CASE STUDY

Secure Operational Technology Connectivity for Oil and Gas

BlastWave

Achieving Operational Agility and Security Resilience

The security of geographically dispersed Operational Technology (OT) networks poses a uniquely challenging problem for the global energy sector, characterized by acute logistical, architectural, and talent deficits. This case study examines the strategic deployment of a BlastWave within a significant North American energy producer, outlining the architectural changes required to manage hundreds of remote sites securely and efficiently. Traditional OT connectivity models struggled significantly with the twin problems of overlapping local IP addresses and the financial burden of sending specialized personnel to remote locations for routine maintenance, a practice known as "truck rolls."

By adopting a software-defined overlay, the organization successfully decoupled security policy enforcement from the underlying, messy network topology. The core strategic benefit of this approach was demonstrated during a major acquisition challenge, where the operator had to integrate a large volume of new assets rapidly. The deployment successfully expanded network segmentation coverage from approximately 5,000 devices to a remarkable 20,000 devices in under a month. This result validates a high-speed, cost-effective paradigm for Industrial Control System (ICS) security, demonstrating that industrial-grade protection can be achieved with ease of use comparable to that of consumer-grade solutions.

The Industrial Imperative: Addressing Logistical and Cyber Challenges in Distributed Oil & Gas Networks

Oil and Gas (O&G) operations are characterized by immense geographical scale, involving highly sensitive, yet often unpatchable, control systems distributed across remote, harsh environments. The security solution selected had to overcome fundamental challenges rooted in operational design, legacy system constraints, and economic viability.

Analyzing the Total Cost of Ownership (TCO) Associated with Remote Network Complexity

A primary source of inflated Operational Expenditure (OPEX) in the oil and gas (O&G) sector is the necessity of sending personnel—the "truck roll" dilemma—to distant operational sites for system updates, new equipment installations, and routine maintenance. This labor-intensive requirement is not merely a logistical annoyance; it is a symptom of architectural complexity. The underlying problem is that across multiple sites and geographies, Internal IP Addresses may be locally assigned and managed by the local firewall system, often leading to identical or overlapping IP schemes (e.g., 10.1.x.x) at different locations.

When network devices at two distinct sites share the same local addressing scheme, any attempt to connect them remotely or centralize their management requires intricate routing fixes or, more commonly, manual reconfiguration by specialized personnel on-site. The inherent complexity of managing firewall rules and resolving IP conflicts during consolidation (especially during an acquisition) dramatically increases the difficulty and cost of maintaining security and connectivity. The frequency of physical site visits is thus directly linked to the need for local IP resolution and policy adjustment. By addressing the root cause, i.e., the architectural rigidity imposed by overlapping IP address spaces, the deployment mechanism simultaneously generates a significant return on investment by eliminating a major component of field OPEX, fundamentally shifting the business case for security from purely risk mitigation to tangible cost savings.

The Overlapping IP Challenge:
A Fundamental Barrier to Consolidation and Acquisition

The crisis created by overlapping IP address ranges represents a core technical and business bottleneck, particularly in a sector driven by mergers and acquisitions (M&A). When a company acquires new assets, the process of network integration is drastically challenged because acquired networks often use the same private address space as the existing enterprise. Traditionally, resolving this overlap requires extensive and risky network re-addressing, which can severely delay system updates, new equipment installs, and the overall integration schedule. This inability to quickly and seamlessly merge networks often stalls the realization of business efficiency intended by the M&A activity.

The security and operational model employed must be inherently adaptable, enabling seamless integration of newly acquired assets into network security, regardless of the underlying IP address structure. This adaptability is essential because security solutions should adapt to the existing operational network, rather than forcing the high-risk, expensive task of adapting the network to the security solution.

Risk Mitigation: The Necessity of Securing Highly Distributed WAN Links and Unpatchable OT Assets

The nature of oil and gas (O&G) operations introduces specific cyber risks that conventional IT security mechanisms often fail to address. Remote sites rely heavily on Wide Area Network (WAN) connectivity, which frequently suffers from unpredictable availability and requires Multi-WAN Link Redundancy. Moreover, these public or unencrypted connections expose crucial data, such as trade secrets, capacity metrics, and new field discoveries, to potential intrusion and eavesdropping by industrial espionage or hostile state actors.

Furthermore, the remote sites contain legacy Operational Technology (OT) devices, such as Human-Machine Interfaces (HMIs), Programmable Logic Controllers (PLCs), and various Sensors, that are frequently unpatchable due to age, vendor restrictions, or certification constraints. The security solution must be architected to protect these remote site devices from network discovery and subsequent exploitation via ransomware or malware, without relying on the ability to update their inherent firmware security. This requirement mandates a security framework capable of completely isolating the asset, focusing on controlling who or what can communicate with it, rather than attempting to secure the device itself.

Voice of the Stakeholder: Defining the Requirements for Adaptable OT Security

The customer's requirements emphasized a mandate for security that was simple, cost-effective, and deeply integrated into operational workflows. These requirements were not merely suggestions for convenience but foundational principles necessary to minimize human error and ensure economic scalability across hundreds of distributed, low-margin sites.

Simplicity as a Security Vector:

Minimizing Human Error Through Plug-and-Play Deployment

The solution had to be operable and maintainable under conditions of severe resource constraints. A fundamental requirement stipulated that remote site deployments must be "plug and play" and capable of being "Installed by a non-IT professional". This necessity arose partly from the observed scarcity of OT security talent, "Especially at Remote Sites".

To mitigate complexity and the resulting human error, configuration and management needed to be handled remotely via an easy-to-use centralized User Interface (UI), managing policies for hundreds of devices and sites.1 Moreover, the capability for rapid scaling demanded that adding systems and users be easy, supporting the "Import thousands of devices and users with a single click".

This mandate for simplicity is recognized not as a luxury but as a critical cybersecurity measure, embodying the concept of Human-Centric Cybersecurity. When security controls are complex, the likelihood of misconfiguration by system administrators (whether due to lack of specialized training or sheer volume of work) increases dramatically. Data indicates that firewalls are involved in 100% of breaches, not because the technology is flawed, but due to human misconfiguration. Given the critical shortage of specialized security professionals in the field, a successful architecture must actively "engineer out the need to train" and ensure that human errors are "inconsequential to risk". Therefore, the demand for plug-and-play field installation is the architectural response to mitigating the single highest source of security failures: human administrative error at the edge.

Achieving Economic Scalability:

The Mandate for Industrialized, Cost-Effective Hardware

To achieve comprehensive security coverage across an operational footprint spanning hundreds of remote sites, economic feasibility was a paramount consideration. This low-cost threshold was essential to ensure the solution could be deployed ubiquitously, even at smaller, unmanned drilling or sensor sites where the return on investment (ROI) would not justify traditional, high-cost security appliances.

Furthermore, the hardware itself needed to be durable and flexible. The requirement specified that the remote site hardware must be "industrialized and portable," capable of operating in environmentally challenging conditions (high temperature, humidity, dust, etc.), and designed to be moved and reused as sites are relocated, such as when drilling rigs transition to new pads.

Operational Continuity:

Ensuring Secure Third-Party and Remote Maintenance

Workflow Integrity

A core tenet of OT security is ensuring that security measures do not impede vital operational workflows. The chosen solution had to ensure that the "Operations and Maintenance workflow is maintained." This included keeping Remote Sensor traffic unimpeded, enabling remote operations, and, critically, supporting secure 3rd party maintenance access without the need for on-site visits. The solution was required to deliver "Industrial-grade security with consumer-grade ease-of-use", ensuring that protection was pervasive yet transparent to the operator and the core process logic.

The constraints and requirements defined by the customer necessitated a cybersecurity framework that solved for logistical complexity, economic viability, and security resilience simultaneously.

Table 1: Voice of the Customer: Key Requirements and Implementation Metrics

Requirement Category	Key Requirement/Challenge	Target/Metric	Strategic Mitigation by BlastShield
Simplicity/ Human Factor	Deployment & Management	Plug and play; centralized UI; single-click import	Eliminates human misconfiguration (e.g., complex firewall rules) at the edge.
Cost Effectiveness	Scalability CapEx	Under $1k/site	Enables economic deployment across hundreds of remote sites, improving ROI.
Operational Agility	Network Integration (M&A)	Seamless integration of new sites without re-addressing	Bypasses IP overlap conflicts critical during rapid acquisition.
Security Resilience	Asset Protection	Protect remote devices from discovery and exploitation (unpatchable assets)	Utilizes secure, encrypted P2P connectivity and dark networking principles.

Architectural Analysis: BlastShield's Secure Overlay Technology

The successful deployment hinged on the adoption of Secure Overlay Technology, an architectural paradigm that fundamentally changes how network resources are identified, accessed, and secured within a highly fragmented environment.

Decoupling Policy from Topology:

How Overlay Addressing Resolves IP Conflict

The central innovation of the Secure Overlay Technology is its non-invasive nature. The design explicitly avoids the disruptive process of network re-architecture by mandating that the system "keeps all local IPs as they exist on the network today". This respect for existing local addressing is crucial in OT environments, where changes to network configurations can carry significant operational risk.

The solution applies a new, separate network addressing scheme (the Overlay IP Addresses) to the network. This layer of abstraction achieves two primary goals: first, it eliminates the need to re-address local devices, thereby bypassing the challenge of overlapping IP addresses during system updates or M&A integration. Second, it provides an additional layer of security independent of the physical infrastructure. The overlay layer also employs Overlay DNS Names (e.g., plcx-site1.company.com), allowing systems and users to refer to devices logically, without needing to know or interact with the conflicting internal IP schema.

This architectural choice represents a necessary shift from traditional perimeter-based security, which relies on Layer 3/4 enforcement based on network topology (IP and VLAN definitions). Since overlapping IPs inherently break topology-based zoning, the Secure Overlay provides a persistent, logically defined identifier for every device. By allowing security policy enforcement to occur at this logical, abstracted layer, the solution ensures policy consistency across the entire enterprise, regardless of the device's physical location or underlying IP address. Consequently, security policies can be defined once and applied everywhere, enabling true scalability and transforming network architecture complexity from a constraint into a non-issue. New sites can be integrated simply by installing a gateway, immediately resolving any local IP conflicts with hundreds of existing remote sites.

Granular Access Control:

Implementing Software-Defined Zones and Conduits

The Software Overlay is utilized to establish a structure of Software-Defined Zones and Conduits between specific zones and users. This mechanism enables the segregation of security policies based on function and identity, utterly independent of geographical location. The conduits themselves enforce secure (encrypted) Peer-to-Peer (P2P) connections between all sites and users. Access is highly granular, ensuring that communications are only established between explicitly authorized endpoints, conforming to a strict Zero Trust model. Policy granularity is defined across crucial functional strata within the OT environment:

- Safety Zones are established for critical physical security and process oversight assets, such as Operator stations, IP Cameras, Sensors, and Controllers. This structure ensures that systems responsible for Health, Safety, and Environment (HSE) maintain prioritized, secure communication paths.
- Process and Control Zones encompass assets such as Actuator PLCs, HMIs, and SCADA controllers, which manage real-time process execution.
- Supervisory Zones handle management interfaces such as PAM Servers, Patch Servers, Jump Servers, and Historians.
- User Zones categorize access based on identity and role, including Admin Users, Engineering Users, and Temporary Users, allowing for precise, role-based access control.

Zero Trust Principles in the ICS Domain:

Encrypted P2P Connectivity and Device Protection

The deployment of Software-Defined Zones and Conduits fundamentally adheres to Zero Trust principles, which are critical for safeguarding unpatchable legacy OT devices. The architecture operates on a principle of default denial: connectivity is only established via a secure P2P conduit when explicitly authorized between a specific user, device, and target asset.

This approach prevents widespread network exposure. By wrapping remote site devices in an encrypted overlay and controlling access via these narrow conduits, the solution effectively protects remote devices from network "discovery and exploitation". This is vital for unpatchable or exposed legacy devices, as they become invisible to unauthorized network reconnaissance or lateral movement attempts by attackers who may have gained access elsewhere on the network.

Furthermore, the end-to-end encryption applied to all P2P connections ensures that WAN connectivity is protected from intrusion and eavesdropping. This mechanism is essential for maintaining confidentiality, preventing bad actors from gleaning trade secrets, capacity utilization data, or new field discoveries through network traffic analysis.

Table 2: BlastShield Software-Defined Zone Architecture

Software-Defined Zone	Associated Assets and Services	Security Policy Focus
IT Zone	IT Services, OT Remote Access	Administration and boundary enforcement
Supervisory Zones	PAM Server, Patch Server, Jump Server, Historian, Thin Clients	Centralized management, data archiving, and maintenance tools
DMZ Zone	SCADA, Thin Clients	Interface between supervisory and process layers (data mediation)
Process Information Zone	Monitoring, DB Server	Visibility, data collection, and historian interaction
Process & Control Zones	Actuator PLC, HMI Controller, Workstation, SCADA	Real-time control execution and operator interface/interaction
Safety Zones	Operator, IP Camera, Sensor, HMI, Controller, Workstation, SCADA	Physical security monitoring and personnel safety systems, prioritized access
User Zones	Admin Users, Engineering Users, Temporary Users	Granular, role-based, identity-defined access control (Conduits)

Implementation Dynamics: Deployment and Zone Segmentation

The implementation strategy focused on a rapid, standardized deployment across the geographically dispersed upstream assets, emphasizing secure management for critical access scenarios, particularly third-party maintenance.

Phased Rollout in Upstream Operations:

Securing Manned, Unmanned, and Exploration Sites

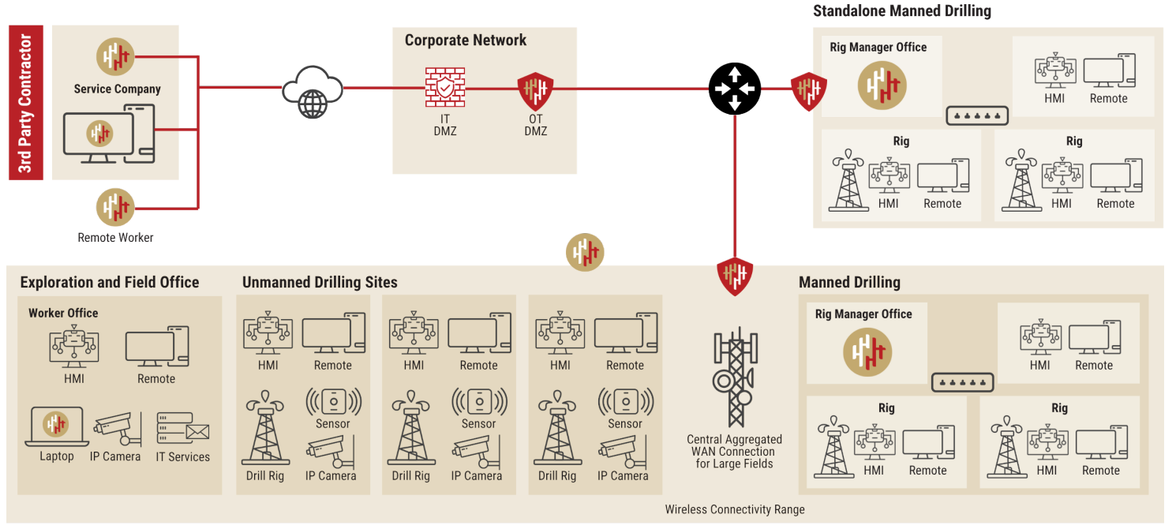
The initial deployment focused heavily on the Upstream portfolio, which includes the most dispersed and resource-constrained environments. Secure connectivity was established for Standalone Manned Drilling Sites, Unmanned Drilling Sites, and Exploration/Field Offices. These sites feature a typical mix of OT assets, including Rig Manager Offices, HMIs, IP Cameras, and Sensors.

The implementation involved placing BlastShield overlay gateways directly at these remote operational sites. These gateways manage the local OT network traffic, ensuring that all communications leaving the site are encapsulated and encrypted via the secure overlay, which connects back to the Corporate Network through defined IT and OT DMZs. The solution was designed to support multiple WAN links, taking into account the unpredictable nature of remote connectivity.

This deployment was further enriched by the implementation of communication towers within the large drilling sites. At these sites, the BlastShield gateway is installed at the central tower, and all connectivity to the site is managed through the gateway, allowing the entire extended site to be protected with a single gateway deployment featuring primary and backup communications links (cellular and fixed).

These large sites may cover multiple miles, but are all within the transmission range of various wireless communications technologies, enabling the customer to save a significant amount of money and removing the need to connect the systems in a contained geographic area individually.

Diagram 1: Oil and Gas Upstream Field OT Security



Detailed Mapping of Security Policies to Software-Defined Zones

The operational success of the deployment is evident in the granular segregation of security policies by functional zones. The Software-Defined Zoning ensures that essential communications for safety and control are prioritized and isolated, providing a secure foundation for operations. For instance, traffic destined for the Process Zone (Actuator PLCs) is strictly governed by rules applicable only to that zone, regardless of whether the physical device is located on a drill rig or at a centralized field processing facility. Conversely, Safety Zones, encompassing critical assets such as H2S detectors or safety controllers, receive policy priority, reflecting the industry's focus on safety above all other concerns. This architecture provides necessary segmentation between, for example, Engineering Users who require broad access for maintenance and Temporary Users whose access must be minimal and time-limited.

Integrating Remote Workers and Third-Party Contractors via Secure Conduits

One of the most persistent attack vectors in critical infrastructure involves compromised third-party vendor credentials accessing the network via broad VPN solutions. Historically, third-party contractor access was often granted through a traditional VPN, effectively creating a network-level perimeter that bypassed the OT environment.

The implemented secure P2P conduit model directly addresses this risk. When a third-party service company or remote worker requires access, a secure connection is established directly between the user's endpoint and the single, specific asset they need to reach (e.g., a particular HMI or PLC). This conduit is identity-based and time-bound, ensuring that the vendor's machine cannot discover, probe, or laterally move to any other device on the network that it is not explicitly authorized to contact. This Zero Trust approach eliminates the need for legacy, broad network access methods, protecting the vast majority of remote assets, especially unpatchable legacy devices, from incidental or malicious discovery.

Empirical Results:
Demonstrated Scaling and Acquisition Agility

The true validation of the Secure Overlay architecture lies in its demonstrated performance under high-stress scenarios, particularly during large-scale network consolidation, and its proven cost efficiency.

Operational Efficiency Gains: Quantification of Reduced On-site Visits

The requirement for plug-and-play installation by non-IT professionals, combined with centralized policy management capability, resulted in immediate and quantifiable operational efficiency gains. By remotely resolving IP address conflicts and managing policy configuration via the centralized UI, the underlying requirement for specialized personnel travel was drastically reduced. The initial primary challenge—avoiding "truck rolls to remote networks"—was functionally resolved because the solution enables remote diagnosis, configuration, and management for connectivity issues and system updates.1 Furthermore, the architecture's inherent ability to support multiple WAN links addresses the issue of unpredictable WAN availability at remote sites, contributing to improved uptime and reduced intervention requirements.

Metrics of Success:

Achieving Rapid Segmentation from 5,000 to 20,000 Devices

The definitive test of the solution's scalability and architectural agility occurred during the acquisition process. Integrating a newly acquired company typically involves months or years of intense effort dedicated to network reconfiguration and segmentation to ensure proper security separation.

In this instance, the Secure Overlay deployment achieved an extraordinary rate of growth, as expanded network segmentation was applied to 15,000 new devices, scaling the total managed network from 5,000 to 20,000 devices in under a month.

This metric provides quantitative proof of M&A security acceleration. Traditional methods would have been bottlenecked by the requirement to resolve overlapping IP addresses across the two merging enterprises. Because the Secure Overlay architecture completely bypasses the need for local IP re-addressing, the organization was able to onboard and segment four times its existing device count in approximately four weeks. This capability transforms network integration from a high-risk liability (which typically forces a prolonged period of vulnerability) into a competitive asset, enabling rapid, low-risk integration and minimizing the security debt that often follows corporate M&A activity.

Financial Impact Assessment

The operational strategy required a solution that was economically feasible for widespread deployment. This financial structure optimizes for efficiency in cost, deployment time, and ongoing management complexity. The low per-site cost, combined with the drastic reduction in OPEX associated with truck rolls, ensures a high return on investment that justifies the strategic deployment across hundreds of locations. This deployment resulted in a payback of less than one year for the initial deployment, and the ROI continues to grow each year and with each new acquisition that the customer executes.

Table 3: Selected Potential ROI Factors for BlastWave Oil and Gas Deployments

Capability	Benefit	Estimated Time/$ Savings Per Site	TOTAL Cost Savings
Can deploy witout downtime, re-IP	Accelerated acquisition integration	40-80 Hours/site (52 sites)	**$208k-$416k**
Deply in S/W or COTS	Low cost site segementation	Save $5k-$10k per small site (20)	**$100k-$200k**
Built-in remote management VNC	Eliminate truck rolls for config/3rd Party	$1000-$2000/site and $1k-$3k 3PP	**$100k-$300k**
More resilient comms	Lost connectivity can trigger shutdowns and delays	2hours/site @ $5k per hour of outage	**$260k-$780k**

Extending the Security Model Across the O&G Value Chain

The architectural flexibility of the Software-Defined Zones proved easily extendable beyond the initial Upstream deployment, allowing the organization to establish a unified security posture across the entire oil and gas (O&G) value chain: Upstream, Midstream, and Downstream.

Upstream Production:

Ensuring Sensor and Drill Rig Integrity

The Upstream deployment successfully secured complex mobile and fixed assets, including Drill Rigs, Unmanned Drilling Sites, and Exploration Offices. The ability to deploy industrialized, portable hardware facilitates the rapid securing and redeployment of security infrastructure as mobile assets, such as drilling rigs, move between physical locations. This consistency ensures reliable connectivity and security for essential field assets, including HMIs, IP Cameras, and Sensors. Aggregating connectivity at large sites through a central communications tower was a high cost savings and simplification enabled by BlastShield's software-defined segmentation capabilities.

Midstream Logistics:

Protecting Pipelines, Compressor Stations, and Control Centers

In the Midstream segment, the Software-Defined Zone model is applied to high-value, geographically extensive infrastructure essential for transport and storage, including Gas and Oil/Liquids Pipelines, Compressor Stations, Pump Stations, and Terminals. The overlay provides critical isolation for control assets such as PLCs, Controllers, Remote Terminal Units (RTUs), and PIG sensors, ensuring that these devices remain isolated from external discovery and exploitation even when connected via long-distance, aggregated WAN links. The Control Center environments (including SCADA workstations and operational storage) are segmented into Supervisory and DMZs to ensure safe access mediation.

Downstream Processing:

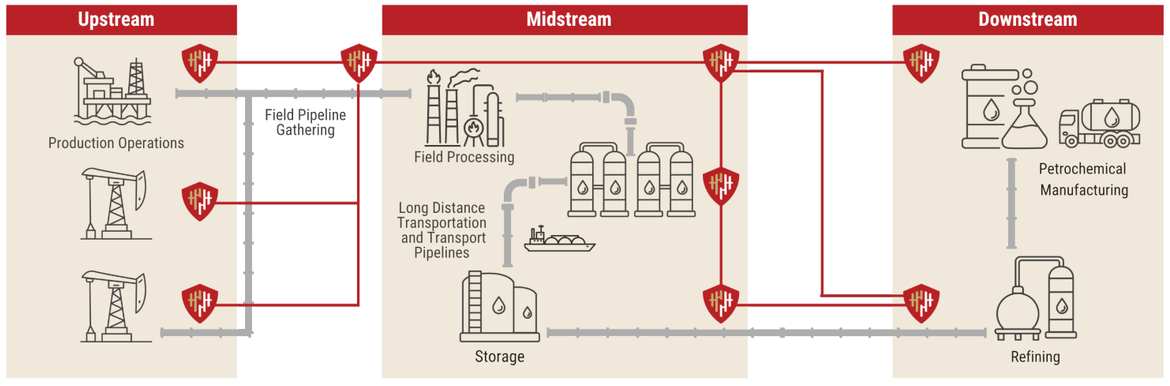
Securing DCS, Safety Systems, and Instrumentation Networks

In the highly complex Downstream environments, which encompass refining and petrochemical manufacturing, the zone model secures critical systems managed by Distributed Control Systems (DCS) and Operational Business Systems.

The solution segments complex instrumentation networks (including ISA 100/WIHART systems) and Process Control & Safety Systems. Crucially, the isolation of these safety and control assets, such as H2S detectors and IEDs (Intelligent Electronic Devices), ensures that potential cyber threats propagating from the corporate network or physical security monitoring systems cannot move laterally into the most safety-critical process measurement layers.

By applying the same functional zoning architecture across all three business segments, for instance, treating a "Process Zone" PLC in a refinery identically to a "Process Zone" PLC on a drill rig, the organization establishes a unified security posture that is agnostic to the physical segment or business unit. This architectural uniformity dramatically simplifies enterprise-wide risk management, compliance documentation, and the application of security policies across disparate environments.

Diagram 2: BlastShield deplyment across Upstream, Midstream and Downstream Oil and Gas network



Strategic Conclusions: Cybersecurity as a Pillar of Operational Resilience

The strategic shift to a Secure Overlay Zero Trust architecture fundamentally addressed the twin challenges of complexity and risk inherent in modern distributed OT operations. The resulting architecture positions cybersecurity not as a cost center, but as an enabler of operational agility and resilience, directly supporting critical business functions such as rapid M&A integration and field OPEX reduction.

The Dangers of Legacy IT Firewall Architectures in OT Environments

The case reinforces the critical distinction between IT and OT network security requirements. Reliance on conventional, perimeter-based IT firewalls as the primary OT security measure is dangerous because it inherently overlooks the fundamental differences between the two environments, particularly the OT's prioritization of safety and operational continuity. Traditional firewalls are designed to allow traffic, and their complexity makes them vulnerable to misconfiguration.1 The evidence suggests that removing the reliance on complex, manually configured edge firewalls and replacing them with a simple, centralized Software-Defined Overlay mitigates the high probability of human error, which is the root cause of 100% of breaches involving firewalls.

Engineering for Safety:

Aligning Cybersecurity Measures with HSE and Operational Continuity Mandates

The ultimate strategic objective in protecting O&G networks extends beyond mere breach prevention; it is intrinsically linked to "ensuring operational continuity and protecting health and safety and avoiding spills". By establishing robust segmentation through Software-Defined Zones and isolating critical Safety and Process assets, the implemented solution builds cyber resilience directly into the infrastructure's fabric. This architectural resilience ensures uninterrupted energy delivery and mitigates the risk of catastrophic physical consequences resulting from cyber intrusions. The entire architecture is designed to prevent cybersecurity interruptions from translating into operational disruptions.

Recommendations for Future Critical Infrastructure Security Investment

Based on the quantifiable success of this deployment, the following strategic recommendations are crucial for critical infrastructure operators facing similar challenges of scale, complexity, and distributed assets:

1. **Shift to Identity-Based Segmentation:** Prioritize the adoption of Zero Trust-inspired network overlays to decouple security policy from physical network topology fundamentally. This capability is paramount for enabling rapid, low-risk M&A integration and effectively managing geographically dispersed assets without the need for manual network reconfiguration.
2. **Mandate Economic Scalability and Simplicity:** Adopt solutions that meet strict cost targets (e.g., sub-1,000 USD per site) and require minimal specialized expertise for deployment. This minimizes the risk of human misconfiguration, addresses the industry-wide security talent gap, and ensures that protection can be affordably extended to every edge asset, not just high-value central sites.
3. **Integrate Security with Operational Workflow:** Ensure that any solution supports operations and maintenance requirements, particularly secure, fine-grained access for third-party vendors, thereby eliminating the security risks associated with traditional broad VPN access while supporting remote service capabilities.

Table 4: Mapping Operational Challenges to Secure Overlay Solutions

Oil & Gas OT Operational Challenge	Technical Solution Provided by Secure Overlay	Primary Strategic Benefit
Locally assigned, overlapping IP addresses	Application of Overlay IP/DNS scheme	Enables rapid M&A integration and eliminates costly network re-addressing (Agility).
Reliance on personnel for remote maintenance ("Truck Rolls")	Remote installation, P2P encrypted conduits, centralized UI	Drastic reduction in OPEX and improved operational response time (Efficiency).
Securing unpatchable legacy devices and WAN eaves-dropping	Software-defined Zones/Conduits & secure P2P encryption	Protects assets from discovery and exploitation, ensur-ing trade secret confidentiality (Resilience).
OT Security Talent Gap	Plug-and-play install by non-IT staff	Engineers out human misconfiguration risk at the edge (Safety/Human-Centric).

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

v20251010

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