Securing the Connected Energy Operator

A Zero Trust approach to unifying security and enabling safe AI adoption across upstream oil & gas

Wragby Business Solutions & Technologies Limited

www.wragbysolutions.com

White paper v1 | Whitepaper | Cybersecurity

July, 2026

Executive Summary

Energy operators sit at the intersection of two pressures that few other industries face together: they hold data representing years of exploration investment, and they operate infrastructure designated as critical national energy supply. That combination makes them a priority target — and yet many run their security on estates assembled tool-by-tool over years of cloud adoption, with gaps between the layers that an attacker can move through unseen. The arrival of generative AI has added a further exposure: sensitive data flowing into tools the organisation does not govern.

This paper sets out the approach Wragby uses to bring such estates under control: a Zero Trust security program, delivered as a service on the Microsoft platform, that unifies identity, devices, data and threat intelligence into one coherent posture — and, in doing so, establishes the governed foundation an operator needs to adopt AI safely. We describe the method, illustrate it with a recent de-identified deployment for a mid-sized upstream operator, and explain why a single integrated platform succeeds where a stack of point products does not.

1. The Security Reality for Energy Operators

To understand why this matters, start with what an operator is protecting. For an upstream oil & gas operator, data is the core asset. Geological and seismic interpretations, production performance, joint-venture commercial terms and health-and-safety records together represent years of investment and competitive advantage. The systems that hold this data are also the systems that run the business — and increasingly they are cloud systems, as operators adopt Microsoft 365 and Azure to collaborate and scale.

This concentration of value attracts well-resourced adversaries. Energy infrastructure is targeted by criminal groups seeking ransom, by competitors and brokers seeking intellectual property, and by state-aligned actors who treat energy supply as a point of leverage. A successful intrusion threatens far more than data: it can disrupt production, breach regulatory obligations, and carry national-economic weight.

Against that threat, most operators' security estates have accreted incrementally rather than by design. Protection tends to accumulate in layers — each tool acquired to solve a specific problem, none of them integrated. The result is a set of recurring weaknesses we see repeatedly across the sector:

- Inconsistent identity controls. Multi-factor authentication applied unevenly, and privileged access that has grown without regular review — the conditions in which credential theft, the starting point of most breaches, succeeds.
- No common device standard. Endpoints managed to differing baselines, so a single unpatched or compromised laptop becomes an uncontrolled entry point.
- Ungoverned data movement. Sensitive files moving across email and collaboration tools with no classification and no rules to prevent loss.
- Fragmented visibility. Security signals scattered across disconnected tools, with no single console and no ability to correlate an endpoint event with a suspicious sign-in or an unusual data transfer.

2. The Wragby Approach: Zero Trust, Delivered as a Service

To these long-standing gaps, generative AI adds a new one. As employees adopt AI tools, unclassified and ungoverned data can be exposed to systems outside the organisation's control — and most operators have no policy governing how AI may be used or what it may access.

Wragby addresses these gaps not by adding further point products, but by consolidating onto a single integrated platform built on Zero Trust principles — the security model that assumes no user, device or connection is trusted by default, and verifies each one continuously. On the Microsoft platform, the six Zero Trust pillars — identities, devices, data, applications, infrastructure and networks — are defended by capabilities that share intelligence and reinforce one another, rather than operating in isolation.

The engagement model is deliberately structured and repeatable, built on the Microsoft Solutions Framework and delivered in defined stages:

- Assess. Every engagement begins with an envisioning and security assessment that scores the operator's current maturity against each Zero Trust pillar and ranks the gaps by the business risk they carry — regulatory exposure, operational downtime, and loss of competitive intelligence.

- Deploy. The plan is delivered in phases across the six pillars. Identity is brought under uniform, phishing-resistant multi-factor authentication and conditional access with Microsoft Entra. Devices are standardised with Microsoft Intune. Sensitive data is classified and protected with Microsoft Purview. Security signals are consolidated into Microsoft Sentinel, with Microsoft Defender XDR standardising detection and response.

- Operate. Detection and response run as an ongoing managed service. Automated playbooks handle the repetitive first response to common alerts, while a subscription security operations capability provides continuous monitoring and posture improvement.

3. In Practice: A Mid-Sized Upstream Operator

The approach is best illustrated by a recent deployment for a mid-sized upstream oil & gas operator running a growing Microsoft 365 and Azure environment. Its security carried every weakness described above: uneven MFA, unreviewed privileged access, no unified device standard, sensitive geological and commercial data moving without controls, and visibility split across disconnected tools.

Following the assess–deploy–operate method, Wragby unified the estate in two phases. The first closed the most urgent identity, device and data gaps with Entra, Intune, Purview and the initial Sentinel deployment. The second extended data-loss prevention across collaboration tools, hardened the underlying directory infrastructure, and consolidated more than fourteen previously disconnected data sources into Sentinel — giving the operator, for the first time, a single view of threats moving across its whole environment.

The outcomes followed the pattern the method is designed to produce. Phishing-resistant MFA and conditional access were extended across the entire workforce — a control set Microsoft's research credits with blocking more than 99 percent of identity-based attacks.[1] Consolidating signals into one SIEM delivered organisation-wide visibility the operator had never had, with a measurable improvement in its Microsoft Secure Score. Automating the response to routine alerts reduced the time to contain threats and freed analysts from repetitive triage. Retiring overlapping point tools reduced both complexity and licensing cost, and the program was delivered without disruption to operations.

4. Why a Single Platform, Not a Stack

The case illustrates a question operators frequently raise: why consolidation onto one vendor's platform is preferable to integrating best-of-breed point products. Security improves materially when defences share context. When identity, endpoint, data and network signals live in separate tools, each sees only its own slice, and the connective tissue between an attacker's steps is precisely where adversaries operate undetected. A single platform with native cross-domain correlation closes those seams — and, by removing duplicated tooling and integration overhead, lowers total cost of ownership at the same time.

Consolidation does not mean discarding existing investments wholesale. A modern SIEM can ingest telemetry from third-party tools where it makes sense to retain them, standardising detection without forcing wholesale replacement. The goal is a unified posture, not single-vendor consolidation as an end in itself.

5. The Foundation for Safe AI Adoption

The most consequential benefit of this approach is an outcome operators often underestimate at the outset: the same work that secures the estate is what makes AI adoption safe.

> *AI tools are only as well-governed as the data and identities they touch. An operator that classifies its data with Purview and controls its identities with Entra has, in the process, built the controls that determine what AI can access — turning AI from an ungoverned risk into a managed capability.*

This positions the organisation to adopt AI-assisted security operations, including Microsoft Security Copilot and AI-driven investigation, on a foundation that is ready for them. The sequencing matters: adopting AI before governing data invites exactly the exposure operators fear, whereas governing data first — as a by-product of a Zero Trust security program — makes subsequent AI adoption a controlled, deliberate step rather than an uncontrolled risk.

Conclusion

The connected energy operator cannot secure itself with a patchwork of disconnected tools, and cannot adopt AI safely without first governing its data. Wragby's Zero Trust approach on the Microsoft platform addresses both at once: it unifies a fragmented estate into a single, measurable security posture, and in doing so lays the governed foundation for AI adoption at scale. Delivered as a repeatable, services-led model, it is an approach built not for one operator but for a sector.

References

[1] Microsoft Security research on the effectiveness of multi-factor authentication against identity-based attacks: https://www.microsoft.com/en-us/security/business/security-101/what-is-multifactor-authentication-mfa

Wragby Business Solutions & Technologies is a Microsoft Solutions Partner for Security, holding the Cloud Security and Threat Protection specializations. Wragby helps organisations across regulated industries unify their security on the Microsoft platform through a repeatable, services-led model spanning advisory, deployment and managed security services. To discuss a Zero Trust security assessment for your organisation, contact info@wragbysolutions.com