PARTNER BRIEF

Zscaler™ and Siemens: Partnering on a Zero Trust Solution to Protect Industrial OT/IoT Networks

zscaler™

The challenge of securing remote access to plants and machines

Operational technology (OT) and industrial control systems (ICS) play a vital role in the supply chain of asset-intensive sectors such as manufacturing, pharmaceuticals, and transportation, to name a few. With the rise in hybrid-remote work, expansion into new distributed locations, and increased demand for widespread industrial digitization, OT/ICS environments are facing new cyber risks.

Monitoring, upgrading, and servicing systems remotely has enabled operations leaders to maximize uptime and reduce costs. OT/ICS, however, has unique requirements and limitations when it comes to remote access. OT personnel have traditionally connected to industrial equipment and systems using remote-access VPNs, but these solutions will inadvertently expand the organization's attack surface and open the door for intruders to exploit trusted access to your networks. To protect OT/ICS environments against cyberattacks, equipment failures, and other threats affecting system performance, the zero trust based approach will be used as secure remote access solution.

Zscaler + Siemens: Combining the best of the industrial automation and cloud security worlds

Together, Zscaler and Siemens strengthen cybersecurity for industrial environments by fusing Zscaler's cloud-delivered zero trust network access service with Siemens's powerful local processing platform. With cloud-delivered security, you can dynamically expand existing systems by running Zscaler's Private Access App Connector as a Docker container on Siemens' SCALANCE LPE local processing engine to provide highly secure access to industrial automation environments via a zero-trust connectivity method. Deployment of secure remote access has never been easier.

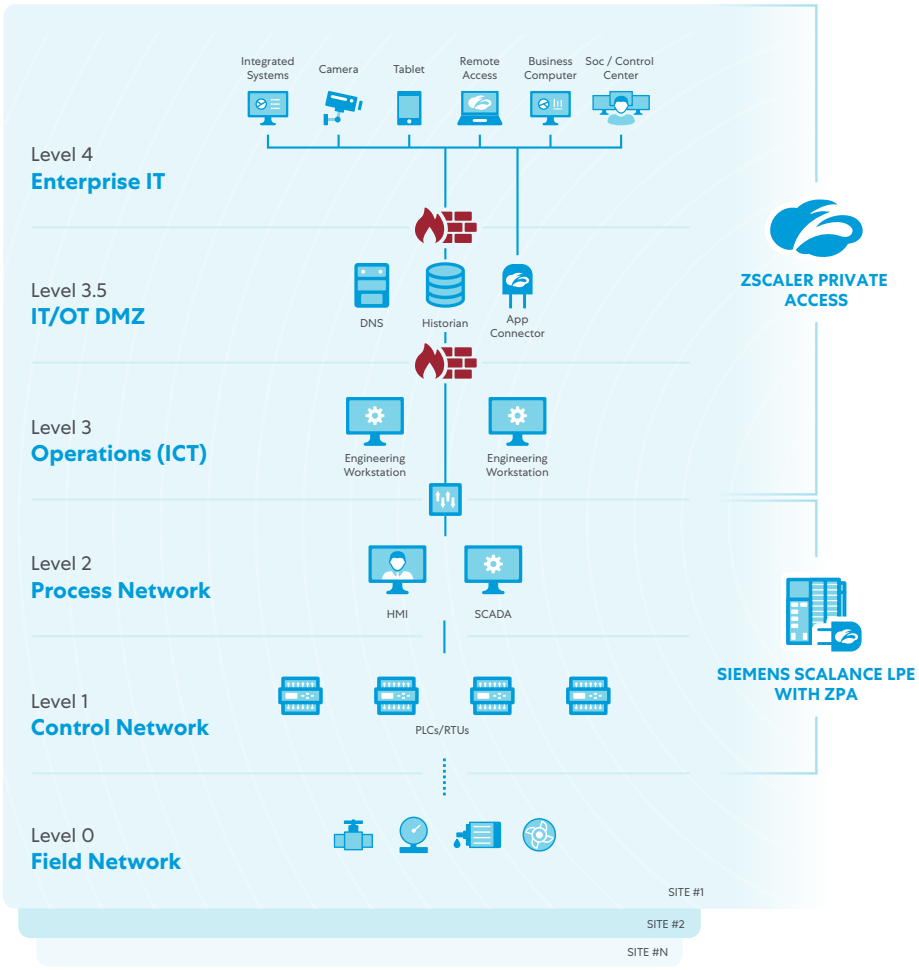
Even Better Together

Zscaler and Siemens have partnered to deliver a modern, zero-trust approach to protect industrial networks against cyber threats and accelerate OT/IT convergence.

- Give employees and third-parties fast, easy and secure remote access to OT/ICS environments
- Boost plant productivity, uptime and security by expanding network connectivity
- Reduce time needed to maintain and repair assets
- Reduce network attack surfaces and limit potential threats from the outside
- Reduce the cost and complexity of traditional network appliances such as VPNs with a fully cloud-delivered secure remote access solution

Seamless and secure communication between OT and IT

Sample Purdue Model: Zscaler and Siemens Deployment Architecture



Siemens

As part of the entire offering for industrial networks including Wireless Communication, Industrial Ethernet, Industrial Security and Industrial Identification and Locating, 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 are able to bring software services inside the systems securely and flexibly. For integration to existing network infrastructure, SCALANCE LPE offers multiple ways to achieve connectivity and visibility to industrial networks without compromising integrity and security.

Zscaler Private Access

Zscaler Private Access (ZPA) enables fast, seamless and secure remote access to your industrial network so employees and third-parties can immediately connect to, monitor, and service assets from anywhere, maximizing uptime and productivity. Using ZPA, authorized users only have access to one application at a time, making lateral movement within a network impossible and reducing the risk of a data breach. The 'air-gap' it creates effectively protects your systems against cyber threats by only connecting users and devices to the specific applications they need without connecting them to your network directly. OT and IT teams never have to worry about users running unchecked across their internal network.

Why adopt zero trust security for the industrial edge?

Historically, OT environments have been physically isolated or air-gapped from the outside world. Today, they are digitized and connected to the internet, making them particularly ripe targets for ransomware and supply chain attacks that have the potential to cause massive operational disruption. The traditional perimeter defense is being challenged. Here's why zero trust is the gold standard for protecting industrial infrastructure against internal and external cyber threats:

- ✓ **Reduces business and operational risk:** You see what's happening on the network and how assets are communicating—whether it's an unauthorized user, a process anomaly or an attacker trying to get in.
- ✓ **Minimizes attack surfaces:** The industrial network becomes invisible to everyone except authorized users, making it unreachable by attackers and providing the best defense for unpatchable assets.
- ✓ **Eliminates excessive trust:** Internal and third-party personnel are only permitted "need-to-know" access to microsegmented systems and applications, resulting in "virtual" air gaps that aren't possible with traditional networks.

To learn more about how Zscaler and Siemens can help, reach out to **siemens@zscaler.com** or **set up time to meet with us →**

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**.

About Siemens
Siemens AG (Berlin and Munich) is a technology company focused on industry, infrastructure, transport, and healthcare. From more resource-efficient factories, resilient supply chains, and smarter buildings and grids, to cleaner and more comfortable transportation as well as advanced healthcare, the company creates technology with purpose adding real value for customers. By combining the real and the digital worlds, Siemens empowers its customers to transform their industries and markets, to transform the everyday for billions of people. Siemens also owns a majority stake in the publicly listed company Siemens Healthineers, a globally leading medical technology provider shaping the future of healthcare. In addition, Siemens holds a minority stake in Siemens Energy, a global leader in the transmission and generation of electrical power. In fiscal 2020, which ended on September 30, 2020, the Siemens Group generated revenue of €55.3 billion and net income of €4.2 billion. As of September 30, 2020, the company had around 293,000 employees worldwide. Further information is available on the Internet at **www.siemens.com.**

Zscaler, Inc. 120 Holger Way | San Jose, CA 95134 | +1 408.533.0288

zscaler™
www.zscaler.com