TANIUM

5 questions manufacturing companies should be asking about their technology





By Tim Morris, Chief Security Advisor, Americas, at Tanium

We hear a lot about the convergence of IT and OT (operational technology) these days. Technology has long been a key part of manufacturing, but factory automation and industrial control systems (ICS) evolved on a separate path from information technology.

Manufacturing and corporate technology domains have historically run independently. Different skill sets and different types of technology create a natural barrier between the two domains.

Fear of operations disruption led to moat-and-drawbridge approaches to protecting plants. That caution was due to operational constraints. OT investment cycles move on a much longer timeline than IT's, so plants can't adopt every new security practice as fast as IT does, and many get only a single maintenance window a year to introduce changes, meaning every change has to be ruthlessly prioritized.

For many organizations, that divide is beginning to shift, but for plenty of others, it still holds. Industry 4.0 accelerated the connectivity and automation of manufacturing environments. The emerging Industry 5.0 vision builds on that foundation by emphasizing resilience, sustainability, and the role of people alongside technology. Both trends make coordinated visibility and risk management across IT and OT increasingly important. Where the barriers do come down, companies operate more efficiently and mitigate risk more effectively.

As that convergence accelerates, industrial companies thinking about modernizing their technology investments need a clear, coordinated view of their manufacturing estate to modernize without disrupting production. **That starts with five questions:**

TANIUM

1. Do we know every asset supporting production, and its operational role?

You can't manage what you can't see, and in today's world, you can't protect it if you can't manage it. In the legacy manufacturing world, asset inventory processes involved manual steps and were heavily dependent on spreadsheets. As more asset types were brought into the plant environment, many went uncaptured by traditional scans. For years, outdated and incomplete information was accepted because it was more important to focus on things that keep the operation running.

Knowing what you have also means understanding each asset's operational role. At a high level, there are two distinct types of technology in manufacturing, layered as defined by the Purdue model and the ISA/IEC 62443 IACS Cybersecurity Standard. In the lower levels are the devices that run the process itself: sensors and actuators, and the controllers that direct them, such as PLCs (programmable logic controllers). This equipment performs high-volume, repetitive work, must run with high efficiency, is intolerant of downtime, and typically runs on real-time operating systems (RTOS) or proprietary systems built and managed by ICS vendors. In the upper levels are the systems that supervise and manage that equipment, such as HMIs, SCADA servers, engineering workstations, and site operations systems, and that communicate with corporate systems. These typically run on standard operating systems like Windows and Linux and require the same type of management and control as systems in a corporate environment. Between the two sits a layer of embedded devices, sometimes called "gateway devices," that translate protocols from the lower tier to the upper tier, often running simplified, embedded versions of standard operating systems.

But discovering an asset isn't the same as safely managing it. Running Windows or Linux doesn't mean a production system can follow the same change and patching practices as a corporate endpoint. The appropriate discovery method, and the appropriate way to act on what you find, depends on where an asset sits in the stack and what role it plays in production.

Today's CIOs and heads of manufacturing understand that the pace of today's threats requires AI and automation, because manual scanning processes can no longer keep up. They need real-time visibility and a simplified, comprehensive view of assets, and their operational role, across the corporate and manufacturing technology estates.

2. Do we understand the dependencies and access paths connecting IT and OT?

Manufacturing environments are inextricably connected to IT environments, and each depends on the other. The IT-like devices in the upper tiers of the stack, and their connectivity to corporate environments, represent a common cyberattack vector and security exposure today. In fact, IBM's 2026 X-Force Threat Intelligence Index found that manufacturing was the most-targeted industry in X-Force's incident response engagements, accounting for 27.7% of the incidents X-Force observed. The embedded gateway devices that translate protocols between the lower and upper tiers sit directly on the IT/OT boundary, making them a critical part of understanding how the two domains connect.

Two connection points deserve more attention than they usually get. The first is shared services. Active Directory, DNS, time synchronization, and patch and file servers often sit in the corporate environment but are relied on by systems on the plant floor. When a plant authenticates against the same directory as the corporate network, an identity problem in one place becomes a production problem in the other. Most teams can tell you where those dependencies exist for corporate systems. Far fewer can say the same for the plant.

The second is vendor remote access. Equipment makers and integrators routinely need to reach the machines they support, and those connections were often set up years ago to solve an urgent problem and then left in place. Over time it becomes hard to answer basic questions: who has access, to which assets, from where, and who approved it. If you cannot answer those questions today, that is the place to start, because these paths cross the boundary between the two domains by design.

There are also workstations and laptops used by factory employees that tend to receive less attention than their counterparts in the corporate environment. Because they sit on the plant floor but also reach the corporate network, they are another connection point that's easy to overlook.

To manage and protect their manufacturing environments end-to-end, manufacturing engineering, IT, and security teams are increasingly collaborating to form unified security operations centers (SOCs) and processes, pushing the best source of management data from these distinct types of technology into shared CMDB, SIEM, and workflow platforms.

3. Can we reduce risk without disrupting production?

Patching remains one of the most effective ways to reduce risk, but in a plant, it is rarely the only option, and sometimes not the first. When an asset is too critical to take down, the question shifts from how to patch it to how to break the attack path to it. Segmentation, restricted access, and monitoring can do that while patching waits for the next maintenance window.

Maintaining the highest possible level of technology hygiene also increases uptime and reduces the effort spent maintaining and fixing problems. Fewer trouble tickets mean your help desk can focus on more valuable work. In manufacturing, IT-like "managed assets" still require similar levels and types of patching as assets in the corporate environment, and you should strive to carefully extend patching practices into the manufacturing space, ideally from the same platform that manages your IT assets.



History has shown that IT practices can't simply be lifted into manufacturing, though. Outdated operating systems, narrow change windows, thin hardware specs, and network segmentation are all traditional challenges to patching in the manufacturing environment. Advances in technology and closer collaboration between IT and OT teams can help manufacturers improve operational reliability and reduce cybersecurity risk while minimizing disruption to production.

Vulnerability management helps focus patching activity on the areas of greatest risk. Driving a patching program from the same platform used to identify and prioritize vulnerabilities eliminates hand-offs, improves results, and drives real productivity gains. For “unmanaged” lower-tier assets, where cyberattack threats are increasingly showing up, best practice is aggregating data from specialized OT vulnerability vendors and your IT systems into that same unified CMDB, SIEM, and workflow platform.

Automation is what makes patching possible at scale, but in a plant it needs boundaries. A workable model starts with plant approval. Changes to production systems are scheduled with plant operations, tied to the available maintenance window, and approved by someone who understands the process the asset supports. IT and security can recommend what needs to change and why, but the plant confirms when it is safe to do so, and confirms again afterward that production is running as expected.

The second part is setting limits by asset, not by technology. A Windows server that collects production data from the line and a Windows workstation used by an engineer may look identical to a scanner, but they carry very different consequences if a patch goes wrong. Define in advance which assets can be patched automatically, which require manual approval each time, and which should never be patched directly and are protected by other controls instead. Where automation is allowed, build in a way to pause or roll back. The goal is not to automate everything. It is to automate what is safe and be explicit about what is not.

4. Can IT, security, and operations respond and recover together?

Given the surge in ransomware attacks, there’s no shortage of advice on incident preparedness. First and foremost, you need an incident response plan that includes manufacturing, and your board of directors and other key executives need to know their roles. You should have agreement on who holds ultimate accountability, and you should determine actions for as many scenarios as possible: Will you pay the ransom if attacked? Can you recover from backups, and if so, how long does it take? Thinking through the implications of many possible attacks in advance means recovering faster when one happens. Test runs and tabletop exercises help ensure all stakeholders understand the implications and are prepared.

This is where the shared-responsibility principle described in the ISA/IEC 62443 IACS Cybersecurity Standard matters: manufacturing engineering, IT, and security are distinct disciplines managing distinct layers of the same environment, and effective incident response depends on all three agreeing on roles and accountability, not just on the underlying technology. Often, the gap isn't a missing policy, it's a missing person. Empowering someone local at each plant to liaise with corporate IT and security gives that plant immediate, on-the-ground authority to isolate or shut down an affected asset, while restoration and return to service become a joint sign-off: plant operations confirming safety and process readiness, IT and security confirming the threat is actually remediated. Pairing that local liaison role with standardized visibility into how similar plants are operating, so a plant manager can see what "normal" looks like elsewhere in the fleet, is a major unlock for making these calls quickly and consistently.

From a systems capability perspective, knowing the state of your environment is always critical during an incident. In an environment where minutes and seconds count, real-time visibility into what's happening is invaluable. A single source of truth is critical, and the ability to take action and control assets from the same platform is a big advantage in crunch time. The best-prepared companies know ahead of time where they're most exposed and, in a resource-constrained world, can minimize impact by prioritizing the resources to remediate. Cloud adoption is growing across the manufacturing industry, too, so it's worth including cloud-based scenarios in your incident response planning regardless of where you are on that journey.



5. Can we scale these practices across plants while preserving local operational requirements?

Is a reluctance to patch machines on the plant floor standing in the way of operational efficiency and output? Traditional manufacturing teams have a long-running aversion to touching anything that's running: factory uptime drives output, and next to safety, output is the primary KPI for plant managers. Infrequent, short maintenance windows are normal, and an "if it ain't broke" mentality is still prevalent in many places.

But industrial environments are full of machines managing other machines, many of which get little human interaction and are "out of sight, out of mind," plus workstations and laptops used by factory employees that receive less attention than their corporate counterparts. Beyond the direct risk, there's an efficiency cost: the resources spent "keeping an eye" on machines, the fallout when one eventually goes down or gets hacked, and the resources spent on regulatory compliance, from traditional ICS frameworks like ISA 62443 to newer connected-product requirements like UNECE R155/156 in automotive.

Now think about what this looks like at scale: multiple factories or industrial operations, each managed independently, in different parts of the world, under different circumstances, with different IT infrastructures, often compounded by acquisitions. That model is inherently inefficient.

It's time to flip the script on managing manufacturing technology. AI and automation make this scale possible. Instead of relying on plant-by-plant manual effort, teams can apply consistent policies across dozens or hundreds of sites at once, freeing local staff to focus on the decisions that require their local process knowledge. With the technology available today, and by embracing good hygiene practices in the plant environment, companies can centralize visibility and apply consistent governance across plants, while still preserving the decisions that require local process knowledge. Beyond improving risk posture, this has a positive effect on output.

In Conclusion

The legacy of separate and independent manufacturing technology is inefficient and makes manufacturers targets for cyberattacks. The solution begins with visibility. Start by unifying your view of IT and OT, and draw confidence from always knowing what you have, where it is, what state it's in, and the role it plays in production. With that foundation, IT, security, and plant operations can work from the same picture to reduce risk, respond faster, and scale consistent practices across every plant without disrupting production

Learn how Tanium Atlas can help manufacturers securely modernize their technology.

Contact us.

Tanium is the Autonomous IT company. As AI accelerates both innovation and risk, Tanium Atlas, the company's autonomous operating system, puts the full depth of the Tanium Autonomous IT Platform behind every IT and security operator — human and agentic. Tanium provides the real-time intelligence, agentic decision-making, and autonomous execution operators need to detect, decide, and remediate at machine speed across their endpoint estate.

The company is recognized as a Leader in the inaugural 2026 Gartner® Magic Quadrant™ for Endpoint Management Tools, as a Leader in the IDC MarketScape: Worldwide Client Endpoint Management Software for Windows Device Management 2025–2026 Vendor Assessment, and as a Leader in The Forrester Wave™: Endpoint Management Platforms, Q2 2026.

To learn how Tanium delivers Autonomous IT for Unstoppable Business, visit **www.tanium.com** and **LinkedIn**.