

Delinea's Operational Technology (OT) Security Privileged Access Management Use Cases

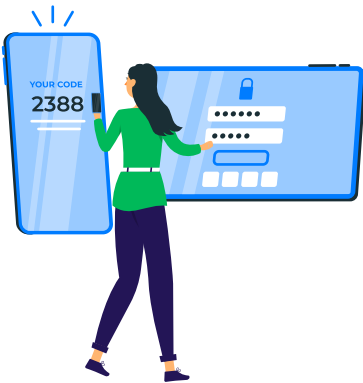


Delinea's Secret Server

Description:

A vaulting solution for securely storing, managing, and automating access to privileged credentials, including passwords, keys, and secrets.

Use Case in OT Industrial Security:



Challenge:

OT environments often rely on shared or hardcoded credentials for legacy systems (e.g., PLCs, HMIs) that are vulnerable to exploitation if stolen.



Solution:

Secret Server can centrally vault and rotate credentials for OT devices, such as SCADA systems or industrial controllers, ensuring that only authorized personnel or automated processes can access them. For example, a technician needing to troubleshoot a production line PLC can retrieve a time-limited credential via Secret Server, reducing the risk of credential misuse or exposure.



How Delinea Solves This:

Delinea Secret Server eliminates hardcoded and static credentials by storing them in an encrypted vault, automatically rotating them on a schedule or after use, and enforcing Multi-Factor Authentication (MFA) for retrieval. It integrates with OT systems via APIs or agents, ensuring compatibility with legacy protocols while providing detailed audit logs of all access events.



Benefit:

Minimizes the attack surface by eliminating static, predictable passwords and provides an audit trail of credential usage, enhancing compliance with standards like NIST 800-82 or IEC 62443.

Delinea's Privileged Behavior Analytics

Description:

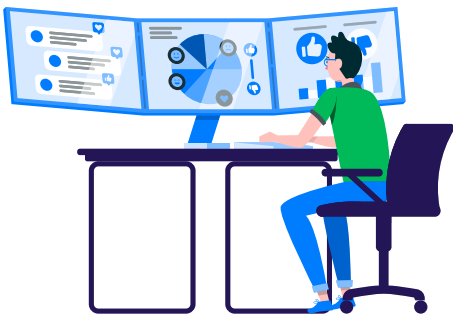
An AI-driven tool that monitors and analyzes privileged user and account activity to detect anomalies and potential threats.

Use Case in OT Industrial Security:



Challenge:

Insider threats or compromised accounts in OT environments can lead to unauthorized changes to industrial processes, such as altering pump settings in a water treatment plant.



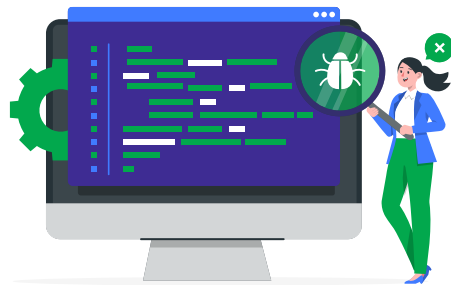
Solution:

Privileged Behavior Analytics establishes a baseline of normal activity for OT administrators and service accounts (e.g., those managing DCS systems). If an account suddenly attempts to access an unusual number of devices or deviates from typical behavior, it triggers an alert for investigation. For instance, it could detect a technician attempting to access a restricted turbine control system outside their shift.



How Delinea Solves This:

Delinea leverages machine learning to analyze patterns of privileged account usage in real-time, correlating OT-specific actions (e.g., logins to HMIs) with contextual data like time, location, and device type. It flags anomalies instantly and can integrate with incident response workflows to lock accounts or escalate alerts.



Benefit:

Enables early detection of malicious activity or misconfigurations in OT environments, preventing operational disruptions or safety incidents.





Delinea's Operational Technology (OT) Security Privileged Access Management Use Cases

Delinea

Delinea's Server PAM (Privileged Access Management)

Description:
Secures and manages privileged access to servers, including those hosting OT applications, with least privilege enforcement and session monitoring.

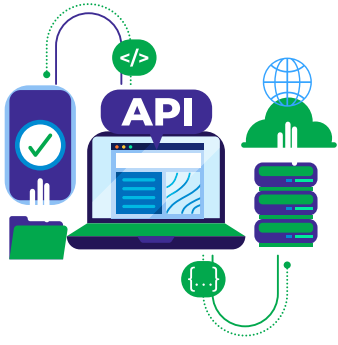



Use Case in OT Industrial Security:

			
Challenge: OT servers running SCADA software or historian databases are often exposed to IT-OT convergence risks, such as lateral movement from a compromised IT system.	Solution: Server PAM enforces just-in-time (JIT) and just-enough privilege for OT server access. For example, an engineer updating a control server in an oil refinery would receive temporary elevated privileges only for the task duration, with the session recorded for auditing. It can also restrict access to specific commands (e.g., preventing unauthorized shutdowns).	How Delinea Solves This: Delinea Server PAM uses a proxy-based architecture to mediate access, enforcing granular policies that limit privileges to specific tasks and timeframes. It records sessions in video or text format, allowing forensic analysis, and integrates with OT server OS (e.g., Windows-based SCADA) without disrupting real-time operations.	Benefit: Reduces the risk of unauthorized access or malware propagation to OT servers while maintaining operational uptime and regulatory compliance.

Delinea's DevOps Secrets Vault

Description:
A high-speed, cloud-native solution for managing secrets in automated workflows, designed for DevOps and machine-to-machine interactions.

Use Case in OT Industrial Security:

			
Challenge: IIoT devices and automated OT systems (e.g., robotic assembly lines) often use embedded secrets or API keys that, if exposed, could allow attackers to manipulate production processes.	Solution: DevOps Secrets Vault securely manages and injects secrets into OT automation scripts or IIoT device communications. For instance, a smart sensor in a manufacturing plant can authenticate to a control system using a dynamically generated key from the vault, rotated after each use, instead of a static credential.	How Delinea Solves This: Delinea provides a lightweight, API-driven vault that generates short-lived, unique secrets for each transaction, eliminating persistent credentials in code or device memory. It supports high-speed OT automation with low-latency secret retrieval and integrates with IIoT platforms via standard protocols like MQTT or OPC UA.	Benefit: Protects automated OT processes from credential theft, ensuring secure machine-to-machine communication in Industry 4.0 environments.

Delinea's Operational Technology (OT) Security Privileged Access Management Use Cases



Delinea's IGA Account Lifecycle Manager

Description:
Automates the provisioning, management, and decommissioning of accounts across systems, ensuring proper control.

Use Case in OT Industrial Security:



Challenge:
Third-party vendors or temporary contractors in OT environments (e.g., maintenance crews for power grids) often retain access longer than necessary, increasing risk.



Solution:
Account Lifecycle Manager automates the creation and removal of privileged accounts for OT systems. For example, a vendor repairing a wind turbine's control system could be granted temporary access that automatically expires after the job, with all actions logged.



How Delinea Solves This:
Delinea automates account workflows using role-based policies, integrating with HR systems or ticketing tools to trigger provisioning/deprovisioning. It ensures OT system compatibility by supporting LDAP, AD, or direct API connections, and logs all account changes for compliance audits.



Benefit:
Prevents orphaned accounts and ensures least privilege, reducing the risk of unauthorized access to critical OT infrastructure.

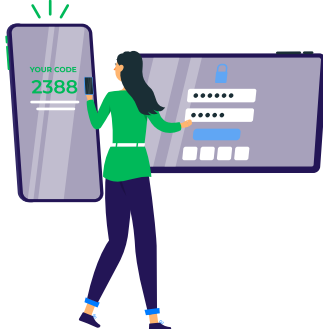
Delinea's Connection Management

Description:
Provides secure remote access to systems with granular control and auditing capabilities.

Use Case in OT Industrial Security:



Challenge:
Remote access to OT systems (e.g., for monitoring a pipeline) is a common attack vector due to weak authentication or unmonitored sessions.



Solution:
Connection Management enables secure, audited remote access to OT assets like HMIs or RTUs. For instance, an operator accessing a gas pipeline SCADA system remotely would use a Delinea gateway with Multi-Factor Authentication (MFA) and session recording, ensuring no direct exposure of the OT network to the internet.



How Delinea Solves This:
Delinea deploys a secure gateway that proxies remote connections, requiring MFA and enforcing zero-trust policies. It isolates OT systems from direct internet exposure, records all session activity, and supports OT-specific protocols like RDP or SSH used in industrial settings.



Benefit:
Secures remote maintenance and monitoring while preventing unauthorized entry, aligning with zero-trust principles for OT.

Delinea's Operational Technology (OT) Security Privileged Access Management Use Cases

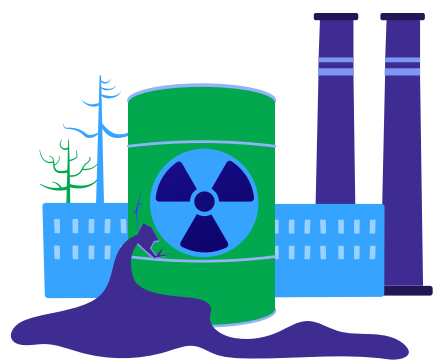


Delinea's Policy and Governance

Description:

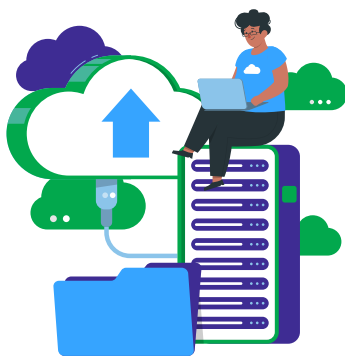
Enforces consistent security policies and role-based access controls across privileged accounts and systems.

Use Case in OT Industrial Security:



Challenge:

OT environments often lack standardized access policies, leading to over-privileged users who can unintentionally or maliciously disrupt operations (e.g., altering settings on a chemical reactor).



Solution:

Policy and Governance defines and enforces role-based access for OT personnel. For example, a plant operator might be restricted to read-only access on a DCS, while a supervisor has approval-based write access, all governed by centralized policies.



How Delinea Solves This:

Delinea centralizes policy management in a single console, applying granular controls (e.g., command whitelisting) across OT systems. It uses workflow approvals for elevated access and audits policy adherence, integrating with existing OT identity stores like Active Directory.



Benefit:

Ensures least privilege and operational safety by limiting what users can do, reducing human error and insider threat risks.

How Delinea's Solutions Address OT Industrial Security Challenges

Legacy System Vulnerabilities

Delinea vaults credentials and enforces least privilege with minimal disruption, using agentless or lightweight integrations tailored to legacy OT protocols.



IT-OT Convergence:

Delinea's session monitoring and behavior analytics detect and block threats at the IT-OT boundary, leveraging real-time analytics and zero-trust access controls.



Regulatory Compliance:

Delinea generates tamper-proof audit logs and enforces access controls that meet OT standards like NERC CIP, ISA/IEC 62443, and NIS Directive, with reporting tools for auditors.



Real-Time Operations:

Delinea's JIT access and high-speed vaulting ensure low-latency security that aligns with OT's uptime requirements, avoiding interference with critical processes.

