USE CASES

Preventing Industrial Cyberattacks for the Energy Industry

Your Relays and RTUs Stop Answering Scans

BlastWave

The deepest anyone can usually see into a substation is the top-of-rack switch. Below that sit relays, RTUs, and controllers installed across three decades, on protection settings nobody wants to touch.

Replacing a substation controller requires an energized outage, a review of protection settings, and a change record. So it gets deferred, and the deferral becomes permanent. This book starts from that reality rather than arguing with it.

The reference event, told accurately

The Waterfall and ICS STRIVE 2026 OT Cyber Threat Report documents the December 2025 attack on Polish distributed energy resources. Russian attackers broke into over 30 small wind and solar generators, plus control equipment at a CHP plant supplying heat to nearly half a million customers, and erased firmware on an undisclosed number of automation devices, rendering them permanently unbootable.

Forensics determined the attackers held administrative privileges on the firewalls deployed at each affected site, having gained access months earlier.

Every one of those sites had a perimeter. None of them stopped the attack.

CONTENTS

Reconnaissance Stopped Being Expensive

Every documented OT attack chain begins the same way. Something scans, and something answers. For three decades, that first step was the expensive one, so attackers selected targets, and most substations were never worth selecting.

That economics is gone. What is measurable is what the scanning is now attached to: CrowdStrike's 2026 Global Threat Report records an 89% increase in attacks by AI-enabled adversaries, a 42% increase in zero-day vulnerabilities exploited prior to public disclosure, and an average eCrime breakout time of 29 minutes.

Set 29 minutes against the replacement cycle for a substation controller. Those two curves crossed some time ago, and they are not crossing back.

One principle, four functions

Network Cloaking. Protected assets do not respond to unauthorized scans.

Passwordless MFA. Access binds to an enrolled device and a live biometric. If you already use MFA, you are not being asked to replace it; what changes is that the credential no longer grants access.

Software-Defined Segmentation. Least-privilege policy without ACLs, VLAN re-architecture, or new hardware.

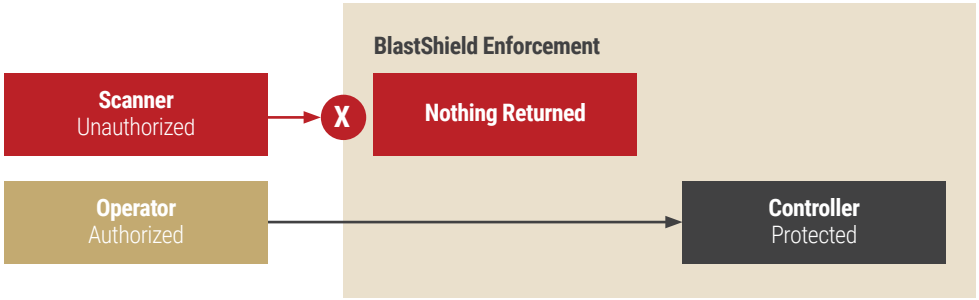
Secure Remote Access. Replaces VPN. No inbound open ports, no concentrator.
Where the Gateway sits

A Security Gateway goes in front of the segment you are protecting. It is where policy is enforced. It is not what an attacker finds.

Unauthenticated packets are silently dropped. Not refused, not reset, not returned with an error. A scanner cannot tell that apart from empty address space.

Several vendors now market asset hiding, so the claim alone is no longer a differentiator. The question worth asking of any of us is whether the packets are dropped without a reply, or whether an appliance in the path must remain reachable to function.

Figure 1: One address. Two outcomes.



An unauthorized scanner's packet reaching a BlastShield enforcement point and being dropped with nothing returned, while an authenticated client reaches the same controller and gets a normal response.

USE CASE 1:

The Asset You Cannot Patch

The Scene

A GE D20-generation substation controller has a public vulnerability with proof-of-concept code, no security firmware track, and a vendor whose answer is a different box. CISA published the alert in 2012. The controller is still in the rack.

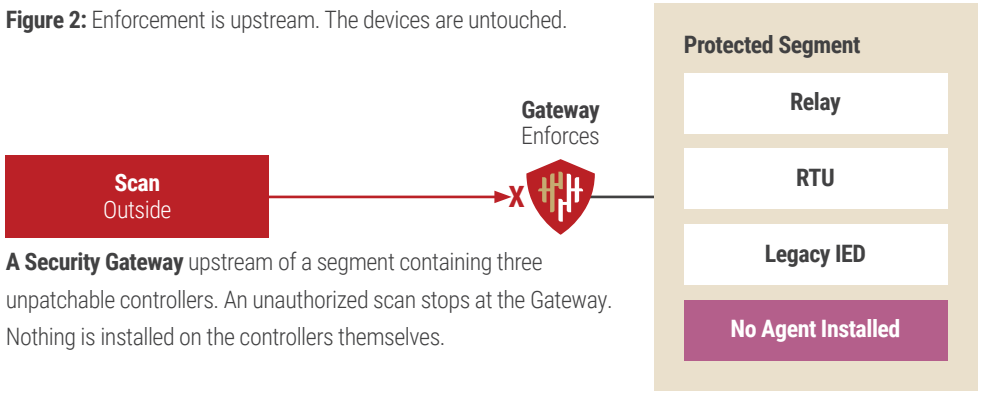
It is not on a patch schedule because there is nothing to schedule, and touching it means an energized outage plus a protection settings review. Most operations teams stopped calling this a security problem years ago and started calling it the site.

The Mechanism

A Security Gateway sits upstream of the segment where those assets reside. Nothing is installed on the IED, no firmware changes, and the protection scheme is untouched. From outside, and from a scanner already inside the segment, the assets stop returning results.

You cannot patch a relay. You can stop it from answering.

Figure 2: Enforcement is upstream. The devices are untouched.



A Security Gateway upstream of a segment containing three unpatchable controllers. An unauthorized scan stops at the Gateway. Nothing is installed on the controllers themselves.

The Objection

"Sixteen substations means sixteen gateways. That is expensive."

It also keeps your substations separate, which is usually the more valuable half. Deploying per substation means we do not create a new aggregation point or a shared enforcement boundary between sites, so our architecture does not pull assets from low impact to medium impact.

There is no cloud dependency either. The Orchestrator runs on-premises; there is no need to send OT traffic anywhere, and the data path does not require internet connectivity to function.

The Evidence

Both failed and permitted access attempts are logged, with configurable retention and four export paths: local storage, API, syslog streaming, and CSV over FTP. For an asset you cannot fix, the failed half is a dated record of everything that tried to reach it.

The Regulatory Hook

No CIP standard requires cloaking by name. Ask the scope question first: municipal or cooperative utility distribution substations are often not registered BES assets, and a project framed around CIP that does not apply is built on the wrong argument.

BlastShield does not patch anything and does not claim to. It changes what an unauthorized scanner can reach, which on a controller whose vendor stopped shipping fixes is usually the cheapest lever left.

USE CASE 2:

The Substation Nobody Visits

The Scene

A distribution substation with limited power and space, a handful of IEDs, and a relay technician who visits on a schedule and does not report to security. On renewable sites, the pattern repeats with different equipment: third-party O&M holds the keys, and the monitoring appliance installed at commissioning is often the most reachable thing on site and the least likely to have been updated since.

Serial-to-Ethernet converters make this worse quietly. A device that was never designed to be routable becomes routable, and nobody records the day it happened.

The Mechanism

The site keeps its connectivity. What changes is that the assets stop answering anything that has not authenticated first, so they do not appear in a scan of the address space they reside in. No truck roll, no firmware change, no argument with the OEM about touching their box.

The easiest asset in your estate to find is the one nobody drives to.

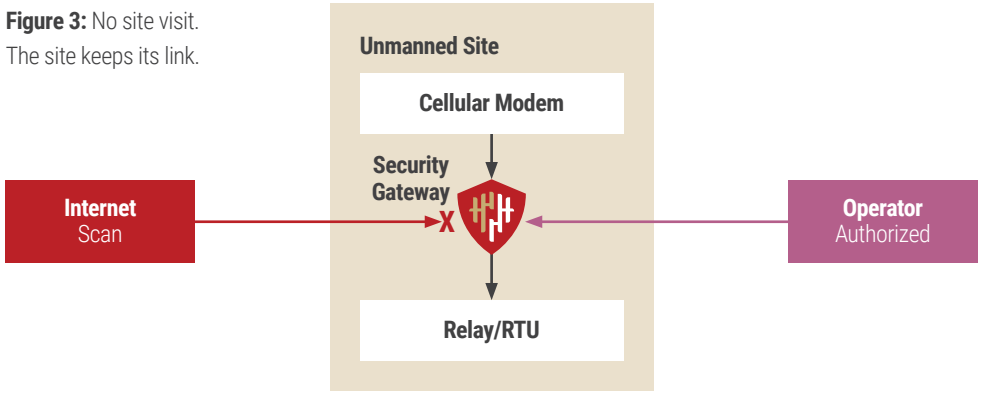


Figure 3: No site visit. The site keeps its link.

An unmanned site holding a cellular modem, a Security Gateway, and one controller. A scan from the internet is dropped and returns nothing. An authorized operator reaches the same controller through an encrypted tunnel.

The Objection

"The relay technician holds the veto and he will not sign off on this."

He is right to hold it, and this is the argument that wins him over rather than the one that overrules him. Nothing is installed on the IED. The protection scheme is not modified. The poll cycle is not rewritten. What changes sits upstream of the equipment he is accountable for, and he keeps every path he uses to do his job.

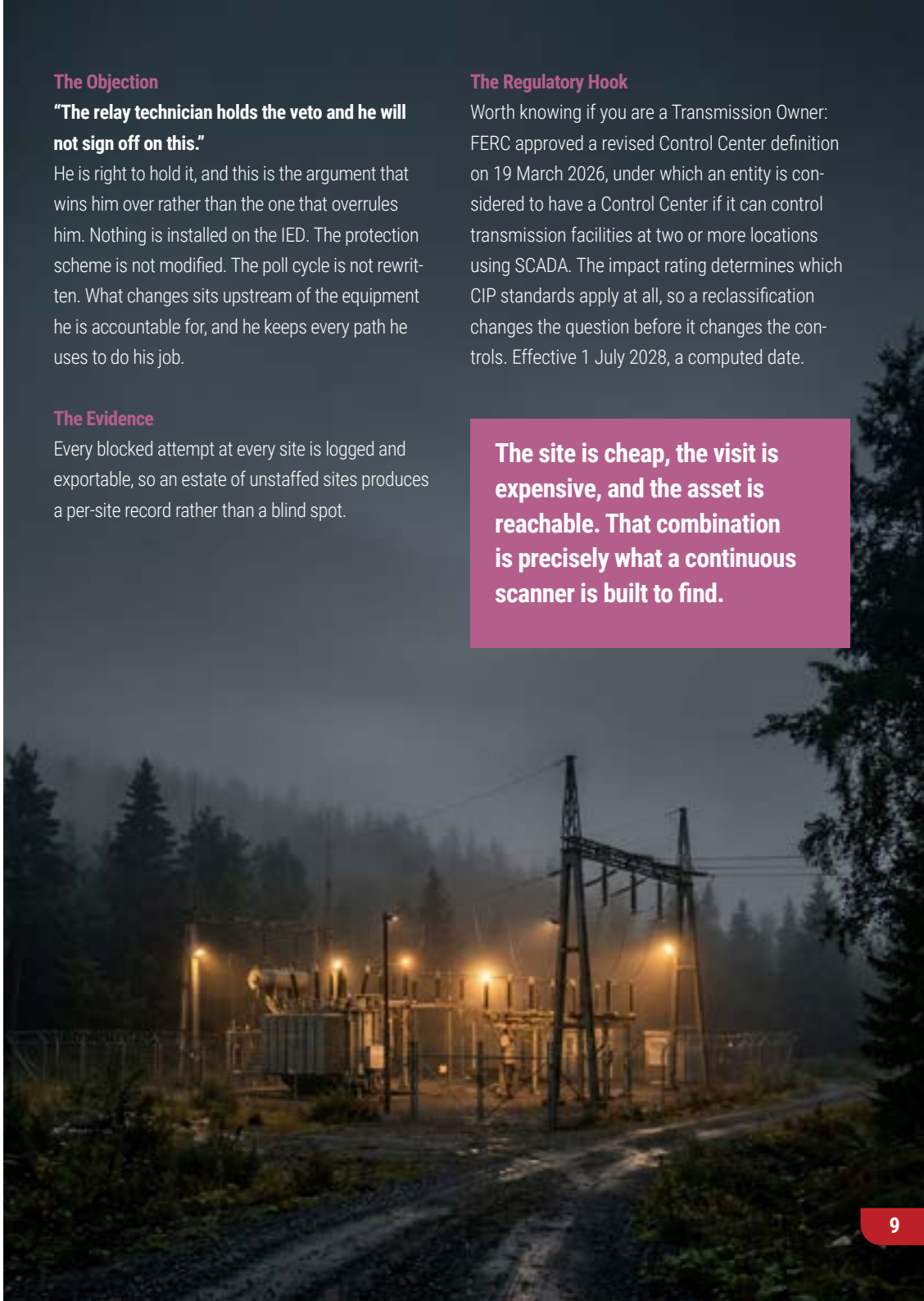
The Evidence

Every blocked attempt at every site is logged and exportable, so an estate of unstaffed sites produces a per-site record rather than a blind spot.

The Regulatory Hook

Worth knowing if you are a Transmission Owner: FERC approved a revised Control Center definition on 19 March 2026, under which an entity is considered to have a Control Center if it can control transmission facilities at two or more locations using SCADA. The impact rating determines which CIP standards apply at all, so a reclassification changes the question before it changes the controls. Effective 1 July 2028, a computed date.

The site is cheap, the visit is expensive, and the asset is reachable. That combination is precisely what a continuous scanner is built to find.



USE CASE 3:

The Vendor Who Already Has Access

The Scene

The integrator who commissioned the SCADA system still has remote access to it. So does the OEM who supports the relays, and the O&M contractor on the renewable sites. Some of that access predates the people now accountable for it, and in the December 2025 Polish attack the adversary held administrative privileges on the site firewalls for months before anyone noticed.

The Mechanism

Vendor access is replaced with least-privilege access scoped to named equipment, bound to an enrolled device, and time-limited to the window you grant. Privileges are granted or revoked in real time by your team rather than by a ticket to IT (an active session can be manually terminated while it is in progress), and every attempt is logged, permitted and failed alike.

The account you cannot revoke is the one that matters.

The Objection

"How does this sit with CIP-005?"

CIP-005 requires Interactive Remote Access to pass through an Intermediate System, so the initiating client does not directly access the Cyber Asset. BlastAccess provides that break: the tunnel runs from the client to the BlastAccess server, never to the end station, and the session is recorded.

Two things follow and we would rather say both. An Intermediate System is itself an EACMS, so BlastAccess sits inside your CIP scope by design rather than by accident, which pulls CIP-004, 006, 007, 009, 010, 011, and 013 onto it. And the determination is yours to make with your auditor. We supply the architecture and the evidence, not the finding.

The Evidence

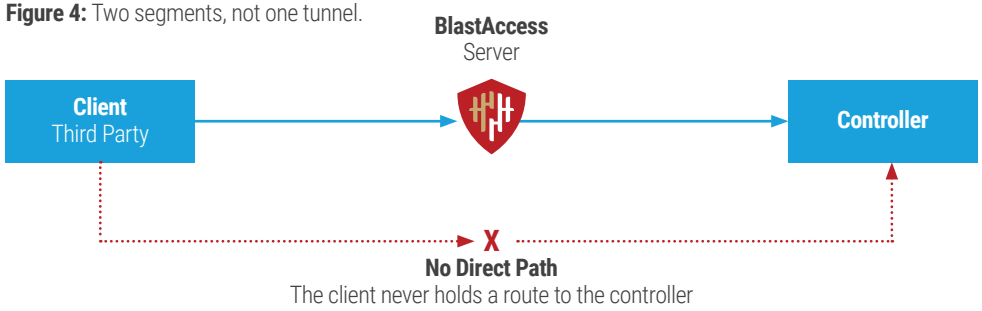
Session recording, the access log covering both halves, and a configuration change log. That is the answer to who reached this, when, and what they did.

The Regulatory Hook

CIP-003-9 has been enforceable since 1 April 2026 and lands on low impact BES Cyber Systems: find where vendor remote access exists, disable it, and detect malicious communications within it. **Two of those three are not ours.** Finding it is discovery and detecting it is monitoring. Disabling it is the product.

CIP-003-11 is the successor, approved 19 March 2026 and effective 1 July 2029 on a computed date. It asks you to authenticate remote users and protect authentication information in transit, and it is the better fit of the two. Plan against both rather than either alone.

Figure 4: Two segments, not one tunnel.



A BlastAccess session in two separate segments, client to BlastAccess server and BlastAccess server to controller, with no direct network path between the user's machine and the controller

This is a category property rather than a BlastWave defect. Anything carrying Interactive Remote Access into an ESP is an EACMS, including every PAM product and every competitor in this field.

USE CASE 4:

The Machine That is Not a Person

The Scene

Grid modernization arrives from the other direction. DER orchestration. AI load forecasting. An advanced distribution management system that wants to read from assets it was never designed to reach.

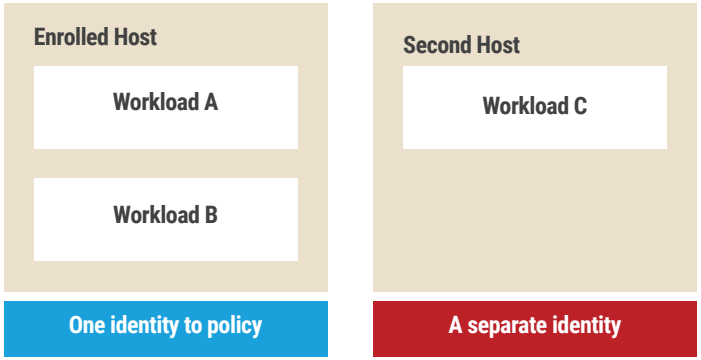
Each of those is a non-human identity that needs a path into the substation, and none of them is handled by controls designed for employees. They do not take training, and they do not get offboarded. They are introduced by an engineering or planning team, and the first security conversation usually happens after the pilot is running.

The Mechanism

The connectivity these platforms need is the connectivity a technician needs: identity-bound, least-privilege, and not discoverable from anywhere else. BlastShield Agent protects at the server level and permits connections only from verified clients. Strict egress policy enforcement means that a host attempting to reach an unauthorized external destination is blocked rather than detected afterward.

Your DER orchestration platform cannot sit through security awareness training.

Figure 6: Separating workloads means separating hosts.



Two AI workloads running on a single enrolled host, indistinguishable to BlastShield because enforcement is bound to the host. A second, separate host beside it showing that separating workloads means separating hosts.

The Objection

"Security is what is holding up our DER project."

Usually because the platform needs to reach assets on protection settings nobody wants to touch, and the only way anyone knows how to grant that is broadly. Scoped, logged, identity-bound access makes it a narrower request than opening a path into the substation, and the relay technician who holds the veto can see exactly what it reaches.

Be precise about the unit of enforcement. **BlastShield enforces at the enrolled host, not at the workload.** Two models on one server are indistinguishable from each other to it. If they need separating, separate the hosts

The Evidence

The same access and configuration logs, plus egress enforcement records. For a workload nobody can interview after an incident, a dated record of what it was permitted to reach is most of the account you will get.

The Regulatory Hook

None yet, and be skeptical of anyone who says otherwise. No CIP standard sets requirements specific to autonomous platforms in the substation. You will be assessed against the existing access control and remote access requirements.

Two agents on a single enrolled host are a single identity to BlastShield. That is a real limit, and it is better to hear it now than during a design review.

USE CASE 5:

What BlastShield Does NOT Do

The Scene

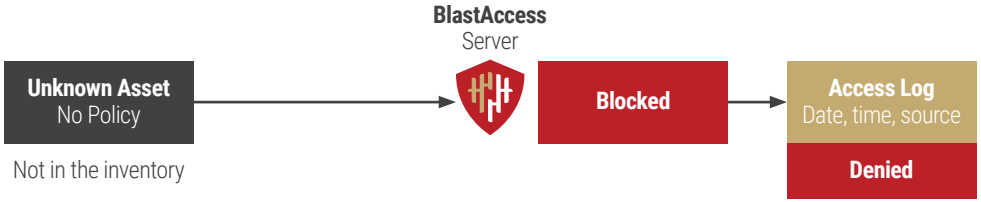
Most security questionnaires open with inventory, and it is the question most utilities cannot answer honestly, because the inventory was accurate when it was made, and equipment has moved since. The usual vendor response is to promise discovery. Ours is to say where this control ends, because a CIP compliance manager reads the standard for a living and will find the edge anyway.

The Mechanism

BlastShield does not perform active asset discovery or produce a topology or connectivity export. There is no network diagram at the end of a deployment.

What it does is bound the consequences of an incomplete inventory. A system with no configured policy is blocked and logged the moment it tries to communicate. The block is the security outcome. The log records what the inventory missed.

Figure 7: The block is the outcome. The log is the evidence.



An asset with no configured policy attempting to communicate, being blocked, and appearing as a dated entry in the access log, which is the evidence feed of what the inventory missed.

The Objection

"Does this satisfy CIP-015?"

No, and anyone telling you otherwise is worth a second look. Internal network security monitoring is the inspection of east-west traffic inside the Electronic Security Perimeter. Blocking and logging unauthorized access are separate controls that address different requirements.

FERC approved CIP-015-2 by letter order on 10 August 2026, so the phasing is real planning work. BlastShield is not the answer to it.

The Evidence

The default-deny log is the artifact. Most vendors have no answer to what happens to the assets you do not know about. This one is a dated list of them, generated by the assets themselves at the moment they tried to talk.

The Regulatory Hook

One more gap, stated before an auditor finds it. The Orchestrator has no formal policy approval workflow, so a separation-of-duties requirement runs through the permission model plus an after-the-fact change log rather than through two-person review.

With cloaking active, BlastShield fails closed and protected assets stop answering. Redundant gateways are the availability answer, established sessions are retained through failover, and an unreachable Orchestrator is not a traffic outage.

The Regulatory Picture Without the Fiction

No CIP standard requires network cloaking by name, and a vendor telling you otherwise is selling you something. What this table records is which instrument binds which entity, what date attaches to it, and what BlastShield supplies as evidence inside it.

Ask the scope question first: distribution substations at a municipal or cooperative utility are frequently not registered BES assets. Dates marked computed are derived from an implementation plan rather than printed in the standard, and your Regional Entity is the authority on your own status.

Instrument	Binds	Date	What BlastShield supplies
CIP-005	Registered entities, for Interactive Remote Access	In force	The protocol break the Intermediate System requirement describes. BlastAccess is then an EACMS itself
CIP-003-9	Low impact BES Cyber Systems, vendor electronic remote access	Enforceable since 1 Apr 2026	Disabling vendor remote access. Not finding where it exists, which is discovery, and not detecting malicious communications, which is monitoring
CIP-003-11	Low impact BES Cyber Systems with external routable connectivity	1 Jul 2029, computed	Remote user authentication, and protection of authentication information in transit. Not the detection requirement
CIP-002-8, revised Control Center definition	Transmission Owners controlling facilities at two or more locations by SCADA	1 Jul 2028, computed	Nothing directly. It is a reclassification instrument, and impact rating decides which standards apply at all
CIP-015	High and medium impact BES Cyber Systems, internal network security monitoring	Phased, and no date belongs in a vendor document	**Nothing. We do not satisfy this standard**
Order No. 919, virtualization	Entities using virtual or shared infrastructure	1 Jul 2028, computed	Nothing directly. It defines Shared Cyber Infrastructure, the term CIP-015-2 uses for its applicable systems
IEC 62443	Nobody on its own. A standard, widely written into contracts	None	Zones and conduits, in policy rather than hardware

BlastWave publishes compliance mappings for IEC 62443, NERC CIP, TSA Security Directives, NIS2, the EU Cyber Resilience Act, CMMC Level 2, and DoW OT Zero Trust. A mapping is not a certification, and we do not claim to make an entity compliant with anything.

Proof, and How to See it

600,000,000+ device hours of production operation in OT networks across the customer base. Treat that as a floor rather than a total, because the counter only moves one way.

Independent performance testing

Tolly Report #222138, September 2022, commissioned by BlastWave and tested in August 2022. BlastShield delivered 2.5 Gbps client-to-application throughput across three clients, 2.2x to 34x the throughput of Tailscale, Twingate, OpenVPN, and Perimeter 81, and 2.67 Gbps site-to-site, 6.2x Tailscale and 6.6x OpenVPN.

Certified hardware

OnLogic CL210G and K410, Axiomtek iNA110 and ICO120-E3350.

Published compliance mappings

For seven frameworks, listed opposite.

Hackopedia

Our published analysis of 23 OT attacks that defeated firewalls, VPNs, and air gaps.

What we do not claim

We publish no breach-rate figure and no undefeated record. Neither would survive the next question an engineer would ask: **How you would know?**

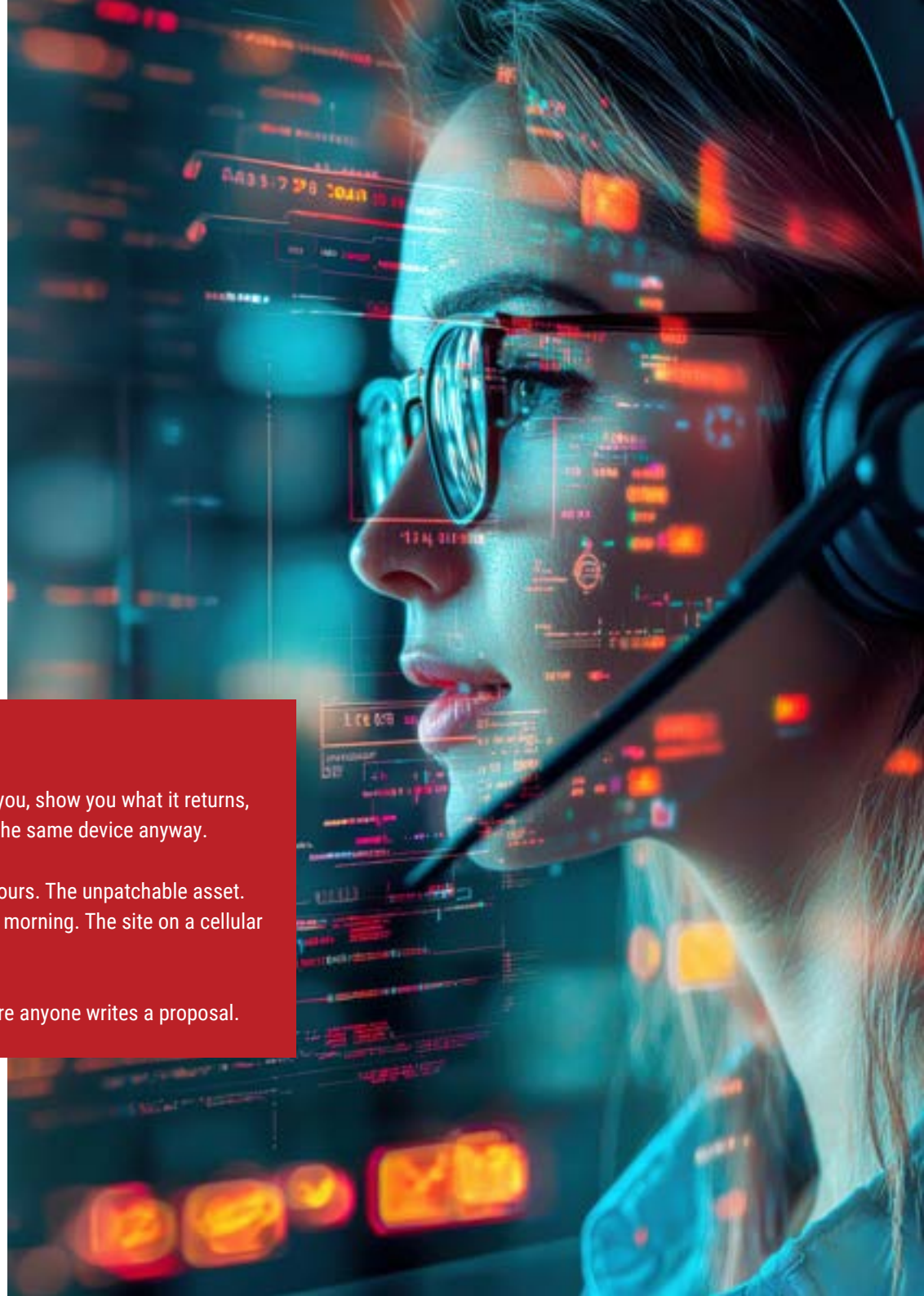
See it before you scope it

Ask us for a demo.

We will scan a protected controller in front of you, show you what it returns, and then have an authorized operator access the same device anyway.

Bring your own scenario rather than watching ours. The unpatchable asset. The integrator who needs access at two in the morning. The site on a cellular modem that nobody visits.

You will know whether this fits your plant before anyone writes a proposal.



BlastWave protects Industrial Control Systems, Operational Technology, and Critical Infrastructure networks. BlastShield consolidates network cloaking, passwordless MFA, software-defined segmentation, and secure remote access into one deployment, so that protected assets stop answering unauthorized scans.

Visit **blastwave.com** to learn more.

v20260910

1045 Hutchinson Ave.,
Palo Alto, CA 94301 USA

T: +1 650 206 8499

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS