Delinea

Securing Operational Technology & Industrial Control System Environments

Gain zero-trust control over Operational Technology (OT) and Industrial Control Systems (ICS) by ensuring every administrator, engineer, and vendor connects through tightly governed, credential-hidden sessions with full audit trails and deep session insight across IT–OT boundaries.

OT / ICS security challenges

- Legacy systems, segmentation, limited patching, proprietary protocols
- Strong separation using the Purdue Model (levels 0–5) to isolate control, supervisory, DMZ, enterprise zones
- Privileged access paths (e.g. to HMIs, PLCs, SCADA servers, engineering stations) are high-value attack vectors
- Insider threats, credential misuse, lateral movement across zones
- Regulatory, safety, and availability imperatives

The Delinea Solution, Integrated with the Purdue Layers

Delinea delivers an integrated set of capabilities that enforce least privilege, preserve OT and IT segmentation integrity, and provide full visibility into every privileged session across your environment.

Privileged credentials are centralized inside your OT network in a secure vault, typically deployed within a DMZ or Level 3 zone. Credentials for PLCs, SCADA servers, HMIs, engineering workstations, and service or domain accounts are stored and rotated automatically. Role-based access controls, MFA, approval workflows, and time-bound access policies ensure users receive only the access they require, while passwords remain hidden and never directly exposed.

Remote access is brokered and controlled without weakening segmentation. Users, vendors, and engineers launch clean source browser-based RDP, SSH, and VNC sessions that proxy connections through approved jump points within the Purdue architecture. Credentials are injected behind the scenes, preserving network separation while enabling tightly governed, monitored access for maintenance and troubleshooting.

Benefits

✓ **Zero trust privileged access**
No sharing or exfiltration of credentials; just-in-time privilege injection

✓ **Full session visibility & forensic insight**
IT / Security teams see exactly what happened during privileged sessions

✓ **Risk-based alerting**
Auditing powered by Iris AI flags anomalous or dangerous commands for rapid response.

✓ **OT-safe deployment**
Vault and jump hosts can live in DMZ or boundary zones, isolating control zones

✓ **Compliance, audit readiness**
Detailed logs, reports, summary export, session traceability

✓ **Scalability & adaptability**
Supports many OT and IT devices, protocols, automation, credential types

Every privileged session is recorded and analyzed to deliver searchable audit trails and rapid forensic insight. Session activity, keystrokes, and process behavior are converted into structured audit data, with AI-driven analysis highlighting high-risk actions such as privilege escalation, sensitive command execution, suspicious file activity, or lateral movement. This provides both operational accountability and defensible compliance reporting.

OT / ICS use cases

- Engineering teams performing maintenance on PLC / RTU controllers
- Firmware upgrades or patching on SCADA servers
- Emergency access to cell controllers
- Audit & compliance with NERC CIP, IEC 62443, ISA/IEC standards
- Incident investigation after detection of anomalies

Why Delinea?

- Quantum-safe vaulting with full control over data and no cloud exposure
- Seamless integration of vaulting, remote access, and AI-driven auditing
- Auditing powered by Iris AI for enhanced anomaly detection
- Mature product, strong track record in enterprise PAM
- Supports credential rotation, check-out, RBAC, MFA, and delegated approvals

How it works — typical access workflow

1. User requests access (via portal) to OT target system (e.g. PLC server)
2. Request is checked, workflows / approvals assessed, MFA enforced
3. Privileged Remote Access launches session (RDP/SSH/VNC) by injecting credential from Secret Server vault
4. The session is recorded and/or observed
5. Auditing by Iris AI automatically analyzes session, labels risky activities, and provides summaries for security/ops teams
6. After session, credentials may be rotated, logs stored, reports generated

Learn More:

- Contact us for further discussions on reference designs, privileged access workstation placement, segmentation, and access policies
- Proof-of-concept offer –> test with your own OT zone

Delinea

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across modern enterprise. It applies context and intelligence throughout the identity lifecycle, across cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. Delinea uniquely provides intelligent authorization for all identities, allowing precise user identification, appropriate access assignment, interaction monitoring, and swift response to irregularities. The Delinea Platform accelerates adoption and boosts productivity, deploying in weeks, not months, requiring just 10% of the resources compared to competitors. Discover more about Delinea on **Delinea.com, LinkedIn, X,** and **YouTube.**

© Delinea