LET OT BE

THE WHITE PAPER

BLASTWAVE

A BlastWave
Tribute Whitepaper

$66\frac{1}{6}$

SIDE 1

BLASTWAVE
LET OT BE

2D
BLWV 101
220260126

© 2026

Produced by BlastWave Marketing

BLASTWAVE
LET OT BE

A BlastWave
Tribute Whitepaper

$66\frac{1}{6}$

SIDE 2

2D
BLWV 101
220260126

© 2026

Produced by BlastWave Marketing

YESTERDAY

All our security troubles seemed so far away. The air gap was our primary defense. But now, it looks as though connectivity is here to stay. We're plugging control systems into the enterprise because we have to for predictive maintenance and real-time analytics.

But **Help!** IT is trying to force-feed us their standard Privileged Access Management (PAM) tools. You know the drill: centralized jump hosts and clunky browser sessions. That architecture was built for static data centers, not the plant floor. It creates lag that makes us want to Twist and Shout, relies on vulnerable browsers, and treats safety-critical systems like just another server.

This ebook cuts through the noise to compare the traditional approach against BlastWave. We break down why retrofitting IT tools leaves us saying **I Need You** in terms of performance and security, and how a new approach can help us **Get Back** to operational efficiency.

THE LONG AND WINDING ROAD

Remember when security was simple? If you needed to program a PLC, you walked to the cabinet. It was secure, but inefficient. Those days are gone. Whether it's OEMs troubleshooting remotely or historians pushing data to the cloud, we've had to punch holes in the Purdue Model. We're working Eight Days a Week keep these plants running, and connectivity is the only way.

Fixing a Hole

When those connections started popping up, IT tried to fix it with the tool they had: PAM. They gave us centralized jump boxes. You log in and stare at a loading screen. That might work for a SQL server, but for OT, it's a drag. Routing control traffic through a centralized stack introduces latency that can kill timing-sensitive protocols. Even worse, once you're past the jump host, the network is often wide open. If an attacker gets in, they can travel **Here, There, and Everywhere**

BlastWave

Pay No attention to the text in this little box.

stereo

DO YOU WANT TO KNOW A SECRET?

The threat landscape has shifted. Attackers aren't breaking down the firewall; they're just logging in. It's no longer a secret: 86% of breaches involve stolen credentials.

She Came in Through The Bathroom Window

Here is the uncomfortable truth about password vaults: they rely on passwords to protect passwords. It's a single point of failure. If an attacker swipes the credentials to access the portal, the vault just hands them the keys. They don't need to crack the safe; they just need to look like the Fool on the Hill who owns the account.

Nowhere Man

Look at state-sponsored actors like Volt Typhoon. They are "Living off the Land," using valid admin credentials. In a traditional PAM, if they get an SSO login, the system waves them through. The PAM checks the ID at the door, but it doesn't know if the person is a Real Nowhere Man or a legitimate engineer.

Imagine

BlastWave takes a Zero Trust approach: we don't need passwords, so we got rid of them. You can't steal a secret that doesn't exist. By moving to biometric keys, we neutralize the threat. An attacker can't replay a face scan.

We Can Work It Out

For OT engineers, the choice between native apps and RDP isn't just a preference. It dictates whether you can do your job. While traditional PAM says You Can't Do That, a realistic strategy recognizes you need both.

Slow Down

RDP relies on streaming video. In high-latency environments, this means input lag. When you're trying to tune a PID loop, a 500ms delay makes you want to shout "Don't Bother Me." And don't get me started on USB dongles. Trying to redirect hardware keys over RDP is a losing battle.

Getting Better

BlastWave supports a Full Interactive Client. You run TIA Portal or Studio 5000 locally on your laptop. A secure tunnel connects specifically to the PLC.

- **Performance:** Your laptop handles the graphics. No more "laggy mouse." It's getting better all the time.
- **Firmware Safety:** Native apps handle network jitter gracefully. You won't brick a controller because of a screen freeze.

Traditional PAMs have a "hard shell, soft center." Once an attacker cracks the shell, they land in a flat network. If Workstation A is infected, it can attack PLC B easily. It's like leaving a hole in the roof where the rain gets in.

You Won't See Me

BlastWave flips the script. We drop a Gateway that operates in "deny-all" mode. If I'm an unauthorized user, your assets don't just look secure; **I'm Looking Through You** They are invisible. You can't attack a PLC if you can't find it.

I Me Mine

We enforce policy on all traffic. You can say, "The HMI can talk to the PLC, and **Run for Your Life** if you try anything else." It wraps a virtual firewall around every asset.

Cloud PAMs force traffic to go Across the Universe from your house, to a cloud server, and back to the plant. This Magical Mystery Tour creates latency.

From Me To You
BlastWave uses a Peer-to-Peer mesh. The connection is direct.

- **Speed:** Tests show a 34x performance gap. That's the difference between "instant" and "waiting a long, long, long time."
- **Resilience:** If the internet dies, local mesh connections stay up. **We Can Work It Out** so you don't have to.

CARRY THAT WEIGHT

Deploying PAM is a career event. You're building a server farm – Vaults, Proxies, Connectors. You need expensive pros to get it running and the "Consultant Tax"? It's high.

Daytripper

Here is the ROI: stopping the truck rolls. When you acquire a new facility with overlapping IPs, usually you have to get out there to fix it. BlastWave's overlay handles it automatically. If I'm a service engineer, I won't have to **Drive My Car** three hours each way, just to reboot a router.

HERE COMES THE SUN

In **The End** the data is clear. To secure the physical world, we must abandon the legacy tools of the virtual one.

- Use BlastAccess for third parties (Compliance).
- Use Native Tunneling for engineers (Performance).

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.

All You Need Is Love
(and a combined OT security solution).

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

**And in the end,
the security you take
is equal to the architecture
you make.**

v20260129

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.

©2025 BlastWave Inc.

BlastWave

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