact approach rather than the automated scanning techniques standard in IT environments.

4.3.2 CHANGE IS THE MOST DANGEROUS MOMENT IN OT

Minor configuration changes can produce operational consequences that were never documented. Updating a switch, replacing a PLC, modifying a firewall rule, or introducing a new remote-access path can create issues that only reveal themselves under load or during specific production states.

This is why OT teams often hesitate to modify a working environment, even if security improvements are needed.

Security must respect the operational reality that **“stable” and “safe” are not the same thing, but stability is non-negotiable.**

4.3.3

DEVICES THOUGHT TO BE ISOLATED OFTEN ARE NOT

During discovery, it is common to find equipment assumed to be isolated but still reachable through undocumented links, leftover connections, or vendor-installed pathways. These “unisolated” assets create silent high-risk points because the organization believes they are protected when they are not. They often appear only after proper measurement tools are deployed or after traffic is observed over several days or weeks.

In one of our clients’ recent brownfield assessments, a packaging line PLC that was assumed to be fully isolated was found to be reachable via an old vendor VPN appliance left online after commissioning. The connection was undocumented, unknown to plant staff, and effectively bypassed existing perimeter controls.

05

BUILDING THE OT-FIRST SECURITY MODEL

Building the OT-First Security Model

(METHODOLOGY & APPROACH)

Turning the four foundations into a working security model requires a method that respects how industrial environments actually operate. Plants cannot absorb large, disruptive changes. They cannot risk untested assumptions. Moreover, they cannot rely on tools alone to interpret decades of technical decisions embedded in equipment, logic, and network architecture.

For this reason, the OT-First Security Model is built around a phased, controlled approach. It moves from understanding to action in a sequence designed to limit operational risk, uncover hidden conditions, and enable teams to make decisions based on facts 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 deliberately avoids automated tooling and focuses on establishing a factual baseline through observation, validation, and controlled verification. The objective is not depth, but safety: creating an initial picture that teams can trust before introducing any form of active discovery.

- Reviewing existing diagrams and comparing them with reality.
- Identifying logical points where safe discovery can begin.
- Using non-intrusive methods to observe traffic and relationships.
- Documenting what is known, what is suspected, and what is clearly missing.

This phase often reveals previously unrecognized gaps, such as devices added over time, undocumented vendor changes, or systems running obsolete firmware. The goal is not to achieve perfect visibility in one step, but to create a reliable starting point for everything that comes next.

5.2

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

Phase 2 builds on the baseline by introducing targeted tooling to deepen insight. Unlike IT environments, where broad automated scans are routine, OT systems require precision and restraint. Tools are selected, configured, and deployed incrementally to expand visibility without introducing instability or unintended process behavior.

This phase typically enables:

- Detection of previously unknown assets.
- Identification of communication patterns across segments and subnets.
- Mapping of vulnerabilities tied to firmware or protocol versions.
- Visibility into how systems behave under normal load.

The key here is control. The objective is to expand understanding without interrupting production or triggering unexpected behavior on older devices.

5.3

PHASE 3: PREPARE THE ENVIRONMENT FOR CONTINUOUS MONITORING

This phase begins only once the environment is sufficiently understood and stabilized. At this stage, continuous monitoring becomes viable. Sensors and monitoring platforms can observe changes over time, providing early warning without interfering with operations. This marks the transition from episodic assessment to sustained operational security.

Continuous monitoring at this phase allows teams to:

- Detect new devices or unexpected communication flows.
- Identify deviations from baseline behavior.
- Track vulnerabilities over time.
- Receive early warnings when standard traffic patterns begin to drift.

This is where operational security shifts from reactive to proactive.

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, robust redundancy, and rapid failover options. OT does not. In manufacturing, even a single incorrect change can affect safety, throughput, or quality.

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

- Operational continuity
- Process stability
- Respect for legacy equipment
- Low-impact change sequencing
- Vendor coordination
- Regulatory alignment

This is also why the model avoids premature automation. AI- and rules-based engines are valuable once the environment is understood and stabilized, but they cannot replace the judgment required during the early phases of discovery and segmentation.

5.5

DEFINING WHAT "GOOD" LOOKS LIKE

A key advantage of this methodology is the clarity it provides. Once the visibility–segmentation–access–governance sequence is established, teams can define what a "healthy" OT security posture truly means for their environment.

In practice, a healthy OT security posture is characterized by:

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

This becomes the foundation for every audit, every compliance requirement, and every investment decision. With the methodology defined, the next challenge is putting it into practice. 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 wins are essential for securing organizational support.

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. The OT-First Security Model, therefore, defines four implementation principles (pilot, greenfield, brownfield, and quick wins) that reflect how security can be introduced progressively without destabilizing production. These principles are integral to the model, ensuring that improvements are sequenced according to operational reality rather than theoretical maturity models.

The Model uses a phased implementation approach that aligns security improvements with operational stability and business value. The sequence typically begins with a controlled pilot, extends to greenfield projects, and eventually adapts to brownfield plants, where most challenges reside. Throughout the journey, targeted quick wins help maintain momentum and demonstrate practical impact early.

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

While every environment differs, organizations that apply the OT-First Security Model in a structured way tend to observe a similar set of early shifts:

- Greater clarity on what is connected, communicating, and exposed in the OT environment
- Reduced uncertainty during changes, as dependencies and communication paths become visible and documented
- Fewer high-risk access paths, particularly around unmanaged remote access and legacy connections
- Clearer ownership and decision-making across IT, OT, and operations when security-related changes are required
- Increased confidence to proceed with pilots, upgrades, or segmentation steps without destabilizing production

These outcomes do not represent the completion of an OT security program. They indicate that the organization has established a reliable foundation from which security improvements can be introduced safely and sustained over time.

6.1

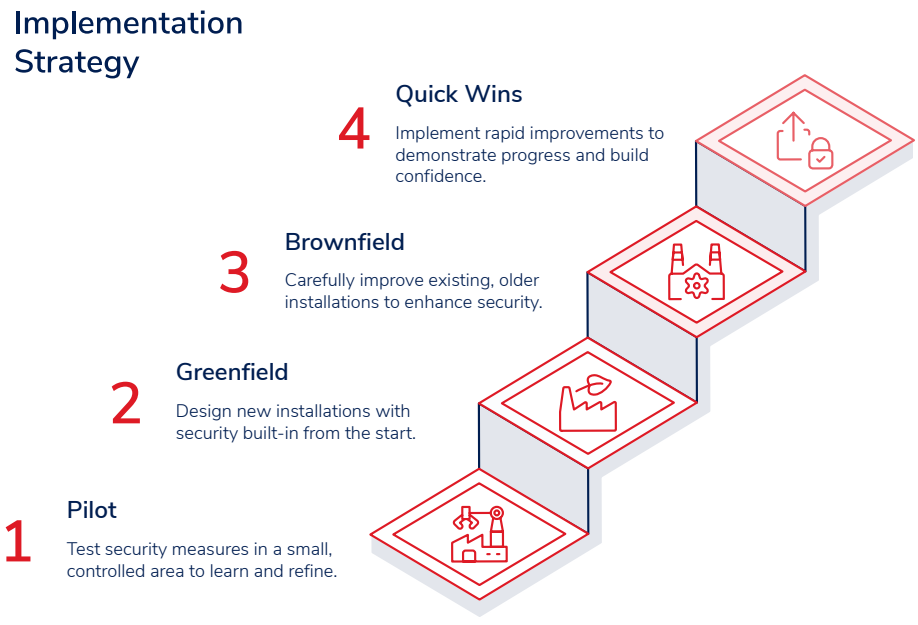
START WITH A PILOT: CONTAINED, CONTROLLED,AND MEASURABLE

A pilot provides a low-risk learning environment that allows teams to validate the OT-First Security Model in practice. It proves value before scaling, exposes hidden dependencies early, and reduces uncertainty for larger rollouts.
The first implementation should never target the most complex or critical area of a plant. A pilot needs a defined boundary and enough diversity to reveal real conditions without putting core production at risk.

Strong pilot candidates often include:

- A standalone production line
- A support subsystem (e.g., utilities, packaging, wastewater)
- An area with known visibility gaps but manageable risk
- A location where vendor involvement is limited or stable

A pilot validates more than technical controls. It tests the methodology in practice: how discovery behaves, how segmentation impacts communication, how access control changes daily routines, and how governance works across teams. It also uncovers hidden variables that no diagram or tool can anticipate, such as unofficial connections, undocumented logic, vendor-specific behaviors, or dependencies that only become evident under load.
A well-run pilot becomes the reference model for every subsequent rollout.



6.2

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

In greenfield projects, applying the OT-First model early prevents technical debt. Security controls are cheaper, more straightforward, and more effective to implement before legacy constraints appear, reducing future retrofit costs and compliance risk.

Greenfield sites offer a rare advantage: security can be embedded before vendors, integrators, and equipment variations introduce complexity. It is an opportunity to apply the OT-First model from day one, aligning architecture, segmentation, access control, and governance with the new plant's long-term goals.

Key benefits include:

- Clean network design without legacy limitations
- Segmentation aligned with the intended production flow
- Clear access rules established before vendors begin work
- Well-documented environments that remain consistent across teams
- Faster alignment with NIS2, IEC 62443, and internal governance

Greenfield environments also help refine internal templates, standards, and playbooks—creating clarity that can later be adapted to existing sites.

6.3

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

Brownfield environments typically carry the highest exposure and the least visibility. Applying the OT-First model here delivers the greatest reduction in operational and cyber risk, while sequencing changes to avoid production disruption. Most OT security challenges surface in brownfield environments. These plants contain decades of operational history: equipment upgrades, vendor interventions, last-minute fixes, and undocumented changes. No two areas behave exactly alike, even within the same facility.

Brownfield rollouts require:

- A slower, observation-first approach
- Discovery techniques tuned to older equipment
- Realistic expectations about hidden assets and shadow networks
- Close coordination with OT teams who know the environment's personality
- A change management rhythm that respects production and maintenance windows

Brownfield work often reveals:

- Devices that were forgotten or repurposed
- Networks that evolved without design
- Controllers running outdated firmware tied to critical sequences
- Remote access paths created years ago and never removed
- Integrator-specific practices that vary across lines or plants

These environments cannot be reshaped overnight. The strategy must prioritize what delivers the greatest risk reduction with the least operational impact, one controlled step at a time.

6.4

DEMONSTRATE QUICK WINS: PROVING VALUE EARLY AND OFTEN

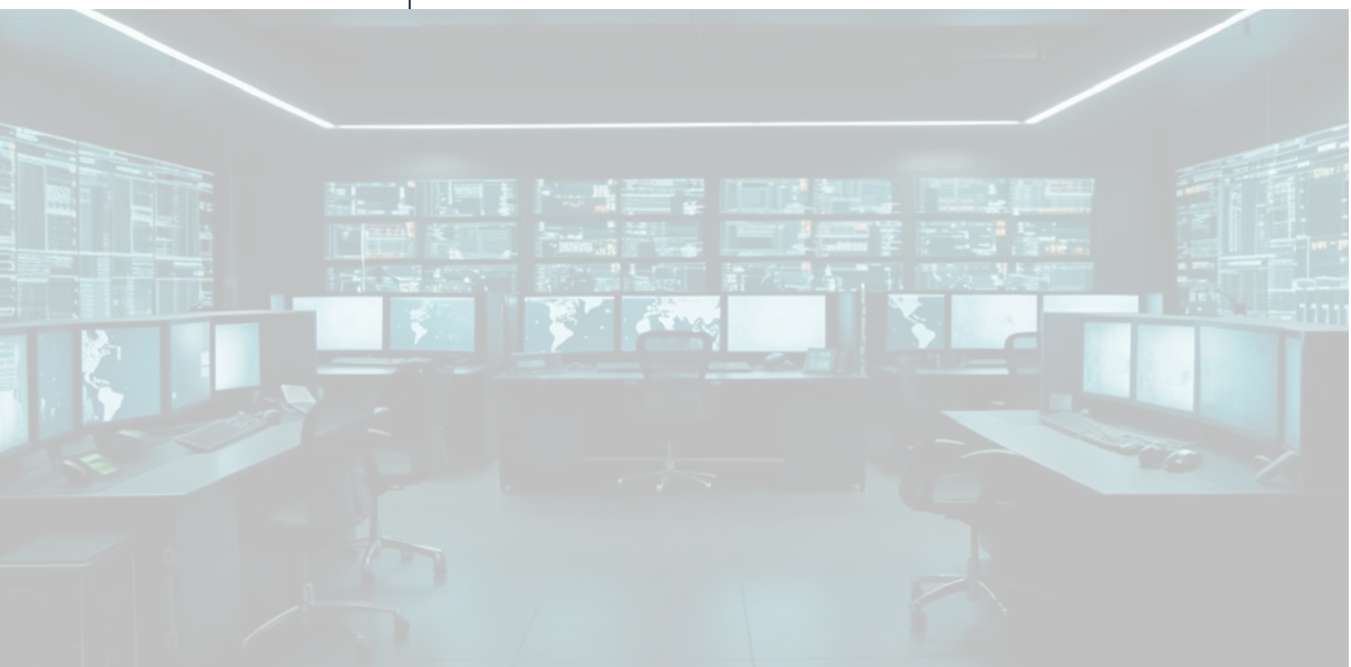
Quick wins demonstrate impact in weeks rather than years. They build trust with OT staff, justify investment, and demonstrate that security can improve operations rather than complicate them. These wins do not replace long-term milestones, but they create the momentum essential for large-scale change.

Typical examples include:

- Cleaning up unused remote access accounts
- Restricting high-risk communication paths
- Documenting previously unknown assets
- Fixing outdated firmware on non-critical equipment
- Applying segmentation rules to a single zone with measurable results
- Standardizing user roles for internal teams and vendors

Quick wins reinforce confidence that the methodology works. They show progress while larger, more complex phases move forward in the background.

With the implementation strategy defined, the next step is to illustrate how the OT-First approach delivers measurable results in practice. Real-world examples help translate methodology into outcomes, showing how visibility, segmentation, access control, and governance converge 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 based on multiple industrial projects. It reflects common conditions encountered in brownfield manufacturing environments and demonstrates how the OT-First Security Model is applied in practice.

CHALLENGE

A large, multi-site food manufacturing organization engaged AG Solution to improve the security of its factory systems. Many of the plants operated under strict production and quality constraints, relied on legacy equipment, and carried a significant technical backlog accumulated over years of incremental change. Network documentation was incomplete, and no one could reliably explain which systems needed to communicate with which, or why.
Applying traditional, rule-by-rule firewalling or intrusive discovery was considered too risky. The organization's primary concern was avoiding disruption to production while regaining control.

SOLUTION

The engagement began by addressing obvious exposure first. Known backdoors and unmanaged remote access paths were closed, reducing immediate risk without changing core production behavior. From there, visibility was introduced carefully, using controlled firewall-based observation to monitor actual traffic flows rather than assumptions based on outdated diagrams.

Observed traffic was captured and consolidated into structured overviews using targeted scripts. This allowed the teams to classify and understand the vast majority of communication flows based on function and process context. Approximately ninety-nine percent of observed traffic could be explained, documented, and justified without requiring changes on the shop floor. For the remaining cases, local OT teams were involved to validate purpose and necessity before any decisions were made.

RESULTS

Once this baseline was established, firewall rulesets were progressively tightened to permit only verified communication paths. This significantly reduced exposure while preserving operational continuity. Remote access was restructured using monitored, time-bound VPN access, providing vendors and specialists with the access they needed while restoring accountability and control.

Beyond security improvement, several plants reported operational benefits over time. Increased visibility and clearer governance reduced trial-and-error during changes, improved preparation for maintenance and upgrades, and led to more stable operations. In multiple sites, teams reported improved operational stability and fewer trial-and-error iterations during changes, as a by-product of better control, documentation, and change discipline.

This example illustrates how the OT-First Security Model enables organizations to break down complex, high-risk environments into manageable steps, reducing exposure, improving stability, and building confidence without disrupting production.

08

CONCLUSION & NEXT STEPS

Conclusion & Next Steps

Manufacturers today face a security landscape defined by growing exposure, tighter regulation, and complex operational realities. Legacy infrastructure, dispersed vendor activity, undocumented changes, and constrained resources make it difficult to build resilience using generic IT-driven models. The OT-First Security Model provides a structured way through that complexity, starting with visibility, moving through segmentation and access control, and stabilizing the environment with governance that aligns with regulatory expectations.

The strength of this model is not in any single component. It is in the sequence.Visibility without segmentation leaves organizations aware of risk but unable to contain it. Segmentation without access control still allows threat actors or vendors to move freely. Governance without monitoring quickly becomes outdated as equipment and processes evolve.

By applying the foundations in a controlled, incremental manner, organizations can strengthen security without disrupting operations, a balance essential in industrial environments.
The methodology described in this whitepaper is based on real conditions found in manufacturing: the limits of legacy equipment, the difficulty of predicting PLC behavior, the inevitability of "shadow OT," and the operational risk associated with even small changes. These realities underscore the need for a deliberate, experience-driven approach rather than a tool-centric or compliance-only mindset.

For most organizations, the next step is not a large, sweeping program. It is choosing a place to begin: a pilot area, a greenfield opportunity, or a brownfield line where visibility gaps or access concerns are already known. From there, the model scales naturally (site by site, zone by zone), building momentum through quick wins and measurable improvements.

The OT-First Security Model is not a theoretical framework; it reflects how security is introduced, challenged, and sustained in real industrial environments. It is a practical way to build resilience across industrial operations. With a structured approach, clear sequencing, and governance that grows alongside regulatory demands, manufacturers can reduce exposure, protect continuity, and support long-term operational excellence.

AG Solution continues to help organizations apply this model in real environments, balancing security with production, and supporting teams through every phase of their OT security evolution.

About AG Solution

AG Solution is a consultancy and engineering partner specializing in **OT-first modernization and security of industrial operations**. With teams across Europe and the United States, we help manufacturers strengthen their operations through **OT-first security and modernization of industrial environments,** combining structured methodologies, practical expertise, and deep knowledge of production systems.

We apply the OT-First Security Model described in this whitepaper through structured visibility assessments, segmentation programs, controlled access design, and vendor-aligned governance frameworks, supporting both single-plant initiatives and multi-site industrial operations.

Our work spans **OT-first cybersecurity and industrial modernization**, including automation, manufacturing execution systems, data and AI initiatives, and transformation programs across pharmaceuticals, food and beverage, chemicals, energy, and other process and batch-driven industries. We combine operational understanding with technical depth, helping organizations protect continuity, meet regulatory expectations, and modernize their plants without disrupting production. Whether supporting a new greenfield facility, implementing an OT-first visibility and segmentation program, or guiding complex brownfield environments, AG Solution brings a hands-on, integrated approach shaped by years of field experience.

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