imprivata®

Simple, secure access management for manufacturing: Challenges and opportunities

When it comes to manufacturing, there's no question about it: every second of critical work must stay both frictionless and secure. And that dichotomy creates a tricky balancing act for IT leaders. As part of that, the prevalence of shared devices, legacy systems, and third-party access further complicates the ability to pull off that feat.

In this eBook, we'll take a look at the key challenges at hand in striking that all-important balance, and access management strategies designed to overcome them.

CHALLENGES AT HAND ...

Industry 4.0 is transforming the way manufacturers operate. Connecting systems, equipment, and data enables organizations to unlock new levels of efficiency and customer satisfaction. From industrial automation to predictive maintenance, these advances help manufacturers stay competitive in an environment where cost, quality, and speed are always top priorities.

But there's a flip side: while the impact of Industry 4.0 is powerful, digital transformation also introduces new risks. With every new connected device, application, or integration, manufacturing organizations expand their attack surface — leaving factory floors and warehouses increasingly vulnerable to cyberattacks.

With every new connected device, application, or integration, manufacturing organizations expand their attack surface...

Connectivity vulnerability – a closer look

Many access management solutions were designed for office settings, where users typically operate a single device and access primarily cloud-based applications. Manufacturing environments are clearly different. Workstations are shared across shifts. Mobile devices move between operators. Legacy systems run alongside modern platforms. Operational technology must be secured without interrupting production.

Access management strategies that don't account for these realities often struggle to balance security and usability. Bottom line: manufacturers need authentication and access controls built specifically for shared device ecosystems, hybrid infrastructures, and continuous operations.

Rising cybersecurity risks

The greater connectivity and resulting security vulnerabilities of manufacturing's digital transformation have clearly caught the attention of ransomware attackers. Because they know that every minute of system downtime is costly, they'll make steep demands and require a tight timeframe for paying the ransom. In many incidents, unauthorized access begins with compromised credentials. An account with excessive privileges or a poorly secured remote connection can provide a foothold. From there, attackers often move across systems until they reach critical production environments.

Manufacturing is in fact now one of the most targeted industries for cybercrime, with costly results. According to the ***IDC InfoBrief, sponsored by Imprivata, Manufacturing's Digital Transformation Dilemma***[1]***:***

- **57% of manufacturers** experienced a ransomware attack in the past year, compared with 49% across all industries
- **Roughly 30% of those manufacturing organizations** paid a ransom to regain access to their systems/data at an average cost of over $175,000
- **Recent IDC studies have shown the** cost of one hour of unplanned downtime to be over $125,000

Manufacturing

is in fact now one of the most targeted industries for cybercrime, with costly results.

These figures illustrate just how high the stakes are. A single incident can lead to IP theft, data loss, brand damage, and the loss of customer trust … all while production grinds to a halt.

[1] IDC InfoBrief, sponsored by Imprivata, Manufacturing's Digital Transformation Dilemma, (IDC #US53662525, July 2025)

Third-party vendor risks

Walk through any modern manufacturing operation, and you'll quickly see how much of it depends on external partners. Vendors maintain equipment, update software, monitor systems remotely, and keep supply chains moving. In many cases, they're as essential to production as internal teams. But the connectivity that keeps operations running also introduces risk caused by a worrisome gap in visibility and control.

For perspective, several of the most damaging data breaches in recent history started with attackers exploiting third-party access to get to organizations' sensitive system. Taking advantage of a trusted partner's connection to gain entry into an environment has long been a common cybercriminal attack tactic, but it's even more prevalent today. According to Verizon, 30% of breaches in the past year involved third-party access, a 15% increase from the previous year. The Ponemon Institute found an even higher incidence of this type of attack. Its report, *The State of Third-Party Access in Cybersecurity*, revealed that 47% of organizations had suffered from a third party-related breach in the past year.

Legacy infrastructure and budget constraints

Manufacturing organizations must also perform a second balancing act: between modernization and financial realities. A unified access framework bridges legacy and modern environments, ensuring visibility and consistency across **workstations**, shared devices, and cloud applications, enabling transformation to move forward securely and efficiently. But saddled with budgetary constraints and logistical challenges, many manufacturers continue to rely on aging operational technology (OT) not designed for today's threat landscape. According to the same ***IDC InfoBrief***[2]:

- **50% of manufacturers** state that the average age of their OT assets is 15 years or more
- **Only 30% of manufacturers** reported the ability to provide front-line employees with real-time operational data

The reliance on outdated equipment includes the use of operating systems, proprietary software, and aging hardware that lack modern authentication protocols, encryption standards, and patching capabilities. This creates vulnerabilities that attackers can exploit, especially as these systems are increasingly connected to corporate IT networks and the internet.

[2]IDC InfoBrief, sponsored by Imprivata, Manufacturing's Digital Transformation Dilemma, (IDC #US53662525, July 2025)

Dependence on legacy infrastructure also makes it difficult to implement important identity and access management measures, including multifactor- and risk-based authentication, as well as role-based access controls. Without these vital security practices in place, gaps are created that are difficult to see but easy to exploit. Tools that layer authentication on top of older systems can bring them into a consistent access workflow without requiring costly replacements.

Dependence on legacy infrastructure also makes it difficult to implement important identity and access management measures

The convergence of IT and OT

Manufacturing plant security used to rely on physical isolation. Operational technology systems were often separated from broader networks. Today, that separation is far less common. Smart factories depend on connected sensors, programmable logic controllers, robotics, and cloud-based monitoring tools. These systems generate valuable insights, but they also introduce new access points.

If access controls are not extended into OT environments, attackers may exploit these pathways. Generic logins on shared workstations reduce accountability. Limited session monitoring makes it difficult to trace suspicious behavior. Overlapping permissions between IT and OT environments increase the risk of lateral movement.

The result can include production manipulation, equipment damage, safety incidents, and compliance violations. Manufacturing network security now requires unified visibility and identity governance across both IT and OT systems.

Security controls that add friction quickly meet resistance

"Maximize uptime" is the daily mantra of manufacturing organizations as they operate under constant pressure to keep the wheels turning. Delays have real consequences, from missed production targets to financial loss. Because of this pressure, the all-important access/security balance is severely tested.

Security controls that introduce friction often lead to workarounds. Credentials get shared. Sessions remain open longer than they should. Over time, these behaviors increase risk in ways that are difficult to detect. The challenge is not simply to restrict access, but to shape it in a way that aligns with how work actually happens.

Cybersecurity risks are not the only consequence of weak access controls. Operational efficiency also suffers. When login processes are cumbersome or inconsistent, employees spend unnecessary time navigating authentication steps. Help desks become overwhelmed with password reset requests. In addition to sharing credentials, frustrated workers may leave systems unlocked to save time.

The most effective access controls for manufacturing reduce both risk and friction by protecting systems while supporting fast, seamless workflows.

These behaviors increase security exposure while also reducing employee productivity. In high-volume production environments, small delays at each login accumulate across shifts and facilities. Over time, the organization pays for that friction in lost output and increased IT overhead. The most effective access controls for manufacturing reduce both risk and friction by protecting systems while supporting fast, seamless workflows.

... AND STRATEGIC OPPORTUNITIES

Five foundational steps to achieving simple, secure access

Here are five practices that lay the groundwork for a strong access management program:

Start with two pivotal principles

- Zero trust is a comprehensive cybersecurity approach grounded in the principle of "never trust, always verify." It assumes that both internal and external users pose threats and must be continuously authenticated and authorized before being allowed to access resources, regardless of location, role, or device used.

- The principle of least privilege is focused on answering the question "What's the right level of access?" It states that users should be granted the absolute minimum level of access needed to do their jobs and should be strictly limited in scope and duration.

Strengthen identity and access governance

- Apply role-based access controls (RBAC) to ensure users — employees, vendors, and contractors — only access what they need

- Implement Identity Threat Detection and Response (ITDR), which provides continuous threat assessment triggering real-time enforcement actions or alerts

- Employ automated provisioning and de-provisioning to reduce risk from temporary staff and contractors

Modernize authentication everywhere

- Adopt multifactor authentication (MFA) and passwordless options such as biometrics or FIDO authentication

- Use single sign-on (SSO) for fast, frictionless access to both legacy and cloud applications

- Enable consistent authentication across shared workstations, mobile devices, and connected equipment

- Incorporate No Click Access™ for instant, secure shared workstation logins

Empower frontline productivity

- Choose solutions designed for shared and shift-based workflows
- Simplify interfaces and authentication steps, as ease of use is essential in driving adoption and ROI
- Deliver personalized, fast access without shared credentials
- Use access analytics to identify and eliminate login friction that slows production

Build a culture of operational security

- Form cross-functional teams to align IT, OT, and operations leadership
- Establish a clear escalation and review process for access issues
- Tie identity management metrics to business outcomes — uptime, productivity, and compliance
- Regularly refresh training so every worker understands their role in achieving secure, efficient operations

A practical framework for operational security governance

Next, use the seven steps below to design, deploy, and sustain operational security without clogging workflows:

1. **Map roles to tasks and systems**

Build a clean catalog of job roles, tasks, and the applications or equipment each task requires. Include shop floor software, historian views, quality systems, and device management portals. This creates the baseline for least privilege and role-based privilege.

2. **Standardize authentication for shared environments**

Shared devices and workstations are common in plants. Choose identity authentication that supports fast sign-in and sign-out, online and offline access, and consistent behavior across shifts. Avoid one-off exceptions that confuse users. Simplicity here is a major driver of adoption.

3. **Segment external access**

Vendors and contractors should never use staff accounts or be provisioned broad access rights. Provide secure remote access that isolates sessions, enforces approval workflows, and records activity. Apply time limits and restrict access to only the systems in scope. This reduces the likelihood of a third-party data breach and improves audit readiness.

4. **Design for resilience and offline access**

Manufacturing sites face network brownouts, planned downtime, and maintenance windows. Ensure identity access controls only fail in predictable ways and support offline access for essential tasks. Document fallback procedures and test them in drills.

5. **Enforce reviews and recertification**

Access that's never reviewed will expand silently. Set clear recertification cycles for privileged roles, shared device entitlements, and vendor access packages. Tie these reviews to change events such as shift changes, contractor offboarding, and equipment upgrades.

6

Instrument for visibility

Collect access telemetry that shows login times, failed attempts, and privileged session activity. Use this to spot friction that hurts productivity, and to catch suspicious patterns early. Analytics should inform both user experience wins and unauthorized access prevention.

7

Train for clarity and confidence

Digital literacy gaps are real. Replace long manuals with short, role-based guides and quick demos. Select an access management solution that makes it simple to request access, escalate identity authentication when required, and end sessions on shared devices.

Build a third-party risk management program

Organizations that approach vendor management as a continuous, identity-driven process are better positioned to manage this complexity. They gain clearer visibility into access, stronger control over permissions, and greater confidence in their ability to respond to risk. Here are four key steps to success:

Understand your vendors and your risks

The first stop on the road to Zero Trust-based third-party risk management is an assessment. Begin by developing an understanding of what's going on in your environment. If you don't have a detailed inventory of all the vendors with access, that's an immediate blind spot that needs to be addressed. It's critical to be able to answer questions such as: "Who has access to resources in my environment?" "Which organizations, and which individual employees within those organizations?" "What systems or software do these service providers have access to?" "What data is present in these environments?" "How are they accessing these systems?" "What controls are in place to manage that access?"

Organizations that approach vendor management as a continuous, identity-driven process are better positioned to manage this complexity.

Categorize vendors based on risk

The next step is to define and document the scope of permissible access for each vendor — which systems, data, or applications they should be allowed to access, and under what conditions. Then the vendors can be tiered based on how critical the systems are that they work on and the amount of privileged access they need. You'll also want to consider how much control you currently have over that vendor's access. Generally, the less control, the higher the risk.

Choose and implement a technology solution

Once you understand how much access each of your vendors should have, you'll need to identify a technology solution that can enforce the policies you're building. The solution needs to be able to manage all the third-party identities in your environment, segment and isolate access down to the individual user level, enforce controls, and support audit readiness.

A comprehensive vendor privileged access management solution will have been expressly designed to meet these requirements. Unlike traditional privileged access management tools — which are built for internal users — vendor privileged access management is built specifically for third-party partner and vendor identities. It can enforce fine-grained access permissions, enabling identity-based segmentation across the entire network, while also providing session monitoring and audit trail capabilities. Vendor privileged access management additionally supports onboarding, reviews, approvals, and full lifecycle management for third-party users, eliminating manual errors and making it easy to enforce uniform policies.

Migrate and maintain

Starting with your highest-priority vendor, define the access policies that your solution will need to enforce — which groups or individuals can access which systems or assets, and on what schedule. Create a documented process for requesting, approving, and revoking third-party access.

With that process in hand, you can determine which department or employee manages each individual vendor's access approvals. Self-registration capabilities in a vendor privileged access management solution make this kind of delegation possible, while removing administrative burden from security teams.

Adopt a cohesive, comprehensive approach to access management

Modern manufacturing success depends on secure, seamless access. By adopting a cohesive access management strategy, organizations can accelerate transformation, improve compliance, and protect critical operations from disruption.

Progress usually comes from treating access as an identity and workflow problem, not a list of disconnected controls. The goal is to achieve consistent authentication that's usable at shared stations, clearer separation between standard and privileged activity, and audit evidence that's easy to retrieve.

How Imprivata can help

Imprivata approaches these challenges with identity-first access solutions designed for fluid environments with shared devices and workstations, as well as virtual desktops. This includes SSO, MFA, and passwordless options that can reduce friction while improving accountability in settings where office-style login patterns don't work well.

While the common assumption is that security hinders productivity, compromise isn't necessary with the right technology in place. After all, access controls should work with your systems – enabling an easier workflow that can actually help you improve productivity and uptime. Our innovative platform of simple, secure access management solutions includes:

Imprivata Enterprise Access Management – supporting passwordless multifactor authentication and single sign-on for shared workstations and legacy and modern applications, helping frontline workers move quickly while maintaining strong identity authentication.

Imprivata Vendor Privileged Access Management – providing secure third-party remote access with granular authorization, session monitoring, and automatic expiration to reduce data breach risk.

Imprivata Privileged Access Management – adding enterprise credential vaulting and oversight for internal users' administrative tasks.

Together, these solutions reinforce operational security governance across users, devices, and applications, while supporting online and offline access in demanding environments.

imprivata®

Imprivata delivers simple and secure access management solutions for healthcare and other mission-critical industries to ensure every second of crucial work is both frictionless and secure. The Imprivata platform of innovative, interoperable access management and privileged access security solutions enables organizations to fully manage and secure all enterprise and third-party identities to facilitate seamless user access, protect against internal and external security threats, and reduce total cost of ownership.

For more information, please contact us at:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0) 208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +61 3 8844 5533

4041-2026_EB-Manfacturing