White Paper

3 Essential Zero Trust Principles for Reducing Security Risk in OT Environments

By Nicole Bucala
Head of OT Partnerships, Zscaler

The post–pandemic era demands greater agility in manufacturing and a sharper focus on cyber risk reduction to improve uptime and people & plant safety. Global staffing shortages that roil the globe as COVID–19 waves through different regions, plus supply chain problems leading to material shortages, are problematic enough—not to mention the growing threat of cyberattacks shutting down production lines. In light of this, cyber risk must be treated as business risk, leaving industrial operations teams with unprecedented complexity.

Technological innovation has the potential to make these complexities simpler to manage, but they also pose cyber risks such as ransomware and malware which could yield business losses. In this paper, we will examine the issues facing Operational Technology network managers and discuss how zero trust principles can be beneficial to digitalization initiatives.

Four challenges OT network managers must overcome

1. **Hyperconnectivity and digitalization is dissolving the air gap**
Industry 4.0 initiatives seek to increase the ability of factories to take advantage of IT innovations such as cloud-delivered services and AI/ML to enhance the precision of production lines. Predictive maintenance and remote maintenance also requires technicians to access OT systems remotely over the internet. Such initiatives to modernize factories involve connecting OT/IIoT assets to the internet, which consequently exposes industrial networks to common IT-sourced threats like ransomware. One common answer is to revert to a completely air-gapped environment, but this flies in the face of progress, leaving organizations begging for a solution that allows secure factory-to-internet connectivity while reducing risk.

2. **Legacy network security approaches create a massive attack surface**
Firewalls and VPNs are publicly-exposed to the internet, creating a rather large attack surface that attackers can use to exploit vulnerabilities, take advantage of excessive privileges, and move laterally across the network until a target is reached. This unfettered access can be an avenue for ransomware to spread, leading to unplanned downtime or putting people and plant safety at risk. In addition, as CISA notes in its latest warnings on OT vulnerabilities, VPNs are only as good as their latest patch. In fact, vulnerabilities in VPNs have been a primary attack vector for hackers to exploit in the past 24 months.

3. **Unpatched OT assets pose serious risks to operations**
Not only are most OT systems unpatchable or infrequently patched in many production environments, but these tools cannot afford to be taken offline for long periods. This creates a conundrum for security strategists who recognize the risks but aren't sure how to mitigate them using traditional technologies. Using the IT security playbook of "patch as soon and as often as possible" opposes the goals of plant operations teams to improve uptime and avoid unplanned downtime. A different security approach, other than avoiding patching or patching often, is needed to handle these risks.

4. **Cost and complexity of operating hardware based infrastructure**
Managing and deploying perimeter firewalls and VPNs to deliver consistent security across all users, applications, devices, and locations is operationally complex and costly. Rolling out new appliances, or hardware, to locations in different countries is expensive and can take months. As the number of OT/IIOT devices and corresponding bandwidth demands increases, operational costs will increase as well and may require capacity planning and expensive upgrades to underlying physical infrastructure—whether physical firewalls onsite, or their virtual counterparts. Staffing too can not scale to manage perimeter policy deployment, updates, and patches.

Undoubtedly, the pain points are clear and the status quo for OT security is ripe for a change.

The value of incorporating zero trust principles into OT environments

Plant and people safety is paramount, and reducing cybersecurity threats that can impact physical safety or downtime should begin with a thorough assessment of the attack surface. When it comes to knowing where to start changing things up, security professionals often choose to evaluate how to better secure the access and transport layer between the outside world and the factory network. That's because it's the first entry point for an attacker targeting high-value OT assets. As a result, an improved ability to measure and reduce risk at this level has the greatest potential to keep the good guys in and the bad guys out, removing the possibility of interference with OT assets and production lines.

Many OT security professionals are now turning to their IT counterparts, seeking to learn about how zero trust revolutionized IT security architecture. Some are working on plans to bring zero trust principles into their OT network as a layer on top of traditional defense-in-depth strategies. To successfully improve security and lower costs with zero trust, there are three guiding principles to follow:

#1 Prevent compromise with a platform approach

Increasingly, OT security strategists are seeking a way to enable all users and all devices to communicate securely through a unified and simplified platform. As it turns out, a zero trust policy exchange that sits between users and devices can simultaneously address their requirements while providing the power of continuous security updates and complete redundancy to prevent connectivity failure. For example, a market-leading SaaS-based zero trust cloud exchanges are powered by 100s of worldwide data centers, can stop 7 billion threats per day, and provide up to 200,000 security updates daily to all of its customers. They also handle tremendous transaction volumes, with their power clocking in, for comparison, at 15x the transaction volumes processed by Google's search engines.

The global connectivity offered by a dynamic, distributed exchange delivering zero trust policy can enable factories and third parties to communicate with each other across continents to address the following use cases, providing a single, comprehensive solution to most factory connectivity needs:

a. Privileged remote access for employees, third party technicians or contractors needing to access the factory from afar to perform remote troubleshooting, monitoring and maintenance with ease

b. Secure device-to-device access for machines at different plant sites to allow secure communication across geolocations

c. Secure device-to-internet access to enable IIoT, ICS, and SCADA systems to securely share data with public cloud apps

d. Secure device-to-private application access to allow secure communication between OT systems communicate and private apps

e. Zero trust policy on the factory floor is an additional capability needed when access within the factory floor must be fast and direct, without hair pinning to data centers.

#2 Reduce the attack surface

Zero trust offers fully encrypted, inside-out connections through a zero trust cloud-based exchange at the Purdue level of 3 or 3.5 level, significantly reducing the attack surface when compared to hardware based VPN and firewall combinations.

A deeper dive into such a solution reveals rich security benefits. When it comes to the Privileged Remote Access use case, for example, ZTNA provides remote workers and third-party vendors with clientless remote desktop access to sensitive RDP and SSH production systems without having to install a client on unmanaged devices or log into jump hosts and VPNs. Through zero trust, a factory can connect internal and external users to RDP and SSH target systems with full isolation, allowing users to connect from unmanaged endpoints and untrusted networks. It also enables third-party users to access data securely while blocking data from being copied, pasted, uploaded from or downloaded to their local unmanaged device, and allows 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. Direct connectivity via the zero trust exchange makes it fast for users to connect to and repair equipment, minimizing plant downtime, and gives easy access for remote workers and third-party vendors without the friction of conventional VPN. It is for this very reason that NIST and many other reputable expert bodies have advocated eliminating the use of VPN and replacing it with a zero trust Architecture.

#3 Scale and Simplify Without Hardware

Zero trust network access architectured through a multi-tenant, SaaS-delivered policy service is effectively a hardware-less solution. This comes with all the financial benefits around reduced CAPEX expenditures and the operational benefits around greater scalability of the solution. It also can be easily rolled out to locations around the world with the promise of a consistent user experience everywhere. In addition, maintenance and real-time security updates are automatically included, which saves OT operators money and time on the traditional operations and maintenance work otherwise involved in scaling out a hardware-based solution. As an example, companies such as Siemens rolled out zero trust network access to over 300,000 users in a couple of weeks.

With the power of a zero trust connection, factories are able to progress faster than ever before towards the OT/IT convergence implied by Industry 4.0, which embodies their quest to use advanced technologies like AI/ML and big-data to improve efficiency and automation. While traditional defense-in-depth concepts work well for the internal OT network, it is no longer sufficient for the case of external access to improve plant and people safety. This is especially true in a world that demands, ever more, immediate access and agility between global sites and remote employees or contractors . Fortunately, zero trust secures the OT systems while also preventing production networks and assets from downtime, damage, misuse and espionage.

> “The Zero Trust principles are incredibly relevant to smart factory initiatives. Operators are embracing digitalization to bring more automation and intelligence to their production. But it also brings a new dimension of connectivity between shopfloors and the internet.”

Herbert Wegmann
General Manager, Siemens Digital Industries

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