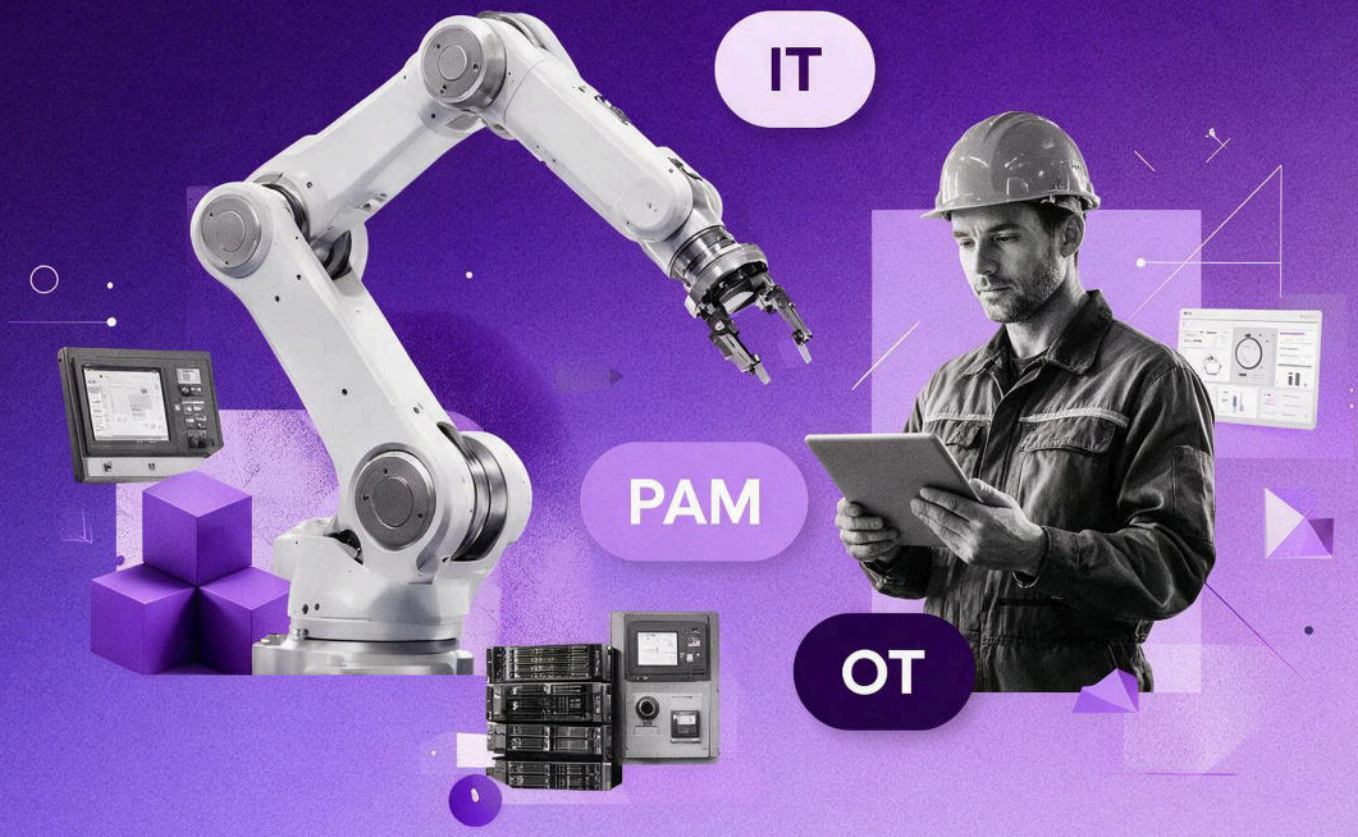
Securden

Privileged Access Security Use Cases for Manufacturing

How Unified PAM Supports Manufacturing IT, OT, and Security Teams



Privileged Access Security Use Cases for Manufacturing

How Securden Unified PAM Supports Manufacturing IT, OT, and Security Teams

Modern manufacturing environments rely on a connected mix of IT, OT, ICS, SCADA systems, engineering workstations, endpoints, cloud platforms, third-party vendors, automation tools, and legacy industrial infrastructure. These systems keep production moving, but they also create multiple attack paths when privileged access is not properly controlled.

Real-world cyber incidents show how ransomware, compromised third-party access, weak remote access controls, exposed credentials, and unmanaged administrator privileges can disrupt production, delay orders, and force manufacturers into manual recovery. In manufacturing, privileged access security is not just an IT requirement. It directly supports uptime, plant safety, operational continuity, and audit readiness.

Securden Unified PAM helps manufacturers centralize, control, monitor, and secure privileged access across IT and OT environments. It enables just-in-time access, removes standing privileges, protects credentials and secrets, secures third-party access, records privileged sessions, and supports compliance without disrupting production workflows.

1. Securing Privileged Access to ICS, SCADA, and OT Systems

(OT Security, Plant Operations, and IT Teams)

Manufacturing Challenge

Manufacturing plants depend on ICS, SCADA, PLCs, HMIs, engineering workstations, and other OT systems to keep production running. Many of these systems are legacy, sensitive to change, and difficult to replace. When admin credentials are shared, reused, or accessed without monitoring, attackers can gain control over production-critical systems.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Privileged Account Discovery and Vaulting	Discovers and secures admin and service accounts across ICS, SCADA, servers, and OT systems
Just-in-Time Access	Grants access only when required for approved operational tasks
Password-less Remote Sessions	Allows users to access critical systems without exposing credentials
Session Monitoring and Recording	Captures privileged activity across OT systems for review and investigation

Outcome

Manufacturers can secure privileged access to production-critical OT systems without exposing credentials or disrupting plant operations.

2. Securing Remote Vendor and OEM Access

(Vendor Risk, OT, IT, and Security Teams)

Manufacturing Challenge

OEMs, machine vendors, contractors, maintenance partners, and system integrators often need remote access to plant systems for troubleshooting and support. If this access is permanent, unmanaged, or routed through shared credentials and VPNs, it increases third-party risk and creates audit blind spots.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Time-bound Vendor Access	Grants vendor access only during approved maintenance windows
Approval Workflows	Ensures every vendor access request is reviewed and approved
Password-less Remote Sessions	Prevents vendors from seeing, copying, or storing privileged credentials

Securden Feature	How It Applies in Manufacturing
Session Recording and Playback	Records vendor activity for audits, investigations, and accountability

Outcome

Manufacturers can support remote vendors without giving them permanent access or direct exposure to privileged credentials.

3. Preventing Production Disruption from Supplier and Third-Party Risk

(Supply Chain Security, IT, OT, and Risk Teams)

Manufacturing Challenge

Attackers targeting manufacturers often go after suppliers, contractors, or equipment vendors that may have weaker cybersecurity controls. Once compromised, these third parties can become a trusted entry point into the manufacturer's environment.

Direct vendor connections, shared credentials, poor password hygiene, excessive privileges, and persistent remote access can expose critical IT and OT systems to credential theft, malware, unauthorized activity, and lateral movement across production-connected environments.

How Securden helps

Securden Feature	How It Helps Secure Supplier Access
Vendor Privileged Access Management	Places supplier and contractor access behind a controlled PAM layer instead of allowing direct access to critical IT and OT systems.
Password Vaulting	Secures privileged credentials and prevents suppliers from viewing, sharing, or retaining administrator passwords.
Automated Password Rotation	Regularly changes supplier-access credentials and prevents stolen or previously used passwords from being reused.
Role-Based Access Control	Restricts each supplier to only the systems and resources required for its assigned work.

Securden Feature	How It Helps Secure Supplier Access
Just-in-Time Access	Grants access only for an approved maintenance window and removes it after the task is completed.
Approval Workflows	Requires supplier access to be reviewed and authorised before critical systems can be reached.
Privileged Session Monitoring and Recording	Monitors and records supplier activity, helping security teams detect suspicious behaviour and investigate incidents.
Session Termination	Allows administrators to immediately disconnect suspicious sessions before attackers move further into the environment.
Service Account Management	Secures credentials used by supplier applications, integrations, and machine-to-machine connections.
Secure Offline Access	Enables authorised access to approved credentials in disconnected or air-gapped environments without insecure password sharing.

Outcome:

Manufacturers can prevent compromised supplier credentials and remote access from becoming an unrestricted pathway into critical IT and OT systems. By limiting access by system, role, and duration, Securden helps contain suspicious activity, prevent lateral movement, and protect production environments without disrupting authorised supplier maintenance.

4. Eliminating Local Admin Rights on Manufacturing Endpoints

(Endpoint Security, IT Operations, and Plant Support Teams)

Manufacturing Challenge

Engineering workstations, operator terminals, plant-floor systems, and employee endpoints often carry permanent local admin rights to avoid delays in daily operations. These privileges increase the risk of ransomware, unauthorized software installation, malware execution, and insider misuse.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Endpoint Privilege Manager	Removes permanent local admin rights from endpoints
Application-based Elevation Policies	Allows approved applications, scripts, and tools to run with elevated privileges
Just-in-Time Privilege Elevation	Grants temporary admin access only when required
Audit Logs for Elevations	Tracks who elevated what, when, and why

Outcome

Manufacturers can reduce endpoint attack surface while allowing engineers, operators, and employees to perform approved tasks without productivity loss.

5. Reducing Ransomware Spread Through Least Privilege

(Security Operations, Endpoint Security, and IT Teams)

Manufacturing Challenge

In manufacturing, ransomware can bring physical production to a standstill. It often enters through a phishing email or malicious download on a Windows endpoint, then spreads to engineering workstations, operator terminals, and production-connected systems. This spread is enabled by two common gaps: standing local administrator rights and the ability to run unapproved applications.

Legacy ERP, MES, and control applications often require elevated privileges, leading manufacturers to retain permanent admin access on plant-floor and engineering machines. Attackers can exploit these privileges to disable security controls, encrypt files, and move from IT systems into production environments. The result is halted output, delayed shipments, and a forced return to manual operations.

How Securden Helps

Securden Feature	How It Helps Contain Ransomware
Local Administrator Rights Removal	Eliminates unnecessary standing administrator rights, preventing ransomware from using elevated privileges to disable defences, alter system settings, or spread across endpoints.
Application Control	Uses application allowlists and blocklists to prevent unauthorized or malicious applications, scripts, and installers from running.
Privilege Elevation Policies	Elevates approved applications for authorized users without granting them full local administrator rights.
On-Demand Application Privilege Elevation	Allows users to request elevation for exceptional applications, subject to an approval workflow.
Just-in-Time Access	Grants application elevation or temporary administrator access only when required and for a limited duration.
Privilege Management Audit Trails and Reports	Records elevation requests, approvals, application execution, and administrative access to support investigations.

Outcome

Manufacturers can reduce ransomware spread by removing standing administrator rights, blocking unauthorized applications, and granting elevated access only when required. This helps contain malware at the endpoint, prevent lateral movement into production-connected systems, and minimize operational disruption.

6. Controlled Privileged Access for IT and OT Administrators

(IT Infrastructure, OT Operations, and Security Teams)

Manufacturing Challenge

IT and OT administrators need privileged access for patching, maintenance, troubleshooting, upgrades, and incident response. Without controlled access, organizations often grant broad or standing privileges to avoid delays, increasing the risk of misuse and unauthorized changes.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Role-Based Access Control	Grants access based on job role, plant location, and system criticality
Just-in-Time Privileged Access	Provides temporary access that expires automatically after use
Approval-based Access Requests	Adds control for sensitive systems and high-risk actions
Centralized Admin Console	Gives unified visibility across plants, servers, endpoints, and cloud systems

Outcome

Manufacturers can give IT and OT teams the access they need while enforcing least privilege across the environment.

7. Managing Default, Shared, and Service Account Passwords

(IT Operations, OT Security, and Compliance Teams)

Manufacturing Challenge

Many industrial systems, legacy applications, service accounts, and devices rely on default, shared, or rarely changed passwords. These credentials are often known across teams, stored insecurely, or left unchanged for long periods, creating a major entry point for attackers.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Credential Vaulting	Stores privileged credentials in a centralized encrypted vault
Automated Password Rotation	Rotates passwords regularly and after access events
Access Control Policies	Restricts who can retrieve, use, or request privileged credentials
Password-less Access	Allows users to launch sessions without viewing the password

Outcome

Manufacturers can eliminate insecure password practices and reduce the risk of credential misuse across IT and OT systems.

8. Securing DevOps, Automation, and Machine-to-Machine Access

(DevOps, Platform Engineering, Automation, and Security Teams)

Manufacturing Challenge

Modern manufacturing environments rely on automation tools, scripts, CI/CD pipelines, robotic workflows, APIs, and machine-to-machine communication. These workflows often use service accounts, API keys, certificates, tokens, and secrets. If these secrets are hardcoded, shared, or unmanaged, they become high-value targets.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
DevOps Secrets Management	Secures API keys, tokens, certificates, and service account credentials
Dynamic Secret Injection	Eliminates hardcoded secrets in scripts, tools, and pipelines
Automated Credential Rotation	Rotates secrets regularly to reduce exposure
Access Policies for Non-Human Identities	Controls which applications, tools, and workflows can access secrets

Outcome

Manufacturers can secure automation and machine-to-machine access without slowing down production, engineering, or development workflows.

9. Privileged Session Monitoring and Forensic Investigation

Security, SOC, Audit, and IT Teams

Manufacturing Challenge

When a privileged account is misused, security teams need to know exactly who accessed the system, what actions were performed, and when. Without session visibility, investigations become slow, incomplete, and dependent on fragmented logs.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Privileged Session Monitoring	Monitors live privileged sessions across IT and OT systems
Session Recording and Playback	Enables forensic review of admin and vendor activity
Tamper-proof Audit Logs	Maintains centralized records of privileged access events
Alerts and Reports	Helps security teams detect and review suspicious activity

Outcome

Manufacturers get complete visibility into privileged activity and can investigate incidents with reliable session evidence.

10. Meeting Manufacturing Compliance and Cybersecurity Requirements

(Risk, Compliance, Audit, and Security Teams)

Manufacturing Challenge

Manufacturers need to demonstrate strong cybersecurity controls for frameworks and requirements such as CMMC, NIST, and IEC 62443. Manual access tracking, shared accounts, incomplete logs, and unmanaged privileged access make audits difficult and increase compliance risk.

How Securden Helps

Securden Feature	How It Applies in Manufacturing
Policy-based Access Controls	Enforces secure access policies across IT and OT systems
Access Reviews and Certifications	Helps validate privileged access periodically
Audit-ready Reports	Generates reports for security and compliance reviews
Centralized Audit Trails	Maintains records of privileged access, approvals, and sessions

Outcome

Manufacturers can move from audit-time firefighting to continuous compliance readiness.

Conclusion

Manufacturing operations depend on secure, reliable access to critical IT and OT systems. Real-world incidents show how compromised credentials, ransomware, uncontrolled vendor access, and excessive privileges can disrupt production and create significant operational and business impact.

Securden Unified PAM helps manufacturers secure privileged access across plant floors, data centers, endpoints, cloud platforms, automation workflows, legacy systems, and third-party connections. Through just-in-time access, least privilege, automated password rotation, endpoint privilege management, session monitoring, secrets management, and audit-ready reporting, manufacturers can reduce cyber risk, contain threats, and maintain operational continuity.