



Connect the Dots in Data & AI

Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

► Cloud-native

► Agentless

► Enterprise-Scale

► Fast & Accurate

Data Access Governance & Data Activity Monitoring for the Agentic Era

Governing Non-Human Identities
in a World of Autonomous AI



Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

Data Access Governance & Data Activity Monitoring for the Agentic Era

Executive Summary

As enterprises rapidly adopt agentic AI, the definition of “identity” is expanding. Autonomous agents, service accounts, and AI-driven workflows now access, move, and act on sensitive data at machine speed—often without direct human oversight. While these agents unlock productivity and innovation, they also introduce a new class of data risk that traditional IAM, monitoring, and governance models were never designed to handle.

To govern the agentic era securely, organizations must shift from identity-only controls to a **data-centric security and governance model**—one that continuously understands what data exists, who or what can access it, and how it is actually being used. Two capabilities become foundational in this shift:

- **Data Access Governance** – controlling and minimizing who and what has access to sensitive data
- **Data Activity Monitoring** – observing and responding to how data is accessed and used in practice

Together, these capabilities enable organizations to govern both human and non-human identities with confidence. BigID uniquely unifies both—on top of deep data intelligence—to deliver security, governance, and trust in the agentic era.

THE AGENTIC SHIFT: WHY TRADITIONAL CONTROLS FALL SHORT

AI agents and non-human identities (NHIs) are no longer edge cases. They:

- Continuously access large volumes of sensitive data
- Operate across cloud, SaaS, data platforms, and unstructured sources
- Make autonomous decisions and take actions without direct human approval

Yet most security programs still rely on:

- Static entitlement reviews
- Identity-centric IAM controls
- Fragmented activity logs without data context

These approaches were built for human users—not autonomous agents. As a result, organizations face critical blind spots:

- Over-permissioned service accounts and AI agents
- No visibility into what sensitive data agents actually access
- Alert fatigue without clarity on real risk
- Inability to explain or audit AI-driven data access

In the agentic era, **governance must follow the data—not just the identity.**

DATA ACCESS GOVERNANCE: CONTROLLING WHO AND WHAT SHOULD HAVE ACCESS

What Data Access Governance Means in the Agentic Era

Data Access Governance extends beyond traditional access reviews. It answers a more critical question:

Who—or what—should have access to this specific data, given its sensitivity, usage, and risk?

In an environment filled with NHIs and AI agents, this requires:

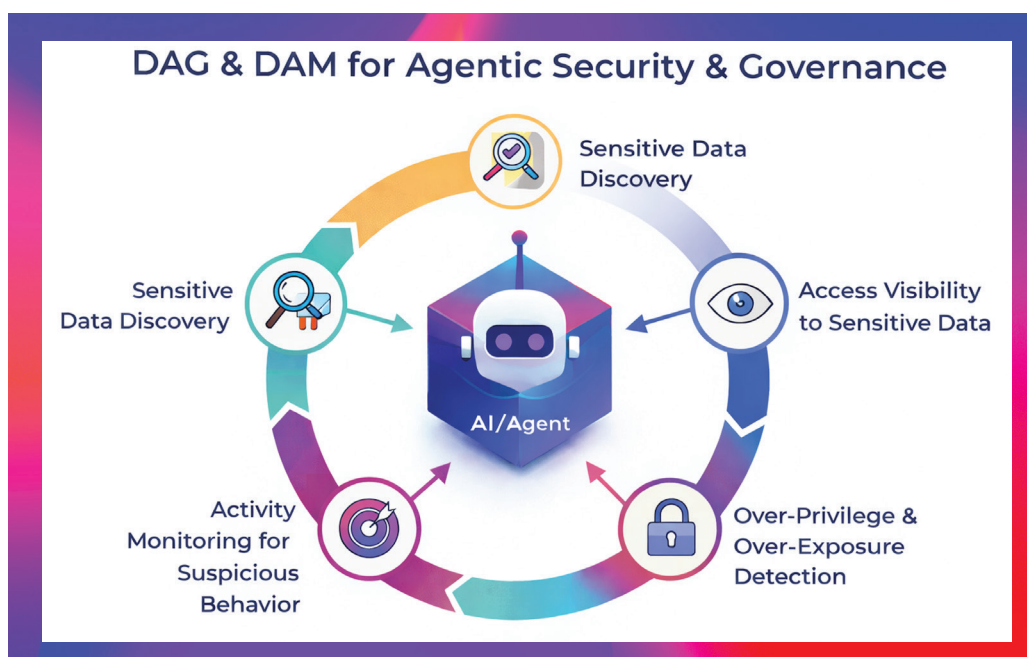
- Deep understanding of data sensitivity and context
- Visibility into all identities—human and non-human
- Continuous evaluation of over-privilege and overexposure

How BigID Enables Data Access Governance

BigID takes a **data-centric approach** to access governance by fusing data intelligence with access visibility:

- **Complete Access Visibility**
- Discover and classify sensitive data, then map who—and what—has access across cloud, SaaS, on-prem, and AI pipelines.
- **Non-Human Identity Coverage**
Extend governance beyond users to include service accounts, automated workflows, and AI models accessing data.
- **Over-Privilege & Overexposure Detection**
Identify excessive permissions and overexposed sensitive data to prioritize what matters most.
- **Automated, Policy-Driven Remediation**
Revoke unnecessary access and enforce least privilege directly through BigID or integrated IAM tools.

With BigID, access governance becomes **continuous, risk-aware, and scalable**—not a manual checkbox exercise.



DATA ACTIVITY MONITORING: GOVERNING HOW DATA IS ACTUALLY USED**Why Monitoring Matters More Than Ever**

Access alone doesn't equal risk—**usage does.**

AI agents may have legitimate access yet still:

- Exfiltrate sensitive data unintentionally
- Access data outside intended purpose
- Amplify mistakes at machine speed

Without continuous monitoring, organizations cannot answer fundamental questions:

- What data did this agent access?
- Was that access expected or risky?
- What is the blast radius if it's compromised?

How BigID Delivers Context-Rich Data Activity Monitoring

BigID's Data Activity Monitoring provides continuous, contextual insight into who is accessing what data, when, how, and why—across users, service accounts, and AI agents.

Key capabilities include:

- **Unified Activity Visibility**
Monitor data activity across AWS S3, OneDrive, SharePoint, Google Drive, file shares, and more—from a single view.
- **Contextual, AI-Powered Detection**
Correlate activity with data sensitivity, ownership, permissions, and identity to distinguish real risk from noise.
- **Unified Investigation with Activity Explorer**
Rapidly investigate incidents with a complete audit trail across human and non-human actors.
- **Automated Risk Response**
Trigger remediation actions such as access revocation, quarantine, or Cloud DLP enforcement.
- **Audit-Ready Reporting**
Maintain compliance and explainability for regulations and emerging AI governance requirements.

In the agentic era, monitoring is not about logging—it's about **understanding behavior in context.**

STRONGER TOGETHER: WHY ACCESS GOVERNANCE + ACTIVITY MONITORING MUST BE UNIFIED

Individually, access governance and activity monitoring provide value. Together—on top of data intelligence—they become transformational.

BigID uniquely unifies:

- **What data exists and how sensitive it is**
- **Who or what can access it**
- **How it is actually being used**
- **What action to take—automatically**

This unified approach enables organizations to:

- Govern AI agents with the same rigor as humans
- Reduce attack surface before incidents occur
- Detect misuse faster and respond with precision
- Enforce Zero Trust based on real usage, not assumptions
- Build trust, transparency, and auditability into AI systems

WHY BIGID IS THE FOUNDATION FOR AGENTIC DATA GOVERNANCE

BigID is purpose-built to govern data and AI at enterprise scale. With cloud-native, agentless architecture and deep data intelligence, BigID helps organizations:

- Find and classify sensitive data everywhere
- Govern access across humans and non-human identities
- Continuously monitor data activity with context
- Automate remediation and enforcement
- Support security, privacy, compliance, and AI governance from a single platform

As AI agents become first-class actors in the enterprise, **trust will depend on data-centric governance.**

BigID is the platform that makes it possible.



Connect the Dots in Data & AI

Know your data and AI. Control your data and AI.

Cloud-native and agentless — built for speed, accuracy, and scale.

► Cloud-native

► Agentless

► Enterprise-Scale

► Fast & Accurate

About BigID

BigID helps organizations connect the dots across data & AI: for security, privacy, compliance, and AI data management. BigID enables customers to find, understand, manage, protect, and take action on high risk & high value data, wherever it lives.

Customers use BigID to reduce their AI & data risk, automate security and privacy controls, achieve compliance, and understand their data throughout their entire data landscape: from the cloud, on-prem, and everywhere in between.



Tools like BigID are the future.

Organizations should be leveraging these tools to remove the manual processes from data discovery, provide better visibility, and help with prioritization of controls.



Ryan O'Leary

Future of Trust: Battling Data Discovery Confusion