DataXray

PRACTICAL GUIDE

Governing Data Access in the Age of AI

A Practical Guide to Data Access Governance (DAG) Across Unstructured Data Environments

Unstructured file access is a major blind spot in enterprise data governance.

Every day, teams share documents, spreadsheets, contracts, and reports across platforms like Google Drive, SharePoint, and Box. Access permissions pile up. Files get duplicated. Collaborators come and go. Over time, access becomes opaque. And worse, impossible to audit.

This isn't just a security gap. It's a governance failure. One that slows audits, undermines AI compliance, and keeps CISOs, CDOs, and privacy teams on the defensive.

Left unresolved, this creates hidden operational drag such as repeated audit delays, duplicated reviews, and reactive clean-up work.

EVERYDAY PRACTICES THAT CREATE LONG-TERM EXPOSURE

You've likely seen this first-hand:

- A former employee still has edit rights to a sensitive folder.
- You can't tell which contractor downloaded what during a project.
- Teams resist revoking access because "someone might still need it."
- Data shows up in an AI training pipeline, but you don't know where it came from.

A STRUCTURED APPROACH TO GOVERNING ACCESS ACROSS UNSTRUCTURED DATA

DataXray was purpose-built to address this exact challenge without forcing a major rearchitecture or migration. It integrates across your cloud and on-prem environments to show you:

01 **What unstructured data you have**

02 **Where it lives**

03 **What's inside it**

04 **And who has access to it**

> With DataXray's industry-leading discovery and classification engine, you can finally govern file access based on content, not just folder structure or default permissions. This helps you create a governed inventory of unstructured data that's searchable, auditable, and policy-aligned.

CHALLENGES YOU'RE LIKELY FACING	WHAT DATAXRAY ENABLES
Overexposed files no one is tracking	**See who has access and why**
Unclassified sensitive content	**Auto-label files by PII, IP, credentials, etc.**
Inconsistent permissions across platforms	**Standardize visibility across cloud + on-prem**
Missed risks in AI model inputs	**Align file governance with AI compliance requirements**
Manual audits and access reviews	**Automate with policy packs and audit-ready workflows**

CUSTOMER STORY

What changed when a global enterprise brought file access under governance

A global bank used DataXray to assess file access risks across 120+ SharePoint and OneDrive instances. Within days, they uncovered:

40,000+
files with sensitive content shared externally

Dormant access
from contractors who hadn't logged in for months

AI exposure
files accessed by AI applications, including outdated, misclassified files

60%+ They reclassified over 60% of high-risk files, launched access review workflows, and built a defensible audit trail ahead of a cross-border compliance review.

WHY TEAMS IMPLEMENT DATAXRAY ALONGSIDE EXISTING TOOLS

Traditional DLP tools weren't built to govern content in collaboration platforms. They flag incidents at the edge. And IAM solutions rarely touch unstructured data, leaving file-level permissions completely unverified. DataXray replaces brittle manual reviews and incomplete discovery efforts. It's designed to:

01 Deploy quickly without agent installation

02 Scale across petabytes and multiple cloud providers

03 Integrate with tools like data catalogs for data and AI governance and DLP platforms

04 Provide file-level auditability for compliance and AI readiness

05 Surface actionable risk

Teams choose DataXray because it helps them close the governance loop on their most opaque data layer, and do it in a way that fits how they already operate.

Talk to us about evaluating your access posture.

DataXray

dataxray.io
hello@dataxray.io
+44 330 222 0016 · +1 917 633 7719