KROLL™

Protecting Manufacturing Continuity through Identity Security

White Paper

1. Introduction:

The New Imperative for Identity Security for Operational Technology (OT) in Manufacturing

The convergence of accelerated digitalization, complex global supply chains and the rapid adoption of artificial intelligence (AI)-driven automation has elevated the importance of identity security. Combine this with the traditional and fragmented identity management approaches typical in manufacturing environments, and risk is multiplied.

Failing to tackle identity now becomes a direct threat to production continuity, regulatory compliance and competitive advantage. With operational disruption, intellectual property theft and safety considerations in the balance, securing identity is now foundational to maintaining operational resilience.

Identity has moved from a technical concern to a critical business imperative.

This white paper examines the evolving identity security challenges facing the manufacturing sector and outlines how a modern, converged identity security platform can help organizations reduce risk, strengthen governance and support long-term resilience without compromising operational efficiency.

2. The High Stakes:

Quantifying the Cost of an Identity Breach

A modern identity breach creates far-reaching impacts that extend well beyond immediate financial loss. For manufacturers, identity compromise can trigger cascading consequences across operations, regulatory compliance, supply chains and brand reputation. As production environments become more interconnected, the cost of failure continues to rise in both scale and duration.

2.1 Severe Financial Impact and Operational Disruption

Identity-driven cyber incidents frequently result in prolonged operational downtime, particularly within manufacturing and industrial environments, where systems are tightly coupled to physical processes.

- In recent Kroll research, business **downtime and recovery costs from a cyber incident averaged USD 2.2 million (mn),** with **overall potential loss reaching USD 20.9 mn.**
- In other research, manufacturing-specific downtime caused by cyberattack was up to **USD 17K per minute**, compared to **USD 125K per hour** for the industrial sector.
- Labor downtime losses related to global manufacturing ransomware (2025 projection) were **USD 18 billion (bn) globally, USD 4.4 bn in Europe**, based on average 13-day attack duration.

Sources: *Technology Radius; IBM Cost of a Data Breach Report (Industrial Sector); Kaspersky and VDC Research.*

2.2 Escalating Regulatory Fines and Insurance Costs

Regulatory exposure continues to increase as identity controls become a core compliance expectation. In parallel, cyber insurance providers are tightening underwriting standards.

- GDPR penalties are up to **EUR 20 mn** or **4% of global turnover** for severe violations.
- Cyber insurance premiums continue to rise year-on-year; insurers increasingly demand evidence of identity maturity.

Sources: *GDPR; market observations (broker/insurer reports).*

2.3 Exposure via Third-Party and Vendor Weaknesses

Manufacturers operate within complex ecosystems that rely heavily on suppliers, contractors and service providers. Identity compromise within any part of this ecosystem can rapidly propagate risk.

- Approximately **29%** of global breaches are linked to third-party vectors.
- Verizon DBIR (2025): **about 30%** of breaches involve external supply chain entities.

Sources: Kroll cyber resilience research, *SecurityScorecard Global Third-Party Breach Report (2024); Marsh analysis referencing Verizon DBIR 2025.*

2.4 Lasting Reputational Damage and Customer Trust Erosion

Beyond direct financial and operational losses, identity breaches inflict long term damage to brand trust and customer confidence. While impact varies by organization and sector, studies consistently show that major incidents result in sustained revenue pressure across multiple quarters as customers reassess trust, reliability and resilience.

Sources: *Industry consumer trust surveys; market analysis.*

3. Why Manufacturing Is Uniquely Vulnerable:

The Accumulation of Identity Debt

Global manufacturers face a unique cluster of operational and structural weaknesses that amplify identity risk.

3.1 Legacy Systems and Fragmented Infrastructure

Large manufacturers run aging IT/OT environments with fragmented identity controls, making sero trust adoption complex.

Many industrial control systems were built long before identity governance was a consideration. Legacy human machine interfaces, HMIs, supervisory control and data acquisition (SCADA) platforms and controllers frequently rely on local user stores, shared operator logins, or even hard-coded credentials embedded in applications. These OT environments predate modern identity and access management (IAM) practices.

As a result, identity hygiene in OT environments deteriorates over time. Accounts are added for projects, outages or vendor support and are rarely reviewed or removed. The longer systems remain in production, the more identity debt accumulates.

3.2 Production Uptime Wins Out over Security

In manufacturing, the primary directive is not to stop production, which means that identity controls are routinely bypassed. Shared operator logins are created to maintain operation and avoid emergency access issues. Vendor access could be left open “just in case” of emergency. By granting access broadly instead of precisely, excessive access becomes the norm.

3.3 High Turnover and Complex Roles Break Identity Life Cycles

Manufacturing workforces are dynamic. Plants often rely on seasonal labor and rotating contractors during turnaround. Role changes can be driven by turnarounds, shifts, production lines or sites. Plants may onboard and offboard workers locally, and contractors may never enter corporate HR systems.

Identity governance depends on clean joiner, mover and leaver signals. In manufacturing, those signals are frequently incomplete, delayed or missing altogether.

Access is rarely adjusted in real time, and deprovisioning is often manual and inconsistent. This leads to users retaining access long after their role has changed or after they have left the organization entirely.

3.4 Identity Ownership Is Fragmented across the Organization

Who “owns” identity and access within an organization is complex. While OT teams control production systems and engineering works with integrators and original equipment manufacturers (OEMs), vendors tend to manage their own personnel. And while IT typically manages IAM tools, security is accountable for risk and HR only partially governs employee life cycle data.

This fragmentation makes governance extremely difficult. Decisions about joining, leaving and access management are distributed. Therefore, accountability is unclear and enforcement is inconsistent. Identity policies may exist in the company; however, translating and implementing those in operational reality across plants and systems is a constant struggle.

3.5 Cross-Jurisdictional Regulatory Complexity

Manufacturers face growing regulatory and customer pressure around cybersecurity. Standards such as ISA/IEC 62443 and NIST 800-82; regulations such as NERC CIP (North America) and NIS2 (EU); and increased scrutiny from insurers and customers all require stronger access controls and accountability.

Identity governance programs in manufacturing environments were not built for that role and struggle to account for employees, contractors and vendor access along with the nonhuman identities.

To compensate, organizations rely on assessments, manual reviews, spreadsheets and isolated controls. These approaches are labor-intensive and brittle, and they rarely provide the level of assurance auditors or regulators expect.

4. The Strategic Response:

Building an Identity-Centric Security Foundation

Industrial modernization initiatives such as the Industrial Internet of Things (IIoT) and Industry 4.0 are rapidly transforming manufacturing environments. At the same time, organizations continue to operate legacy industrial control systems that rely on shared accounts, unmanaged third-party access and limited visibility into who or what has access to critical systems. In this environment, traditional perimeter-based defenses are no longer sufficient.

Most manufacturing organizations begin their OT security journey with network-centric controls such as OT threat detection technologies, asset inventory and segmentation. Secure Remote Access (SRA) is often adopted as the primary identity control for OT environments, driven by the immediate need to enable remote access for engineers, OEMs and vendors. While SRA reduces short-term risk by controlling how high-risk users connect to OT systems, it remains a narrow and largely static control.

SRA solutions focus on access paths rather than identity life cycles. Authorization is often broad and at the asset level rather than within applications. These platforms emphasize session control rather than identity posture and are unable to identify lateral movement paths; detect privilege accumulation over time; or correlate access across converged IT, OT and cloud environments.

To achieve sustainable risk reduction, manufacturers must adopt a new holistic identity security approach. This requires governing all identities, privileges and entitlements across IT and OT environments, continuously assessing identity risk and adapting access based on context. A converged identity platform enables remote access that is both secure and operationally resilient.

The following sections outline a practical adoption sequence for identity controls that aligns with operational realities, minimizes disruption and incrementally reduces OT security risk.

4.1 Identity Governance and Administration (IGA)

Effective identity security begins with visibility. Organizations cannot secure or monitor identities without first understanding which identities exist and what access they hold.

IGA establishes foundational visibility and control by governing user and service identities across enterprise and operational systems. It enables organizations to answer essential questions such as who has access to OT and OT-adjacent systems, why that access exists and whether it remains appropriate.

IGA centralizes identity life cycle management across joiner, mover, and leaver events, ensuring access aligns with job roles, shifts, plant assignments and operational responsibilities. In manufacturing environments, where identities are fragmented across IT systems, engineering tools, Manufacturing Execution System (MES) platforms, historians and plant-specific applications, IGA helps address orphaned accounts, excessive entitlements, role sprawl, acquisitions and site-specific exceptions.

4.2 Privileged Access Management (PAM)

Privileged identities represent the highest potential impact in manufacturing environments and must be controlled early. Shared credentials, hard coded passwords and unmanaged administrator access remain common across industrial systems.

PAM secures high-risk accounts used by administrators, engineers, OEMs and service providers. PAM reduces the attack surface by vaulting credentials, enforcing session controls, enabling just-in-time access and providing full auditability for privileged actions. These capabilities extend across engineering workstations, SCADA servers, Programmable Logic Controllers (PLC) management tools, historians and supporting infrastructure, creating accountability without disrupting operations.

4.3 Access Governance and Least Privilege Management

Once identities and privileged access are under control, organizations can safely address excessive operational permissions. Access governance focuses on the detailed permissions and authorization models that exist within manufacturing applications and platforms.

While IGA answers who should have access, access governance answers what actions those identities are permitted to perform. Manufacturing systems often include granular permissions that control recipe changes, quality parameters, configuration settings and production workflows. Access governance enables organizations to reduce excessive permissions in a controlled manner, preserving uptime while enforcing least privilege access.

4.4 Identity Risk and Exposure Management

As identity governance and privileged access controls mature, organizations gain the ability to continuously evaluate identity-related risk across IT and OT environments. Identity risk and exposure management focuses on identifying conditions that increase the likelihood or impact of unauthorized access, privilege misuse, or lateral movement.

This capability builds upon existing governance and access controls by analyzing relationships between identities, privileges, systems, and access paths. It helps organizations identify excessive access, inactive accounts, segregation-of-duty conflicts, privilege accumulation, and other risk conditions that may not be apparent through periodic reviews alone.

By continuously assessing identity-related risk and prioritizing remediation efforts based on operational impact, manufacturers can improve security outcomes while minimizing disruption to production environments.

5. Conclusion:

The Next Phase of OT Security Is Identity

While identity governance and security are well-established practices within enterprise IT environments, their adoption within OT remains constrained by legacy systems, shared operational models and safety-driven access requirements. Advancing identity security maturity in OT environments requires adapting governance principles to industrial realities—focusing first on OT-adjacent systems and on reducing the potential operational impact of identity-related compromise—rather than attempting to directly replicate enterprise IAM models.

Manufacturing organizations can successfully secure OT identities by adopting a pragmatic, phased approach. This includes using IGA to establish visibility and governance, PAM to control high-risk access, access governance to reduce excessive permissions and identity risk management capabilities to continuously assess and prioritize risk. When applied thoughtfully, these capabilities extend proven enterprise identity principles while respecting the safety, availability and reliability demands of industrial environments.

Although the process can be challenging, organizations can take practical steps to strengthen identity-related controls within OT environments by following these guiding principles:

1. Establish identity visibility before enforcing restrictive controls.
2. Introduce role models based on operational function and potential impact (e.g., operator, engineer, or vendor) and read only vs. change capable roles, avoiding overly granular role design early on.
3. Prioritize governance of OT adjacent systems such as MES platforms, historians and engineering workstations.
4. Use PAM to compensate for inherent limitations within legacy OT systems.
5. Adapt identity life cycle processes by progressively aligning access with employment status and role changes.
6. Gradually reduce shared access where operationally feasible.

Modern identity security is no longer discretionary. It is foundational infrastructure for protecting manufacturing operations, preserving safety and enabling long term operational resilience.

Across 36 Countries and Territories

The Americas

Atlanta
Austin
Bogotá
Boston
Buenos Aires
Chicago
Dallas
Hamilton
Houston
Los Angeles
Mexico City
Miami
Morristown
Nashville
New York
Philadelphia
Richardson
San Francisco
São Paulo
Seattle
Secaucus
Sunnyvale
Toronto
Washington, DC

Caribbean

British Virgin Islands
Cayman Islands

Europe, Middle East and Africa

Abu Dhabi
Agrate Brianza
Amsterdam
Berlin
Birmingham
Dubai
Dublin
Frankfurt
Gibraltar
Jersey (CI)
Johannesburg
Leeds
Lisbon
London
Luxembourg
Madrid
Manchester
Mauritius
Milan
Munich
Padua
Paris
Riyadh
Rome
Turin
Zurich

Asia Pacific

Bangalore
Beijing
Christchurch
Guangzhou
Hanoi
Hong Kong
Hyderabad
Jakarta
Kuala Lumpur
Manila
Melbourne
Mumbai
New Delhi
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.