SailPoint

eBook

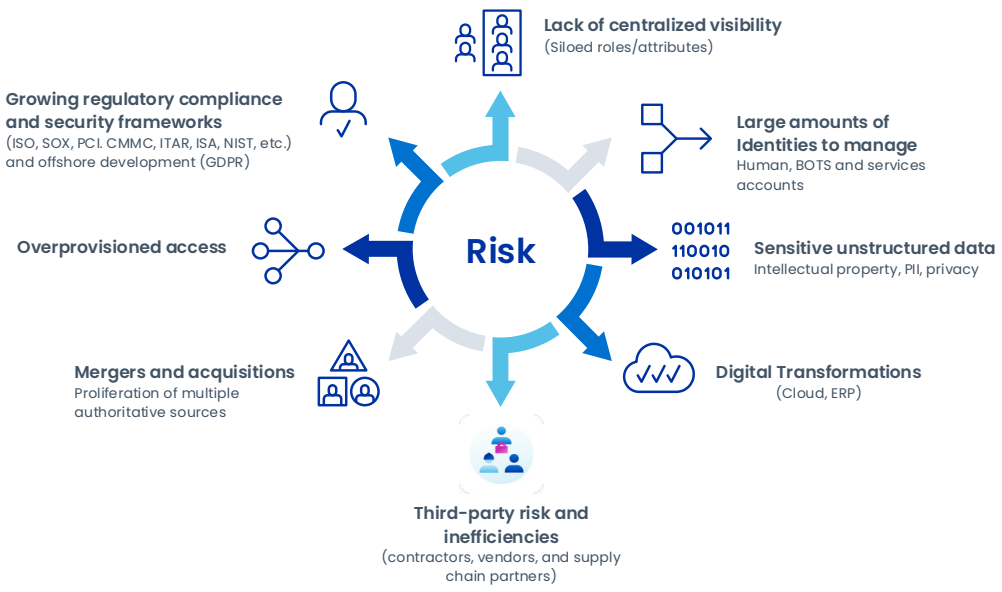
Identity security for manufacturing

A how-to guide to reduce cyber, compliance, and business risk

The state of manufacturing identity security

Advances in digital technology are essential for optimizing today's manufacturing processes, but rapid transformation can introduce significant risk. Cybercriminals now have more opportunities than ever to infiltrate your operation and disrupt your business. We've seen an explosion both in cyber threats — including software supply chain attacks, ransomware, advanced persistent threats — and, at the same time, ever-changing regulations placing unprecedented compliance demands on manufacturing organizations.

Manufacturing common challenges



Manufacturers experiencing organic growth or expansion through mergers and acquisitions often result in large numbers of new identities to manage – humans, bots, services accounts. If these identities are unmanaged or improperly managed, significant risk can come to the organization. Additionally, manual lifecycle management simply can't keep pace.

Overprovisioned access to employees and third parties introduces risk to valuable intellectual property and other competitively sensitive unstructured data. It is critical to minimize the attack surface so that the impact of any security breach can be reduced. By limiting internal access, you make it easier to prevent, identify, and protect against dangerous activity.

Data breaches pose a serious risk to manufacturing organizations, with consequences ranging from significant financial loss to reputational damage and operational downtime. If your organization has recently suffered a breach, you know first-hand it takes just one compromised identity to potentially cost your organization tens (to even hundreds) of millions of dollars in lost revenue and regulatory fines.

Manufacturing resilience requires an identity-first strategy, with centralized visibility and control over all identities. Identity security is the critical line of defense to mitigate potential existential threats to your manufacturing business.

Let's identify common risks the industrial sector must address and navigate through the crucial role of identity security in mitigating risks to manufacturing, highlighting its significance in reinforcing an organization's defenses against the ever-growing spectrum of cyber threats.

Cyber risk, business risk, and compliance risk

Our manufacturing survey, **2024 State of Identity Security in Manufacturing**, revealed the industry's top challenges and key objectives in reducing risk. One challenge cited is that an astounding 90% of attacks on manufacturing organizations are specifically targeted, either as retaliation, competitively motivated, geopolitically driven, ransom demands, or from disgruntled employees.

Across the three key categories of risk — cyber risk, business risk, and compliance risk – are essential issues and threats that must be addressed:

Cyber risk

Identity-related targeted attacks
63% of manufacturing executives reported a cybersecurity breach resulting from an identity-related issue in the last 24 months. These breaches can result in costly operational disruption, and stopping a production line for even minutes can result in insurmountable financial costs.

Overprovisioned access
81% indicated overprovisioning increases their cyberattack vulnerability. Manufacturing innovation and scale have largely outpaced cybersecurity maturity, leaving identity blind spots that can impact cyber risk, operational uptime, and compliance.

Siloed identities/lack of centralized visibility
The #1 top identity governance challenge is lack of real-time identity visibility across all locations. 36% of respondents cited this as their biggest governance challenge, signaling the issue of inadequate identity security tools.

Unmanaged machine identity populations
74% confirmed that machine identities are more difficult to manage than human ones. Growing machine identity populations, orphaned accounts, and manual efforts can create risk, underscoring the need for stronger identity tools to control access.

Business risk

Exposed intellectual property data
94% stated that protecting sensitive data is an important part of their identity security strategy. Targeted attacks make protecting access to sensitive intellectual property data critical.

Insider threats exploiting vulnerabilities
62% indicated their attacks were employee motivated. Bad actors seeking to exploit vulnerabilities and gain access to sensitive intellectual property can do significant damage.

Competitive threats
60% believed their attack was driven by competitive espionage. Manufacturers revealed that the sources of their attacks included employees that may intend to do harm or gain profit from selling intellectual property, and competitors seeking to gain a competitive advantage.

Lost revenue from delayed onboarding
71% reported that too many manual processes are required for everyday staff identity changes like onboarding, offboarding, and transfers. To improve productivity, manufacturers need to automate processes which can also help secure against insider threats, external threats, and third-party risk.

Compliance risk

Error from manual processes
The #1 challenge to achieving identity-related compliance is too many manual processes. 46% of respondents cited this as their biggest identity-related compliance challenge, which can manifest from rubber stamping the wrong amount of access, signaling the issue of inadequate identity security tools.

Separation of duty violations
68% reported an identity-related audit finding in the last two years – which can also indicate cyber and business risk.

Lack of centralized visibility
90% of manufacturers have more than one team responsible for identity security. A lack of centralized visibility has caused siloed roles/attributes, and plant identities kept separate from corporate ones.

10 steps to a more modernized identity security program

Taking a siloed, manual approach to managing and governing access reduces a manufacturer's capabilities to govern and reduce risk in hybrid, multiple-application business systems and manufacturing processes.

The need is clear: to strengthen your identity security posture and protect your sensitive intellectual property data. Robust identity security measures are a critical component of an overall cyber risk mitigation strategy. Without a unified identity security program and governance measures in place, manufacturing security measures fail.

This is why organizations must put proper access controls in place to protect against a cyber-attack – but where do you begin?

1. **Increase centralized visibility and control:** Enhancing the ability to monitor and manage access rights for all identities (employees, third-party contractors, suppliers, partners, and machines) across all departments (corporate and plant) provides organizations with the tools needed to identify potential vulnerabilities before they can be exploited.
2. **Enforce least privilege:** Employing roles and policy logic to ensure that access is granted based on the principle of least privilege provides individuals with only the access necessary to perform their job functions — nothing more, nothing less.
3. **Automate identity access processes:** Streamlining the provisioning and deprovisioning of access rights help prevent overprovisioning and backdoor access, minimizing the chances of unauthorized entry into the system.
4. **Keep sensitive data protected:** Identify and classify your critical data assets (trade secrets, manufacturing processes, industrial designs, etc.), who has access, and how they're using it. Real-time activity monitoring and alerting provides robust data access security.
5. **Automate workstreams** for administrators and reviewers to ensure simplified, accurate periodic access review cycles. Keep your entire team — IT, audit, compliance, security business owners, and board members — continuously informed of threats with timely reports. Proactive reports and insights can help reduce risky access and regulatory compliance issues.
6. **Leverage AI-driven insights to help make access decisions and improve the operating effectiveness of controls:** Intelligent insights can also help you identify and prevent access risk before provisioning and have the intelligence needed to run "What If" scenarios. For example, put in place a process to elevate or grant emergency access with automated controls and streamlined reviews.
7. **Proactively detect and remediate:** Leveraging technology to swiftly identify and correct instances of excess or inappropriate access ensures that access rights remain aligned with organizational policies and user requirements.
8. **Secure and manage all machine identities:** Ensuring that all non-humans — from service accounts to bots and RPAs — are accounted for within your organization's overall identity security strategy.
9. **Resolve policy violations:** Addressing and rectifying policy violations, including separation-of-duty (SoD) conflicts, helping to maintain a secure and compliant operational environment.
10. **Continuously monitor:** With dynamic and constantly evolving cyber risks, implementing the practice of continuous monitoring enables organizations to quickly adapt to new threats and vulnerabilities as they arise.

Longer term, today's manufacturing organizations must make cyber risk mitigation a part of security design, implementations, and remediation activities. Adopting these strategies enables organizations to build a stronger, more resilient defense, ensuring that digital assets and operations are securely protected in an increasingly interconnected world.

How SailPoint can help

SailPoint harnesses the power of AI and machine learning to revolutionize identity security, offering forward-thinking solutions to mitigate cyber risk in manufacturing. AI plays a significant role in strengthening security by helping to detect and remediate vulnerabilities, while also improving operational efficiencies. It enables organizations to easily spot risky users and access outliers, helping you be more secure, more resilient, and future proof.

With SailPoint, you gain a proactive partner with the expertise you need to secure digital identities across large, complex IT environments.

The advantages of SailPoint's robust solutions for risk mitigation include:

- **Detecting and managing access risks:** Pinpoints and manages potential security vulnerabilities early on
- **Providing robust analytics:** Tracks, reports, and gauges the value of your identity security program. 360-degree visibility and anomalous insights help reduce risk at scale.
- **Extending data access security:** Identifies your sensitive, regulated, and critical data assets, who has access to it, and how it's being used with real-time activity monitoring and alerting.
- **Simplifying the management of non-employee identities:** Implement risk-based identity access and lifecycle strategies for third-party non-employees to boost operational efficiency and reduce third-party risk.

As a manufacturing organization grows, it may be difficult to view and control access for every identity. SailPoint identity security ensures that each identity has the right access needed to do their job —no more, no less. With a 360° view of all human, machine, and third-parties, SailPoint can help enterprises follow the principle of least privilege access, identify data trends and anomalous access, prevent workforce access delays, and help simplify audit readiness. As a result, manufacturing organizations can feel confident to accelerate their digital transformation and accommodate an expanding organization.

This includes improving your productivity, establishing centralized visibility, reducing operational costs, and securing against insider threats, external threats, and third-party risk. With the most sophisticated identity technologies that can scale to support the most complex, global enterprises, SailPoint can help streamline your identity journey and drive your manufacturing company forward. Learn more at **www.sailpoint.com/solutions/industries/manufacturing**.

SailPoint

About SailPoint
SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.