Solution Brief

Secure Access for OT and IoT Systems with Universal ZTNA

Operational technology (OT) and industrial internet of things (IIoT) systems are more connected, and targeted, than ever. Netskope One Private Access delivers secure, zero trust remote access with visibility, control, and performance, without the risks of perimeter-based security.

Quick Glance

- Enforce zero trust access and session controls to secure OT systems from internal and external threats.
- Enable agentless, browser-based remote access without exposing infrastructure.
- Apply adaptive, identity-aware policies using AI-driven risk scoring for users, devices, and machines.
- Maintain uptime and performance with low-latency access via NewEdge network.
- Support compliance standards like NERC CIP and IEC 62443 with full session recording and access logs.

"Access control issues surged 123%, highlighting ongoing identity and access management challenges in OT environments."

Nozomi Networks OT/IoT Cybersecurity Trends

The Challenge

The rise of IIoT and Industry 4.0 is driving greater connectivity across OT environments like manufacturing and utilities. As more systems come online for real-time insights, the boundary between IT and OT is fading, introducing serious security risks:

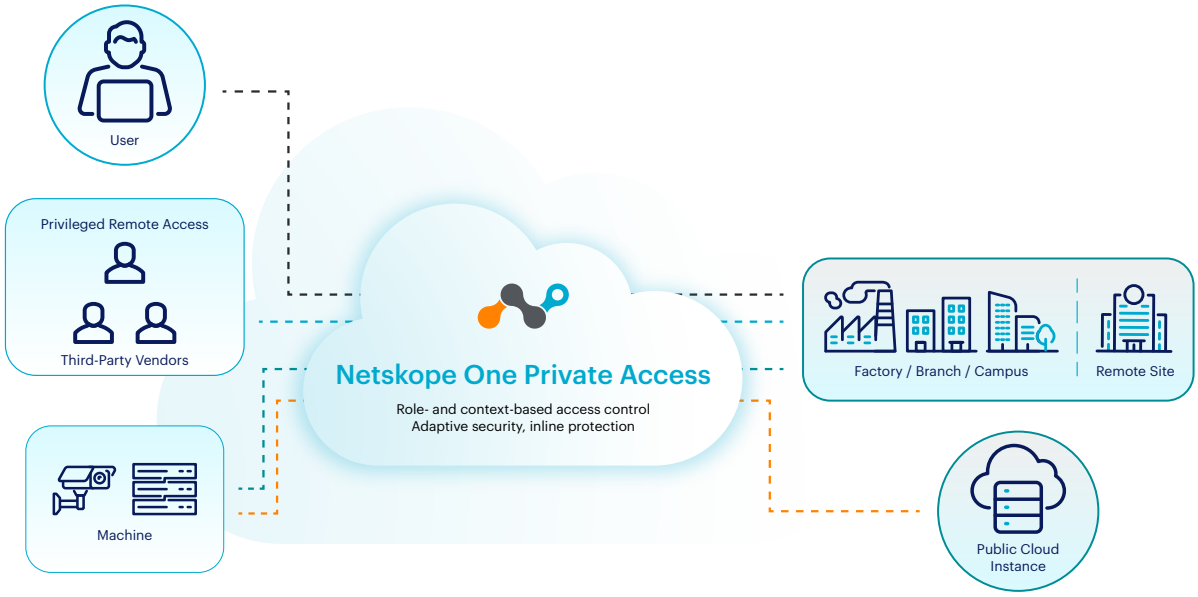
- Most OT devices lack centralized management, monitoring, or update mechanisms.
- Broad, unsegmented access and unsecured external connections increase the attack surface.
- Latency issues disrupt real-time operations, while limited user-level control hinders compliance and response.

Organizations need a modern Zero Trust approach to deliver adaptive, granular access, while preserving uptime, safety, and operational continuity.

The Solution

Netskope One Private Access delivers zero trust network access (ZTNA) purpose-built for OT and IIoT environments with continuous, adaptive, and context-aware policy enforcement. It replaces legacy VPNs by providing secure access to critical systems, without exposing the network, through policies based on user identity, device posture, location, activity, behavior, threat intelligence, and data risk.

Built for high availability and low latency, it ensures secure, reliable access to critical OT systems like supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), or human-machine interfaces (HMIs), supporting uptime, safety, and compliance with simplified operations and real-time visibility.



Unified, Secure Access for OT and IIoT Environments

Secured control access and privileged access control (PAM)

Netskope One Private Access uses a zero trust model to ensure that only the right users, under the right conditions, can access critical OT environments, while enabling secure operations at scale in industries where availability and safety are non-negotiable.

With built-in support for browser-based, agentless access to web, RDP, and SSH, Netskope enables secure remote control for internal operators, third-party vendors, and contractors, all without exposing underlying infrastructure. A user portal provides visibility into authorized applications and leads to a seamless user experience. For environments requiring greater endpoint control, Netskope One Enterprise Browser provides in-session protections such as restricting screenshots, file download, watermark, and print functions to safeguard sensitive interfaces and reduce insider risk during remote operations.

In addition to standard remote access, Netskope One Private Access supports key privileged access management (PAM) use cases, including credential injection via vault integration, session recording for compliance, and data protection controls for sensitive OT systems. These capabilities help organizations enforce least-privilege access, eliminate password risks, and meet audit requirements, without disrupting industrial workflows.

Supported scenarios:

- **User-to-machine**: The most common OT remote access scenario typically involves internal users, contractors, or third-party vendors connecting to industrial systems for maintenance, monitoring, or support.
- **Machine-to-machine**: Communication between OT devices, systems, or services across environments (e.g., IoT gateway to cloud analytics, HMI to backend, sensor to PLC).
- **Machine-to-cloud**: When OT/IIoT systems upload telemetry or receive commands from cloud platforms.

Enforce secure control and privileged access to OT systems with zero trust, session protection, and in-browser controls.

Consistent zero trust policy enforcement across all OT environments

Modern OT and IIoT environments require more than perimeter-based controls. Organizations need granular, identity-aware policies that adapt to risk and protect critical systems like SCADA, PLCs, and HMIs, regardless of where users or machines connect from.

- **Granular, role- and context-based access control**
  Netskope One Private Access enforces least-privilege access using user identity, device posture, location, activity, behavior, threat intelligence, and data risk context, ensuring both users and devices only access the OT resources necessary for their role or function.
- **Continuous adaptive policies, inline protection, and threat inspection**
  Powered by the Netskope Zero Trust Engine and Device Intelligence, AI/ML-driven discovery and risk scoring dynamically inform access policies, adapting to behavioral risk indicators from both users and machines. If a typically low-risk device (e.g., a camera) begins abnormal activity like SSH attempts, its risk score rises, triggering automated segmentation via Netskope One Private Access. Inline DLP and threat inspection work together to block unauthorized actions, such as copying, downloading, or transferring malicious content, ensuring sensitive OT environments remain protected from both insider misuse and external threats.

Protect OT environments with identity-aware, adaptive zero trust access, AI-driven risk scoring, and inline threat inspection for users and machines.

Boosting uptime and operational continuity

Downtime in OT and IIoT environments can lead to safety risks, production delays, and significant financial loss. Legacy VPNs are not optimized for industrial operations; they often introduce latency, require complex setup, and create single points of failure. Netskope One Private Access ensures secure, seamless remote access to OT systems while maintaining the performance and availability these environments demand.

Agentless, instant access
Netskope One Enterprise Browser enables browser-based access to systems like SCADA, HMIs, and PLCs using RDP or SSH, without endpoint agents or device reboots. This lightweight method allows quick, secure access for field engineers, emergency responders, and remote operators, supporting uptime without added complexity.

Low-latency global access with NewEdge
Netskope's NewEdge infrastructure intelligently routes traffic over the shortest latency path to deliver fast, reliable access to globally distributed industrial sites. This eliminates the bottlenecks and backhauling associated with traditional VPNs, ensuring operations remain efficient and uninterrupted.

High availability and centralized visibility
A cloud-native architecture ensures built-in redundancy and scalability for 24/7 operations, backed by enterprise-grade SLAs. Centralized policies and real-time telemetry provide consistent enforcement and visibility across HQ, remote sites, and third-party access, while protecting sensitive OT interfaces.

Together, these capabilities help maintain operational continuity and reduce downtime risks across industrial environments.

Strengthening compliance and audit readiness

Industrial organizations must meet strict compliance standards, such as the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), the International Electrotechnical Commission 62443 (IEC 62443) standards for industrial cybersecurity, and the National Institute of Standards and Technology (NIST) guidelines, while ensuring secure, well-governed access to critical OT systems. Netskope One Private Access supports these requirements with built-in capabilities for session visibility, access traceability, and centralized policy enforcement across internal users, third-party vendors, and remote sites.

- **Privileged session recording**
  Capture and store full session activity for high-risk users and contractors accessing sensitive OT systems. This supports forensic analysis, audit readiness, and regulatory reporting.
- **Detailed access logging**
  Maintain a full record of who accessed which systems, when, and from where, including session duration, user identity, accessed systems, and injected credentials. These logs support zero trust verification and can be easily retrieved for audits or investigations.

With these capabilities, organizations can confidently meet compliance demands while maintaining operational flexibility in their OT environments.

BENEFITS	DESCRIPTION
Zero trust access to OT systems	Secure remote access to OT/IIoT systems, like SCADA, PLCs, and HMIs, without VPNs, ensuring least-privilege access everywhere.
Continuous adaptive, risk-aware policy control	Enforce dynamic access policies using AI-driven risk scoring and behavior analysis to mitigate threats in real time.
Agentless access	Provide fast, secure browser-based access for contractors, vendors, or emergency responders; no agent deployment required.
Compliance-ready controls	Streamline audit readiness with detailed logging, session recording, and policy controls aligned with NERC, IEC, and NIST.
Secure credential injection	Reduce credential risk through vault-based injection and session-level logging, enforcing secure, passwordless access.
Centralized visibility & management	Unify policy enforcement and monitoring across sites with centralized controls that simplify governance and reduce overhead.
Low-latency global access	Improve user experience and system performance by eliminating VPN bottlenecks with direct, optimized access through NewEdge.
Built-in high availability	Ensure business continuity with a resilient, cloud-native architecture that supports 24/7 uptime, even during disruptions.

10/25 SB-903-2