Key Insight Brief

3 Strategies to Secure Remote Access in Manufacturing Environments

wallix

Remote support is revolutionizing operational efficiency in industrial settings, making a significant impact in our increasingly digital and fast-paced environment.

From diagnostics and monitoring to data transfer and troubleshooting, the demand for strong remote access solutions is higher than ever.

However, securing remote access is no small feat; it's a complex puzzle that requires strategic thought.

Be the Champion in Managing Remote Access

Let's face it, remote support is crucial these days.

However, the rapid and sometimes **disorganised deployment of VPN gateways** by manufacturers and external contractors has significantly increased the attack surface of industrial networks.

This situation forces industrial organizations to balance operational efficiency with the need for strong cybersecurity.

But **securing remote access isn't exactly a walk in the park**. It's extensive and complex, and sometimes, you can find yourself at a loss because you don't know where to start. What will really help at this point is to come up with a solid plan of action.

And to make it even simpler, we've broken it down into three straightforward strategies.

3 Strategies to Secure Remote Access in Manufacturing Environments

01 Implementing Zero Trust Security Frameworks

You've probably heard about Zero Trust security frameworks. The concept might sound familiar, but you probably haven't implemented it in your organization yet.

Don't delay any longer—Zero Trust is a must now.

Let's rewind a bit: Unlike traditional security models that assume trust within a network perimeter, **Zero Trust architecture requires continuous verification** of all users and devices, no matter where they are or how they're accessing the network.

This strategy ensures that only authenticated and authorized entities can access specific network resources.

So, where do you start? It is common to first assess and map all your assets and network resources to get a clear picture of your environment. However, at the same time, it is crucial to deploy the first layer of your security to lock down access to your production network. Implement granular access controls with privileged access management tools (PAM). This will allow you to continuously verify and monitor network access and activity.

Why go through all this effort? The benefits speak for themselves:

> Significantly **reduce unauthorised access.**

> **Improve visibility** and control over network activities.

> **Prevent lateral movement** of attackers within the network.

02 Centralise and Unify to Simplify

After segmenting your network, a crucial step in protecting your OT environments, **deploying a single-entry point for accessing your OT systems** is essential. This approach simplifies remote connections through a centralized tool, eliminating the need for numerous uncontrolled VPN access points.

However, this must be done with **user-friendly tools** that perfectly align with the existing OT processes to ensure seamless security without disrupting production.

This is precisely what **privileged access management** (PAM) tools provide, with their main objectives being:

> **Isolating your production environment** through a protocol break managed by a centralized PAM.

> **Traceability** of all remote connections, regardless of their origin (service providers, manufacturers, internal teams, etc.).

> **Monitor** what the authenticated person does on the targets systems.

> **Restrict access** to specific areas or equipment to prevent unauthorized actions.

> **Delegated management** of user accounts to allow production teams to add third-party personnel in real time.

03 Continuous Monitoring and Anomaly Detection

Why is this so important?

Because using advanced, centralised cybersecurity tools to **detect unusual activities or breaches in real-time** allows for quick responses before significant damage occurs.

Integrate behavioral analysis solutions and anomaly detection tools. Configure real-time alerts for suspicious or unauthorized activities, feeding this information into a SIEM (Security Information and Event Management) system to strengthen access management and minimize risks associated with excessive privileges.

Continuous monitoring offers several benefits:

> **Logging all events** through logs.

> **Early detection of attacks.** Combined with a SIEM, it becomes easy to stop threats before they cause damage.

> **Analyzing events** to improve security posture.

> **Compliance** with increasingly numerous standards (NIS2, IEC 62443, ISO 27001, etc.).

Case Study

The leading manufacturer of high-quality workwear is safeguarding its critical servers and infrastructure, ensuring seamless operations and unmatched reliability.

Do you want to know about the game-changing steps they took?

Keep reading.

How the go-to manufacturer for high-quality workwear secured its critical servers and infrastructure components

Let's talk about Engelbert Strauss, a renowned manufacturer of high-quality workwear. With an extensive setup that includes 80 servers, 1,200 employees, and 10 offices, they faced several challenges:

> **Stable and Secure IT Infrastructure:** Ensuring their network environment remained reliable and protected.

> **Password and Identity Management**: Establishing a robust system for managing passwords and identities.

> **User Experience:** Streamlining procedures to create a seamless user experience.

> **Balancing Security and Usability**: Achieving high-security standards without compromising ease of use for the team.

Solutions to the Rescue

We implemented a solution that centralised the control and monitoring of privileged access to Engelbert Strauss's critical assets, enabling detailed oversight of who accessed each resource.

Additionally, we integrated the Privileged Access Management (PAM) system with the Security Information and Event Management (SIEM) system they were already using.

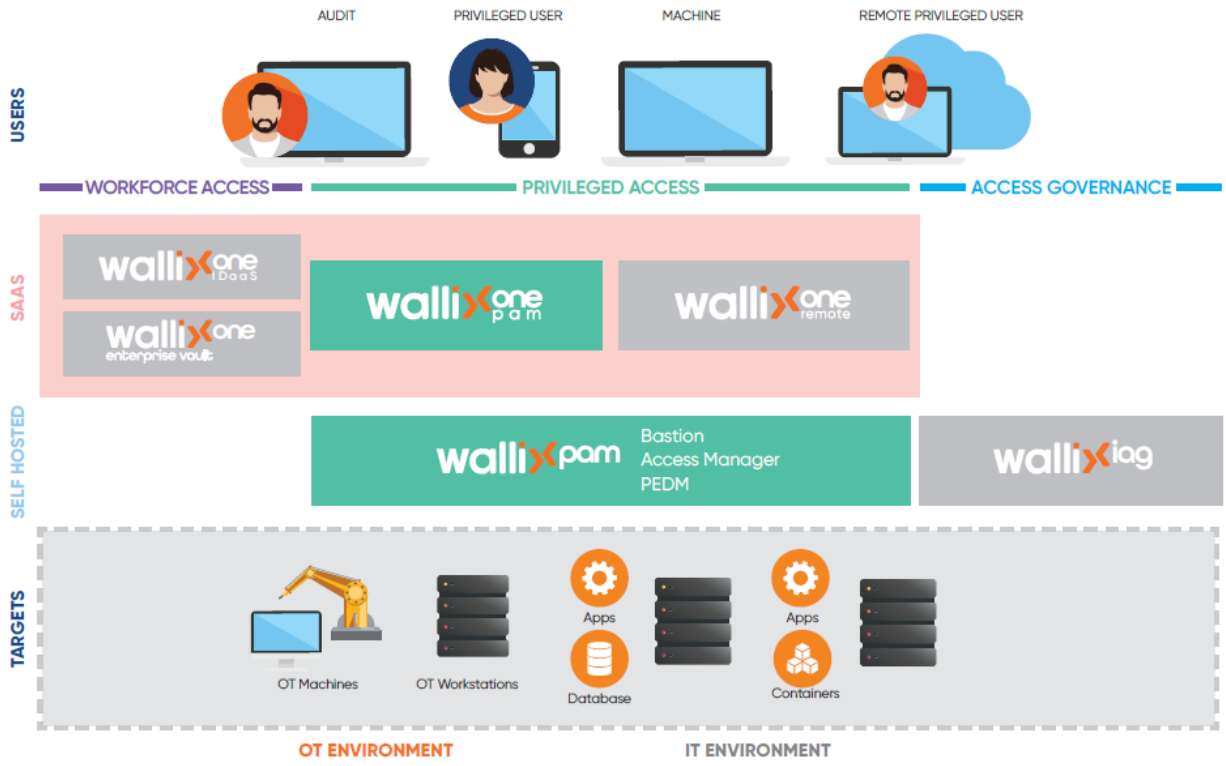
This integration facilitated control over authorised access to systems and ensured strict isolation between primary and secondary session connections.

The main benefits were:

> More effective use of the IT department's resources

> Better control and monitoring of server access

> Very few support requests



Summary

GWENDAL AZOUS

› Large Accounts & OT Specialist

I hope this document has helped clear up some questions for you. When I started working on it, I knew I wanted to focus on the advantages of digitalisation in manufacturing. However, as I went along, I also thought it made sense to show everything that comes with this journey, including its challenges and hurdles. Digital transformation is exciting, but it's important to do it right: making sure that remote access is secure and that all necessary regulations are being followed.

If you have any more questions, feel free to reach out to me here.

wallix

WALLIX is a cybersecurity software developer operating worldwide. Founded in 2003, WALLIX is now a world leader in identity and access security recognized by the most prestigious analyst firms. Its mission is to provide a simple and secure identified access service, so that our customers can operate securely everywhere in digital and industrial environments.

- 1 Ropemaker Street, LONDON, EC2Y 9ST, United Kingdom
- +44 7525146892
- contact@wallix.com