zscaler™ | SIEMENS

Partner Brief

Zscaler and Siemens

Delivering an Integrated Zero Trust Access Solution to Protect OT Networks

Maximizing plant productivity and minimizing third-party risk with zero trust

Secure and needs-based remote access is a key technology that enables production monitoring and predictive maintenance in smart factories. The ability to securely connect to production and field assets and view machine data enables remote workers and third-party vendors to monitor, troubleshoot, and repair equipment in real time to maximize plant efficiency and uptime.

Whenever users and their devices interact with your production plants, you want to ensure they have only the necessary access to systems and machines. Giving them broad access at the network level exposes your production environment to risks from unauthorized and overprivileged users. By incorporating zero trust principles with cell protection, you can mitigate those risks. Zero trust-based access enables you to grant remote workers and third-party vendors only the access they need to perform their jobs while providing flexible access to equipment. The result is less risk to uptime, availability, and worker safety on the shop floor.

Zscaler and Siemens: Accelerating digital transformation with an integrated zero trust access solution built for OT

Together, Zscaler and Siemens offer an integrated IT-OT access solution that provides fast, secure connectivity to production plants and helps accelerate digital transformation initiatives. The joint solution combines Zscaler Private Access™ for OT, a cloud-delivered zero trust network access service, with SCALANCE LPE, Siemens' flexible local processing platform, to provide convenient clientless access from the user's web browser. There's no need to install a client on an unmanaged device or connect through a jump host and VPN. The joint solution integrates seamlessly with your existing OT network through a lightweight Docker container installed on SCALANCE LPE.

Even Better Together

Zscaler and Siemens have partnered to deliver a holistic and secure IT-OT access solution that applies the principles of zero trust to provide increased protection against cyberattacks in OT environments. The solution:

- Boosts uptime and productivity with direct connectivity for users to connect to and repair equipment
- Increases plant and human safety by making networks and systems invisible to the internet
- Gives users an exceptional experience by providing easy access for remote workers and third parties
- Accelerates OT/IT convergence by extending zero trust security to field locations and the factory floor

Seamless and secure communication between OT and IT

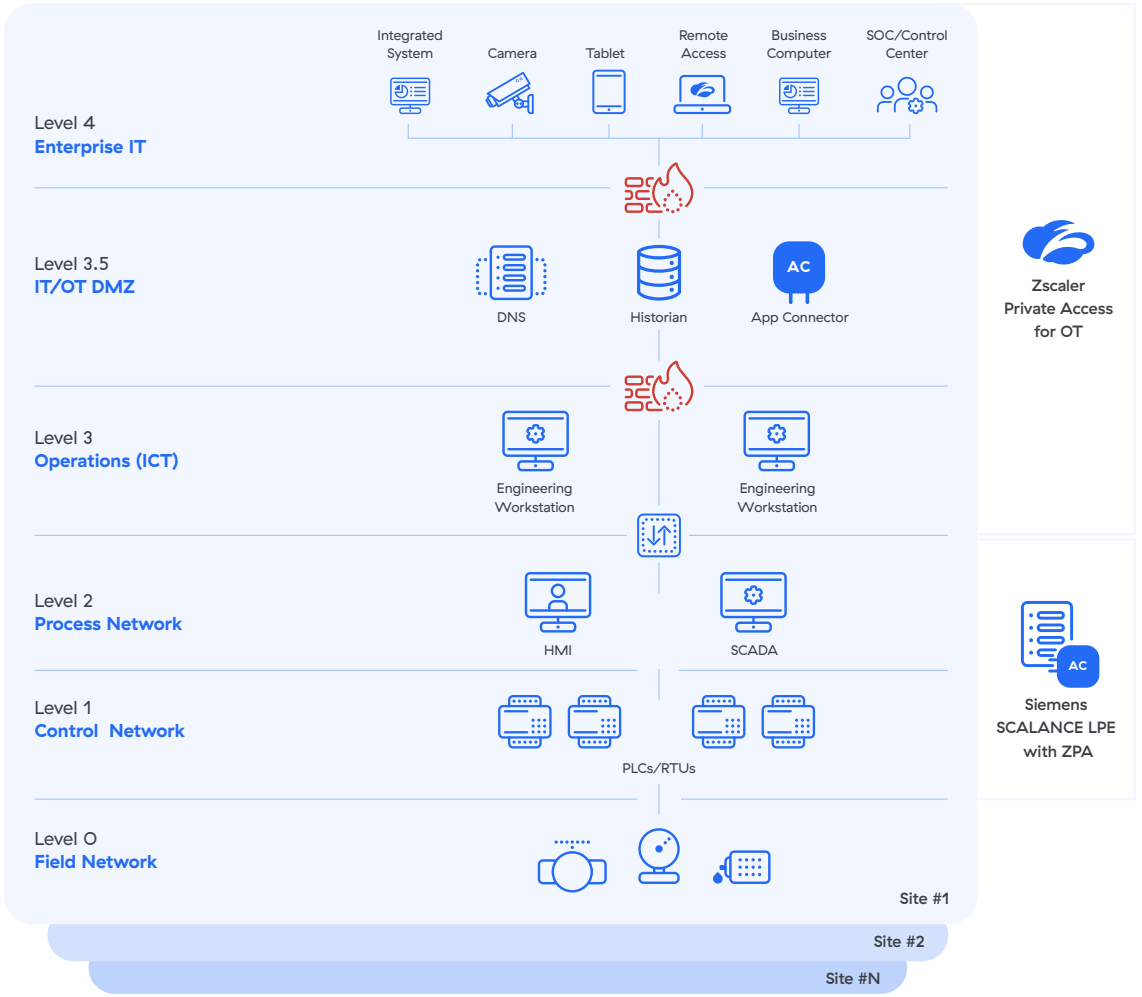

Figure 1: Sample Purdue Model: Zscaler and Siemens deployment architecture

Siemens SCALANCE LPE

As part of the entire offering for Industrial Communication and Networking, the SCALANCE LPE9403 is an industrialized and robust local processing engine with capabilities of running multiple applications (e.g., predictive maintenance or anomaly detection) at the same time in a secure OT environment. Running multiple applications (e.g., based on Docker) on the SCALANCE LPE enables different use cases with remote access that fills the gap between zero trust and traditional OT security concepts.

With SCALANCE LPE, operators can bring software services inside systems securely and flexibly. For integration with existing network infrastructure, SCALANCE LPE offers multiple ways to achieve connectivity and visibility to industrial networks without compromising integrity and security.

Zscaler Private Access for OT

Zscaler Private Access for OT enables fast, direct, and secure access to operational technology (OT) assets from field locations, the factory floor, or anywhere. Remote workers and third-party vendors benefit from convenient and frictionless access from any device or web browser without the need to install a client or log in and out of jump hosts and VPNs.

Zscaler Private Access for OT provides user connectivity based on the zero trust principle of least privilege, granting access on a one-to-one basis from an authorized user to a specific named application, rather than granting full access to the production network. This prevents unauthorized and overprivileged users from moving unchecked across internal OT systems and reduces the risk of bad actors disrupting industrial processes.

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. Zero trust is the key to preventing unplanned downtime and ensuring maximum productivity for industrial systems, enabling you to:

- **Minimize 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's impossible for bad actors to discover and exploit.
- **Eliminate lateral movement:** Grant authorized users one-to-one access to apps, 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:** Don't depend on traditional IT security playbooks that rely on patch management and castle-and-moat security. Zero trust minimizes the risk of attacks and exploits targeting out-of-date or unpatchable assets.

To learn more about how Zscaler and Siemens can help,
reach out to siemens@zscaler.com

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**.

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