SSH

Meeting ISA/IEC 62443 Recommendations for Secure On-Site and Off-Site Access

Guide

Index

Introduction

What is ISA/IEC 62443?

ISA/IEC 62443 is a set of **global standards offering a systematic approach to fortifying cybersecurity measures to secure Industrial Automation Control Systems (IACS) and operational technology (OT) networks**. It is a fundamental framework within Industry 4.0, addressing multiple security aspects, such as security policies, risk assessment, network security, incident management, and access control.

The complex networks and controls behind manufacturing lines, power plants, or transportation systems are the backbone of our modern world. With the rise of Industry 4.0, which emphasized the integration of digital technologies into manufacturing and other industries, the equipment and systems powering various sectors rely strongly on technology.

But as the interconnectivity and technology advancements continue to grow, these systems also become more vulnerable to cyberattacks.

Picture a scenario where someone maliciously tries to disrupt these systems or where a glitch accidentally causes a breakdown in operations – it is a concerning reality.

Why is ISA/IEC 62443 essential for OT security?

Think of ISA/IEC 62443 set of standards as a 'protective shield' for IACS. It lays out **a series of best practices and guidelines that businesses operating in the OT industry can take to keep these systems secure**.

ISA/IEC 62443 also helps bridge the gap between IT and OT security by offering a tailored, risk-based approach specifically designed for the unique constraints of OT systems.

It addresses critical aspects like network segmentation, secure device design, access management, and incident response - all crucial for protecting OT systems from increasingly sophisticated cyber threats.

Put simply, it's not only about preventing cyberattacks and the potential widespread disruption they may cause; it is also about ensuring the continuous smooth and safe operation of these systems.

All SSH Communication Security OT products fully follow and adopt the ISA/IEC 62443 standard.

What is the purpose of this guide?

This document puts special focus on how OT busineses can secure on-site and off-site access to productions sites, digital assets, applications, industrial control systems (ICS), and other critical IT/OT targets - within the framework of the ISA/IEC 62443 standards.

The ISA/IEC 62443 series of standards

The ISA/IEC 62443 Series of Standards is a comprehensive set of guidelines and requirements developed to secure Industrial Automation and Control Systems (IACS) across various sectors, including manufacturing, energy, water, and transportation. Created by the International Society of Automation (ISA) and adopted by the International Electrotechnical Commission (IEC), this series is widely recognized as the global standard for securing industrial environments.

Structure of the ISA/IEC 62443 series

The ISA/IEC 62443 standards are divided into four groups, each addressing different aspects of cybersecurity for industrial control systems:

1 General (62443-1-X)

This part provides foundational concepts, terms, and models used throughout the series, establishing a common understanding and framework for the standards. Key topics include the cybersecurity lifecycle, risk assessment, and foundational terms.

2 Policies and procedures (62443-2-X)

This section focuses on establishing security policies and procedures for industrial systems, including risk management, incident response, and program management. These standards provide guidance on creating and implementing cybersecurity programs within an organization and highlight roles and responsibilities within OT (Operational Technology) and IT teams.

3 System requirements (62443-3-X)

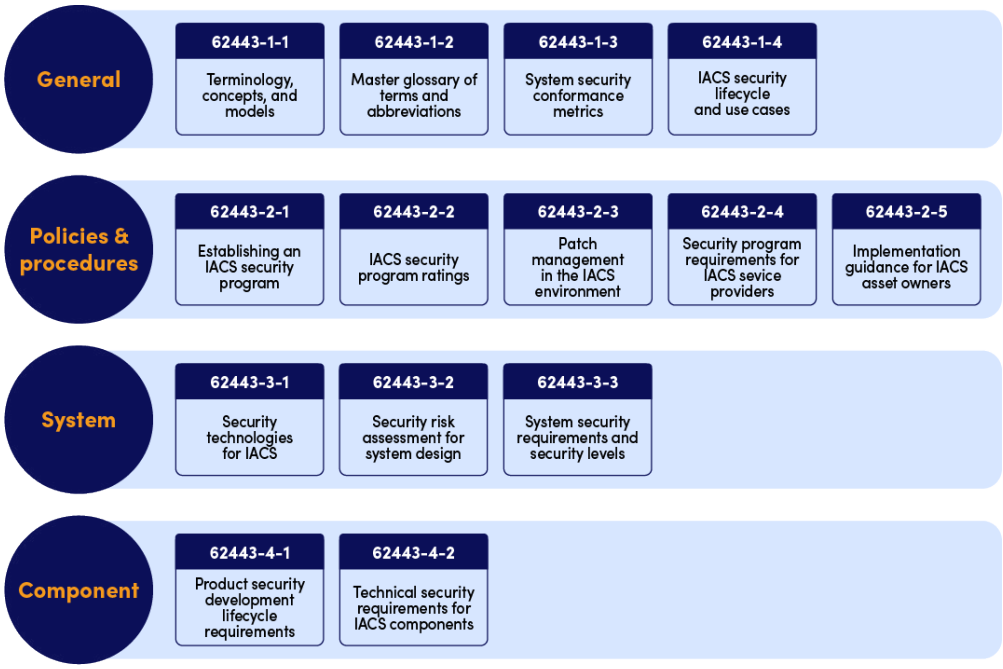
The system requirements section addresses the security needs of entire systems, focusing on network architecture, system design, and zone and conduit approaches.

Key components here are:

- **Zones and Conduits:** This model segments the network into zones based on security levels and uses conduits (controlled communications pathways) to separate and secure interactions between zones, reducing the risk of lateral attacks.
- **Security Levels:** Security requirements are tailored for different risk levels, allowing for a risk-based approach that adapts security measures to the operational importance and threat level of different parts of the system.

4 Component requirements (62443-4-X)

This part specifies cybersecurity requirements for individual components within a system, such as controllers, sensors, and communication devices. The component-level standards ensure that each piece of hardware or software in the system has security measures aligned with the overall network requirements.



The ISA/IEC 62443 series overview. For example, the ISA/IEC 62443 requirements 3-3-2 and 3-3-3 are mainly used for local and remote access management and controls.

Design principles of ISA/IEC 62443

When designing your IACS, it is crucial to focus on the access management part. This means controlling who can access important systems, data, and resources within your IACS environment.

Why is the access management aspect crucial in IACS design? Reasons include:

- **Security:** Access management controls can access critical systems, data, and resources, preventing unauthorized entry and reducing cybersecurity threats, such as data breaches and sabotage.
- **Compliance:** Many industries operating in industrial sectors, must adhere to regulatory standards, such as NIS 2.0 and ISA/IEC 62443, to avoid legal and financial repercussions.
- **Risk management:** Access management mitigates risks, such as insider threats and unauthorized access, by implementing granular controls and monitoring privileged activities.
- **Operational efficiency:** Streamlining authentication processes ensures authorized personnel access resources efficiently, enhancing operational efficiency and productivity.
- **Protection of intellectual property:** Access management protects sensitive information and intellectual property, limiting access to authorized users only and implementing encryption for asset protection.

In addressing these essential design aspects, our OT PAM solution, PrivX OT Edition, offers simplified access management that:

- Consolidates all access requirements into a single platform.
- Utilizes consistent tools, interfaces, and workflows across the board.
- Automatically generates audit trails for third-party or specialist access.
- Sends audit events to external tools for additional analysis and insights.
- Auto-generates audit trails for all third-party or specialist access.
- Ensures uniform session recording and monitoring functionalities for critical sessions.

Key aspects of ISA/IEC 62443 in OT security

Defense-in-depth for OT environments

ISA/IEC 62443 emphasizes layered security through a defense-in-depth approach, which is crucial for OT security where each layer adds additional security controls, from the physical layer up to network and application layers. This is especially important in OT environments, where single points of failure can disrupt critical infrastructure.

Zone and conduit model

The zone and conduit model is central to IEC 62443 and is highly applicable to OT environments. This model segments the OT network into different security zones based on risk levels, with conduits controlling communications between zones. By isolating higher-risk areas from critical operations, this approach helps prevent the lateral spread of threats, a critical component in safeguarding OT systems.

Risk-based approach

ISA/IEC 62443 promotes a risk-based approach, allowing organizations to tailor their security efforts based on the risk profile of each system and its importance within the operational process. This is critical in OT environments where systems must balance security with operational continuity, and downtime could have significant safety, financial, or regulatory repercussions.

Component and System Security Requirements

The 62443 series defines specific security requirements for both individual components (like PLCs, sensors, and HMIs) and larger systems, which are important in OT environments where specialized devices often lack native security features. It also provides standards for secure development practices, emphasizing secure-by-design principles that manufacturers can follow to create inherently more secure OT devices.

Compliance and Continuous Monitoring

Compliance with ISA/IEC 62443 helps organizations meet regulatory requirements and industry best practices, providing a structured way to audit and improve OT security over time. Continuous monitoring and regular assessments are key parts of OT security, as they ensure systems remain resilient to emerging threats.

How PrivX OT addresses key elements of the ISA/IEC 62443 standards

The ISA/IEC 62443 set of standards was created to address various cybersecurity elements throughout the lifecycle of OT networks. Some of the key components are as follows:

1. Covering the secure deployment of IACS, including software, hardware, network setups, and user access controls. (Part 2-5: 2018)

When deploying IACS, ensuring the security of the software, hardware, network configurations, and user access is very important for compliance and boosting operational efficiency.

Our PrivX OT Edition can help organizations achieve these needs:

- **Software management:** Centralized access control and automatic audit trails for secure software lifecycle management.
- **Hardware protection:** Secure access controls to prevent unauthorized interaction with devices, such as programmable logic controllers (PLC) and Supervisory Control And Data Acquisition (SCADA) systems.
- **Network security:** Advanced protocols and encryption to safeguard data transmission within the IACS network.
- **User access controls:** Comprehensive privilege management to mitigate insider threats and unauthorized access risks.
- **Strong user authentication:** PrivX OT Edition automatically syncs with multiple directory and/or identity and access management (IAM) services for identities. The solution then maps the identities with the right roles and grants access to verified-only users based on strong (biometric) authentication.
- **Device trust and continuous authentication:** PrivX OT Edition can be extended with device trust that continuously monitors the security posture of the user end-point device and terminates anomalous sessions automatically if the device's security posture is downgraded (for example, when the anti-virus software goes offline).
- **Credential management:** PrivX OT ensures that the passwords or authentication keys required to access a target are always secured and enables fully passwordless and keyless authentication for just-in-time (JIT) and Zero Trust access. This model ensures that users never see or handle any secrets, nor can they share or lose them when authentication is fully credential-less. The solution can also automatically prevent or terminate user access from an unauthorized location, at an unusual or unexpected time, or based on other unexpected or policy-contravening activities.

2. Emphasizing routing upkeep, updates, and patch management to fortify the system against evolving threats. (Part 2-3: 2015)

In today's rapidly evolving technological landscape, ensuring the security and reliability of OT systems cannot be overstated. Emphasizing routing upkeep, updates, and patch management is very important to fortify the systems against vulnerabilities and threats.

PrivX OT Edition offers comprehensive features tailored to meet the unique challenges of OT security:

- **Holistic lifecycle management:** By integrating granular privilege restrictions, it ensures that only authorized personnel can perform necessary tasks on OT targets, thereby minimizing the risk of unauthorized access and potential breaches.
- **Seamless deployment and maintenance:** Deployment processes are streamlined, and downtime is minimized, facilitating seamless updates and patch management. This ensures OT systems remain up to date with the latest security enhancements and are fortified against potential breaches without disrupting critical operations.
- **Simplified secure access control:** Built-in features for workflow approvals and credential lifecycle management simplify the process of maintaining secure access to OT infrastructure. Our solution enables organizations to efficiently manage access rights, ensuring that only authenticated users with the appropriate permissions can interact with OT systems.
- **Enhanced security posture:** Overall, our solution enhances the security posture of OT systems by tightly controlling and monitoring access to critical assets. By implementing secure access control measures and providing comprehensive audit trails, it helps organizations mitigate the risks associated with unauthorized access and potential cybersecurity threats.
- **Secure file transfers and uploads:** PrivX file scanning, based on the Internet Content Adaptation Protocol (ICAP), helps prevent malware, viruses, and other bad payloads to reach critical targets.

3. System security requirements and security refers to the requirements for an IACS system based on security level, this information being primarily intended for control system suppliers, system integration, and asset owners. (Part 3-3:2013)

In the context of secure access management, system security requirements are extremely important for IACS. These **requirements dictate the level of security necessary for protecting critical infrastructure**, with implications for control system suppliers, system integrators, and asset owners.

Secure access management, such as that provided by PrivX OT Edition, plays a crucial role in meeting these requirements and safeguarding IACS environments against evolving cybersecurity threats. By aligning with system security requirements, PrivX OT Edition enables centralized access control, granular privilege restrictions, and streamlined workflow approvals, ensuring that only authorized users and devices can access critical OT targets.

PrivX OT Edition allows organizations to get control over the access to different OT vendor systems in a uniform fashion, without having to use vendor-specific point solutions. It also allows granting temporary access to third parties for maintenance jobs with automatic offboarding after the allocated time period expires. Setting up emergency access is fast, easy, and secure at the same time.

With its comprehensive features and emphasis on access security lifecycle management, our solution facilitates the implementation of secure access practices that adhere to system security requirements, promoting the resilience and integrity of IACS systems.

IACS security through the lens of ISA/IEC 62443

ISA/IEC 62443 categorizes IACS security by assessing an organization's cybersecurity management capabilities and the necessary security levels for its systems or components. **This framework enables organizations to systematically evaluate and implement tailored cybersecurity measures** based on their specific system security requirements.

PrivX OT Edition is designed to cover access to physical and virtual targets alike from a single solution:

- **Handling access to both IT and OT targets from a centralized solution** with uniform user experience, auditing, and logging.
- **Uniform access using industrial protocols or standard IT protocols** (SSH, RDP, VNC, HTTP(S), Profinet, EtherNet/IP, Modbus TCP, OPC UA, and more).

SSH

- **Using strong identity-based authentication and phishing-resistant MFA** for critical connections. Adding mandatory approval from, for example, a site manager for particularly critical tasks.
- **Increasing the controls as per criticality of the target or the task at hand.** All sessions are identified and produce a solid audit trail, but certain sessions can be recorded and monitored live if necessary.
- **Syncing with multiple directories and identity and access management (IAM) systems** to link identities to roles in a straightforward fashion. Roles can be matched with assets that have similar security needs to streamline linking the identity to the role and then granting that role access to the right target.
- **Building secure communication pathways**. PrivX OT Edition can be extended with direct quantum-safe tunnels between sites, networks, data centers, or clouds. These tunnels can contain any data - even unencrypted - but the transmissions are safe even over the open internet with quantum-safe encryption.

PrivX OT: Full-scale secure access control for OT

PrivX OT is a cost-efficient software solution that centralizes on- and off-site secure access management to any OT/IT target. It allows plant-wide, global, or local IT/OT access control at industrial scale without investing heavily into cybersecurity hardware.

Maintain and troubleshoot remotely

- Maintain, upgrade & optimize operations off-/on-site
- Instant access for troubleshooting
- Strong biometric authentication and device trust-based access to production sites

Centralized control

- Access hundreds of machines or other critical IT/OT targets from a single digital gatekeeper
- Work with multiple directories or IDMs and map them with the right roles for role-based access control (RBAC)
- Audit trails, session recording, and monitoring for compliance (NIS2, ISA/IEC 62443)

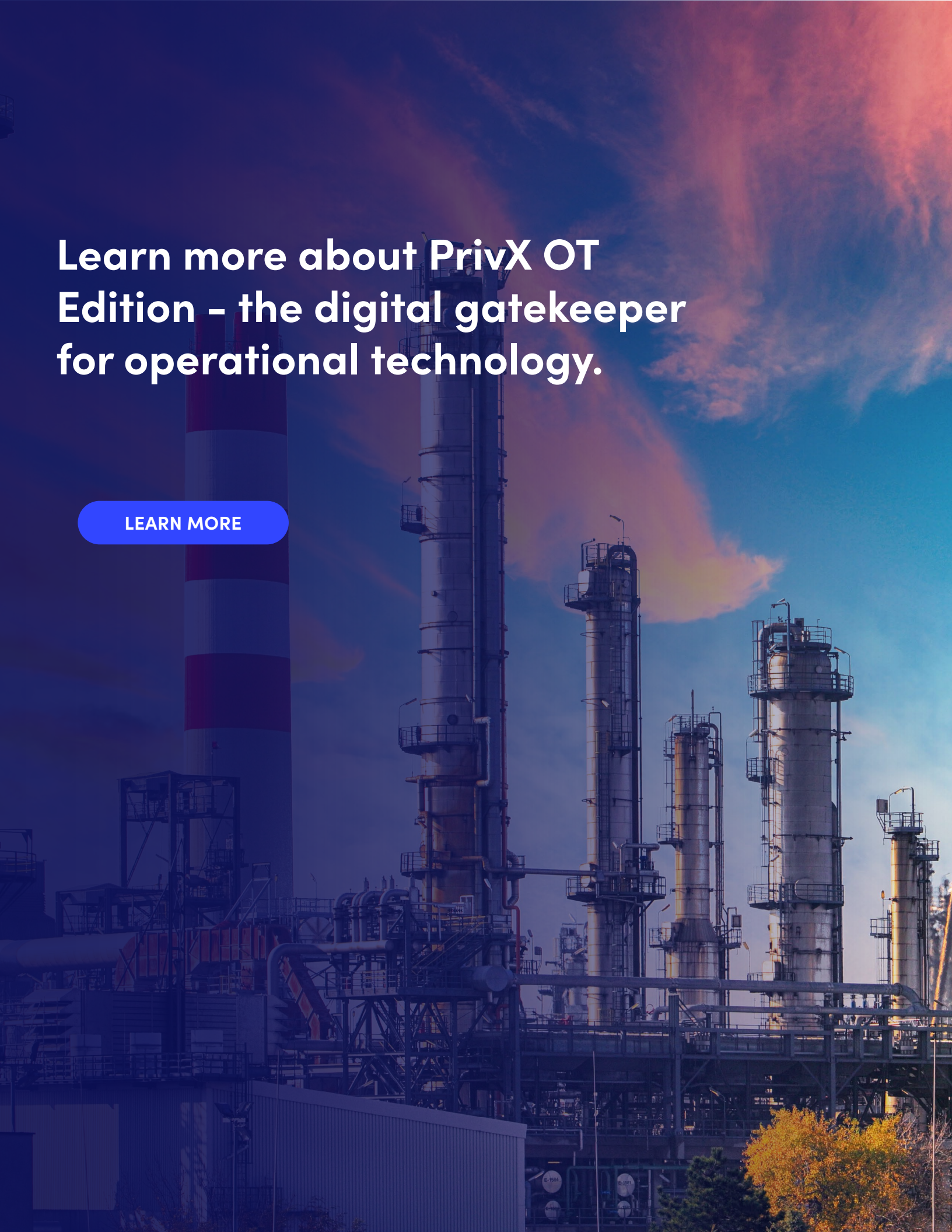
Approve, restrict, authorize

- Workflows for job approvals or integrations to ticketing systems
- Restrict the access to the minimum to get the job done

- Manage credentials and migrate to passwordless and keyless authentication for efficiency and true Zero Trust security

Save on costs

- Scalable, flexible, and easy to deploy: No costly hardware
- Uniform access using industrial protocols or standard IT protocols (SSH, RDP, VNC, HTTP(S), Profinet, EtherNet/IP, Modbus TCP, OPC UA, and more)
- Software from leading security experts with a strong footprint in demanding projects in OT, banking, healthcare, and MSPs


Learn more about PrivX OT Edition – the digital gatekeeper for operational technology.
LEARN MORE

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH Communications Security Oyj
Karvaamokuja 2B, Suite 600
00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel: +1 (212) 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Singapore

SSH CommSec Pte. Ltd.
6 Raffles Boulevard, Marina Square, #03-308
Singapore 039594
Singapore
Tel. +65 6338 7160
sales.asia@ssh.com

SSH