SSH

Secure Remote Access Lifecycle Management for Operational Technology (OT)

Buyer's guide



Index

Digital transformation brings safety and security together. 3

Challenge #1: IT/OT convergence 5

Solution: Connectivity to OT and IT targets alike. 5

Challenge #2: Costs 5

Solution: Digital gatekeeper 6

Challenge #3: Lack of centralized access 6

Solution: Centralization 6

Challenge #4: Sharing and accessing data insights 7

Solution: Secure data management 7

Challenge #5: MFA phishing and untrusted devices 7

Solution: Strong identity and device trust 8

Challenge #6: Maintainability 9

Solution: Agentless operations 9

Challenge #7: User-friendliness. 9

Solution: Simplicity. 10

Challenge #8: Changing environments with a mix of old and new 10

Solution: Automation. 10

Challenge #9: Deployment 11

Solution: Rapid deployment. 11

Challenge #10: On-boarding and off-boarding. 11

Solution: Leveraging identities and user roles 11

How does PrivX OT Edition overcome these challenges? 12

Digital transformation brings safety and security together

Operational technology (OT) is used to control, monitor, and manage physical systems. This might include systems found in the manufacturing sector. Like IT environments, **OT environments must be safeguarded against cybersecurity attacks** and other risks.

It used to be common for companies to forget comprehensive OT security. The reasons for this include:

- **Isolated systems:** IT systems used to be fully isolated from any outside access, so the need to secure these systems wasn't a high priority.
- **Financial:** The cost of implementing these "additional" OT security measures offered low business value for high cost.
- **Lack of in-house expertise:** Having focused strongly on safety, security has been a secondary concern in OT.
- **Regulations not covering OT:** IEC 62443 as a set of standards has addressed cybersecurity, but other regulations (like NIS, NIS 2.0, and CER) are a more recent development.

Nowadays, **the integration between IT and OT systems — known as the IT/OT convergence — has changed the landscape**, and many critical tasks are now performed remotely, off-site as digital transformation is gaining momentum in the OT industry.

However, many companies still use legacy tools, such as firewalls, VPNs, or point-security remote access solutions (physical or digital), that protect or limit access to sites to secure their OT environment — but these older technologies no longer make the cut for modern-day cybersecurity needs. Their access management lifecycle capacities are limited, they provide too broad access, and they're hard to scale when business needs change.

Instead of using complicated manual tools to solve the OT cybersecurity challenge, **OT organizations need to leverage reliable and comprehensive solutions that were built with OT in mind**.

One such solution can be found in Privileged Access Management (PAM), which has been protecting IT environments for decades. **A PAM solution specifically built for OT can protect essential industrial OT targets**, including:

- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA) & SCADA-as-a-service
- Programmable logic controllers (PLC)
- Discrete process control systems (DPC)
- The human-machine interface (HMI) remote terminal units (RTU)
- Period of time instantly and even ahead of time

This guide explores the major challenges organizations face when choosing a secure remote access (SRA) solution, including PAM for OT, so you can choose the best tool for securing your enterprise OT.

Whether you're looking to implement an OT PAM solution for the first time or replace your existing security solution with a fluid and future-proof approach, selecting the right PAM tool for OT will allow you to reap real business value from your investment.



Challenge #1: IT/OT convergence

The IT/OT convergence refers to the integration of information technology (IT) environments with operational technology (OT) environments. As enterprise technology advances, with OT becoming increasingly accessible remotely, this convergence increases.

The IT/OT convergence is a relatively new endeavor for many organizations, especially with the rise of remote machine operations.

In the recent past, **traditional OT companies have focused primarily on safety over security**. OT administrators addressed questions of site and engineer safety, leaving the IT department to handle cybersecurity issues. **Now, IT and OT are no longer two separate worlds.** As a result, there's a shortage of skilled personnel who can properly manage the joint IT and OT operations which makes it in turn also difficult to introduce new technology.

Organizations that do not converge their OT and IT departments effectively can suffer significant consequences. When there's no synergy between IT and OT, there's no common understanding of the safety and security risks within a company and how they interact.

Without full visibility into IT and OT targets, you can't know how big your attack surface is — and as a result, you're not able to properly protect your proprietary data.

Solution: Connectivity to OT and IT targets alike

To ensure connectivity between your IT and OT departments, **utilize a PAM system that provides a centralized inventory of all access points**. This will give you complete visibility into your attack surface. Look for PAM tools that can be:

- Controlled and maintained with minimal input
- Utilized by a host of cybersecurity experts, in both IT and OT
- Centrally accessed anywhere, anytime
- Easily leveraged for system checks and monitoring

Challenge #2: Costs

In OT, **continuous uptime, operations, and production yield are critical**. Businesses have often accumulated dozens of years of information about how to optimize the production of paper, cardboard, port operations, etc. Therefore, any additional costs become an issue.

Physical remote access solutions (like Remote Terminal Units or Line Modems) are commonplace but expensive and labor-intensive to set up, and maintenance is required for each target separately.

Software-based solutions like VPNs and firewalls, on the other hand, open too broad access to targets and can be hard to configure to be more restrictive.

Solution: Digital gatekeeper

A new age requires new types of solutions. **A software-based PAM solution is likely to be more affordable than physical ones, and it also beats VPNs and firewalls with a richer set of controls.**

Look for a solution that:

- Is purpose-built for IT and OT to cover all access needs from a single solution
- Can manage access requiring IT protocols (like SSH, RDP, VNC, or HTTP(S)) as well as proprietary OT protocols (like Profinet, EtherNet/IP, Modbus, OPC UA, and more)
- Allows access only to the right target per task for technicians for security
- Offers the same consistent access experience every time, regardless of the target or the task
- Manages credentials (both passwords and authentication keys) and allows the transition to passwordless and keyless authentication for full Zero Trust

Challenge #3: Lack of centralized access

OT networks comprise disparate systems, often requiring administrators, technicians, and maintenance engineers to move between a wide variety of individual tools, interfaces, and logic. This makes it far more difficult to ensure logical and consistent session recording, audit event forwarding, and audit trails — all of which are critical to OT administration.

Unfortunately, a lack of centralized access in OT is all too common. There are already copious devices, machinery, and other unique targets in OT networks, and the number only grows as OT and IT continue to converge. **OT admins now need to manage access to traditional OT targets alongside a variety of IT targets** — and it's very important to ensure secure integration between them.

Solution: Centralization

For a reliable, sustainable, and secure PAM OT system, **leverage a centralized PAM tool**. This mitigates the risk of inconsistencies, complacency, and human error by simplifying access management.

Look for a tool that:

- Centralizes all access needs under one roof
- Uses the same tools, interfaces, and logics throughout
- Leverages automatic audit trails of all third-party and specialist access
- Has consistent session recording and monitoring capabilities for critical sessions
- Forwards audit events to external tools for further analysis

Challenge #4: Sharing and accessing data insights

A major challenge that OT companies face is sharing their learnings, discoveries, and actionable insights with other departments, particularly the IT department. When organizations can't safely and efficiently leverage the data coming in from critical machinery, they miss out on opportunities to optimize business operations.

For example, OT enterprises with multiple sites might benefit from sharing insights and analytics between sites, so that optimizations can be made. **If OT data isn't being shared between sites, it's a missed opportunity that could otherwise have been extremely lucrative for the enterprise.**

Too many companies don't trust their existing security practices when it comes to sharing internal insights, and rightly so. The data available in OT environments can be extremely valuable to the enterprise, but the risk of exposure or compromise if shared means that many OT enterprises choose not to share it at all.

Solution: Secure data management

Organizations should **utilize a PAM solution that supports safe sharing, access, processing, and analysis of critical data**. To promote secure data management, your PAM tool should leverage:

- Security measures like end-to-end encryption
- The least privilege principle, in which only the necessary parties can access the data they are authorized to access with the minimal level of authorization to get the job done
- Internet Content Adaptation Protocol (ICAP) capabilities, which scan all user files and uploads for malware or ransomware
- Intuitive, easy-to-use data sharing tools and features

Challenge #5: MFA phishing and untrusted devices

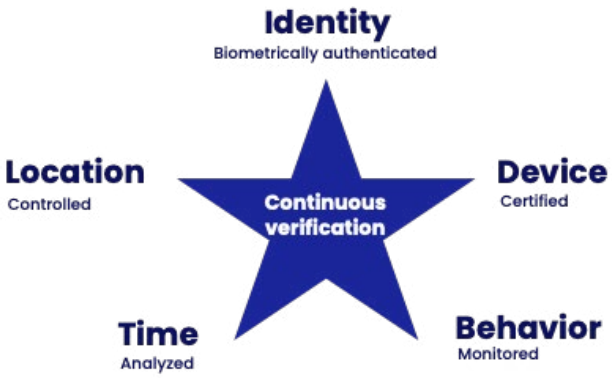
In IT as well as OT, you need to ensure that only verified users are allowed access to the right target. This is why multi-factor authentication (MFA) solutions are more commonplace. Unfortunately, **traditional MFA solutions are susceptible to man-in-the-middle, MFA fatigue, and token theft attacks** that can compromise MFA.

Then there are devices. **Many devices accessing critical OT targets aren't bound to an identity, nor is their security posture continuously monitored for security.**

Since OT targets are critical, it makes sense to take the security posture management a step further.

Solution: Strong identity and device trust

OT security needs authentication that transcends traditional MFA or identity-only based authentication tools. By using five key elements for authentication and continuous session validation, a phishing-resistant MFA ensures that every high-impact session is established by verified users and devices only.



By verifying

- identity,
- device,
- behavior,
- time,
- and location

for each session the solution creates a strong, phishing-resistant MFA solution tailor-made to access critical targets by high-impact users.

Look for a solution that:

- Uses the five elements for authentication and binds them to your security policies for security posture verification
- Ensures that if any of them fail during authentication the session request is denied or an additional verification is required
- Continuously monitors the security posture of any of the elements for anomalies during the session (e.g. firewall goes down, anti-virus is offline, anomalous behavior) and then terminates the session automatically or requires that the security posture of the device changes before the user is allowed to log in again
- Can require authenticated users to be authorized by site managers or other administrative people before getting access to a target

Challenge #6: Maintainability

A key challenge associated with many secure remote access solutions is **the need for continuous maintenance**. **Many secure remote access tools require OT administrators to install agents** for certain technologies, but having many agents can turn into a maintenance nightmare. If each target requires an agent to be installed for secure access to work, it leads to inconsistencies every time there's a change.

Basically, this leads to a type of cat-and-mouse game where the admin tries to remove the software agents that no longer should be there, upgrade the ones that are outdated, and install new ones as new targets are introduced. The solution is never properly installed since it's being continuously configured to work and be safe.

If the experience of maintaining your PAM system is poor, it'll be more challenging for critical stakeholders to ensure secure OT within enterprise networks.

Solution: Agentless operations

To ensure a productive and pleasant user experience, **invest in an OT PAM tool that leverages consistent logic throughout end-user operations**. This improves end-user efficiency regardless of what type of data they're accessing and contributes to less error-prone PAM operations.

Ideally, you want a solution that is as agentless as possible, so you don't have to install components across your OT network or on your clients. Look for solutions that:

- Boast largely agentless architecture for fast installation and easy maintenance
- Don't require end-users to install anything on their client
- Allow for the use of *vanilla* browsers for access, minimizing the need for whitelisted applications
- Minimize the need for endpoint security, since there is no client software that needs to be secured

Challenge #7: User-friendliness

The need to learn **a host of different systems, logics, and interfaces is detrimental to user experience**. Having disparate systems means that your on-site or off-site maintenance engineers need to juggle multiple systems simultaneously.

Not only do maintenance teams need to learn and access dozens of tools or more, but all these tools must be audited too. Your staff cannot consistently and reliably audit dozens of disparate OT systems, nor can they maintain consistency between them. On top of that, traditional secure access management tools often need reconfiguration, especially in the case of older

OT architecture, forcing administrators to continuously learn new tools and relearn existing ones.

If the user experience of your system is inconsistent, it'll be more difficult to use, and difficult-to-use systems tend to get bypassed or not be used at all.

Solution: Simplicity

Centralized PAM solutions are easier to learn, operate, and update. To maximize the efficiency of the PAM tool you choose, look for a solution that:

- Requires a single logic for end-users regardless of the target
- Permits user access for relevant and authorized targets only
- Provides single sign-on (SSO) for users to their available list of targets only
- Dynamically adapts to reflect changing roles and environments

Challenge #8: Changing environments with a mix of old and new

Generally, OT environments have been static over time, with the same machinery and technology in use for decades. Many of these **OT machines are expensive and designed to last, but they were designed before the IT/OT convergence** occurred. As a result, the machines weren't designed to be compatible with IT systems which means that administrators often need to grant access to each individual tool as and when necessary.

Using all the separate tools and proprietary protocols provided by each individual manufacturer of each individual machine makes **maintaining secure remote access incredibly difficult, resource-consuming, and frustrating for end-users**. This is especially true for larger networks with tens (if not hundreds) of access tools for OT. **Not only does this make security processes unsustainable, but it opens your OT system to a host of cybersecurity concerns.**

All the challenges associated with changing environments are further exacerbated by the rise of remote OT access. In the past, OT changes were made by on-site maintenance engineers, but modern OT systems are controlled remotely. This has spurred a need for more dynamic and secure access management for OT networks.

Solution: Automation

A PAM system that leverages automation can streamline access within dynamic environments, allowing for fast and secure OT access. Look for an OT PAM tool that can automatically:

- Discover and handle changes in environments, for example, by auto-discovering cloud hosts

- Support secure remote access lifecycle management consistently in OT and IT
- Grant target-agnostic access for consistency across IT/OT landscapes
- Support temporary access needs for relevant projects

Challenge #9: Deployment

For many businesses in OT, operational downtime is a critical concern and challenge. **The consequences of OT operational downtime can be incredibly steep, with disruptions and slowdowns negatively impacting all related business processes.** Even a single day of OT downtime can lead to millions of dollars lost.

Many OT security access solutions are not centralized and are unnecessarily complex, meaning **it can take a significant amount of time to deploy them — leading to further unnecessary downtime and the associated costs**.

Solution: Rapid deployment

To avoid deployment downtime when implementing your OT PAM, **opt for continuous deployment that requires zero downtime to set up and run**. Look for a solution that supports:

- Rapid and reliable deployment
- Agentless deployment for less disruption
- Reduced loss of resources and energy
- Streamlined operations with zero OT downtime

Challenge #10: On-boarding and off-boarding

Along with deployment-related downtime, c**omplex management processes for OT networks result in lengthy and complicated onboarding and offboarding processes**. It could take days for new employees to be granted the access rights they need to start being productive, which often leads to **employees sharing OT target credentials during onboarding**. This creates disorganization and increases cybersecurity risk.

A challenge associated with onboarding and offboarding of, specifically, maintenance engineers is the workflow requirements for OT access management. There must be workflow approvals to ensure the right users get access to the right machinery at the right time. When existing security controls can't support an easy and trustworthy process for granting authorization, critical OT operations can become compromised.

Solution: Leveraging identities and user roles

Organizations should invest in a solution that supports **consistent, secure, and straightforward privileged user management and verification**. Look for tools that support the following features for effective OT onboarding and offboarding:

- Built-in workflow management and visibility
- Straightforward processes for approving and rejecting requests
- Seamless integration between ticketing systems
- Multi-factor authentication or biometric identification
- Automatic mapping of identities to the right roles and staying in sync with any changes for fast joiners-movers-leavers processes

How does PrivX OT Edition overcome these challenges?

With PrivX OT Edition from SSH, you can overcome the challenges associated with implementation, maintenance, and lifecycle management of secure remote access management for OT.

PrivX OT Edition leverages our long-standing expertise in IT and applies built-in features that tick all the boxes of a successful OT PAM solution:

- Full-blown secure remote access lifecycle management and remote troubleshooting
- Uniform user experience and audit trail logic for accessing IT and OT targets alike
- Straightforward workflow approvals and credential lifecycle management
- Granular privilege restrictions for remote OT sessions with least privilege to get the job done for each session
- Joiners-movers-leavers processes made easy: Automated linking of the right identities to the right roles and keeping them in sync with any changes
- Cost-efficient software-based solution with low hardware costs
- Secure remote sharing of valuable OT process optimization data for rapid and reliable IT/OT discoveries
- Regulatory compliance across a variety of industry OT requirements
- Embedded ICAP feature for secure file sharing and uploads

Along with protecting your OT network and promoting reliable enterprise OT operations, PrivX OT Edition also enables you to introduce modern, future-proof OT PAM technology at your own pace.

With PrivX, you can maintain all existing authentication keys and credentials in your OT and IT environments, while simultaneously moving towards just-in-time (JIT) access for verified, role-restricted ephemeral access rights. This shift eliminates the need to manage, rotate, and vault credentials, helping your organization keep pace with the growing OT/IT convergence while immediately supporting the security of your existing OT.


Learn more about PrivX OT Edition and future-proofing your OT PAM approach.
LEARN MORE
SSH

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

Let’s get to know each other

Want to find out more about how we safeguard mission-critical access for leading organizations around the world?

We’d love to hear from you.

REQUEST A DEMO