

Still playing data hide and seek?

Striving toward a Zero Trust data pillar?

You can't protect what you can't see; most data is unstructured and hiding in plain sight, ungoverned and uncategorized.

Many security leaders and IT decision-makers agree data is a barrier to Zero Trust.¹

Federal agencies have made progress on identity and devices...the data pillar remains unresolved.

Overcoming the governance gap: where the remaining exposure lives.

- Contracts, forms and correspondences in unmanaged file shares
- Personally Identifiable Information (PII) buried in email threads and attachments
- Regulated content in cloud collaboration tools
- Legacy repositories without policy or ownership

Zero Trust data control is critical as a launch point for reliable AI and machine learning.

- Discover and categorize unstructured data
- Apply comprehensive rules, policies and terms the entire organization can manage
- Take control of unstructured data for improved decision making
- Enforce Zero Trust policy

You can't enforce least-privilege access on data you haven't cataloged.

You can't govern what you haven't found.

The gap between a Zero Trust policy and Zero Trust reality is often a data capture and governance problem.

- Access controls built on an incomplete data inventory
- Unstructured data is often ungoverned data
- Unstructured data is often an unmonitored threat surface
- Zero Trust strategy built with a structural blind spot due to unstructured data

¹ CYBER360: Defending the Digital Battlespace. Herndon, VA: Everfox, February 2026. Survey conducted October 2025 by Censuswide; n=500 cyber professionals in government, defense, and critical services across the U.S. and UK. Available at: <https://info.everfox.com/cyber360-defending-the-digital-battlespace>

Colibra Public Sector solution

- **Complete data inventory across the data estate:** Structured databases, unstructured repositories, hybrid environments – surfaced, categorized and cataloged continuously without manual effort
- **Sensitive data categorized before it causes exposure:** Personally Identifiable Information (PII), regulated content and confidential files identified and tagged at scale without a manual classification project
- **AI governance grounded in a comprehensive data layer:** Unstructured content enriched with metadata before it reaches AI pipelines; so models use governed, trusted, AI-ready assets
- **Policy enforcement, not just good intentions:** Retention schedules, access controls and data ownership defined in Colibra – applied across asset classes

Key outcomes

Zero Trust Data pillar, fully grounded

Automated discovery feeds a living catalog. The catalog enforces access policy. Every asset – structured or not – is visible, classified and governed. That's not just better compliance. That's the data foundation Zero Trust actually requires.

Colibra + Data X-Ray

Find and manage structured and unstructured data. Scans petabytes of unstructured content – file shares, cloud storage, email, PDF, CMS platforms – using Machine Learning (ML) and Natural Language Processing (NLP) to surface sensitive data, PII, and regulated content wherever it lives. Continuous discovery means your catalog stays current, not stale.



Request a demo. <https://www.publicsector.com>