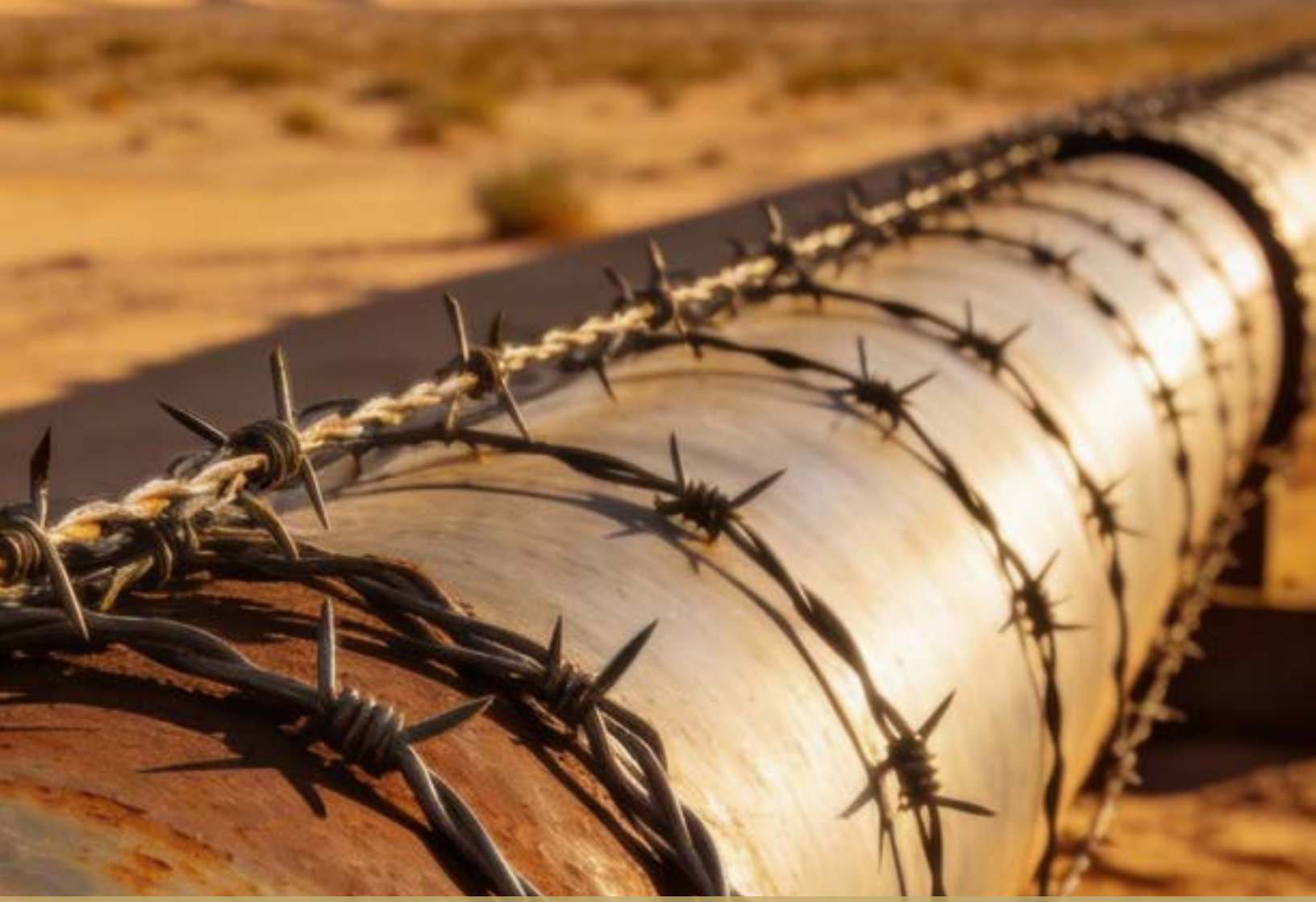


SOLUTION BRIEF

What SD Pipeline-2021-02G Requires, and What BlastShield Can Prove

BlastWave

Colonial Pipeline's OT Network Was Never Compromised

The ransomware hit IT. Colonial halted pipeline operations anyway, from 7 to 12 May 2021, for two reasons: the business systems it needed to bill for deliveries were down, and it could not be certain the attack had not reached the control systems.

The second reason is the one TSA has been legislating against ever since. SD Pipeline-2021-02G, signed 1 May 2026 and effective 3 May 2026 through 2 May 2027, is less interested in which products you bought than in whether you can show what your controls did. Section III.G requires a Cybersecurity Assessment Plan that assesses whether your implementation plan is effective, and Section IV.C.2 lists what the TSA can request for inspection: firewall rules, network diagrams, log files, and snapshots of East-West and North-South traffic.

So the useful question is no longer "Are we segmented?" It is "Can we prove it, on the day it matters, to someone who does not work here?"

The Clause Most Operators Underestimate

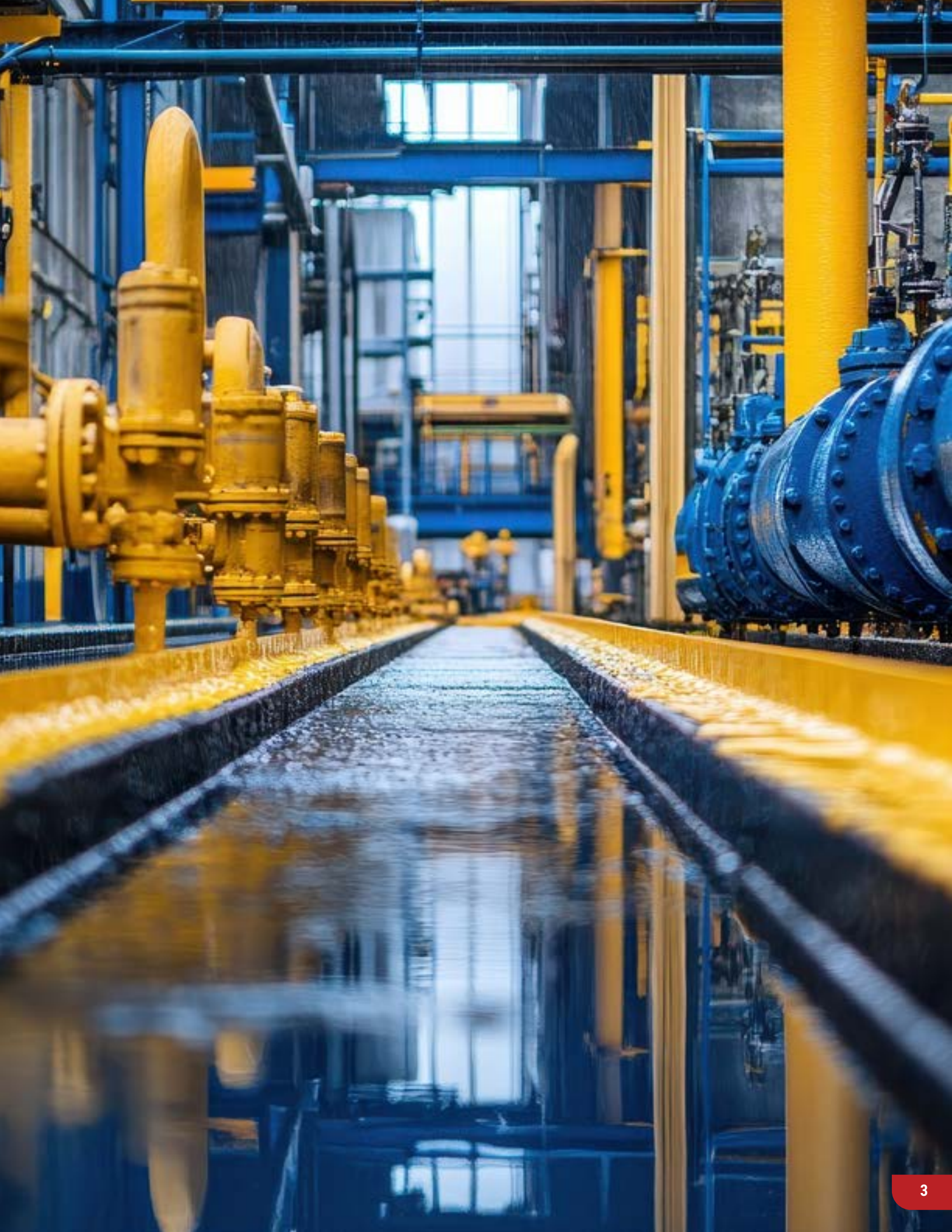
Section III.G.2.d sets a schedule. At least one-third of the policies, procedures, measures, and capabilities in your TSA-approved Cybersecurity Implementation Plan must be assessed every year, and 100 percent over any three-year period. Section III.G.2.b adds a cybersecurity architecture design review at least once every two years, including verification and validation of network traffic and system log review.

Standing controls up once is the easy half. Producing evidence that they were operating, on a rolling third of your estate every year, to a plan TSA has approved and reports on annually, is what the assessment cycle actually costs. A control that generates its own audit trail is doing part of that work for you.

Note: BlastWave publishes compliance mappings. BlastWave is not certified or accredited to any regulatory framework, and no vendor product confers compliance on an operator. This document describes how BlastShield controls support specific required outcomes under SD Pipeline-2021-02G. It supports, but does not replace, an operator's own implementation plan, assessment plan, and formal determination by TSA.

What BlastShield Records

Record	Detail
Access attempts	Both permitted and denied. Failed attempts are logged, not just successful ones, which is what makes an access record defensible rather than partial
Configuration changes	Logged, with a record of what changed
Policy configuration	Exportable. Can also be saved and reapplied, as a backup or to clone a configuration onto a new system
Vendor and third-party sessions	Full session recording through BlastAccess
Retention	Configurable, so it can be set to match your assessment cycle rather than the reverse
Export	Four paths: local storage, API export, syslog streaming, or FTP in CSV format



Clause-level Mapping

Clause	What it requires	BlastShield function
III.A	Identify Critical Cyber Systems	None
III.B.1	List and describe IT and OT interdependencies, all external connections, and zone boundaries organized by criticality	Policy configuration defines zones and permitted paths
III.B.2.a	Controls to prevent unauthorized communications between zones	Software-defined segmentation
III.B.2.b	Prohibit OT services traversing the IT system unless content is encrypted in transit	Software-defined segmentation. OT traffic crossing the BlastShield boundary is carried in encrypted peer-to-peer tunnels
III.C.1.b	Documented mitigation measures for components that will not have passwords reset on schedule, plus a timeframe	Passwordless MFA
III.C.2	MFA, or controls supplementing password authentication with commensurate risk mitigation	Passwordless MFA: QR challenge-response, local biometrics, device keystore
III.C.3	Manage access rights on least privilege and separation of duties. Where not technically feasible, describe compensating controls	Segmentation plus permission model
III.C.4	Limit shared accounts. Individuals who no longer need access must not retain knowledge of the shared password	Passwordless MFA
III.C.5	Schedule for review of domain trust relationships	None
III.D.1	Capabilities against malicious email, malicious IPs, malicious web domains, unauthorized code execution, and command and control traffic	None
III.D.2.b	Document and audit communications between the OT system and an external system that deviate from the identified baseline	Segmentation enforcement
III.D.3.b	Ensure log data is maintained for sufficient periods to allow effective investigation	Configurable retention
III.D.4	Mitigation measures or manual controls to ensure ICS can be isolated when an IT incident creates risk to OT safety and reliability	Software-defined segmentation
III.E.3	Where patches cannot be applied without severe degradation of operational capability, describe additional mitigations and a timeline addressing the risk of not patching	Network cloaking
III.F.1.b	Segregation of infected networks and devices during incident response	Software-defined segmentation
III.F.1.d	Established capability and governance for isolating IT and OT systems during an incident that could cause operational disruption	Software-defined segmentation
III.G.2.b	Cybersecurity architecture design review at least every two years, including verification and validation of network traffic and system log review	Access and enforcement logs
III.G.2.c	Incorporate other assessment capabilities, such as penetration testing of Information Technology systems and red or purple team testing	Network cloaking is the thing under test
III.G.2.d	At least one-third of the CIP is assessed annually, 100 percent over three years	None directly
IV.C.2.e	On request, produce log files and snapshots of East-West OT traffic and North-South IT to OT traffic	Access and enforcement logging
IV.C.2.c	On request, produce network diagrams, switch and router configurations, architecture diagrams and VLANs	None

Coverage	Evidence
Out of scope	Operator determination. BlastShield does not perform asset discovery
Supports	Exportable policy configuration. Note: This clause also expects architecture documentation. BlastShield does not produce network or topology diagrams
Directly addresses	Exportable policy set, plus logs of permitted and denied crossings. No ACLs, VLAN re-architecture or new hardware required
Directly addresses	Policy configuration showing the encrypted path. The encryption is a property of the transport, not a configuration option that can be left off
Directly addresses	This is the clause for legacy assets that cannot take a password policy. Passwordless access is the mitigation, and it removes the credential rather than managing it
Directly addresses	Access logs. Relevant to the control-room carve-out for 49 CFR 192 and 195 workstations, where compensating controls must otherwise be specified
Supports	Least privilege is directly enforced. Separation of duties on policy change is not: see the assessor questions below. This clause expressly allows compensating controls to be described where the principle is not technically feasible
Supports	Where there is no password, there is no residual password knowledge to manage. Shared account policy remains the operator's
Out of scope	Operator-owned
Out of scope	BlastShield does not do this. Requires email security, web filtering, endpoint and network detection tooling
Provides evidence for	Denied-attempt logs are the deviation record. Permitted paths are the baseline, expressed as policy
Supports	Retention is set by the operator to match the investigation and assessment window
Directly addresses	Policy change isolates without physical re-cabling or VLAN work. Change is logged and takes effect immediately
Directly addresses	Side-by-side scan output showing the asset does not answer. This is the clause that contemplates exactly this control. The operator still needs its own asset inventory and firmware tracking under III.E.1
Supports	Segregation by policy rather than by physically pulling cable. Procedures remain the operator's
Directly addresses	The capability is the product. The governance is yours. Change logs evidence that isolation was exercised
Provides evidence for	Logs are the reviewable material. The review itself is the operator's, and the architecture diagrams it expects come from elsewhere
Provides evidence for	A dated side-by-side scan artifact. Note the clause names IT systems in its example; a cloaking verification scan sits under the clause's broader "other assessment capabilities" language rather than under the named example
Provides evidence for	Exportable policy configuration and retained logs are the assessable material for the segmentation and access-control third of the plan
Provides evidence for	Exportable by API, syslog or CSV. This clause names the artifact class directly
Out of scope	BlastShield does not produce topology or architecture diagrams. Your existing network documentation still has to carry this

In summary: BlastShield directly addresses seven clauses, supports five, and produces evidence for five. Four are entirely yours. Any vendor claiming to cover Section III end-to-end is describing a product that does not exist, and Section III.D.1 alone will catch them.

Questions Your Assessor Will Ask

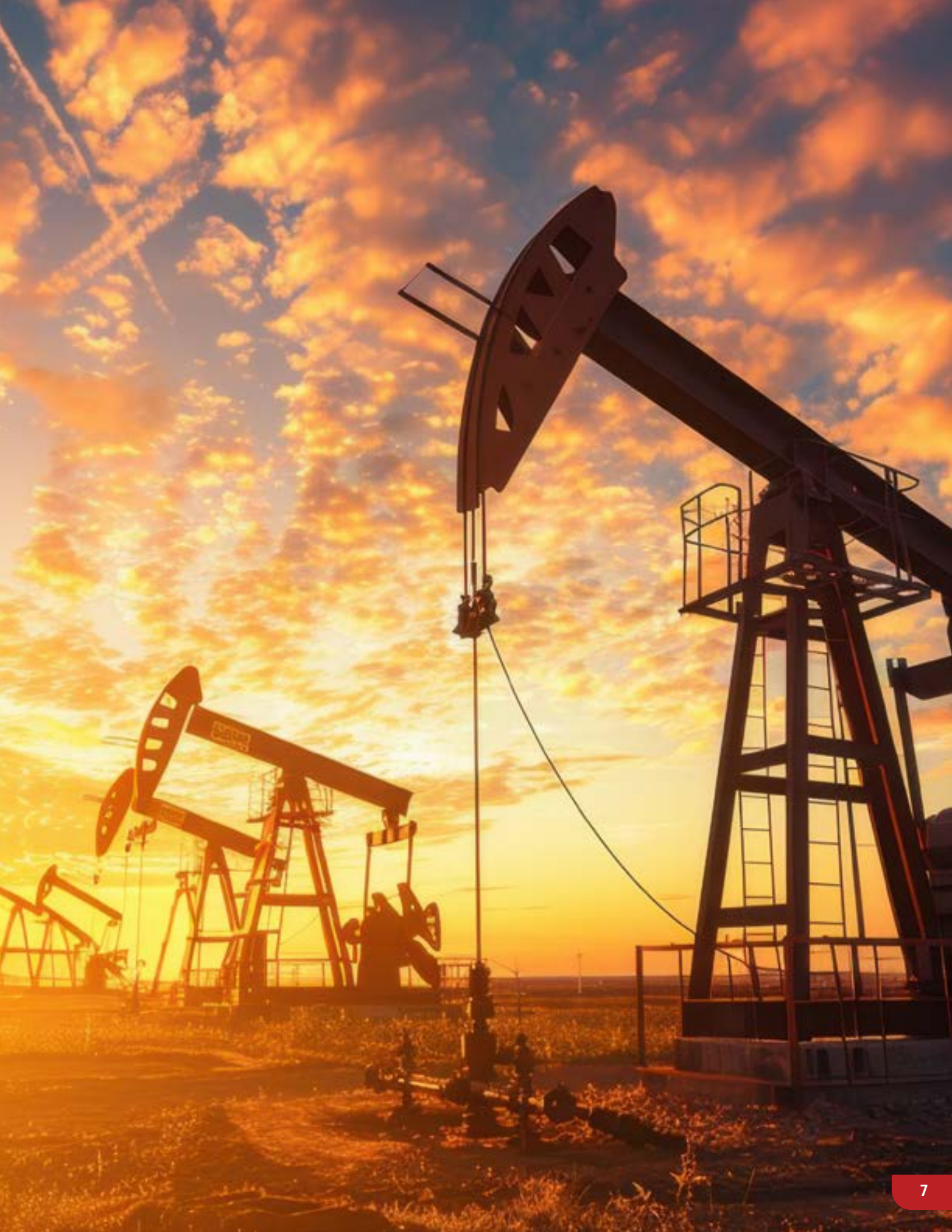
Question	Answer
Where is the boundary, and what enforces it?	Per identity and per asset rather than per network segment. Enforcement occurs at the BlastShield Gateway and Agent, with the policy distributed by the Orchestrator. No ACL or VLAN dependency, so the boundary does not move when the network is re-addressed
Is OT traffic protected when it crosses the IT network?	Yes. OT traffic crossing the BlastShield boundary is carried in encrypted peer-to-peer tunnels. This is what satisfies Section III.B.2.b, which permits OT services to traverse the IT system only where the content is encrypted in transit
Who administers policy, and how are changes reviewed?	The Orchestrator, on-premises or cloud. Change rights are governed by the permission model. There is no staged approval workflow. If a user's permissions allow a policy change, it takes effect immediately. Review is after the fact through the configuration change log, not before the fact through a second approver. Section III.C.3 requires separation of duties and expressly allows compensating controls to be described where the principle is not technically feasible. That is the right place to document your permission model and your own change management procedure. We would rather tell you this now than have your assessor find it
What evidence exists that the control was operating, not just installed?	Access attempts are logged whether permitted or denied, so the record shows the control acting rather than merely present. Configuration changes are logged separately. BlastAccess sessions are recorded in full. Retention is configurable and export runs over API, syslog, local storage or CSV
What happens when the control fails?	With cloaking active, BlastShield fails closed. Protected assets stop answering. That is deliberate: a security control that fails open has stopped being a control. Availability is addressed by deploying redundant Gateways, and already-established sessions are retained through failover, so an operator working in a live session is not dropped. Orchestrator failure is a different case and is not a traffic event. If the Orchestrator becomes unreachable, the Gateway keeps enforcing the policy already configured. The Orchestrator is the policy plane, not the data path, and it can itself be deployed redundantly, on-site, in the cloud, or both
How is the control tested?	A twenty-minute side-by-side port scan, unprotected against protected. It produces a dated artifact for Section III.G.2.c, and it is the fastest way to establish whether the control does what this document says it does

The Threat This is Actually Protecting From

Energy is one of four sectors named in CISA advisory AA24-038A, issued with the NSA, the FBI and Five Eyes partners in February 2024. It documents PRC state-sponsored actors pre-positioning on the IT networks of US critical infrastructure to enable lateral movement to OT assets and disrupt operations in the event of a major crisis. The tradecraft is living off the land: built-in network administration tools rather than custom malware.

Detection-first controls assume an analyst can triage faster than an attacker can move. Against an adversary already inside and behaving like an administrator, that assumption does not hold. An asset that does not answer an unauthorized scan is not on the target list in the first place.

See the BlastWave Volt Typhoon solution brief for the full attack-chain breakdown.



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

v20260819

Prevent industrial cyberattacks, and ensure the world's critical infrastructure stays protected, productive, and profitable. Together we can build a resilient future for OT networks. Join the movement at **www.blastwave.com**

©2025 BlastWave Inc. | 1045 Hutchinson Ave., Palo Alto, CA 94301 USA | T: +1 650 206 8499

BlastWave
PREVENT
INDUSTRIAL
CYBERATTACKS