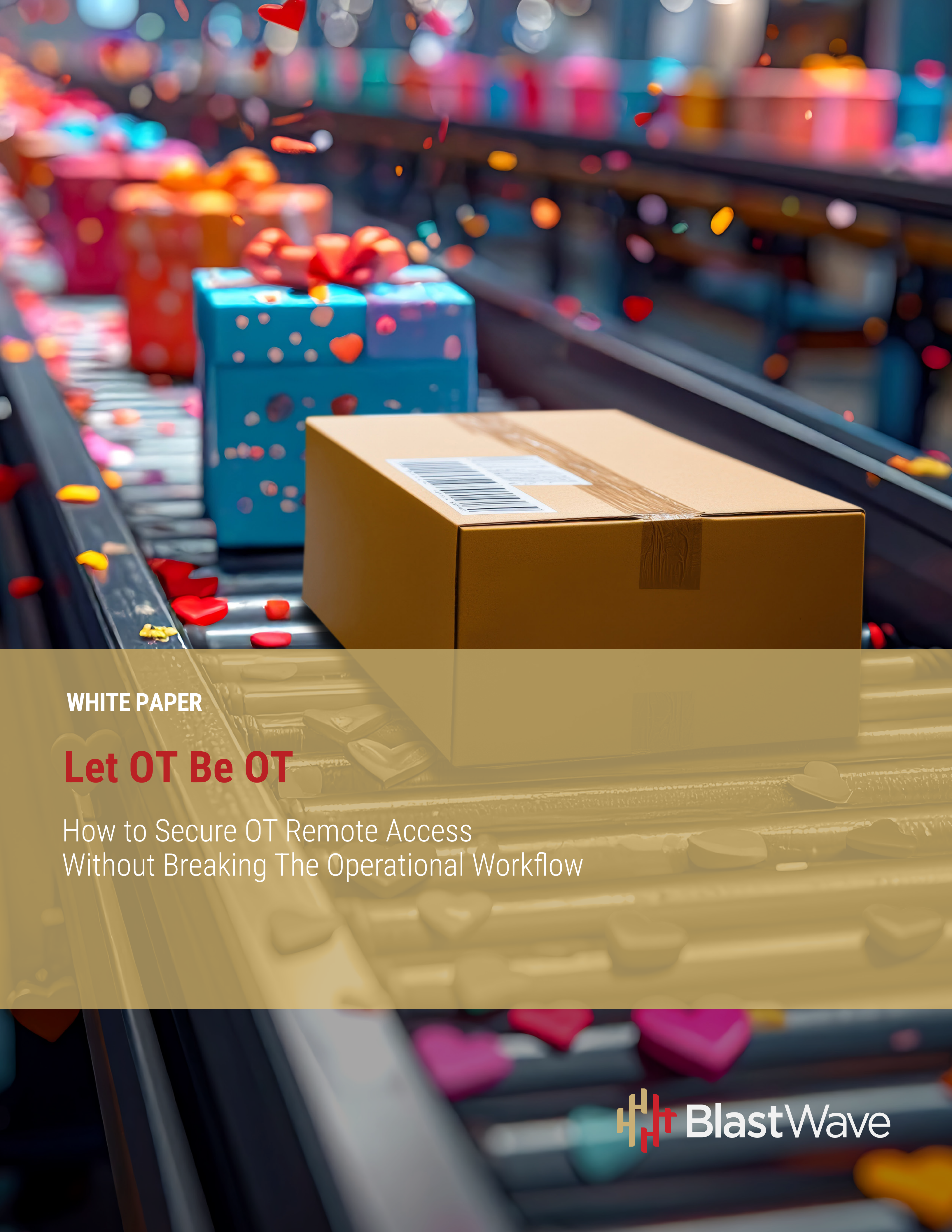

WHITE PAPER

Let OT Be OT

How to Secure OT Remote Access Without Breaking The Operational Workflow

BlastWave

TL:DR

Let's be honest: the air gap is history. We're plugging our control systems into the enterprise network because we have to. We need that data for predictive maintenance, real-time analytics, and remote support. But here is the headache: to secure this new connectivity, IT usually tries to force-feed its standard corporate Privileged Access Management (PAM) tools.

You know the drill: centralized jump hosts, password vaults, and clunky browser-based sessions. That architecture was built for static data centers, not the plant floor. It creates lag we can't afford, relies on vulnerable web browsers, and treats our safety-critical systems like just another server rack.

This whitepaper cuts through the marketing fluff to compare the traditional IT-centric PAM approach against a BlastWave solution that provides both options to customers. We break down why retrofitting IT security tools usually fails in OT, specifically looking at how they struggle with protocol latency and don't actually stop credential theft or lateral movement once an attacker is inside.

Feature	Jump Host / RDP	Interactive Remote Access
Primary Use Case	Compliance audits, vendor monitoring, and basic HMI checks.	Deep engineering, PLC programming, firmware updates.
Application Location	Runs on a remote server (shared resources).	Runs on local laptop (dedicated resources).
Latency Sensitivity	**High:** Input lag affects mouse precision and typing.	**Low:** Local rendering; only data packets traverse the network.
Firmware Safety	**Low:** Session drop can corrupt the upload/brick device.	**High:** Local app manages connection state/retries.
Lateral Movement	**Risk:** The Jump host often has broad visibility of the subnet.	**Restricted:** Microsegmentation limits access to a single IP address and port.
Authentication	**Credential-Based:** Vulnerable to phishing/infostealers.	**Biometric HITL:** Phishing-resistant, binds user to device.
Audit Capabilities	**Visual:** Screen recording of the session.	**Packet/Event:** Logs of who connected to what, when.

CONTENTS

The Evolution and Crisis of OT Remote Access

From "Sneaker-net" to Hyper-Connectivity

Remember when security was simple? The "air gap" was king. If you needed to program a PLC or tweak a VFD, you grabbed your laptop, walked to the cabinet, and plugged it in physically. It was secure, but let's face it: it was inefficient.

Those days are gone. We can't run a modern plant on "sneaker-net" anymore. Whether it's OEMs troubleshooting equipment remotely, historians pushing data to the cloud, or us needing to fix an alarm at 2 AM without driving in, we had to punch holes in the Purdue Model because the business demands connectivity.

Why IT's "Jump Box" Fix Falls Short

When those connections started popping up, IT tried to fix it with the hammer they already had: Privileged Access Management (PAM). They gave us centralized bastion hosts and jump boxes. You know the drill: log into a portal, check out a credential, and stare at a loading screen while an RDP session spins up.

That model might work for managing a SQL server, but it creates a massive choke point for OT. A PLC isn't a server, and treating it like one causes problems. Routing control traffic through a centralized stack introduces latency that can kill timing-sensitive protocols. Even worse, the standard PAM model usually assumes that once you're past the jump host, the network inside is "trusted." It's not. If an attacker breaches that bastion, they can often move laterally across the plant floor without resistance.

The Real Conflict: Security vs. Getting the Job Done

Here is the friction point we all deal with: IT wants rigid access control, but we need operational speed. When PAM solutions force us to navigate complex web portals or endure laggy desktop sessions just to do our jobs, it disrupts our workflow. And we all know what happens next: "Shadow IT."

Engineers start plugging in unauthorized cell modems or installing TeamViewer just to bypass the corporate friction and get things done. BlastWave's approach is to fix that root cause by using a Software-Defined Perimeter (SDP) to make security invisible and fast, so we don't have to resort to risky workarounds just to keep the plant running.

The Identity Crisis: Hacking In vs. Logging In

The "Hackopedia" Reality Check

The threat landscape has shifted. Attackers aren't burning complex zero-day exploits to break down the firewall anymore; they're just logging in. The BlastWave "Hackopedia" makes it clear: the vast majority of modern breaches (about 86%) involve stolen credentials, often initiated by a simple phishing email.

Why Vaults Are a Liability

Here is the uncomfortable truth about the password vaults IT loves: they rely on passwords to protect passwords. It's a single point of failure. If an attacker swipes the credentials to access the PAM portal (which is becoming easier with "Infostealer" malware that grabs browser cookies), the vault just hands them the keys to the kingdom.

They don't need to crack the safe; they just need to look like the person holding the combination.

Case Study: Volt Typhoon

This isn't theoretical. Look at state-sponsored actors like Volt Typhoon. They aren't deploying noisy malware that triggers antivirus detection. They are "Living off the Land", using valid admin credentials to log in and using our own system tools against us. In a traditional PAM setup, if they get an admin's SSO login, the system waves them right through to the HMI.

The PAM checks the ID at the door, but it has no way of knowing whether the person wearing my badge is actually an adversary.

Stop Managing Trust, Start Verifying Identity

PAM's philosophy is "managed trust": they trust the user, so they rotate the password. BlastWave takes a "Zero Trust" approach: we don't trust passwords, so we got rid of them. You can't steal a password that doesn't exist. By moving from shared secrets to public-key cryptography bound to a biometric scan, we neutralize that entire class of attacks.

An attacker can't replay a face scan or steal a private key locked inside a phone's secure enclave.

In 1971, Bob Thomas and Ray Tomlinson at BBN Technologies wrote "Creeper" – a test program designed to self-replicate and spread across computers using ARPANET.

Comparative Analysis:
Interactive Remote Access vs. Jump Host Remote Desktop

For OT engineers and contractors, the choice between running native engineering apps over a secure tunnel versus staring at a Jump Host RDP session isn't just a "preference." It dictates whether you can actually do your job effectively or if you're just fighting the interface. While traditional PAM solutions try to shoehorn every single task into that "Jump Host" model, a realistic OT security strategy knows better. You need both tools in the toolbox, mapped to the specific task at hand, rather than a one-size-fits-all mandate.

Operational Capability: The "Laggy Mouse" vs. The Native Experience

The Jump Host Experience (Remote Desktop/RDP)

In this model, the engineer connects to a centralized server (Jump Host) and controls it remotely. The engineering software (e.g., Studio 5000, TIA Portal) runs on the server, not the engineer's laptop.

- **Best For:** Quick diagnostics, HMI monitoring, and "read-only" supervision.
- **The "HMI Tuning" Problem:** RDP transmits screen updates. In OT environments with high latency (e.g., satellite or cellular connections), this creates input lag. Attempting to tune a PID loop or drag-and-drop ladder logic components can be frustrating and error-prone due to the delay between mouse movement and screen updates.
- **The Peripheral Gap:** Technicians often require physical USB dongles for software licensing or serial-to-USB adapters to connect to legacy PLCs. RDP's USB redirection is usually unstable or disabled by policy, rendering the jump host useless for hardware-dependent tasks.

The Interactive Access Experience (Native Tunneling)

In this model, the engineer runs the software locally on their workstation. A secure, encrypted tunnel connects the application directly to the target device's specific port (e.g., TCP 102 for Siemens).

- **Best For:** Complex programming, firmware updates, and heavy engineering.
- **Performance:** Local execution utilizes the engineer's powerful laptop CPU/GPU. Only lightweight command/control traffic traverses the network, eliminating screen lag.
- **The "Firmware" Criticality:** Updating PLC firmware over RDP is risky. If the RDP session freezes or drops during a file transfer from the jump host, the process can fail, potentially "bricking" the controller. Native tunneling allows the local application to manage packet consistency and retries more robustly.

Security Implications: Attack Surface and Segmentation

Identity and Access Surface

- **Jump Host:** Relies heavily on web browsers for the initial portal login. This exposes the session to "Infostealer" malware and Adversary-in-the-Middle (AiTM) attacks, where session cookies or credentials can be harvested. Once an attacker compromises the RDP credentials, they often gain full GUI access to the jump host.
- **Interactive:** Uses a dedicated client with highly desirable Human-in-the-Loop (HITL) biometric authentication. It does not rely on a browser, neutralizing browser-based credential theft and phishing. The user must physically approve access on a mobile device, binding the identity to a specific machine and person.

Network Segmentation (East-West Traffic)

- **Jump Host:** Typically focuses on "User-to-Device" security. Once a user lands on the jump host, they are effectively "inside" the network segment. If the jump host can "see" 50 PLCs, a compromised user (or malware on the jump host) can scan and attack all 50. It acts as a bridge rather than a barrier.
- **Interactive:** Also enforces Device-to-Device microsegmentation. The encrypted tunnel connects the user only to the specific IP and Port authorized by policy (e.g., "Allow User A to access PLC B on Port 44818 only"). The rest of the network remains "cloaked" (invisible). Even if the user is connected, they cannot scan for other devices or move laterally.

Authentication: Why Are We Trusting Web Browsers with Critical Infrastructure?

The Browser is the Weakest Link

Let's be real about the standard OT PAM workflow: you open Chrome or Edge, go to a web portal, and log in via Okta or Azure AD. Once you're in, the browser effectively becomes your HMI, rendering RDP sessions right there in the window.

Think about that for a second. We are protecting million-dollar industrial processes with the same software used to watch YouTube and download random PDFs. Browsers are incredibly complex, full of holes, and literally designed to execute arbitrary code from the internet. Relying on them as the gateway to the plant floor isn't just a security risk; it's a massive step backward.

The "Standard" IT Stack is Leaking

Using a browser for access opens us up to attacks that standard MFA just can't stop:

- **Adversary-in-the-Middle (AiTM):** Smart phishing kits don't just steal passwords; they proxy the whole login flow. You type your code into a fake site, and the attacker passes it to the real site in real-time. They get the session token; you get hacked.
- **Cookie Theft:** If you pick up malware on your laptop (maybe from a personal email), it can scrape the "session cookies" from your browser storage. Attackers can then "replay" your session later without ever needing your username or password.
- **The Extension Problem:** Bad browser extensions can hook into the data stream after decryption, but before you see it. It's a "Man-in-the-Browser" attack that can capture keystrokes or modify session parameters right under your nose.

BlastWave's Fix: Human-in-the-Loop (HITL)

BlastWave ditches the browser entirely for authentication. We move the verification "out of band" to a dedicated mobile app: the BlastWave Authenticator. It separates the control plane (who you are) from the data plane (the network connection).

Here is how it actually works:

- **Device Binding:** Your identity isn't a password; it's a private key locked inside the secure hardware enclave of your phone. It can't be cloned or exported.
- **Biometrics:** To use that key, you have to prove you are you via FaceID or fingerprint.
- **Real Intent:** When a connection request comes in, you receive a push notification that you must actively approve (via a QR Code).

Security Architecture: North, South, East, and West Lateral Movement

The "User-to-Device" Trap: The "Eggshell" Problem with PAM

Let's talk about the structural flaw in traditional PAM setups. We call it the "hard shell, soft center." The "shell" consists of the authentication portal and the jump host. It looks tough from the outside. But once you crack that shell (or if an attacker compromises the jump host itself) they usually land in a "soft center" where the internal network is flat and wide open.

PAMs are proxies designed to secure your connection to a target. They don't control what happens between those targets. Say an engineer connects to Engineering Workstation A. If that workstation is infected with ransomware, the PAM is powerless to stop it from scanning and infecting PLC B, HMI C, and Historian D on the same subnet. That lack of control over East-West traffic is a massive vulnerability in OT, especially when we're dealing with legacy gear that hasn't seen a patch in a decade.

BlastWave's Fix: Make the Network Invisible

BlastWave flips the script with a Software-Defined Perimeter (SDP). We stop caring about network topology and start building connectivity based on identity.

Network Cloaking (Invisibility Mode)

We drop a BlastShield Gateway in front of your critical assets, and by default, it operates in "deny-all" mode. It literally ignores unsolicited TCP/IP packets. If a hacker runs a scan, they get nothing back. To an unauthorized user or a compromised device, your assets don't just look secure; they look like they don't exist. You can't attack a PLC if you can't even find its IP address. It breaks the "reconnaissance" phase of an attack before it even starts.

Real Microsegmentation (User-to-Device and Device-to-Device)

Unlike a PAM that only watches the front door, BlastWave enforces policy on all traffic through the Gateway. This means we can lock down East-West traffic, too. You can set a rule that says, "The HMI can talk to the PLC on Modbus TCP Port 502, and absolutely nothing else." It wraps a virtual firewall around every single asset. Even if the HMI gets compromised, it can't be used as a launchpad to take down the rest of the line. That is Zero Trust that actually reaches the plant floor.

The “RDP Trap” in OT

Let’s talk about the default setting for most PAMs: Remote Desktop Protocol (RDP). It’s fine if you’re an IT admin resetting a password on a domain controller. But for us? It’s a nightmare. RDP relies on streaming screen video in a high-latency environment (like a site running on a cellular or satellite backhaul), which means input lag.

When you’re trying to drag a slider to tune a PID loop or click a specific button on an HMI, a 500ms delay isn’t just annoying; it’s dangerous. You over-correct, you miss-click, and suddenly you have a safety incident.

And then there’s the hardware headache. We all have that drawer full of proprietary USB dongles for software licensing (looking at you, FactoryTalk) or serial adapters for legacy controllers. Trying to get RDP to redirect a USB device over a WAN reliably is a losing battle. Half the time, IT security policies block it anyway, rendering the session useless for anything that needs a hardware key.

The Nightmare Scenario: Firmware Updates

The biggest risk? Updating firmware. If you’re pushing a firmware update via a file transfer on a jump host RDP session and the packet drops or the session hiccups, you risk bricking a very expensive controller. You simply can’t rely on a “screen scrape” session for critical transfers.

BlastAccess vs. Native Tunneling

BlastWave knows we sometimes need RDP for the auditors or third-party vendors who just need to “look but not touch.” We call that Blast-Access: it gives them a recorded, browser-based session that keeps compliance happy.

But for the engineers doing the heavy lifting, BlastWave supports a Full Interactive Client. This is the game changer. Instead of struggling with a laggy remote screen, you run your native apps (TIA Portal, Studio 5000, etc.) right on your own powerful laptop. The BlastShield client creates a secure, encrypted tunnel specifically for that app traffic directly to the PLC.

- **Performance:** Your laptop’s GPU handles the graphics. Only the command packets cross the network. No more “laggy mouse.”
- **Reliability:** Native apps handle network jitter way better than RDP does.
- **Security:** It’s strictly Least Privilege. We can tunnel only the specific ports the software needs (like TCP 102 for Siemens). You can program the PLC, but you can’t browse the file system or mess with the OS.

Feature	OT PAM Solution	OT SDP Solution
Architectural Model	Centralized Proxy (Hub & Spoke)	Peer-to-Peer Mesh (SDP)
Visibility Scope	User-to-Device (North-South)	User-to-Device (North-South) & Device-to-Device (East-West)
Internal Network Posture	Often Flat / Open behind Jump Host	Microsegmented / Cloaked
Lateral Movement Defense	Minimal (reliant on VLANs/ Firewalls)	High (Identity-based Microsegmentation)
Reconnaissance Defense	Assets visible to internal scans	Assets invisible (Cloaked) to scans

Cloud vs. Mesh: Latency and Performance

Most “Cloud PAMs” force your traffic to “trombone”; it goes from your house, to an AWS server three states away, and then back to the plant. It adds latency and creates a choke point.

BlastWave uses a Peer-to-Peer (P2P) Mesh. The Orchestrator handles the security check, but the data connection is direct: from you to the edge gateway.

- **Traffic Flow:** User (Home) ISP BlastShield Gateway (On-Prem).
- **Direct Path:** The encrypted tunnel is established directly between the user’s client and the edge gateway, taking the shortest possible path across the internet.
- **The Speed Difference:** Independent tests by the Tolly Group showed BlastShield hitting 2.5 Gbps throughput, while cloud-based VPNs struggled at 74 Mbps. That’s a 34x performance gap. If you’re moving CAD files or watching video feeds, that is the difference between “instant” and “go get a coffee.”
- **Efficiency:** Testing showed virtually no wasted bandwidth or retransmissions with BlastShield, whereas cloud-based competitors experienced high retransmission rates due to packet loss in the proxy relays.

Surviving the Outage

Finally, there is the dependency issue. With Cloud PAMs, if the internet connection to their cloud proxy dies, you’re locked out, even if you’re sitting in the plant parking lot. BlastWave separates the control plane from the data plane. If the internet flickers, your local mesh connections stay up, ensuring you maintain control when things go sideways.

Most “Cloud PAMs” force your traffic to “trombone”.

Operational Reality: The Heavy Lift vs. The Easy Button

The Operational Burden of PAM

Let's be honest: deploying a traditional PAM is not a quick install; it's a career event. It creates infrastructure sprawl. You aren't just installing software; you're building a server farm. You need a Vault for storage, a Session Manager for proxying, a Web Portal for access, and Connectors for every network segment. That is a lot of extra VMs to feed, water, and patch on the weekends.

The "Consultant Tax"

Getting it running is even worse. You're looking at complex Active Directory integration, rewriting firewall rules to let the proxies talk, and a months-long "discovery" phase just to find the accounts you need to manage. It usually requires expensive professional services to get off the ground. And the licensing? It's a minefield. It's a high upfront cost with a long tail of hidden maintenance.

Killing the "Truck Roll"

Here is the real ROI for the OT crowd: stopping the truck rolls. We all know the pain of acquiring a new facility or integrating a skid that uses the same 192.168.1.x IP range as the rest of the plant. Usually, that means re-IPing the whole line or driving out to install complex NAT rules. BlastWave's software-defined overlay automatically handles overlapping IP spaces. We cloak the network complexity so you don't have to drive three hours just to reboot a hung VPN router or fix an IP conflict.

.

Conclusion:
The Strategic Move is to Choose a Combined Solution

Recommendation

For a robust OT security posture, organizations need a solution that offers both modalities:

- **Use Secure Remote Desktop** for third-party vendors and auditors who need supervised, recorded access without installing software.
- **Use Interactive Access** for employees and trusted integrators who need high-performance, native access to perform complex maintenance without the operational risks of RDP.

It's time to move past the "jump host-only" paradigm. Instead of forcing every user through a bottlenecked, browser-based portal, we should use a solution that meets both our interactive and remote desktop needs in one place. Consolidating on BlastWave simplifies the stack, reduces TCO, and gives us a resilient foundation that keeps up with production. The data is precise: to secure the physical world, we have to stop using the legacy tools built for the virtual one.

We use a transparent licensing model: no nickel-and-diming for "extra features." And because you aren't managing password vaults or rotating credentials anymore, the daily operational cost drops significantly. You spend less time managing the security tool and more time managing the plant.

Why BlastWave Fits OT Like a Glove

- **Security:** By swapping out passwords for biometric "Human-in-the-Loop" checks and replacing porous firewalls with a cloaked perimeter, it kills the two biggest threats OT networks face: credential theft and reconnaissance.
- **Performance:** That P2P mesh architecture isn't just a buzzword; it delivers 34x the throughput of cloud proxies. That means we can finally use our native, high-performance engineering tools the way they were meant to be used, something RDP just can't handle.
- **Flexibility:** It gives us the best of both worlds. We use BlastAccess to provide contractors and auditors the restricted, recorded web sessions they need, and we use Native Tunneling for our own complex, latency-sensitive work.

Operational Metric	OT PAM Solution	BlastWave Solution
Deployment Time	Weeks to Months (Complex Integration)	**Hours to Days** (Overlay Architecture)
Infrastructure	Heavy (Vaults, Proxies, Balancers)	**Light** (Gateways, SaaS Orchestrator)
Skill Requirement	Specialized PAM Admin Certification	**General Network/OT Knowledge**
Password Mgmt	High (Rotation scripts, broken dependencies)	**None** (Passwordless/Certificate-based)
User Training	Moderate/High (Portal navigation)	**Low** (Mobile App push approval)
Maintenance	High (Patching multiple server roles)	**Low** (Auto-updating Gateways)

BlastWave's OT Protection Solution

BlastWave delivers a comprehensive Zero Trust Network Protection solution to provide the best possible outcome for OT environments. With a unique combination of network cloaking, secure remote access, and software-defined microsegmentation, we minimize the attack surface, eliminate passwords, and enable segmentation without network downtime.

To learn more, come to
www.blastwave.com

v20260126

About BlastWave

BlastWave securely connects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks with Zero Trust Protection and delivers industrial-grade cybersecurity with consumer-grade ease-of-use. Visit **www.blastwave.com** to learn more.

BlastWave

1045 Hutchinson Ave.
Palo Alto, CA 94301 USA
T: +1 650 206 8499