PARTNER BRIEF

Zscaler™ and Nozomi Networks: Extending Zero Trust Security to the Industrial OT/IoT Edge

zscaler™

The challenge of remote operations and connectivity

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 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 security paradigm needs to shift to a zero-trust based approach.

Zscaler + Nozomi Networks: Modern, Zero-Trust Protection For Your IT and OT Networks

Together, Zscaler and Nozomi Networks provide a fully cloud-delivered joint solution that extends zero trust protection to the edge of your OT/ICS network with a complete set of industrial cybersecurity controls, including remote access, network visibility, threat detection, and operational insights. With Zscaler Private Access, admins can remotely access the full Nozomi Networks solution including Guardian sensors, Vantage cloud-based management console, or the on-premises Central Management Console.

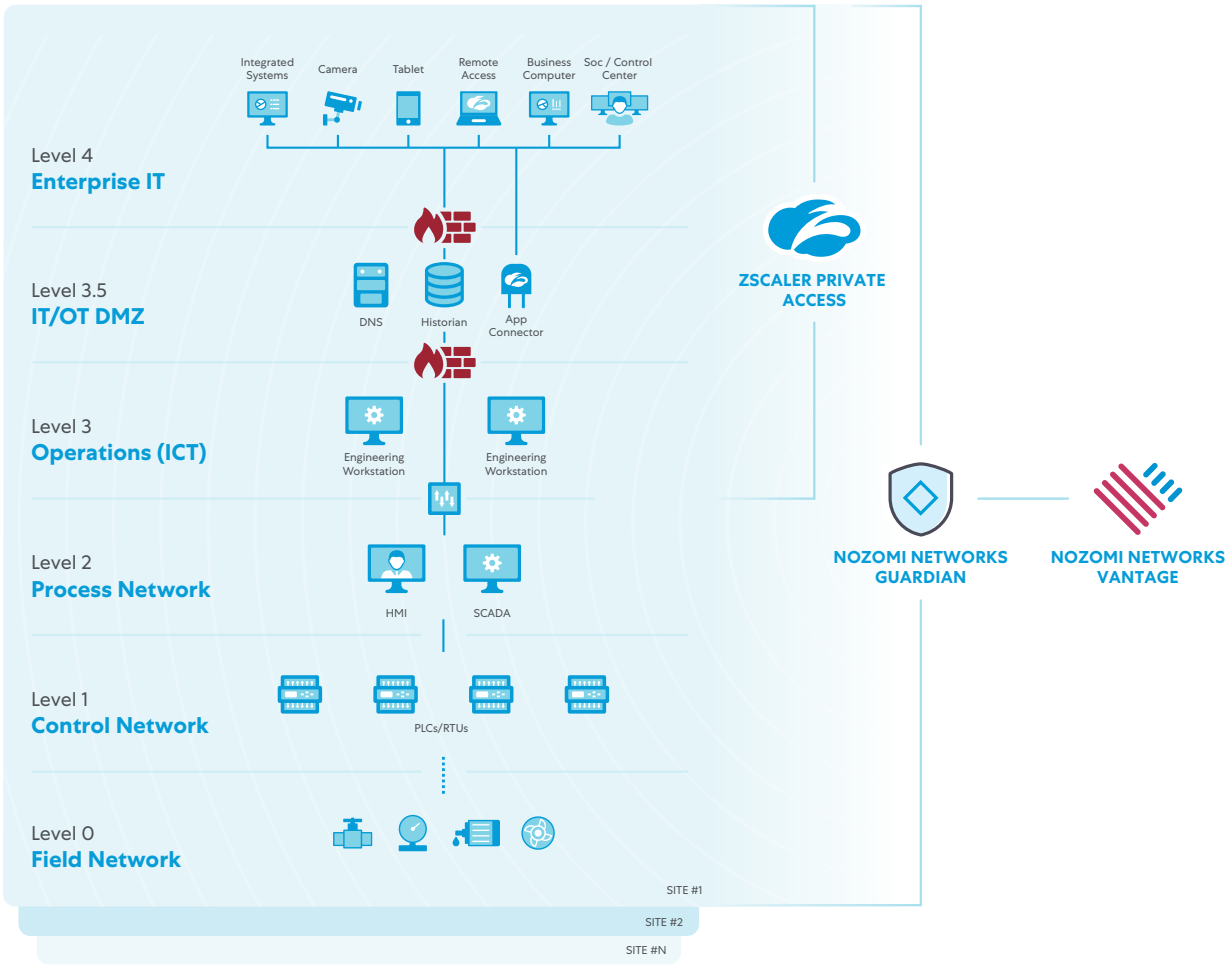
Zscaler Private Access (ZPA) enables fast, seamless and secure remote access to your industrial network so employees and third-parties can immediately connect to, monitor, and service assets from anywhere, maximizing uptime and productivity. Using ZPA, authorized users only have access to one application 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 connecting users and devices to only the specific applications they need without connecting them directly to your network. OT and IT teams never have to worry about users running unchecked across their internal network.

Benefits

Zscaler and Nozomi Networks offer a modern, zero-trust approach to protecting industrial edge networks from cyber threats, enabling security teams to:

- Give employees and third-parties fast, easy and secure access to OT/ICS environments
- Reduce network attack surfaces and limit potential threats from the outside getting in
- Reduce the cost and complexity of traditional network appliances such as VPNs with a fully cloud-delivered secure remote access solution

Sample Purdue Model: Zscaler and Nozomi Networks Deployment Architecture



Nozomi Networks for OT/IoT/IT data convergence

Nozomi Networks Guardian delivers visibility, security and monitoring of OT, IoT and IT devices. With Zscaler Private Access, admins can remotely access the full Nozomi Networks solution including Guardian sensors, Vantage cloud-based management console, or the on-premises Central Management Console. The Nozomi Networks solution provides:

- Asset discovery and network visualization
- Vulnerability assessment and risk monitoring
- Advanced anomaly and threat detection
- Time-saving dashboard and forensic tools
- Scalability with a single guardian sensor monitoring up to 500K assets

Zscaler Private Access eliminates third-party risk

Zscaler Private Access takes a user and application-centric approach to security by default. Whether that user be an employee, vendor, contractor, or third-party partner, ZPA ensures that only authorized users have access to specific internal applications without ever giving access to the network. You no longer has to worry about partners exposing their network to risk because users are never placed on the network; instead, you can create and enforce granular policies for users to access only specific applications through inside-out connections. These connections are fully encrypted and spun up on-demand to enable application segmentation. This means no more over-privileged third-party users. With ZPA's browser access capability, partner access is truly effortless. The feature allows third-party users to freely use their own BYOD devices to seamlessly and securely access an internal web application leveraging any web browser with no client needed on their devices.

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 Nozomi Networks can help, read our **blog** 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 Nozomi Networks
Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience. Learn more at **nozominetworks.com**.

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

zscaler™
www.zscaler.com