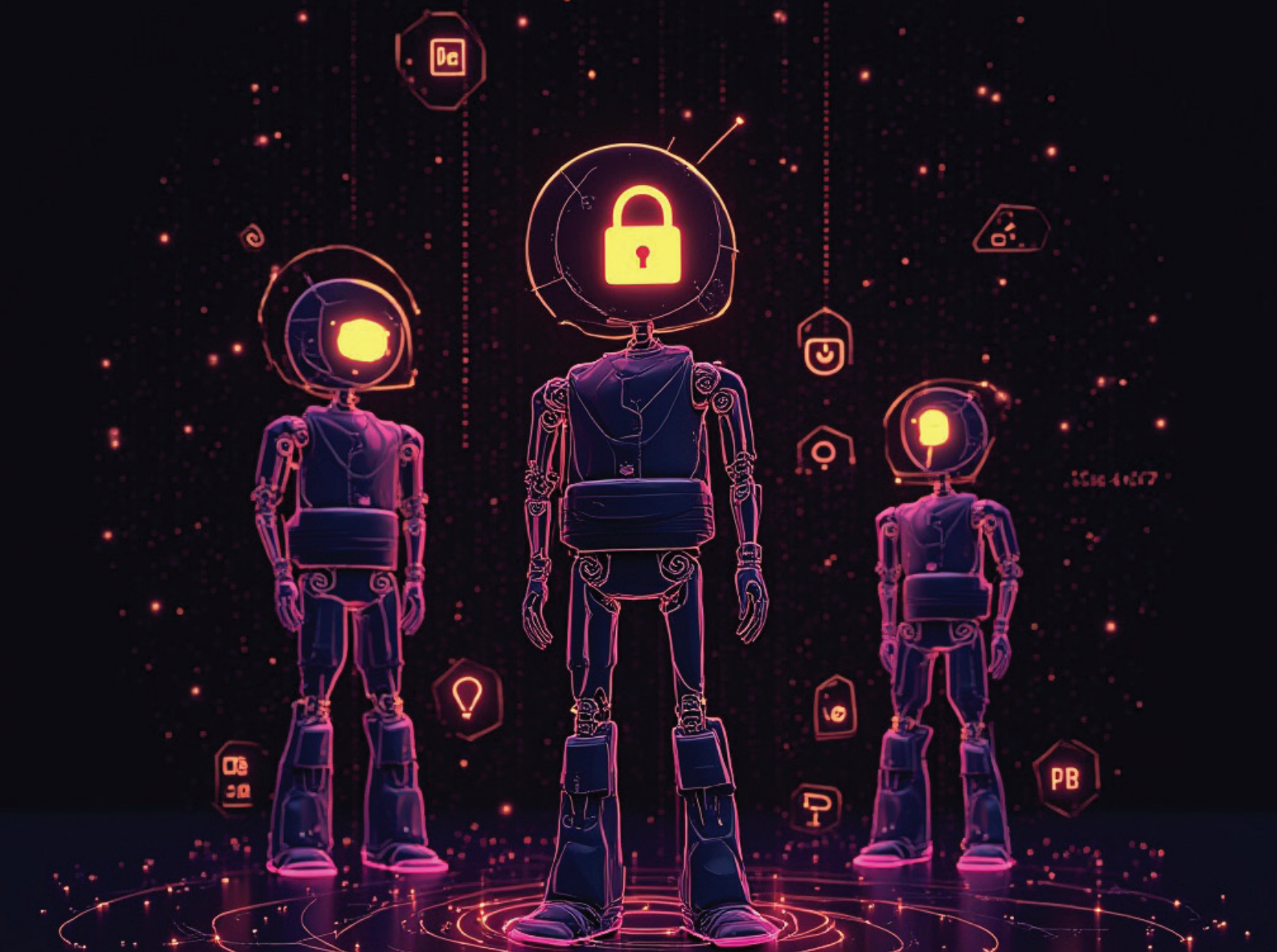
big·id NEXT

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.

A Practical Guide to Agent Access Management (AAM)

A Data-First Model for Governing AI and Non-Human Identities



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

A Practical Guide to Agent Access Management (AAM)

Executive Summary
Non-human identities — including AI agents, service accounts, and automated processes — now represent one of the fastest-growing sources of data risk in the enterprise. These agents operate autonomously, inherit broad permissions, and access sensitive data at machine speed.

Traditional access governance models were not designed for this reality.

This white paper introduces a **practical, data-first model for Agent Access Management (AAM)** — helping security leaders assess maturity, identify gaps, and operationalize governance across **both human and non-human identities**. Within AAM, **Agent Access Control** is the outcome: enforcing least privilege, monitoring usage, and responding to risk in real time.

WHAT IS AGENT ACCESS MANAGEMENT (AAM)?

Agent Access Management (AAM) is the discipline of governing how non-human identities access and interact with enterprise data — including:

- how they obtain entitlements
- what data they can reach
- what actions they perform
- whether access remains appropriate as systems and risk evolve

Agent Access Control is the operational enforcement layer within AAM: applying policy, restricting privileges, detecting misuse, and taking corrective action.

WHY IAM AND AI GOVERNANCE ALONE ARE INSUFFICIENT

IAM tools answer who exists and what permissions were granted.
AI governance tools often focus on model training, deployment controls, and safety.

Neither consistently answers:

- What sensitive data agents can access
- How that access is actually used
- Whether agent behavior introduces risk over time

AAM fills this gap by anchoring governance and control in data context.

THE AGENT ACCESS MANAGEMENT MATURITY MODEL

Level 1: Blind Access

- No inventory of non-human identities
- No visibility into agent access to sensitive data
- Reactive, incident-driven response

Level 2: Identity-Aware

- Basic visibility into service accounts and agents
- Entitlements tracked, but not tied to data sensitivity
- Manual reviews, limited enforcement

Level 3: Data-Aware

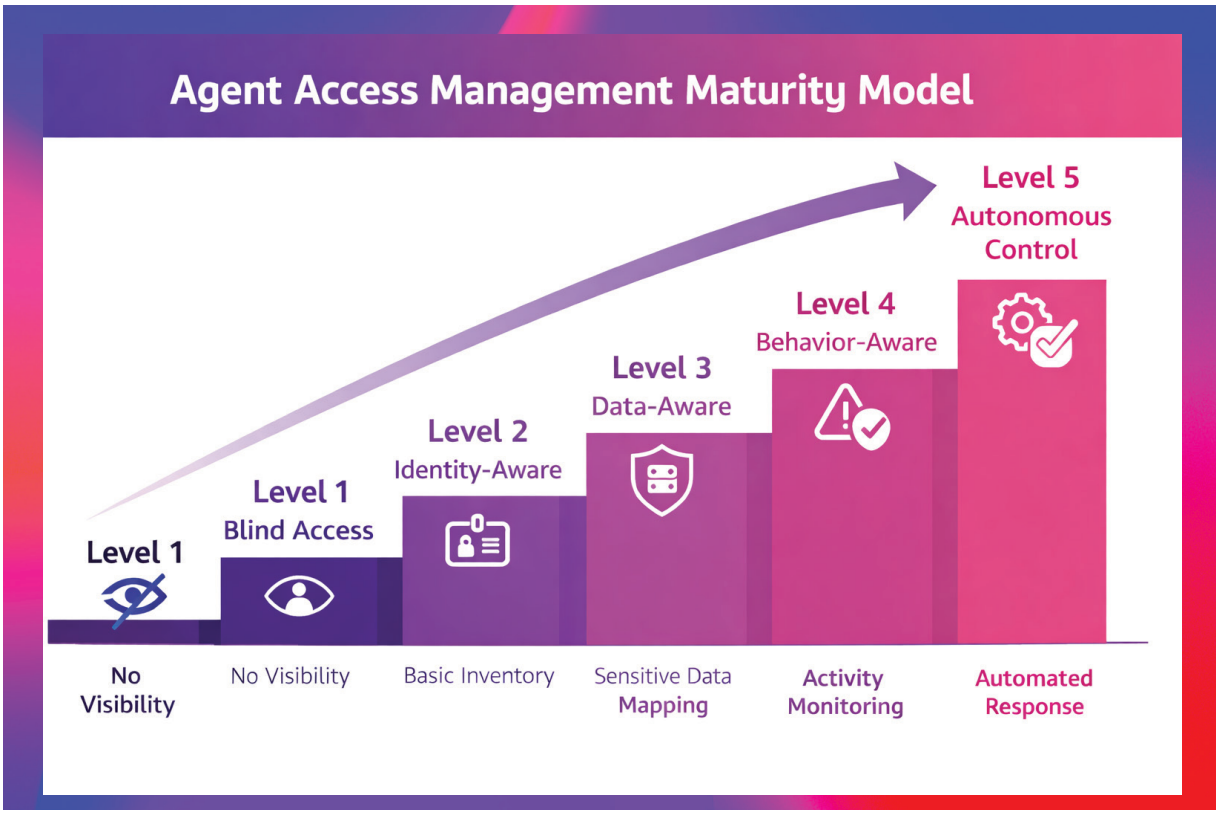
- Sensitive data discovery and classification
- Agent access mapped to data risk
- Prioritized remediation of overexposed data

Level 4: Behavior-Aware

- Continuous monitoring of data activity
- Detection of anomalous or risky agent behavior
- Faster investigation and response

Level 5: Autonomous Control

- Automated policy enforcement
- Risk-based access adjustments in near real time
- Closed-loop remediation at machine scale



AAM READINESS CHECKLIST

Discovery & Visibility

- Can we identify all non-human identities accessing sensitive data?
- Do we know where sensitive data lives across cloud, SaaS, and on-prem?

Access Governance

- Can we determine whether agents are overprivileged relative to the data they can access?
- Can we enforce least privilege tied to data sensitivity and business purpose?

Monitoring & Detection

- Can we monitor agent interactions with sensitive data continuously?
- Can we detect anomalous access patterns and suspicious behavior?

Response & Remediation

- Can we automatically revoke or adjust agent access based on risk?
- Can remediation occur at the data source and be verified?

REFERENCE ARCHITECTURE: AAM REQUIRES DSPM + DAG + DAM

AAM depends on the convergence of:

- **DSPM** → discover and classify sensitive data
- **DAG** → map and govern access paths and entitlements for all identities
- **DAM** → monitor, investigate, and respond to real-world data usag

Unified, these capabilities enable **Agent Access Control** — enforcement, monitoring, and automated risk reduction at scale.

WHY BIGID

BigID is uniquely positioned to operationalize Agent Access Management by delivering:

- industry-leading data discovery and classification
- identity-aware access intelligence across humans and agents
- unified data activity monitoring and automated remediation

Rather than treating agent access as an edge case, BigID enables a unified program to govern **any identity that touches data** — with continuous visibility and scalable control.

CONCLUSION

Agent Access Management is quickly becoming foundational to modern data security. As AI agents and automation expand, organizations must move beyond identity-only governance toward a data-first approach.

By adopting a structured AAM model and unifying DSPM, DAG, and DAM, security leaders can reduce risk, improve accountability, and secure data — regardless of who or what accesses it.

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.

IDC

Ryan O'Leary
Future of Trust: Battling Data Discovery Confusion