Zscaler Privileged Remote Access for OT and IT Systems

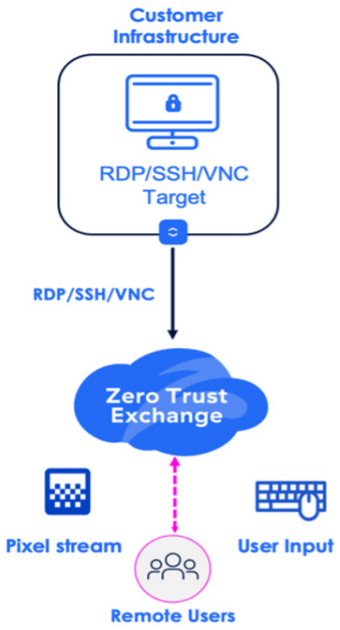
DATASHEET

FAST, DIRECT, SECURE ACCESS TO INDUSTRIAL SYSTEMS AND DEVICES

Zscaler Privileged Remote Access enables fast, direct, and secure access to operational technology (OT), Information Technology (IT), and industrial Internet of Things (IIoT) assets in field locations, the factory floor, or anywhere without relying on VPNs or agents.

Industrial environments now face heightened risks as increasing connectivity across IT, OT, and IIoT systems leaves critical assets exposed to cyberattacks, downtime, and safety threats. Traditional network security methods are no longer sufficient for today's interconnected operations. Organizations need fast, secure, and granular access to all their IT, OT, and IIoT assets without relying on outdated VPNs or legacy PAM solutions. Zscaler Privileged Remote Access enables seamless, zero trust connectivity—offering secure, direct access to privileged systems anywhere, while safeguarding people, operations, and infrastructure.

Zscaler Privileged Remote Access



Key Capabilities

- **Clientless Browser-Based Access:** Enable third-parties and remote technicians to securely connect to RDP/SSH/VNC targets through any browser.
- **Time-bound access:** Access during an allotted window of time including business working hours constraints.
- **Credential Vault and Mapping:** Store shared/privileged credentials of target systems in the Cloud Vault. Perform secret-less brokering using credential map policies.
- **Session proctoring, recording and playback:** Ushered access with control and transfer along with on-screen activity recording.

©2025 Zscaler, Inc. All rights reserved.

Security Challenges for IT and OT Assets

1. Expanded Attack Surface

Traditional access methods—like VPNs and open ports—expose IT and OT assets to ransomware, credential theft, DDoS and data breaches, especially when security patches are delayed or incomplete.

2. Lateral Threat Movement

Legacy solutions lack effective session isolation and least privilege enforcement, enabling broad user access and increasing the risk of lateral movement within sensitive environments.

3. Operational Complexity and Poor Scalability

Managing VPNs, jump servers, and various policies across distributed sites creates high overhead for IT and OT teams, hampering agility and user experience.

4. Lack of Governance Controls

Unmanaged devices and limited session auditing make it difficult to monitor access, enforce policy, and detect threats in real time, undermining compliance and security

BENEFITS

Boost uptime and lower risk

Provide quick, secure access for vendors and partners to systems and equipment, reducing downtime and risk

Enhance safety and security

Make critical networks invisible to the internet, lowering cyberattack risks

Deliver an exceptional user experience

Give remote users fast, hassle-free access to resources—no traditional VPN required.

Accelerate IT/OT convergence

Apply zero trust security across IT, OT, and IoT/IIoT to support digital transformation.

Zscaler Privilege Remote Access (PRA)

Zscaler Privileged Remote Access delivers modern Privileged Access Management for both IT and OT environments, enabling secure, zero trust access to critical systems, applications, and devices—wherever they reside. PRA enables clientless browser-based access for employees, vendors and contractors with complete governance controls and sandboxed file transfers, eliminating the risk of malware infections from unmanaged endpoints.

For thick-client applications, PRA also supports on-demand cloud-based disposable jump boxes that eliminate the need for persistent infrastructure that attackers could use to compromise your critical systems.

With granular controls and full session visibility, organizations can extend seamless, clientless access to remote workers and third-party vendors without increasing exposure or operational complexity. By isolating IT, OT, and IIoT critical assets and delivering robust auditing for all privileged activities, Zscaler's PRA Privileged Remote Access not only streamlines administration but also strengthens an organization's overall security posture.

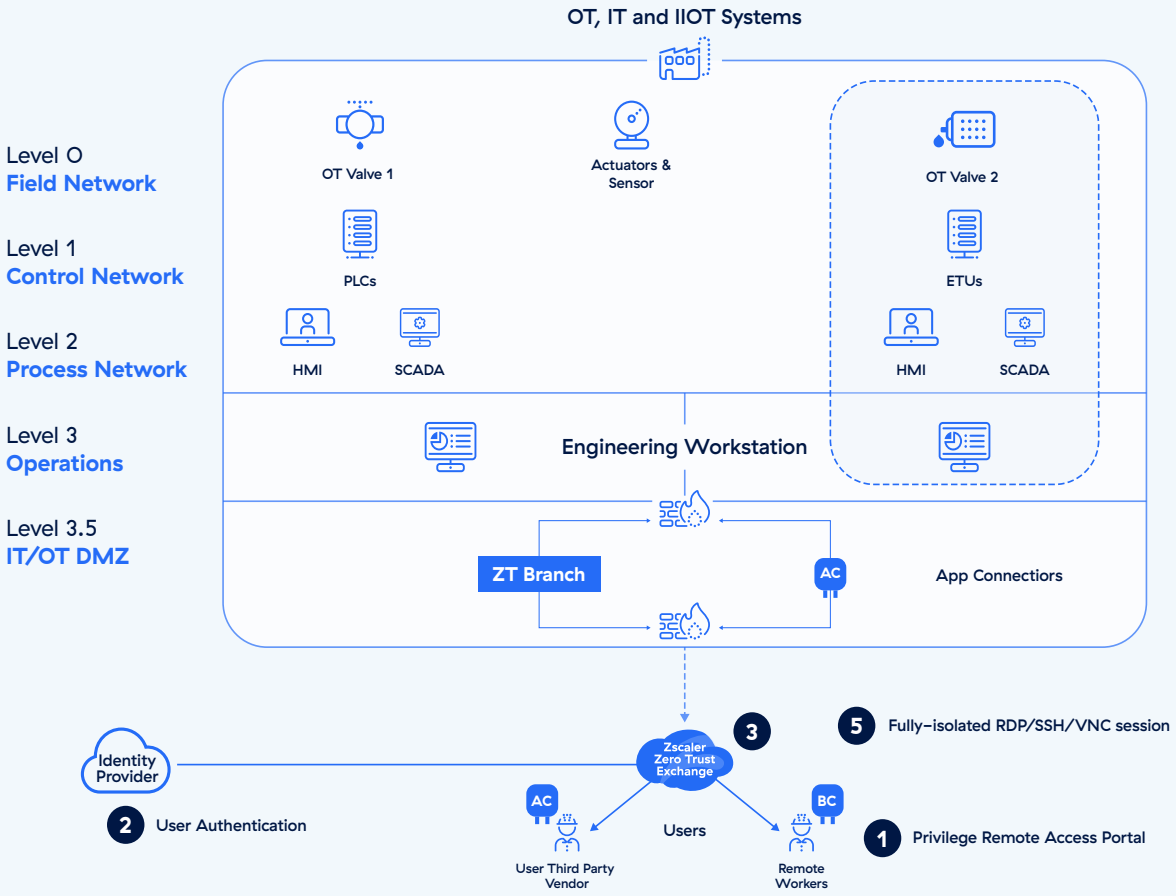
How does Privilege Remote Access (PRA) work?

Privileged remote access tightly controls and monitors how users with elevated permissions connect to critical IT and OT systems. Unlike broad remote access, it enforces granular permissions based on user roles, ensuring

©2025 Zscaler, Inc. All rights reserved.

that only authorized individuals can interact with sensitive data and systems—minimizing insider threats and external breaches. Identity verification through multifactor authentication (MFA) is required before access is granted, and all activities are logged and monitored in real time to create a comprehensive audit trail.

Integrating privileged remote access with a zero trust architecture further enhances security. With zero trust, no user is trusted by default, regardless of their location on the network. Continuous authentication, session monitoring, and dynamic access controls ensure elevated access is granted only when needed and revoked immediately afterward, effectively reducing attack surfaces and limiting the impact of compromised credentials.



1. User logs onto the Privileged Remote Access Portal from any HTML5-capable browser (ex. Chrome, Safari, Edge).
2. The user is authenticated and authorized via the configured SAML/OIDC Identity Provider and sees the authorized consoles in the Portal.
3. The user session is routed to the nearest ZPA Service Edge, which is part of the Zero Trust Exchange.
4. Zscaler App Connector, deployed in the OT environment, initiates an outbound connection to the Zscaler Zero Trust Exchange — no need to expose SSH/RDP/VNC ports outside the network.
5. The user requests an isolated SSH/RDP/VNC session to an OT system. The Zscaler Exchange brokers the connection between the user's console and the corresponding App Connector, according to the user's security and access policies.

The SSH/RDP/VNC connection is initiated between the App Connector and the OT system and pixel-streamed to the user's console session. This eliminates the need for a network connection between the OT system and the remote technician.

©2025 Zscaler, Inc. All rights reserved.

Core Capabilities

Clientless access over HTML5-capable browsers	Connect internal and external users to RDP, SSH and VNC target systems with full isolation, allowing users to connect from unmanaged endpoints and untrusted networks. Enable third-party users to access data securely while blocking data from being copied, pasted, uploaded from or downloaded to their local unmanaged device.
Fully isolated, client- less RDP, SSH, RealVNC and VNC sessions	Allow third-party users to access OT systems from any HTML5-capable browser without the need to install a client or connect through VPN on unmanaged devices.
Clientless access for thick client applications with disposable jump boxes	Enable thick client app access through the browser with dynamic disposable jump boxes instances in a public cloud launched based on user requests, providing just-in-time access to applications.
No network changes	Allow access to systems across multiple sites—even with overlapping IP addresses—without the need for manual and expensive network address translation. Constant firewall changes are also avoided since there is only one outbound connection from the plant floor.
Zero attack surface	OT systems are hidden from the internet and unauthorized users by creating a secure segment of one between an authorized user to a specific device. Remove all inbound connectivity to the OT network.
User identity based OT access	Continuously validate access policies based on user, device, content, and application risk posture with a powerful native policy engine to ensure only valid, authenticated users can access production systems.
Time-Bound Access	Limit access to specific systems and devices for a specific timeframe. Add time-of-day and day-of-week to further limit working hours. Avoid over-provisioned standing access.
Just in Time User Provisioning for Emergency Access	Reduce the burden of provisioning, maintaining and de-provisioning third-party users for emergency access.

©2025 Zscaler, Inc. All rights reserved.

Credentials vaulting	Securely store credentials for access to RDP, SSH or VNC systems in the Zscaler vault. Map users with SAML identities and inject the OT system credentials into target systems using different criteria and avoid sharing OT system credentials with 3rd parties.
Credential Pooling	Allow dynamic management of windows login credentials at run-time in Privileged Credential Policy to ensure multiplexing of user credentials with full attribution. Attribution of shared credentials usage within a time-window for concurrent access of windows terminal services.
Inline A/V and advanced cloud sandboxing for file transfers	Stop ransomware and malware with the inline A/V scans and advanced cloud sandbox detonation of files transferred to the target systems.
Session Recording & Streaming Playback	Save tamper-proof recordings in the cloud with data sovereignty controls. Stream recordings on-demand with role-based access controls.
Session Monitoring	Monitor live PRA sessions to supervise vendor technicians and minimize plant risk. Instantly terminate the session to stop accidental or malicious disruptions.
Ushered Access	Host shared PRA sessions with technicians using screen sharing and mouse+keyboard controls.
Micro Tenants	Delegated admin access to sub-tenants providing fine-grained, role-based access controls.
Fully managed DNS C-name and certs for portals	Zscaler Managed DNS and certificate for Portals without user having to provide custom certificate and configure DNS while registering Portals.

©2025 Zscaler, Inc. All rights reserved.

Licensing

Pricing Model:

- Pricing is based on the number of unique OT and IT applications (RDP, SSH, or VNC targets) secured.

Included Capabilities:

- Standard PRA features include full protocol isolation for SSH, RDP, RealVNC, and VNC.
- Standard PRA also includes Clipboard controls (text copy/paste), sandboxed file transfer with Advanced Cloud Sandbox, and just-in-time/time-bound access are included in ZPA Business Edition, ZPA Transformation, and ZPA Unlimited Editions.
- Standard PRA Entitlement is limited to a total of 10 target systems per ZPA tenant
- Inline cloud sandboxing requires a Zscaler Internet Access tenant with Advanced Cloud Sandboxing functionality.

Add-Ons & Limitations:

- Disposable Jump Boxes are available as an add-on and requirePRA Advanced licensing.

System & Consumption Entitlements:

- For every 10 PRA systems (defined as RDP, SSH, or VNC Privileged Consoles), entitlement includes 1 pair of App Connectors.
- There is a fair use limit: 10 GB of data usage per system per month, pooled across the ZPA tenant.

Technical Specifications

Zscaler Component	Supported Platforms & Systems
Privileged Remote Access	Target systems: Windows — RDP, RealVNC or VNC, Linux/Unix — SSH or RealVNC OIDC/SAML IdP — ZIdentity, Microsoft Azure or Okta1
App Connector	VMware vSphere Hypervisor Docker container for arm64 and amd64 platforms Zscaler Branch Device

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Experience your world, secured.™