# Last Pass for Manufacturers

*The manufacturing industry spans a breadth of essential products and key sectors, from automotive and construction to cosmetics, food and beverage processing, pharmaceuticals, textiles, plastics, machinery, and beyond.*

## Add password protection to the production line

The manufacturing industry, as a critical part of global infrastructure, is an attractive target for cybercriminals seeking to disrupt supply chains, steal intellectual property, or shut down operations. Threat actors often exploit compromised credentials as the easiest and most effective way to gain unauthorized access to sensitive systems. Once in, they can carry out a range of malicious activities, from hijacking accounts to manipulating operational systems or leaking proprietary data. This makes manufacturers particularly vulnerable, as the stakes are high, and a single breach can have cascading effects throughout the supply chain.

The impact of a cyberattack on a manufacturer extends far beyond immediate financial losses. Disruption to operations can halt production lines, delay shipments, and tarnish brand reputation, while stolen intellectual property can give competitors an unfair advantage. The downstream effects of such incidents ripple through the supply chain, impacting everyone from component suppliers to end customers.

Additionally, manufacturers are often required to comply with stringent government regulations regarding data protection, making any breach a potential legal and compliance nightmare. As manufacturers become increasingly dependent on interconnected technologies, safeguarding credentials is critical to minimizing these risks and protecting the integrity of the industry as a whole.

**Ransomware was involved in 71% of incidents, and with attacks increasing by 125% annually, cyber risk is now seen as one of the top three external risks to manufacturers.**

## Secure and streamline your entire business

In the manufacturing industry, where there is often a significant gap between IT teams and frontline workers, standardizing a password management solution across the organization is one of the simplest and most effective ways to reduce credential risks. By implementing LastPass organization-wide, manufacturers can ensure that all employees, from IT professionals to factory floor staff, follow the same secure, streamlined process for password management. This approach reduces the likelihood of weak, reused, or mishandled credentials, which are a major entry point for cybercriminals.

LastPass provides an easy-to-use, cloud-native solution that simplifies password security for all employees, regardless of their technical expertise. It ensures secure creation, storage, and sharing of credentials, while maintaining strict access controls. By adopting LastPass across the board, manufacturers can bridge the security gap between IT and frontline workers, minimize vulnerabilities, and streamline compliance, ultimately improving both security and operational efficiency.

# LastPass Benefits for Manufacturers

The easiest, most affordable, and most reliable way for manufacturers to slash cyber and operational risk is to standardize password management with LastPass company wide.

| | | |
|---|---|---|
| **Secure** | **Prevent unauthorized access** | Help prevent threat actors and unauthorized users from gaining access to applications, online accounts, sensitive information, and systems. |
| | **Stop account takeover and data breaches** | Ensure the reliability and accessibility of online accounts and applications, and the privacy of credentials. |
| | **Control shadow IT** | Give organizations visibility into and management over unapproved and over-provisioned SaaS apps, allowing administrators to track credential sharing, manage access privileges, and spot vulnerabilities. |
| | **Extend secure access management** | Integrate seamlessly with major identity providers (IdPs) like Microsoft Entra, enhancing user management throughout the employee lifecycle. |
| **Comply** | **Meet cyber insurance requirement** | Make it easy for organizations to meet password and access management requirements for cyber insurance. |
| | **Support compliance** | Aids organizations in meeting compliance standards set by regulations like GDPR, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA, and SOX, as well as cybersecurity frameworks such as NIST, CISA, Zero Trust, and NERC-CIP. |
| | **Meet partner security requirements** | Helps organizations comply with strict partner security standards through robust access controls, password sharing rules, strong authentication mechanisms, and actionable reporting. |
| **Streamline** | **Deliver intuitive experiences to every user** | Offers hundreds of customizable policies, flexible privileges, detailed reporting, and various authentication options, making it an indispensable tool in a tech stack. |
| | **Extend secure access management** | Simplify credential management for employees across the entire organization. |
| | **Alleviate help desk friction** | Reduce the burden on IT helpdesks caused by frequent credential issues, such as lost passwords and account lockouts. |
| **Collaborate** | **Maximize teamwork through sharing** | Streamline password and information sharing both inside and outside the company, helping to boost productivity and efficiency for partners, freelancers, and remote workers. |
| | **Maximize adoption + usage** | Boost adoption and usage among employees by offering an intuitive and user-friendly interface that simplifies password management tasks. |
| | **Promote a security culture** | Help administrators ensure all employees actively contribute to a security-focused culture, protecting against common threats like leaked or stolen credentials to uphold fiduciary responsibility. |