



A Modern Data Platform for the Intelligence Community

Everpure for US intelligence and national security missions

Intelligence organizations are being asked to do more than ever—integrate intelligence, surveillance, and reconnaissance (ISR) and cyber data at scale, stand up AI for analysis and targeting, and harden resilience against nation-state threats. At the same time, teams are maxed out, and infrastructure costs keep moving. What used to be a tough engineering challenge is now a volatility problem: component prices spike, contracts shift, and the vendors you relied on start moving the goalposts. Everpure™ helps the intelligence community replace that fragile footing with an always-modern, AI-ready, cyber-resilient data platform built to support mission systems from the tactical edge to on-premises core facilities—operating within each organization’s own accreditation and classification boundary.

The market reality: You didn’t run out of runway, something took it

Intelligence missions were already data-heavy. Sensor feeds, ISR platforms, full-motion video, cyber telemetry, and operational systems were all generating data at a faster pace than budgets could support. Storage costs were climbing, and teams were already stretched thin. There wasn’t much slack left.

Then pricing spiked without warning, contracts shifted, and the vendors you’d built your refresh and recap plans around started changing terms mid-stream. Now you’re explaining why AI pilots are delayed, analytics pipelines are capacity-constrained, and infrastructure costs no longer feel predictable in an environment where “good enough” isn’t acceptable.

But the problem isn’t just pricing. Other underlying issues include:

- **Underutilized, fragmented, inflexible estates** with stranded capacity and hot spots
- **Patchwork architectures** across ISR silos, sensitive compartmented information facilities (SCIFs), and mission networks that make every new requirement a bespoke integration
- **Traditional refresh cycles** that create CAPEX spikes and put command and control (C2), ISR, and analytics systems at risk every time hardware changes

Pricing volatility surfaced the problem, but a fragile model is what took the runway.

Who can you trust?

When the same relationship that sets your pricing is also the one you’re depending on to manage through disruption, that’s not a partnership; it’s a single point of failure. Mission continuity shouldn’t hinge on one vendor’s willingness to hold terms steady.

But the real problem isn't individual vendors; it's that most environments were never built to absorb this level of pressure. They were built for a more predictable world:

- Designed for stability, then stretched to handle AI, cloud, and cyber at intelligence community scale
- Optimized around specific programs or platforms, not for a unified data operating model
- Dependent on one-off contracts and volume deals, not a consistent life cycle

The good news is that this is fixable, and you don't have to figure it out alone. What intelligence organizations need isn't another contract. They need a model built for this, one that translates directly into mission outcomes such as:

- Keeping C2, ISR, and analytics systems online and ready, even as supply, pricing, and requirements shift
- Shortening the time from ingest to finished intelligence by reducing data friction and infrastructure firefighting
- Giving analysts, data scientists, and operators a reliable, high-performance data backbone so they can focus on tradecraft, not workarounds
- Providing leadership with predictable, defensible economics and a path to modernize without putting mission availability or accreditation at risk

The efficiency and predictability problem

Pricing volatility is what surfaced the problem, but the organizations struggling most weren't undone by a single price change. They were running underutilized, fragmented, and inflexible environments with no room to absorb it. These environments are constrained by:

- Underutilized storage islands
- Duplicated datasets across domains and enclaves
- Inflexible architectures that make every capacity change a heavy lift

The need isn't a slightly better storage deal. It's a better model, one built for efficiency and predictability from the ground up. That starts with **maximum efficiency per terabyte:**

- Cut overprovisioning and align spend to what you actually use.
- Consolidate ISR, cyber, records, and analytics datasets on a unified, all-flash platform so you get more from the infrastructure you already have before buying more.

Turn tech debt into an always-modern, AI-ready foundation

Most intelligence community environments are a patchwork of separate ISR silos, analytics stacks, cyber tools, and enclaves. Every shift—a new sensor, mission set, analytics tradecraft, or cyber directive—forces another point solution or integration that results in more spend, more rework, and less predictability. The environment hands volatility back to the mission instead of handling it.

Everpure was built on a different assumption: volatility is the condition, not the exception. The Enterprise Data Cloud is what that vision looks like today:

- **One Unified Data Plane** across block, file, and object workloads, supporting ISR ingest, full-motion video, unstructured intel repositories, and structured operational data
- **One Intelligent Control Plane** for policy-driven automation, telemetry, and AIOps so you manage data as a mission asset, not array by array
- **One operating model** across on-premises, edge, and authorized government/intelligence community cloud environments, with Purity providing consistent data services and controls wherever workloads live

Efficiency and predictability are built in, not bolted on, not because the market forced us to change, but because we've been building toward this for more than 15 years.

What this means for intelligence missions

Most commercial models pass future risk to the customer and try to manage it through contracts. Our model is built to do the opposite: **keep costs predictable, govern services via contractual SLAs, and allow for flexibility as conditions change.**

Cost predictability

- Spend is tied to actual usage and mission demand, not multi-year capacity guesses.
- Evergreen® and Evergreen//One™ keep platforms **continuously current** with nondisruptive upgrades, eliminating forklift refreshes that risk mission downtime or reaccreditation cycles.
- Capacity can be rebalanced and expanded within the estate without stranding investment in older silos.

Operational efficiency

- Capacity and performance move with demand, from bursty ISR ingest at the edge to sustained analytics pipelines at core sites.
- A single control plane reduces manual toil for overstretched engineering, storage, and cyber teams.
- Integrated AIOps surfaces anomalies, hot spots, and optimization opportunities across the fleet.

Deployment and mission flexibility

- Place workloads where they make the most sense—tactical edge, on-premises SCIFs, or authorized government/intelligence community cloud—under a consistent data and policy framework.
- Support modern application patterns with **Portworx**® so containerized AI/ML and microservices can run alongside traditional analytics tools without a second operating model.

Make intelligence data AI-ready without underutilizing GPUs

AI is now central to how the intelligence community detects, understands, and anticipates threats, from sensor fusion and target development to cyber defense and all-source analysis. The challenge is less about algorithms and more about getting intelligence data AI-ready at operational speed and scale.

Everpure helps intelligence community organizations build an AI-ready data layer.

- Run ISR ingest, cyber telemetry, intel repositories, and analytics workloads on an AI-ready, high-throughput platform that unifies structured and unstructured data such as sensor feeds, full-motion video, documents, logs, chat, and external open source intelligence.
- Shorten time from ingest to finished intelligence by reducing data friction and eliminating scattered silos so analysts and data scientists can work against a single, modern data foundation.
- Use Portworx and the Everpure Platform to support modern application architectures (containers and microservices) alongside existing analytics tools, avoiding the complexity of a second parallel infrastructure stack.
- Ensure GPU and accelerator investments are fully utilized by providing consistent, low-latency access to the data they need rather than letting storage and pipelines be the bottleneck.

Intelligence community teams can advance AI and advanced analytics at their own pace—within existing classification, security, and residency constraints—with confidence that the storage and data layer will keep up.

Build cyber-resilient intelligence records, archives, and mission data

The intelligence community stewards some of the government's most sensitive and long-lived data: operational plans, ISR archives, target files, analytics products, and historical repositories that must remain available and trustworthy for years or decades. In a ransomware, data-wiping, or insider event, the question isn't just "Can we restore?" but "How fast can we resume operations without compromising sources, methods, or integrity?"

Everpure is built for **mission continuity**, not just backup.

- **Immutable SafeMode™ Snapshots** create protected copies of critical data designed to resist alteration or deletion—including attempts made with compromised admin credentials—providing clean recovery points for C2, ISR, and analytics systems.
- **Flash-speed rapid restore** enables petabyte-scale recovery in hours, not weeks, so commands can focus on resuming mission execution and analysis instead of rebuilding infrastructure.
- **Policy-driven data protection and replication** align with records management, retention, and compartmentation requirements, simplifying audits and oversight across domains and enclaves.
- **Consolidation into an efficient all-flash footprint** helps intelligence community organizations meet power, space, and survivability objectives in constrained facilities while improving resilience and manageability.

By embedding cyber resilience into the storage and data platform, Everpure helps the intelligence community protect mission data, preserve trust, and maintain continuity under sustained, sophisticated threats.

The outcome

The Everpure advantage for the intelligence community is straightforward and delivers:

- **An efficient data platform you can build on**, from ISR ingest and cyber telemetry to AI and long-term archives
- **Predictable costs you can count on**, even as component markets and mission requirements shift
- **A commitment to innovation and engineering excellence over time**, not one-off projects
- **A vendor that does what it said it would** over the life of the agreement, not just at award

Everpure is engineered to give intelligence organizations room to move again, with a data platform that is always modern, AI-ready, and resilient by design.

Learn more about the Everpure Platform and how it supports [public sector missions](#).

Explore the Everpure Advantage

Visit Our Website

800.379.PURE

