3 Proven Strategies to Strengthen Remote Access Security

By Gwendal Azous
OT Cybersecurity Market Strategist
WALLIX

75% of security experts believe remote working using remote access increases cyberattack risks. Are they right?

According to At Bay, in 2023, **58% of direct ransomware incidents were tied to a remote access vulnerability**.

On top of that, hackers shifted their focus from RDP to targeting self-managed VPNs, which accounted for **63% of ransomware events linked to remote access.**

Remote access security in industrial settings is something I encounter more and more in my daily work. By the way, I also work from home.

While industrial organizations have advanced in digitizing their processes, security hasn't always kept up—especially with remote access.

Legacy systems and weak authentication still leave gaps that cybercriminals exploit. As remote operations expand, securing access is no longer optional—it's essential.

So, what are these critical aspects? Let me name a few to give you an idea:

> **Legacy systems that can't be easily replaced.**

> **IT-OT convergence**, regulatory requirements, and inadequate network segmentation.

> **Internal risks** from users unfamiliar with cybersecurity.

> **Remote access by third-party vendors** and contractors, to name just a few.

You know the drill—PLC issues put production at risk, and your third-party contractor is only available remotely. So, you ask IT to open a VPN to access your OT network.

The problem? They're swamped. **By the time they get to it, your service provider is long gone.** Meanwhile, if that VPN stays open, it's a cyber incident just waiting to happen.

To avoid these risks, here are three proven strategies that work time and time again.

Strategy 1: Implement a Zero Trust Security Framework

Think of a medieval fortress (Game of Throne, here I am!). In the past, if you were inside the walls, you were considered trustworthy.

But that's not how it works anymore. Today, Zero Trust security takes things further: **no one is trusted until proven otherwise**. Whether you're inside or outside the network, every access must be constantly verified.

Where do you start? The first step is usually assessing and mapping out all your assets and network resources to get a clear picture of your environment. But **asset mapping takes time**. That's why it's just as important to put the first layer of security in place right away—locking down access to your production from day one.

For example, implement granular access controls with a **Privileged Access Management (PAM) tool** and use a multi-factor authentication (MFA). This enables continuous verification to monitor and audit network access and activity.

The key here is **to ensure that only the right people/devices access what they truly need**. This way, you're not only keeping intruders out but also preventing potential attackers from moving laterally within your network. It's like locking every door and window in your fortress.

Strategy 2: Centralize and Unify Access to Your OT Systems

I remember a conversation with a plant manager who said, "Gwendal, we have so many VPNs deployed by our vendors and contractors… I don't even know where to start closing them."

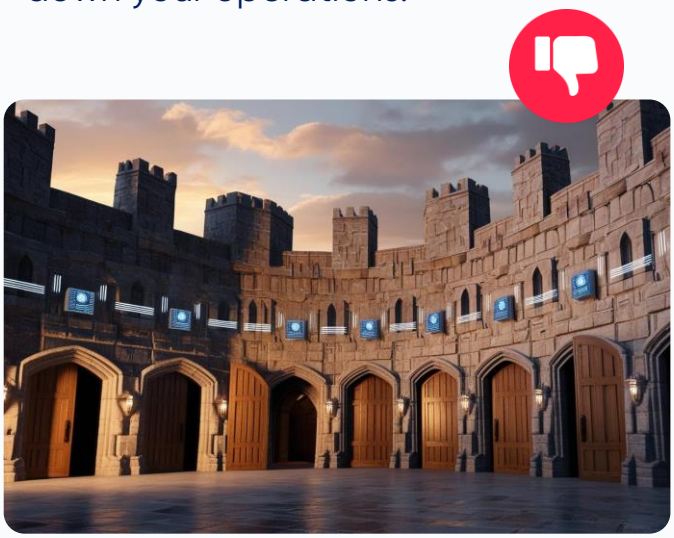
And that's exactly the problem. **The more doors you have, the harder it is to protect your fortress**.

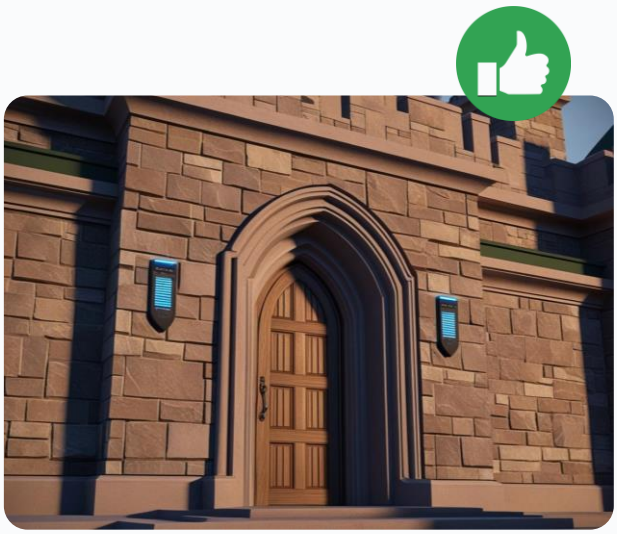
That's why after locking the doors, you should centralize all your accesses to your OT systems into **a single-entry point.**

Not only does this make it easier to manage remote connections, but it also gives you much stronger control over **who gets in and what parts of your network they can access**.

It's like having one drawbridge for your fortress—much easier to monitor and control.

And the best part? You can do this without complicating production. The goal is for security to flow as smoothly as water in a river without slowing down your operations.





Strategy 3: Continuous Monitoring and Anomaly Detection

Here's a little secret: It's not enough to build a wall around your fortress and leave a single entrance door locked by a personalized code. **Your guards need to keep an eye on it 24/7... to ensure security and maintain communication with the command room.** This is where continuous monitoring comes into play.

Deploying sensors and tools throughout your infrastructure **allows you to spot and respond to unusual activity** before it becomes a serious problem.

And, of course, you also need to easily connect your monitoring system to SIEM (Security Information and Event Management) to unify your cybersecurity tools, as we saw earlier (Centralize and Unify!).

I've seen firsthand how this makes a difference.

Once you implement continuous monitoring, **you can detect anomalies in real time and act before the damage** becomes irreversible.

Plus, you get a complete record of everything happening, helping you learn , adjust your security strategy as needed and of course comply to the many regulations.