

WHY NOW

The Cost of Waiting to Take Control of Enterprise Data

Why unstructured data needs executive attention now—not after the next renewal, audit, breach, or AI initiative.

Doing nothing is still a decision – and it has a measurable cost.

Every month an organization delays understanding and controlling its unstructured data estate, more data is created, copied, retained, backed up, exposed, and fed into new workflows. The problem rarely stays the same size. It compounds across infrastructure, security, compliance, AI, and operations.

\$4.99M	146%	60%	30%+
average global cost of a data breach	increase in enterprise HDD cost from Q3 25 to Q3 26 per one market tracker	of AI projects without AI-ready data may be abandoned	of enterprise unstructured data is redundant, obsolete, or trivial

The executive question is no longer “Can this wait?”

It is: What will waiting cost – and how much harder will the problem be to solve later?

The organizations that act first do not begin with a massive transformation. They begin by establishing visibility: what data exists, where it lives, who can access it, what is sensitive, what is inactive, and what should happen next.

Delay turns a manageable data problem into five interlocking business problems

1. **Infrastructure cost** – Inactive, duplicate, and low-value data consumes primary storage, backup capacity, replication, cloud resources, and administrative time. A renewal often locks another year of waste into the run rate.
2. **Security exposure** – Every unnecessary file, copy, permission, and repository expands the amount of data an attacker – or an overprivileged insider – can reach. Ransomware impact grows when more production data remains broadly accessible.
3. **Compliance burden** – Retention schedules, privacy obligations, legal holds, and deletion requests become harder to execute and prove as data spreads. Unknown data cannot be governed consistently.
4. **AI cost and governance risk** – AI initiatives amplify the consequences of poor data quality, unclear ownership, sensitive content, and inappropriate access. Teams can spend heavily preparing the wrong data – or expose information that should never reach a model.
5. **Operational drag** – Infrastructure, security, legal, compliance, and data teams repeatedly investigate the same fragmented estate. Manual reviews and one-off cleanup projects consume time without creating durable control.

Waiting does not preserve today's risk – it raises tomorrow's baseline

TODAY	+6 MONTHS	+12 MONTHS	+24 MONTHS
Unknown data	More copies and silos	Higher renewal baseline	Larger remediation scope
Unclear access	More exposure paths	Audit and breach pressure	More complex containment
Early AI demand	More pilots and data use	Waste and governance gaps	Scaling risk becomes structural

Illustrative cost-of-delay progression. Actual impact depends on data growth, copy behavior, access, retention, infrastructure, and AI adoption.

Four external forces are making unstructured data harder – and more expensive – to ignore

1

Threat actors are moving faster

IBM reports one in four malicious breaches in 2026 were AI-enabled, and the average AI-enabled breach cost \$6 million. Reducing unnecessary accessible data limits the potential blast radius.

2

AI is consuming data before governance catches up

Gartner reported that organizations may abandon 60% of AI projects unsupported by AI-ready data. Data readiness is not only a model problem; it requires context, quality, access control, sensitivity, and ownership.

3

Regulatory expectations require evidence

Privacy and industry obligations increasingly demand that organizations locate regulated data, enforce retention, control access, and demonstrate defensible action – not merely publish policies.

4

Infrastructure decisions create long commitments

Storage, backup, cloud, and migration choices establish multi-year cost structures. Moving or renewing unknown data preserves waste and transfers risk into the next environment.

Recent evidence

- **Breach economics** – IBM’s 2026 report puts the global average breach cost at \$4.99 million, up 12% year over year.
- **Ransomware pressure** – Verizon’s 2026 DBIR reports ransomware involvement in 48% of breaches.
- **AI exposure** – IBM found that AI-enabled malicious breaches cost about \$6 million on average in 2026.
- **AI readiness** – Gartner found poor data quality or limited data availability directly contributed to AI project failure for 38% of I&O leaders who experienced setbacks.
- **Unstructured data growth** – NetApp notes that unstructured data accounts for 80–90% of new enterprise data and grows 3x faster than structured data, with at least 30% of an organization’s unstructured data being redundant, obsolete, or trivial.
- **Increasing hardware costs** – Trendforce reported Enterprise SSD contract pricing increasing 80% in Q1 2026, another 48–53% in Q2, and another 20–25% in Q3.

One data-control initiative can return value across multiple executive priorities

Executive priority	Act now	Value created
CIO / Infrastructure	Identify inactive, duplicate, and low-value data before renewal, migration, or expansion.	Reclaim capacity, lower storage and backup demand, shorten migration scope, and improve recovery efficiency.
CISO / Security	Locate sensitive data and unnecessary exposure; reduce access and segment high-risk inactive data.	Shrink attack surface, lower blast radius, and focus controls on the data that matters most.
GRC / Privacy	Map regulated data to retention, access, and disposition policies.	Improve audit readiness, respond faster to requests, and establish defensible deletion.
CDO / AI	Separate trusted, relevant data from sensitive, stale, redundant, or low-quality content.	Improve AI readiness, reduce wasted preparation and compute, and apply governance before scale.

Start with visibility – not a transformation program

The first decision should be small, measurable, and cross-functional. Establish a factual baseline of the unstructured data estate, quantify the cost and risk of the current state, and identify actions that can deliver value within the next budget or operational cycle.

- **Discover** – what data exists and where it lives.
- **Understand** – age, activity, sensitivity, ownership, access, duplication, and business value.
- **Act** – delete, move, isolate, remediate access, apply policy, and prepare trusted data for AI.

A practical 12-month readiness check

- ☐ Do we know which data is sensitive, inactive, redundant, or broadly accessible?
- ☐ Can we quantify infrastructure spend supporting data with little current business value?
- ☐ Can we prove retention and deletion policies are applied – not simply documented?
- ☐ Do AI teams know which data is approved, relevant, and appropriately governed?

NEXT STEP

Quantify Your Cost of Waiting

A focused Enterprise Insights assessment can reveal where unnecessary cost, exposure, governance gaps, and AI readiness issues exist – before they become part of the next renewal, migration, audit, or incident.

1. Establish the baseline

Create a unified view across on-premises, cloud, and hybrid sources.

2. Quantify the exposure

Measure inactive data, sensitive content, access risk, duplication, and policy gaps.

3. Prioritize action

Build a practical roadmap tied to cost, security, compliance, and AI outcomes.

The goal is not to “boil the ocean.” It is to find the highest-value place to begin – and make the economics of action clear.

>> LET’S ASSESS YOUR ENVIRONMENT <<