COHESITY

MANUFACTURING:

When identity fails, production stops

Manufacturing ransomware attacks surged 56% in 2025, reaching 1,466 incidents—accounting for 50% of all global ransomware attacks.

Why identity puts manufacturing in the crosshairs of cyber crime

Manufacturing sits at the convergence of three critical vulnerabilities and challenges that tied to identity infrastructure:

- **IT/OT convergence creates new attack paths:** 50% of attacks on OT assets originate from IT network breaches. As manufacturing environments connect shop floor systems to corporate networks for Industry 4.0 initiatives, 80% of manufacturing firms experienced a significant increase in security incidents in 2024. Domain credentials that unlock IT systems now open doors to production control systems, MES platforms, and SCADA environments.
- **Zero tolerance for downtime:** Manufacturing operates on razor-thin margins with just-in-time delivery commitments. The average manufacturing facility loses $260,000 per hour during unplanned downtime. This economic reality makes manufacturers attractive ransomware targets—attackers know you'll pay to restore operations quickly.
- **Identity infrastructure is a single point of failure:** In more than 78% of human-operated cyberattacks, threat actors successfully breached a domain controller. In fact, Cohesity's CERT team finds that 95% of security incidents involve AD. Once inside Active Directory, attackers dump credentials, move laterally across production networks, and encrypt everything from ERP systems to robotic assembly lines.

Manufacturing case study

MKS Instruments: Lack of security around access authentication and backup restoration shut down semiconductor manufacturer (February 2023)

Target: MKS Instruments, a Massachusetts-based semiconductor equipment manufacturer with $3 billion in annual revenue.

Attack Vector: Post-incident analysis revealed MKS lacked sufficient security controls around access authentication and backup restoration of their critical infrastructure, including identity.

Business Impact:

- $200 million in lost quarterly revenue—a 20% decrease
- Multiple facilities remained closed more than a month after the attack
- Complete loss of ability to process orders, ship products, or provide services
- Supply chain cascade: chip maker Applied Materials reported $250 million in losses
- Class-action lawsuit from employees over inadequate cybersecurity practices

Cohesity Identity Resilience:
Detect, withstand, and recover from identity-based attacks

Detect	Continuously monitor and harden AD and Entra ID against identity threats and vulnerabilities with threat intelligence from leading identity security experts. Reduce attack likelihood by 25% while spending 40% less time monitoring.
Withstand	Automate rollback of malicious and suspicious identity changes to prevent compromise. Protect AD and Entra ID data with immutable, hardened backups. Simplify identity recovery testing to meet RTO objectives and enhance readiness.
Recover	Fast, automated, malware-free AD forest recovery and Entra ID with a few clicks for 90% faster recovery. Advanced post-breach forensics that speed remediation and prevent follow-on attacks and validate trust in your identity systems.

How identity compromise affects financial services

Your production floor doesn't run on machinery alone; it runs on identity and access management. When identity becomes unavailable:

- Manufacturing Execution Systems (MES) lose authentication
- ERP and supply chain coordination halt
- Robotics and automation controllers fail authentication
- Quality management and compliance systems go offline
- Remote access for engineers and third-party vendors vanishes
- Internal operations (anything from email, file access, to business applications)

Cost of downtime: $260,000 per hour of downtime. For automotive manufacturers, that can be even greater at $2.3 million per hour or $600 per second. Without proven identity resilience capabilities, recovery can take weeks.

Is your identity infrastructure resilient?

- ✓ Have you tested and proven that you can meet your identity recovery RTOs after a cyber-incident in the last 90 days?
- ✓ Do you have immutable backups of AD and Entra ID?
- ✓ Can you detect identity-based attacks (Golden Ticket, DCSync) and automatically remediate them in real-time?
- ✓ Can you validate that your identity recovery is malware-free?
- ✓ Can you perform recoveries without internet access?

If you answered "no" to any of these, your business is at risk.

Get a free identity security assessment today.

Contact your Cohesity rep to schedule a no-obligation assessment of your identity security posture.

© 2026 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity Logo, and other Cohesity Marks are trademarks of Cohesity, Inc. or its affiliates in the US and/or internationally. Other names may be trademarks of their respective owners. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100105-001-EN 5-2026