DATA SHEET

Zscaler Privileged Remote Access for OT and IIoT Systems

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 in field locations, the factory floor, or anywhere without relying on VPNs or agents.

Maximizing Plant Productivity and Minimizing Risks from Vendors/Contractors

Remote access is critical to production monitoring and predictive maintenance in smart factories. Field technicians and third-party vendors need to remotely connect to production/field assets and view machine data, in order to 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.

OT Security Challenges

- **Traditional OT environments are at risk of disruption from ransomware attacks:** attackers can see and exploit vulnerable, externally exposed OT assets. Most OT systems don't get

Benefits

- **Boost uptime and lower risk**
  Zero trust connectivity enables vendors/contractors to quickly connect to and repair equipment, minimizing downtime and risk
- **Increase plant and people safety**
  Make OT networks and systems invisible to the internet so bad actors cannot find/exploit it to disrupt production processes
- **Give users an exceptional experience**
  Provide easy access to remote workers and third-parties without the friction of conventional VPNs
- **Accelerate OT/IT convergence**
  Extend zero trust security to OT and IIoT to accelerate industry 4.0 initiatives

©2024 Zscaler, Inc. All rights reserved.

security patches from vendors as often as they should, and do not have sufficient downtime for regular updates.

- **VPNs have high operational overhead:** 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 bring the user's unmanaged endpoints directly to the OT network, increasing the risk of ransomware and malware into the production floor.
- **Legacy architecture can't scale or deliver fast, seamless user experiences:** VPN clients are cumbersome, slow and often conflict with each other, requiring remote technicians to juggle multiple laptops or make expensive site visits in order to access different OT equipment.

These challenges can ultimately cause plant downtime and potentially pose a physical safety risk to plant workers and equipment. 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.

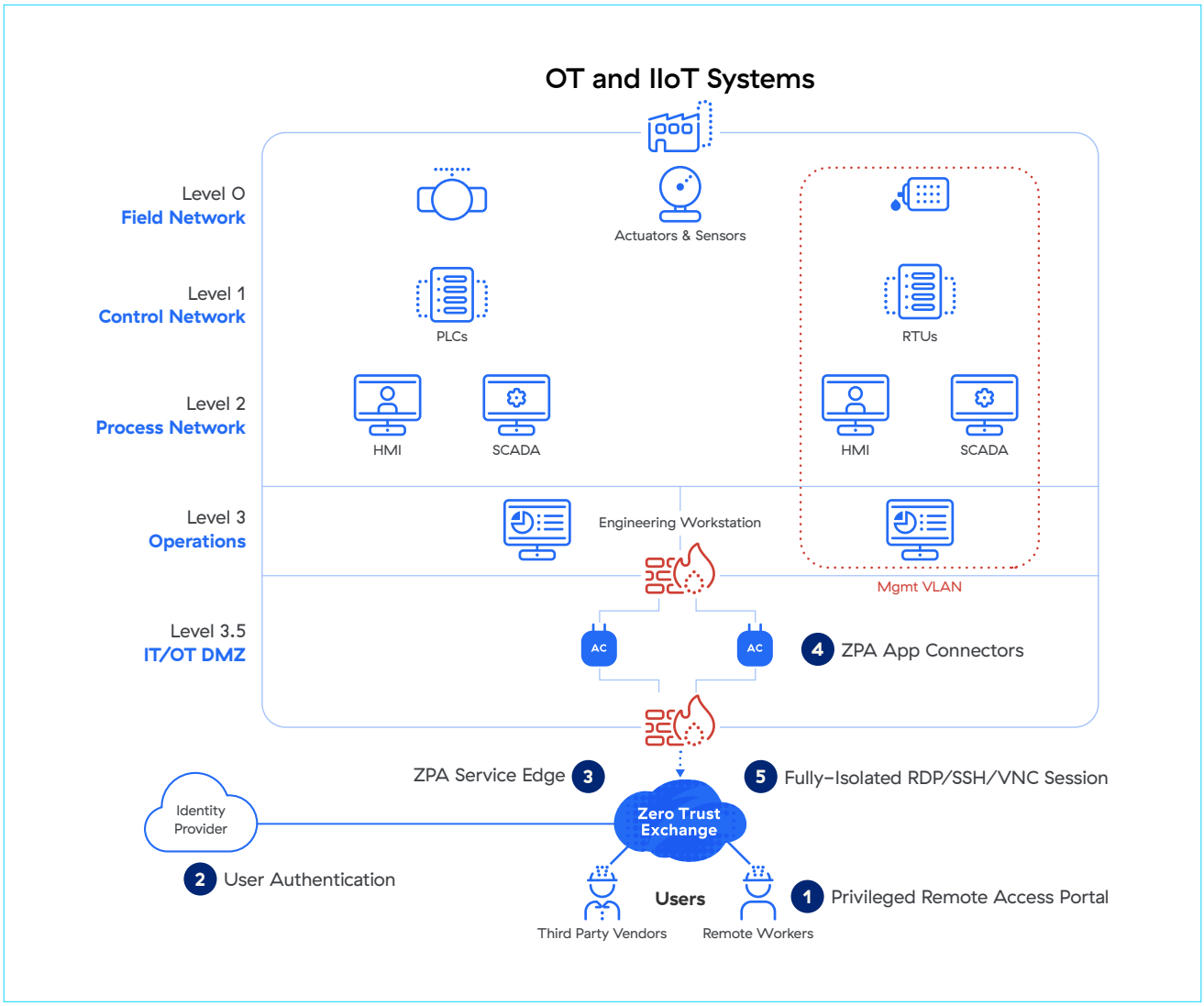
Delivers an exceptional user experience
Clientless access from users' web browsers makes it easy for remote workers and third-party vendors and contractors to access OT systems without the friction of conventional VPN.

Reduces risk with governance controls
Cloud-based session recording, streaming playback, session monitoring and ushered access ensure full supervision and control over third-party remote access sessions.

©2024 Zscaler, Inc. All rights reserved.

How it Works

Privileged Remote Access enables administrators, remote technicians, vendors and contractors to securely access OT/IIoT systems without requiring VPNs or endpoint agents with full cyber threat protection and operational safeguards.



1. User logs onto the Privileged Remote Access Portal from any HTML5-capable browser (ex. Chrome, Safari, Edge).
2. User is authenticated and authorized via the configured SAML/OIDC Identity Provider and sees the authorized consoles in the Portal.
3. User session is routed to the nearest ZPA Service Edge, which is part of the Zero Trust Exchange.

©2024 Zscaler, Inc. All rights reserved.

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 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.

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.

©2024 Zscaler, Inc. All rights reserved.

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.
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

©2024 Zscaler, Inc. All rights reserved.

Licensing

Pricing is based on the number of unique OT applications – RDP, SSH or VNC targets.

Solution Capabilities	PRA Essentials	PRA Advanced
	Entitlement: 1 pair of App Connectors for every 10 PRA systems/consoles. Fair Use limit: 10 GB data usage /system/month pooled across the ZPA tenant. A system is defined as RDP,SSH or VNC Privileged Console	
Full protocol isolation for SSH, RDP and VNC	✓	✓
Interactive authentication	✓	✓
Clipboard controls (text copy and paste)	✓	✓
Sandboxed file transfer with Advanced Cloud Sandbox[1]	✓	✓
Just-in-time/Time-bound access	✓	✓
Credential vaulting & injection		✓
Emergency access		✓
Cloud session recording & playback		✓
Session monitoring		✓
Ushered access		✓

1. Requires ZIA tenant with Advanced Cloud Sandbox.
2. Emergency users not counted towards ZPA user license count. Quarterly active unique Emergency users not to exceed ZPA platform user count.
3. Session recording stored in the cloud for 365 days (Includes 10 hours recording/system/month pooled across entire tenant).

PRA Essentials is included as part of ZPA Business Edition and PRA Advanced is included as part of ZPA Transformation and Unlimited Editions, limited to a total of 10 target systems. Additional licenses can be purchased to expand capacity. Inline cloud sandboxing requires a Zscaler Internet Access tenant with the Advanced Cloud Sandboxing functionality.

©2024 Zscaler, Inc. All rights reserved.

Technical Specifications

Zscaler Component	Supported Platforms & Systems
Privileged Remote Access	Target systems: Windows — RDP or VNC, Linux/Unix — SSH or VNC OIDC/SAML IdP — ZIdentity, Microsoft Azure or Okta[1]
App Connector	VMware vSphere Hypervisor Docker container for arm64 and amd64 platforms Zscaler Branch Connector Device

1. Emergency access is supported with Okta only.

Zero Trust Security Benefits for OT and IIoT

Historically, OT environments have been physically isolated from the outside world. As they become more digitized 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.

- **Minimize the attack surface:** Make OT and IIoT systems invisible to attackers by eliminating the need for exposed ports.
- **Eliminate lateral movement:** Users and OT systems are never connected on the same network, preventing the spread of malware and ransomware attacks.
- **Accelerate OT/IT convergence:** Safely connect and maintain OT systems while retaining the speed and agility of remote management.

zscaler™ | Experience your world, secured.™

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ 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