7 ISLANDS
DEFENSE & INTEL

What institutions buy vs. what vendors sell vs. what operators actually use

***Abstract**: Cybersecurity outcomes degrade when institutions optimize for defensibility, vendors for differentiation, and operators for survivability—coherence emerges only when these logics are explicitly reconciled.*

***Why this matters:** Because cybersecurity outcomes degrade when procurement, product narratives, and operational reality pull in different directions—and nobody owns the coherence.*

***Who this is for:** Institutional buyers, vendors, and security leaders who want adoption that survives procurement, turnover, and day-to-day operations.*

***What to watch for:** If operators quietly narrow, bypass, or disable major parts of what was bought, you don't have an adoption problem—you have a coherence problem.*

***Author**: Nicolas Duguay, Founder, 7 Islands Defense & Intel*

***Date**: January 2026*

Cybersecurity is often discussed as though institutions, vendors, and operators were aligned actors moving along a single value chain. In practice, they operate according to different logics, answer to different incentives, and measure success using incompatible criteria. What institutions buy, what vendors sell, and what operators actually use are connected, but they are not equivalent. Much of what is perceived as dysfunction in the cybersecurity market emerges from this gap.

Institutions purchase cybersecurity under conditions of accountability. Their decisions must withstand audit, political scrutiny, leadership turnover, and public exposure. What is acquired must remain defensible over time, not only technically but procedurally. Procurement logic therefore privileges stability, continuity, and traceability. The objective is not peak performance, but risk reduction that can be justified, documented, and sustained within existing governance structures.

Vendors operate under a different imperative. They sell differentiation. Their narratives emphasize capability, performance, innovation, and comparative advantage. Products are framed around what is new, faster, more automated, or more comprehensive than alternatives. This logic rewards clarity of value proposition and visible superiority, even when those claims rely on assumptions about maturity, staffing, and architectural cleanliness that rarely hold in institutional environments.

Operators inhabit neither of these worlds comfortably.

They are responsible for keeping systems running, responding to incidents, and maintaining continuity under constraint. Their reality is shaped by alert fatigue, partial visibility, legacy dependencies, staffing limitations, and competing priorities. What operators actually use is determined less by what was purchased or promised than by what can be integrated into daily workflows without increasing fragility.

The divergence becomes visible immediately after acquisition. Institutions often buy platforms whose primary virtue is defensibility rather than usability. Vendors deliver solutions optimized to demonstrate breadth and sophistication. Operators respond by narrowing usage to the subset of functionality that delivers immediate operational value. Large portions of procured capability remain unused, disabled, or bypassed—not because operators are resistant, but because the full system is unmanageable in practice.

Procurement cycles reinforce this pattern. Requirements are defined months or years before deployment, often abstracted from evolving operational needs. By the time a solution is selected, the environment it was meant to address has already shifted. Vendors respond by expanding feature sets to anticipate future use cases. Operators respond by simplifying aggressively. Institutions interpret compliance with procurement intent as success, even as operational efficiency stagnates.

Interoperability exposes the gap particularly clearly. Institutions require compatibility at the contractual and architectural level. Vendors advertise integration through APIs and partnerships. Operators care about something more prosaic: whether data arrives in a usable form, at a manageable volume, and within existing analytical workflows. When it does not, they compensate manually. Parallel processes emerge quietly. Visibility fragments.

Automation follows the same pattern. Vendors sell it as force multiplication. Institutions buy it as a modernization narrative. Operators adopt it cautiously, aware that poorly tuned automation amplifies noise, obscures accountability, and introduces failure modes that are difficult to diagnose under pressure. What survives operational reality is conservative, supervised, and limited in scope.

Over time, these adaptations create a strange equilibrium. Institutions believe they have acquired robust capabilities. Vendors believe they have delivered value. Operators have reshaped the system into something workable, often without formal recognition or support. The system functions, but not as designed. Inefficiencies persist silently.

This misalignment is rarely the result of incompetence or bad faith. It reflects structural incentives. Institutions optimize for defensibility. Vendors optimize for differentiation. Operators optimize for survivability. Each position is internally rational. The friction emerges when these logics are treated as interchangeable.

Durable outcomes tend to appear only when this triangle is acknowledged explicitly. When vendors understand institutional accountability constraints. When institutions accept operational

reality rather than procurement abstractions. When operators are not forced to choose between usability and compliance. Coherence does not emerge automatically. It must be designed across all three perspectives.

Absent that alignment, cybersecurity ecosystems appear bloated, expensive, and underperforming—not because technology is lacking, but because the systems surrounding it are incoherent. Understanding what institutions buy, what vendors sell, and what operators actually use is therefore not a rhetorical exercise. It is a prerequisite for building capabilities that persist beyond procurement and survive contact with reality.

Editorial note —
This analysis reflects observations informed by institutional and operational exposure across defense-adjacent security and cybersecurity environments.

For discussion only; not operational guidance.

© 2026 **7 Islands Defense & Intel**. This document and its contents are the exclusive intellectual property of 7 Islands Defense & Intel. Reproduction, distribution, or reuse, in whole or in part, requires prior written permission.

The original version of this text was written in French and translated into English with the assistance of AI-based tools.