

Protect what powers progress

6 steps to building secure and
resilient industrial systems



Content

5 The new cyber battleground: Visibility, velocity and vulnerability

6 Regulations and standards: Turning obligation into opportunity

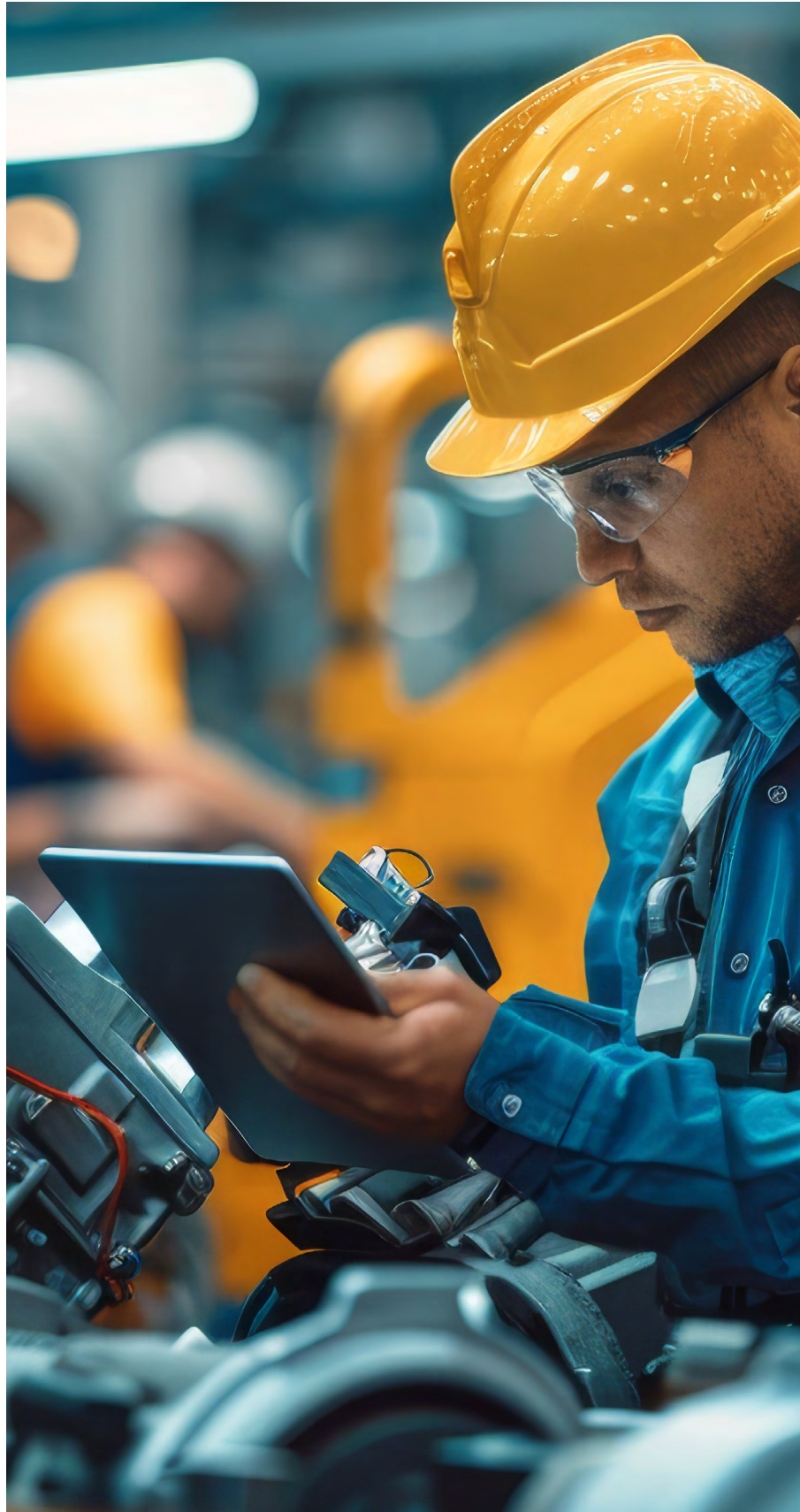
7 NTT DATA's 6-step roadmap to OT security and resilience

11 An eye on the future — The trends shaping OT security

Operational technology (OT) keeps the world running, powering grids, factories, transport and utilities. These systems sit at the intersection of the physical and digital worlds, and their reliability now increasingly depends on cyber resilience. Protecting what powers progress isn't just about defending — it's about the confidence to innovate and grow.

But as IT and OT environments converge, attackers seek to exploit these connections, disrupting production, safety and supply chains. Indeed, more than half of OT breaches begin in IT systems according to research from the SANS Institute, with the consequences extending far beyond downtime. They also affect people, economies and trust.

OT security is the bedrock of operational continuity. Organizations that embed cyber resilience into their operational DNA — not just as protection, but as a principle — are the ones best positioned to prevent costly disruption and turn resilience into a platform for growth and innovation.



The new cyber battleground: Visibility, velocity and vulnerability

Interconnected systems are essential to modern operations. Technologies such as 5G, IoT, cloud and AI bring many benefits, such as intelligence, efficiency, speed and scale. However, they also create new attack surfaces and vulnerabilities. Legacy control systems that may have perhaps been isolated can once again be exposed through the internet or private connectivity for remote maintenance, supplier access and cloud integration.

Today, attackers aren't just organized — they're augmented. AI is now a core weapon in cybercriminal arsenals, enabling stealthier, faster and more adaptive attacks. Industrial environments often rely on legacy hardware that's difficult to patch, creating systemic vulnerabilities across supply chains. Threat actors exploit these gaps — targeting IoT endpoints, outdated systems and third-party integrations.

They also deploy AI-driven phishing and malware tactics that bypass traditional defenses and deceive even cautious users. The result is a threat landscape that's smarter, faster and harder to detect.

A persistent cybersecurity skills gap only compounds these issues. The same SANS research found that while **60% of industrial organizations experienced an incident last year, only 10% have a dedicated OT security team**¹. This imbalance continues to leave critical operations exposed.

Resilience ultimately depends on understanding what's connected, who can access it and how systems behave in real time. So, the ability to see and act quickly is the most valuable control of all.



3 primary attack scenarios

Understanding how attackers target OT is essential for protecting your systems.
Most incidents fall into one of three high-impact categories:

1

Ransomware attacks

Attackers paralyze critical systems with ransomware to extort payment from victims. These disruptions, or even complete production shutdowns, can lead to delivery delays, contractual penalties, accidents or environmental damage if control systems suddenly fail.

2

Theft of intellectual property

Attackers infiltrate infrastructures to steal intellectual property, such as design data or production processes. This information can be used for extortion or sold to competitors, resulting in product piracy and the loss of competitive advantage.

3

Manipulation of OT systems

Attackers tamper with OT systems, causing products to no longer meet quality standards. This can lead to high costs due to defective batches and recalls, as well as consumer protection lawsuits and claims for damages. Additionally, these attacks can introduce risks to human safety and the environment.

¹ 2025 ICS/OT Cybersecurity Budget: Spending Trends, Challenges, and the Future

Regulations and standards: Turning obligation into opportunity

Governments and regulators around the world are uniting around a common goal to ensure stronger resilience across cyber-physical systems.

In Europe, for example, the NIS2 Directive and Cyber Resilience Act extend accountability beyond critical infrastructure operators to suppliers and midsize manufacturers. The new Machinery Regulation also embeds security directly into industrial design.

Read our latest blog: **The EU's Cyber Resilience Act: What it means for manufacturers**

In the United States, CISA's Cross-Sector Cyber Performance Goals and the TSA's pipeline and rail directives have introduced measurable security baselines for industrial sectors. NIST's Cybersecurity Framework 2.0 has expanded guidance for OT environments, integrating safety, risk and continuity management.

And across the Asia-Pacific region, Japan's METI framework, Singapore's Cybersecurity Act and Australia's Critical Infrastructure are just a few examples of reforms tightening controls around industrial and supply chain systems.

Global standards such as ISA/IEC 62443 and ISO/IEC 27001 now work together to form a shared foundation for protecting operational environments. IEC 62443 defines

maturity levels and technical requirements for OT, while ISO 27001 establishes the broader governance structure for information security.

All this highlights how compliance needs to be more than a legal safeguard. It must be a design principle for how organizations need to operate and compete. The visibility and documentation that frameworks demand provide organizations with a clearer view of their assets, interdependencies and vulnerabilities. That same insight also reveals inefficiencies, outdated equipment, unsegmented networks and process bottlenecks that hold operations back. By aligning compliance programs with broader digital transformation goals, you can strengthen security while improving reliability, performance and uptime.

Additionally, when governance, safety and IT teams work together to meet evolving standards, compliance becomes a mechanism for unity and continuous improvement. Certifications such as IEC 62443 and ISO 27001 help you demonstrate due diligence, but they also signal reliability and help you build trust with your partners, regulators and investors. The reporting and analytics developed for compliance feeds operational intelligence, helping you refine responses and plan for future innovation.

When regulation becomes a design principle, resilience, efficiency and trust follow — fueling long-term competitiveness.

NTT DATA's 6-step roadmap to OT security and resilience

NTT DATA helps organizations protect the systems that power production and progress. Our teams work across industries where uptime, safety and reliability are essential. We focus on embedding cyber resilience into daily operations from the beginning. Every engagement aligns with recognized

frameworks, assessing maturity, closing gaps and designing programs that evolve alongside new technology and regulation. At the center of our method is a proven 6-step roadmap that helps you move from uncertainty to clarity, and from reactive defense to proactive resilience.



6 steps to secure and resilient OT





Establish visibility: You can only protect what you know exists

Resilience always begins with visibility. This is because organizations often underestimate the extent to which their OT environment remains unseen. We help you identify every asset, connection and data flow across all your plants, suppliers and remote access channels. Having this complete view helps expose weaknesses and dependencies long before attackers can discover them.

- Create a comprehensive inventory of all OT assets, including hardware, software and network components
- Map communication paths and data flows between systems to identify dependencies and potential attack vectors
- Use automated tools such as asset discovery and network monitoring solutions to detect unknown or unauthorized devices
- Classify assets based on their criticality to production and business operations



Identify and assess risks: You can't fix what you haven't evaluated

Visibility without context is like light without focus. It reveals everything yet clarifies nothing. Our methodology evaluates each system based on its role in safety, production and compliance. Following this, assessments link vulnerabilities to business impact, helping you to focus on the most critical areas for your organization. The result is a clear, prioritized view of your risk that supports informed decision-making.

- Conduct a threat and vulnerability analysis to identify weak points in systems, networks and processes
- Evaluate the likelihood and impact of different attack scenarios, such as ransomware, data theft or sabotage
- Consider external and internal threats, including human error, insider threats and supply chain risks
- Document and categorize risks in a structured risk register to support decision-making and compliance



Develop an OT Security Strategy: Action without direction is just guesswork

Effective OT security requires coordination across multiple disciplines, including engineering, IT and leadership. As part of this process, we design strategies that integrate governance, risk and operational planning. These blueprints define roles, responsibilities and escalation paths that support both compliance and continuity. The result is a plan that fits exactly how your organization actually runs. One that is practical, measurable and sustainable.

- Define clear security objectives and priorities based on the risk assessment
- Establish roles and responsibilities, including the designation of OT security officers and cross-functional teams
- Develop policies and guidelines for the secure operation, maintenance and updates of OT systems
- Plan for the implementation of technical and organizational measures such as network segmentation, access controls and employee training
- Assess compliance with relevant standards and regulations, such as IEC 62443, ISO/IEC 27001 and NIS2, and take the necessary steps to close any gaps



Mitigate top risks: Focus effort where the risk is greatest to the business

Once priorities are in place, it's then about action. We help you implement the right controls where they deliver the most value to your organization, be it segmentation, secure remote access, multifactor authentication, system hardening and vendor governance. These actions help reduce your attack surface, contain potential breaches and build greater confidence among multiple stakeholders.

- Segment networks to limit the spread of malware and unauthorized access across systems
- Implement secure remote access solutions with strong authentication and encryption
- Patch known vulnerabilities in OT systems and components, where possible, without disrupting operations
- Restrict user privileges and enforce the principle of least privilege to minimize potential damage from compromised accounts
- Train employees to recognize phishing attempts and follow security best practices



Evolve continuously: Resilience is built on continuous improvement

Industrial security is an ongoing process and, unfortunately, is never complete. To help, we integrate monitoring, training and feedback loops into daily operations, so your defenses continuously evolve as systems and technologies change. By developing internal expertise, you can sustain and grow your security maturity independently. We often speak of a cybersecurity culture — but it's continuous improvement that makes it real.

- Establish a cybersecurity management system that defines responsibilities, processes and performance indicators
- Integrate security into the lifecycle of OT systems, from procurement and commissioning to maintenance and decommissioning
- Regularly test and update security measures, including backup and recovery procedures
- Conduct recurring training and awareness programs for all employees involved in OT operations
- Collaborate with partners and suppliers to secure the entire value chain



Respond fast: The faster you react, the less you stand to lose

The reality is that even the strongest defenses will face incidents. But it's the speed and coordination of the response that define the outcome. We integrate OT networks with security operations centers (SOCs) to enable early detection and containment. Whether it's incident rehearsals and scenario testing, we prepare you and your team to recover operations quickly and strengthen resilience no matter what's thrown at you.

- Implement monitoring solutions that are tailored to OT environments and can detect anomalies in network traffic and system behavior
- Establish a SOC or integrate OT monitoring into an existing SOC for continuous surveillance
- Define clear incident response processes, including roles, responsibilities and escalation paths
- Conduct regular drills and simulations to test the effectiveness of response plans and train personnel
- Document incidents and lessons learned to continuously improve detection and response strategies



An eye on the future — The trends shaping OT security

As industrial innovation accelerates, so does the complexity of securing it. Technologies like 5G and cloud are transforming operations—enabling real-time connectivity between field assets and data centers. But with that flexibility comes heightened exposure, demanding stronger identity-based access controls and end-to-end encryption.

AI is a double-edged sword: it empowers defenders with faster detection and automated response, yet also arms attackers with scalable phishing, deepfakes and evasive malware.

Virtualization and digital twins offer unprecedented visibility into complex systems—but these virtual environments must be secured with the same rigor as their physical counterparts.

In short, every leap forward in capability brings a corresponding leap in cyber risk. Resilience must evolve in lockstep.

Ultimately, the lesson to be learned here is that these technologies must be viewed as part of a single, evolving risk ecosystem, rather than siloed entities. The opportunity for security teams is to elevate cybersecurity as a core business capability — one that safeguards operations and fosters innovation, market growth and customer confidence.

Strategic protection delivers what money can't buy — confidence. Confidence to innovate boldly, expand securely, and modernize without disruption. Resilience is built on that confidence — earned through preparation, clarity and consistency. This is the foundation for industrial progress.

Partnering with NTT DATA

NTT DATA combines cybersecurity expertise with engineering and industry insight. We work as partners, helping you strengthen resilience through collaboration, transparency and measurable outcomes.

Our services cover every stage of maturity, from assessment to architecture, implementation and managed detection. Whether you're trying to secure legacy control systems or build new digital operations, we help you create protection that endures.

The world depends on industrial systems to function. Securing them ensures that progress continues with confidence and the ability to meet these challenges head-on through meticulous preparation.

Client success story: Bayer AG protects its critical infrastructure from cyberattacks and build cyber resilience

Bayer AG, a global leader in chemicals and pharmaceuticals, sought greater visibility across its complex OT landscape — spanning 15 major pharmaceutical sites worldwide. To boost asset availability and safeguard critical infrastructure from cyberthreats, Bayer selected Nozomi Networks' Guardian appliances and central management console. NTT DATA was chosen to design, implement, and deploy the solution globally.

With the new solutions in place, Bayer AG can optimize network security with precision. Real-time monitoring of network communication and behavior enables rapid detection of anomalies and potential threats — allowing swift intervention before operations are impacted. Meanwhile, advanced threat intelligence identifies both cyberattacks and production risks early, ensuring uninterrupted availability across global pharmaceutical sites. For a sector where uptime is critical, this level of resilience is essential.

Would you like to learn more about how to secure your OT environment?

We're here to help. Contact us.



Let's work together to make your production secure, resilient and future-ready.

Visit nttdata.com to learn more.

NTT DATA is a \$30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.



