

Walking the tightrope of innovation vs. cyber risk in manufacturing

Industry 4.0 adoption fuels efficiency and innovation – but also opens the door to new cybersecurity threats.



Why Industry 4.0 digital transformation matters

- Boosts efficiency and productivity
- Enables faster, secure collaboration
- Creates a scalable foundation for new technologies
- Turns compliance into a competitive advantage
- Powers innovation across connected factories

Source: [Manufacturing Dive, Strategic access management: The backbone of productive and secure industry, 2024](#)



The cyber threat landscape

- **57%** Ransomware attacks in the past year
- **30%** Paid ransoms, average of \$175,000
- **\$125K/hour** Average cost of downtime
- **61%** Attack caused multi-day disruption
- **40%** Say productivity is the top priority

Cyberattacks also cause data loss, IP theft, reputational damage, and customer loss.

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







How manufacturers can balance modernization with security

- Eliminate delays from outdated access systems
- Simplify logins across devices and shifts
- Standardize workflows to reduce errors
- Free IT teams from constant access requests
- Scale securely across legacy + Industry 4.0 platforms
- Unlock full value of connected systems

Source: [Imprivata, Strategic access management: The foundation for Industry 4.0 adoption and enhanced productivity, 2024](#)



The path forward

-  Enterprise access management boosts productivity
-  MFA and passwordless strengthen compliance
-  Track “who, when, where” for accountability
-  Productivity + protection = sustainable Industry 4.0

Source: [Imprivata blog, 2024](#)