Data Sheet

Zscaler Privileged Remote Access for OT and IIoT Security

Fast, direct, secure access to industrial systems and devices

Zscaler Privileged Remote Access enables fast, direct, and secure access to operational technology (OT) and industrial Internet of Things (IIoT) assets from field locations, the factory floor, or anywhere.

Maximizing Plant Productivity and Minimizing Vendor/Contractor Risk

Remote access is a key technology that enables production monitoring and predictive maintenance in smart factories. By granting remote workers and third-party vendors the ability to connect to production/field assets and view machine data, they can monitor, troubleshoot, and repair equipment in real-time for maximum plant uptime and efficiency.

Remote users have historically connected to industrial assets through virtual private networks (VPNs), but VPNs are cumbersome to manage and have inherent security flaws. Legacy remote access approaches using VPNs can be easily circumvented by attackers taking advantage of the inherent trust and overly permissive access of traditional castle-and-moat architectures, including:

- **Traditional OT environments are at risk of disruption from expanded attack surfaces:** Attackers can see and exploit vulnerable,

Benefits:

- **Boost uptime and productivity**
  Direct connectivity with inline zero trust security makes it fast for users to connect to and repair equipment, minimizing downtime
- **Increase plant and people safety**
  Makes OT networks and systems invisible to the internet so bad actors cannot find/exploit it to disrupt production processes
- **Give users an exceptional experience**
  Provides easy access for remote workers and third-parties without the friction of conventional VPN
- **Accelerate OT/IT convergence**
  Extend zero trust security to OT and IIoT to accelerate industry 4.0 initiatives

externally exposed OT assets. Most OT systems are unpatchable, don't get patches from vendors as often as they should, and do not have sufficient downtime for constant patches.

- **Legacy architecture can't scale or deliver fast, seamless user experiences:** VPNs also have high operational overhead since they typically require inbound ports which means constant firewall changes to limit user access. VPNs are sometimes used in conjunction with traditional appliance based privileged access management (PAM) products adding more layers of complexity without providing much protection from ransomware.
- **Lack of least-privileged access allows free lateral movement:** VPNs put users on your network, giving attackers easy access to critical OT assets. VPNs bring the user's unmanaged endpoints directly to the OT network, increasing the risk of ransomware and malware into the production floor.

These cyberthreats can ultimately cause downtime and potentially pose a physical safety risk to plant workers and equipment. With VPN security flaws and ransomware attacks directly affecting revenue, OT operators are looking to zero trust security as a safe and reliable alternative to VPNs.

Zscaler Privileged Remote Access

Zscaler Privileged Remote Access is a cloud-delivered zero trust access solution that enables fast, secure, and reliable connectivity to OT and IIoT devices from field locations, the factory floor—or anywhere. Privileged Remote Access enabled by the ZPA platform, provides remote workers and third-party vendors with clientless remote desktop access to sensitive RDP, SSH and VNC production systems without having to install a client on unmanaged devices or log into jump hosts and VPNs. As the industry's only zero trust-based access solution for OT and IIoT, Zscaler Privileged Remote Access:

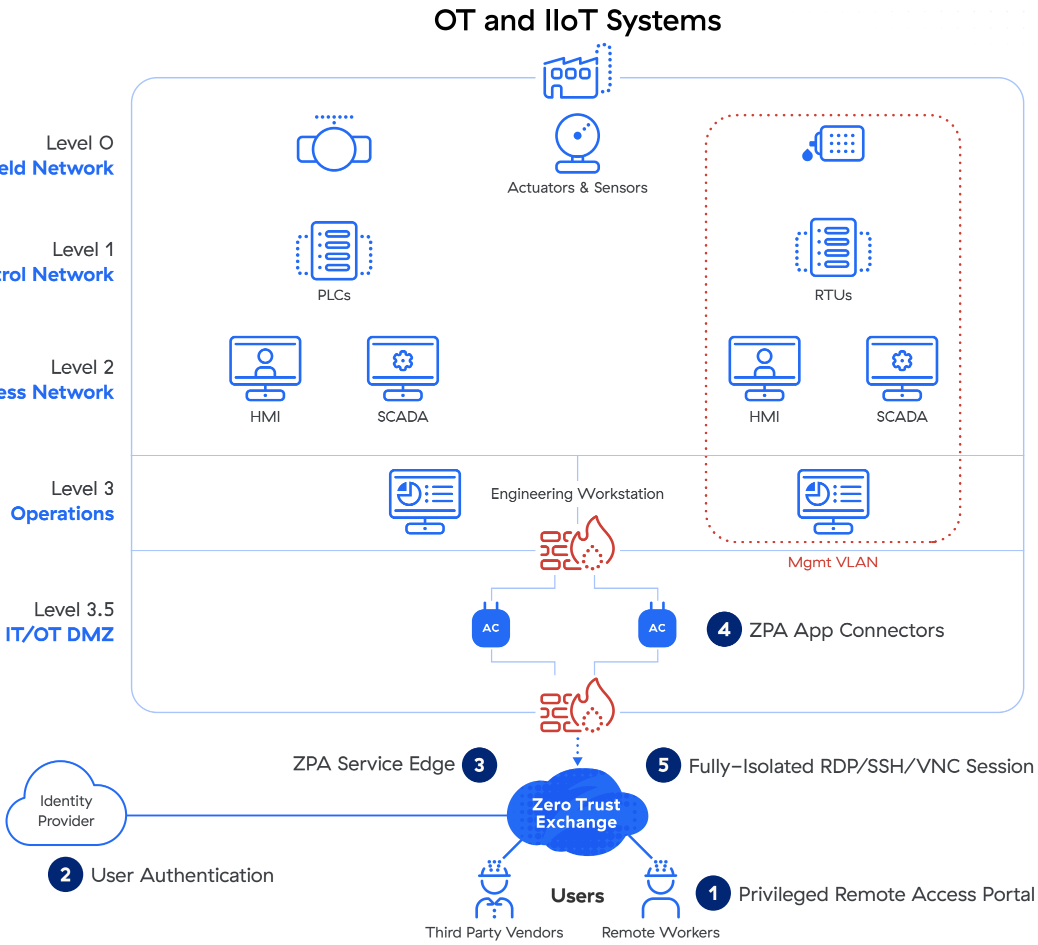
Boosts uptime and productivity
Direct connectivity with inline zero trust security makes it fast for users to connect to and repair equipment, minimizing downtime and eliminating slow, costly backhauling over legacy VPNs and PAM products.

Increases plant and people safety
OT networks and systems are hidden from the internet through inside-out connections, so assets cannot be discovered or exploited by bad actors seeking to disrupt production processes.

Delivers an exceptional user experience
Clientless access from users' web browsers makes it easy for remote workers and third-party vendors and contractors to access OT systems without the friction of conventional VPN.

A unified platform for secure access across apps, workloads, and OT devices

Extend zero trust across private apps, workloads, and OT/IIoT devices to simplify and integrate multiple disjointed remote access tools, unifying security and access policies to stop breaches and reduce operational complexity.



1. From any HTML5-capable web browser like Chrome, Safari or Microsoft Edge, the user goes to the Zscaler Privileged Remote Access Portal.

2. The user logs in with their credentials and is authenticated to the SAML Identity Provider. The Portal displays only the consoles that the user is authorized to access.

3. The user requests a fully isolated RDP/SSH/VNC session. The Portal forwards the user's traffic to the closest ZPA Service Edge, which acts as a broker, where the user's security and access policies are checked and enforced.

4. Next, the ZPA Service Edge determines the application in closest proximity to the user and establishes a secure connection to a ZPA App Connector, a lightweight virtual machine or Docker container installed in the OT environment that hosts your RDP/SSH/VNC OT targets/servers.

5. The RDP/SSH/VNC sessions are terminated at the App Connector and converted to HTML5 streams which are made available to the ZPA Service Edge to stitch back to the user's session.

6 The user enters the credentials – either username/password or username/private key to authenticate with the OT target/system. If a matching Privileged Credential Policy is configured for the user and/or target OT system, the credential is automatically injected.

7 During a session, the user can upload or download files if a Privileged Capability Policy is configured for the user and/or target OT system. Uploaded files can be sent to the Zscaler Advanced Cloud Sandbox for inspection. These files will only reach the target OT system if the Sandbox gives a benign verdict. If the Sandbox flags the file as malicious, the user gets an error that the file didnt pass inspection.

8 Finally, once a connection is brokered between the user's device and the OT targets, the user interacts with the fully isolated remote session via keyboard and mouse, or trackpad.

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, clientless RDP, SSH 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.
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.
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.
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.

Foundational Components

Zscaler Clientless Access
Users can securely connect to OT devices via integrated browser-based access (RDP, SSH or VNC) for clientless access from unmanaged devices.

Zscaler Client Connector
Client Connector is a lightweight application that runs on users' laptops and mobile devices that automatically forwards user traffic to the closest Zscaler Service Edge, ensuring that security and access policies are enforced across all devices, locations, and applications.

ZPA App Connector
App Connectors are lightweight virtual machines that sit in front of private applications deployed in the data center or public cloud, brokering security connectivity between an authorized user and a named app with an inside out connection that doesn't expose apps to the internet.

ZPA Service Edges
Service Edges enforce security and access policies, stitching together the inside-out connection between an authorized user (via Client Connector and agentless access) and a specific private application (via the App Connector). Most customers leverage our Public Server Edges, which are hosted in over 150 exchanges around the world, and handle millions of concurrent users for the world's largest organizations. Private Service Edges, managed by Zscaler, are also available to be hosted at the customer site for providing on-prem users with the shortest-path access to on-prem applications without leaving the local network.

Licensing

A standalone Zscaler Privileged Remote Access plan license is required to access all capabilities. Pricing is based on the number of OT systems or the number of unique OT applications – RDP, SSH or VNC targets. Basic Privileged Remote Access capabilities are included in the user editions of Zscaler Private Access Clientless, Business and Transformation Editions (FY23 or later), limited to a maximum of 10 target systems or devices. Additional licenses can be purchased for advanced functionality and to expand capacity. Inline cloud sandboxing requires a Zscaler Internet Access tenant with the Advanced Cloud Sandboxing functionality.

> **42% of respondents indicate that their control systems had direct connectivity to the internet in 2021.**
>
> Source: SANS, 2021 Survey: OT/ICS Cybersecurity

Technical Specifications

Zscaler Component	Supported Platforms & Systems
Privileged Remote Access	Windows (RDP or VNC), Linux/Unix (SSH or VNC) SAML Identity Provider (Microsoft Azure AD or Okta)
App Connector	Docker container for arm64 and amd64 platforms VMware vCenter or vSphere Hypervisor

Why Adopt Zero Trust Security for OT and IIoT?

Historically, OT environments have been air-gapped or physically isolated from the outside world. As they become more digitalized and connected to the internet, they become more susceptible to malware, ransomware, and supply chain attacks, which can cause disruptions and put workers at risk. It is no longer sufficient to protect OT assets from compromise with traditional perimeter security measures such as firewalls and VPNs. Zero trust is key to preventing unplanned downtime and ensuring maximum productivity in industrial systems. Zero trust:

- **Minimizes the attack surface:** Make OT and IIoT systems invisible by establishing inside-out connections from devices to users. IP addresses are never exposed to the internet, creating a "darknet" that is impossible for bad actors to discover and exploit.
- **Eliminates lateral movement:** Once a user is authorized, access is granted on a one-to-one basis rather than full access to the OT network. Users are never put directly on the network where they could access and compromise assets outside of their privileges.
- **Accelerate OT/IT convergence:** Classic IT security playbooks that rely on patch management and castle-moat-security do not work for OT. Minimize the risk of active attacks and exploits targeted at out-of-date or unpatchable assets.

zscaler™ | Experience your world, secured.™