



The Files Connection: **AI Maturity Drives New Data Imperatives**

FROST & SULLIVAN EXECUTIVE BRIEF

The contents of these pages are copyright © Frost & Sullivan. All rights reserved.

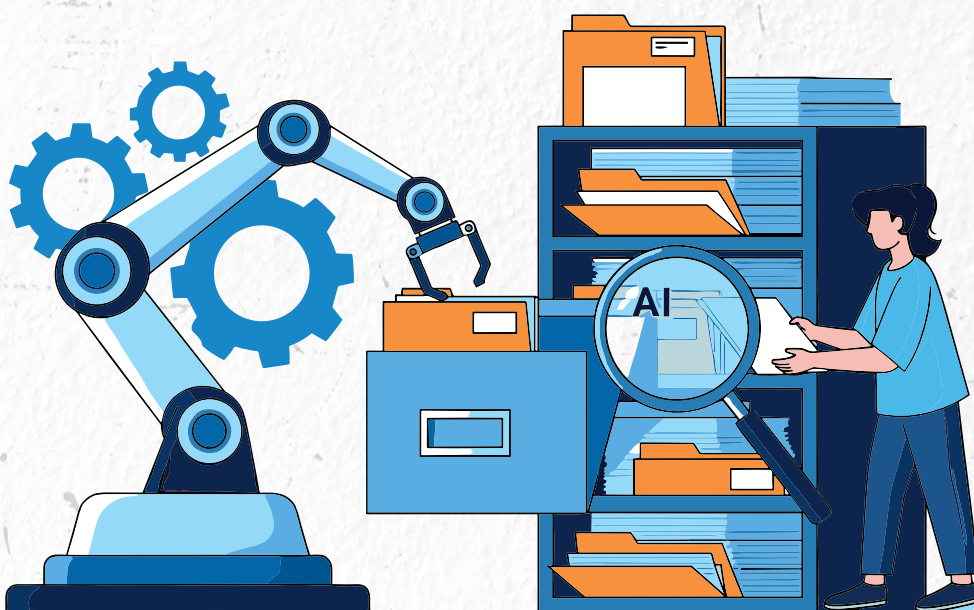
[frost.com](https://www.frost.com)





CONTENTS

- 3** Introduction
- 4** Realization of AI Immaturity Is Forcing a More Disciplined View of AI Deployments
- 5** Why Data Readiness Becomes the Bottleneck at Higher Maturity Levels
- 6** From Experimentation to Maturity: How AI Changes Expectations for File Data
- 7** AI Agents are Transforming Files from Passive Storage into Active Intelligence
- 8** How the Four AI Maturity Pillars Reframe File and Data Services
- 10** Why File Data Unification and Governance Becomes More Strategic as AI Maturity Increases
- 11** The Enterprise Shift from Storage to Data Services
- 12** What Mature Enterprises Do Differently with File and Data Services
- 13** What Enterprises Should Look for in a Data Services Provider to Increase Data Maturity
- 14** The Last Word





Introduction

Enterprises are moving fast on AI. Most are experimenting widely. Very few are scaling it in a way that delivers consistent business value. **The gap is not a lack of tools. It is a lack of alignment.**

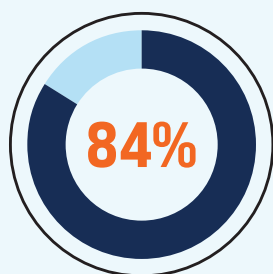
AI maturity is not measured by how many pilots an organization runs. It is defined by how well strategy, data, governance, and technology move forward together. When one pillar lags, especially data, AI progress stalls. This is where many organizations are today.

As companies push beyond experimentation, they discover that their assumptions about data no longer hold. Data is no longer something that businesses collect, store, and occasionally analyze. It is a live input into decision-making systems that need to operate consistently, securely, and at scale. File data sits at the center of this shift.

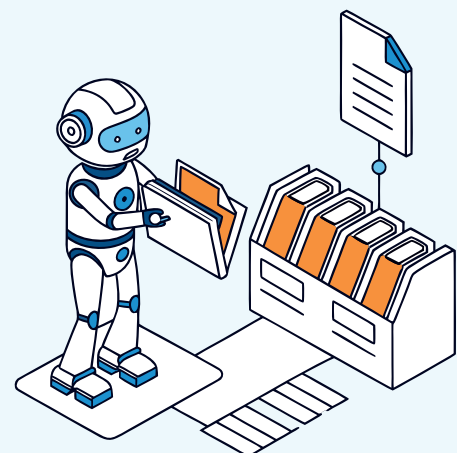
While “unstructured data” is often discussed in broad terms, the reality is more specific. File data, such as documents, images, logs, and operational content, is where a large percentage of enterprise knowledge lives. It has historically been treated as passive content, managed for access and storage, not for execution. That model breaks down in an AI context.

File data is now being used directly in model training and, more commonly, as the source of enterprise context for AI applications. It shapes outputs, influences decisions, and determines whether AI results are relevant or usable. That raises the bar.

Enterprises can no longer treat file environments as a side system. They must become part of a deliberate data strategy built for AI. Frost & Sullivan data reflects how early this shift still is.



Approximately **84% of organizations remain in exploratory or opportunistic stages of AI maturity**, and **fewer than 1% have reached ubiquitous maturity**. Most organizations are still building the foundations required to scale.

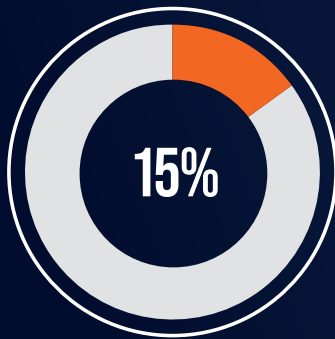




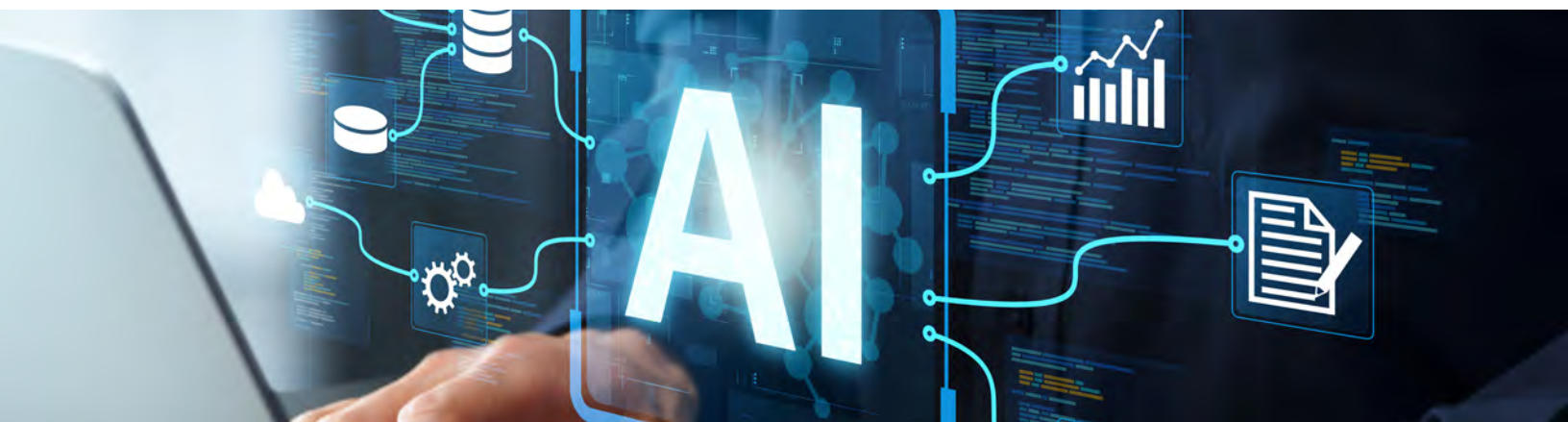
Realization of AI Immaturity Is Forcing a More Disciplined View of AI Deployments

Early AI efforts tend to follow a familiar pattern. Individual teams experiment with tools, test use cases, and deliver localized results. This creates momentum but it does not create scale. Over time, the limitations become clear. Disconnected initiatives lead to inconsistent outputs. Duplicate data creates conflicting results. Gaps in governance introduce risk. What works in one team does not translate across the business. Organizations are beginning to correct for this.

As AI initiatives mature, they shift from opportunistic to intentional. The focus moves from “what can we test?” to “what do we need to deliver, and how do we support it consistently?” This shift changes how data is treated. Fragmented data environments are no longer acceptable. Unmanaged experimentation becomes a liability. Data readiness that was once a downstream concern becomes a prerequisite. Yet most organizations are not there.



Only about 15% report having a mature AI strategy and roadmap. In many cases, technology adoption is moving faster than the ability to support it. That imbalance is now forcing a more disciplined approach to AI deployment, with data at the center of the AI strategy.





Why Data Readiness Becomes the Bottleneck at Higher Maturity Levels

In early stages, organizations can work around data limitations. They curate datasets, move data manually, or accept inconsistencies because the scope is limited. But when AI initiatives are deployed at production scale, those workarounds fail.

As AI expands across functions, fragmented data environments begin to constrain performance. Systems lack consistent context. Outputs vary depending on the source data. Trust erodes. Data readiness becomes the bottleneck.

Leading organizations are responding by reducing reliance on duplication and creating more unified access to data across environments. The goal is not to centralize everything, but to ensure that data, wherever it resides, can be accessed, governed, and used consistently. This approach also supports a key requirement at scale: control.

Enterprises need to maintain data locality for regulatory, operational, or performance reasons. At the same time, they must enforce consistent governance and access. Balancing these requirements is essential for scaling AI safely.



Most organizations are still early in this transition. Only about **12%** report ubiquitous data readiness for AI, and nearly **30%** continue to manage AI-relevant data in siloed environments.

File data presents the biggest gap. It represents a large percentage of enterprise information, but it is often the least structured, least governed, and hardest to access consistently. Without addressing this gap, organizations will struggle to scale AI beyond isolated use cases.



From Experimentation to Maturity: How AI Changes Expectations for File Data

File environments were not built for AI. They were built for collaboration. That difference matters. Collaboration-focused systems prioritize access and usability for people. AI systems require something different: consistency, context, and control. As AI matures, expectations for file data change in three important ways. First, data must be discoverable. If AI systems cannot find relevant content, they cannot use it. Second, data must be governed. Policies around access, usage, and compliance must apply consistently, regardless of where files reside. Third, data must be trusted. This includes quality, accuracy, and security.

Security is not optional in an AI context. File data often contains sensitive or regulated information. It can also introduce risk if it includes malicious content or is exposed without proper controls. Enterprises need confidence that the data feeding AI systems is safe, compliant, and appropriate for use.

At the same time, mature organizations reduce unnecessary data movement. Instead of copying data into separate systems for analytics or AI, they enable governed access to data in place. This reduces duplication, limits risk, and improves consistency. File data is no longer a parallel environment. It becomes part of the enterprise data architecture that supports AI.





AI Agents are Transforming Files from Passive Storage into Active Intelligence

As AI matures, its role in the enterprise is expanding. AI systems are no longer limited to generating insights. Increasingly, they are embedded into workflows: reading information, making recommendations, and taking action. This shift changes how file data is used.

AI agents are interacting directly with file-based content to extract context and support decisions. At the same time, enterprises are investing in other context layers, such as knowledge graphs and structured data environments, to organize relationships and business logic. These approaches are complementary.

File data remains a primary source of enterprise knowledge because it captures how work actually happens: documents, communications, operational records, and domain-specific content are not always reflected in structured systems and AI agents rely on this content to ground outputs in real business context.

To make this data usable, raw files are not enough. Enterprises must add structure through metadata, classification, and policy context. This allows AI systems to interpret what the data is, how it should be used, and what constraints apply.

A unified file access layer can support this by providing consistent access to file data across environments. Its value, however, depends on how well that data is organized and understood. Classification, tagging, and policy context are required to make file content usable for AI. When paired with appropriate controls, a unified layer enables AI agents to work from trusted, relevant content across distributed environments, without introducing fragmentation or duplication. The result is a shift in how file data is viewed. It is no longer passive storage. It becomes an active input into enterprise intelligence.





How the Four AI Maturity Pillars Reframe File and Data Services

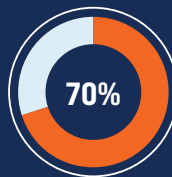
As organizations move from experimentation to scaled AI, expectations shift quickly. What worked in isolated projects does not hold up across the enterprise.

This is where the four pillars of AI maturity—strategy, data readiness, compliance, and technology—begin to reshape how file and data services are managed.

Strategy and Roadmap Articulation

Mature AI organizations start with outcomes. They define what the business needs to achieve and align investments accordingly. That shift elevates the role of data services.

File data governance is no longer just an IT responsibility. It becomes a strategic decision because it directly affects the quality, consistency, and reliability of AI outcomes. Without alignment between data services and AI strategy, organizations risk building on an unstable foundation. This remains a common gap.



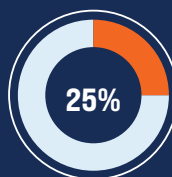
More than **70%** of organizations still lack enterprise-level AI strategy alignment, limiting their ability to scale effectively.

Data Readiness

Data readiness is where most AI initiatives slow down. At scale, AI requires consistent access to structured and unstructured data. File data, which is often the least governed and least integrated, becomes a critical constraint.

To support AI, file data must be integrated into the broader data architecture. It must also be classified, tagged, and governed so it can be discovered, interpreted, and used reliably. Storage alone is not the issue. Context matters more than in the past. Metadata, classification, and policy alignment are what make file data usable for AI systems and agents. Without them, even large volumes of data provide limited value.

Mature organizations address this directly. They enrich file data so that AI operates on content that is relevant, trusted, and aligned with policy. Few organizations have reached this point.



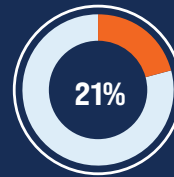
Fewer than **25%** report consolidating enterprise data into unified platforms, highlighting the scale of the challenge.



Regulatory Compliance and Policy Alignment

As AI expands, risk expands with it. File data often contains sensitive or regulated information. When that data is used in AI systems, the requirements for governance increase significantly. Organizations must be able to apply consistent policy controls across all file environments, regardless of location. This includes access controls, usage policies, and auditability. Traceability becomes essential.

Enterprises must understand where data comes from, how it is used, and how it flows through AI systems. Without this visibility, responsible AI is not achievable. Most organizations are still behind.



Only about **21%** report enterprise-level maturity in AI regulatory and compliance capabilities.

Technology Implementation

AI deployment is accelerating. Governance and data readiness are not keeping pace. This creates a widening gap. Many organizations have deployed AI in at least one business function: nearly 40% (based on Frost & Sullivan research), though far fewer have scaled those deployments in a controlled, consistent way. The result is operational and reputational risk.

Mature organizations respond by prioritizing platforms that embed governance, security, and control into how data is accessed and used. Rather than layering these capabilities later, they build them in from the start.





Why File Data Unification and Governance Becomes More Strategic as AI Maturity Increases

As AI matures, the importance of file data increases quickly. At higher levels of maturity, AI systems rely on unstructured data. File-based content, including documents, records, and communications, often contains institutional knowledge that is not captured anywhere else. This creates both an opportunity and a risk.

If file environments are well managed, they provide rich context that improves AI accuracy and relevance. If they are not, they introduce inconsistency, bias, and unreliable outputs. Mature organizations recognize this trade-off. They treat file data as an enterprise asset, not as departmental storage. Governance, access, and usage are managed consistently across the organization, not left to individual teams.

At the same time, the environment itself is becoming more distributed. A growing percentage of file data is created at the edge in branch offices, operational sites, and remote work environments. Centralizing everything is not practical, and often not desirable.

Instead, leading organizations focus on visibility and control across environments. They ensure that file data can be governed and accessed consistently from core to edge, without disrupting workflows or forcing unnecessary data movement. This balance is critical for scaling AI in a distributed enterprise.





The Enterprise Shift from Storage to Data Services

AI is changing how enterprises think about data. Traditional models focused on storage capacity, performance, and availability. But those features are no longer enough. As AI matures, organizations need data services.

Data services prioritize access, governance, and activation. The goal is not just to store data, but to make it usable in a controlled and consistent way across the enterprise. This shift becomes more pronounced at higher levels of maturity.

Enterprises move from managing data as a raw input to managing content as a contextual signal. File-based content carries meaning including intent, relevance, sensitivity, and relationships that AI systems must understand to act correctly. That requires more than simple data access. It requires classification, context, and policy alignment. It requires the ability to expose data to AI systems deliberately, not incidentally.

File and data services have become a foundational layer in this model. They enable organizations to scale AI capabilities while maintaining control over how data is used. The outcome is a more sustainable approach to AI that reduces risk while improving consistency and performance.





What Mature Enterprises Do Differently with File and Data Services

Organizations that scale AI successfully take a different approach to file and data services. They focus on access, not duplication. Instead of replicating data across environments, they enable controlled access to data where it resides. This reduces inconsistency and limits risk. They embed governance into the data lifecycle. Policies are applied consistently from creation to usage rather than enforced after the fact.

Organizations approaching AI in a more evolved, mature way strive to reduce shadow AI. By enforcing enterprise-wide data controls, they limit the creation of unmanaged datasets and unauthorized AI usage that can introduce risk. They also align file services with broader data and AI strategies. File data is not treated as a separate system. It is integrated into how the organization manages and activates data overall.





What Enterprises Should Look for in a Data Services Provider to Increase Data Maturity

As enterprises work to improve data maturity, the role of the data services provider becomes more important. The right provider should support both immediate needs and long-term progress.

Clear visibility into file data



Enterprises need to understand what file data they have and where it lives before they can use it effectively for AI. The right provider delivers centralized insight across environments while allowing teams to keep working the way they do today.

A path forward that does not disrupt the business



Most organizations improve data maturity incrementally. Providers should support progress without requiring wholesale migration, workflow changes, or retraining, allowing governance and control to mature alongside AI initiatives.

Governance that is consistent, not situational



As AI moves beyond pilots, policy gaps become risk gaps. Enterprises should expect governance that applies the same rules everywhere data exists, rather than relying on local controls or manual oversight.

Intentional access to data for AI and analytics



Enterprises need to decide how file data and context is exposed to AI systems and agents, not discover it after the fact. The right provider supports controlled access so data can be used where it adds value, without encouraging unmanaged copies or shadow projects.

Restore with trusted data



Data protection goes beyond recovery. File data must be accurate, secure, and policy-aligned so what you restore is data you can immediately trust for AI and analytics, without repeated validation.

Alignment with broader data priorities



As AI becomes more strategic, file services cannot sit off to the side. Providers should fit naturally into enterprise data and AI strategies, supporting them rather than creating parallel systems that add complexity.



The Last Word

AI maturity is not defined by how quickly organizations adopt new tools. It is defined by how effectively they build the foundations that support those tools. Most enterprises are still early in this journey.

As AI activity accelerates, expectations for data are changing. Environments that were designed for collaboration are not designed for AI. At scale, AI systems and agents require consistent access, governance, and trust. This requires stronger metadata, classification, and policy alignment. It requires ensuring that AI operates on relevant, controlled data rather than raw, unmanaged files. It also requires intentional planning and execution. Enterprises must decide how file content is exposed to analytics and AI systems rather than discovering gaps after the fact.

The organizations that succeed will not be those that move the fastest. They will be the ones that align content, data services, governance, and strategy at enterprise scale. Treating file data as part of a deliberate data and AI maturity journey rather than as a storage challenge is a critical step in making AI both scalable and trustworthy.

About CTERA

CTERA is a global leader in the integrated data intelligence market enabling organizations of all sizes to efficiently and effectively manage, protect, store, and leverage their data across highly distributed environments. With a foundation built on security, scale, and seamless integration, the CTERA Intelligent Data Platform empowers organizations to align their data management strategies to continuously deliver against today's business needs and tomorrow's vision.

Learn more at www.ctera.com

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. →

FROST & SULLIVAN