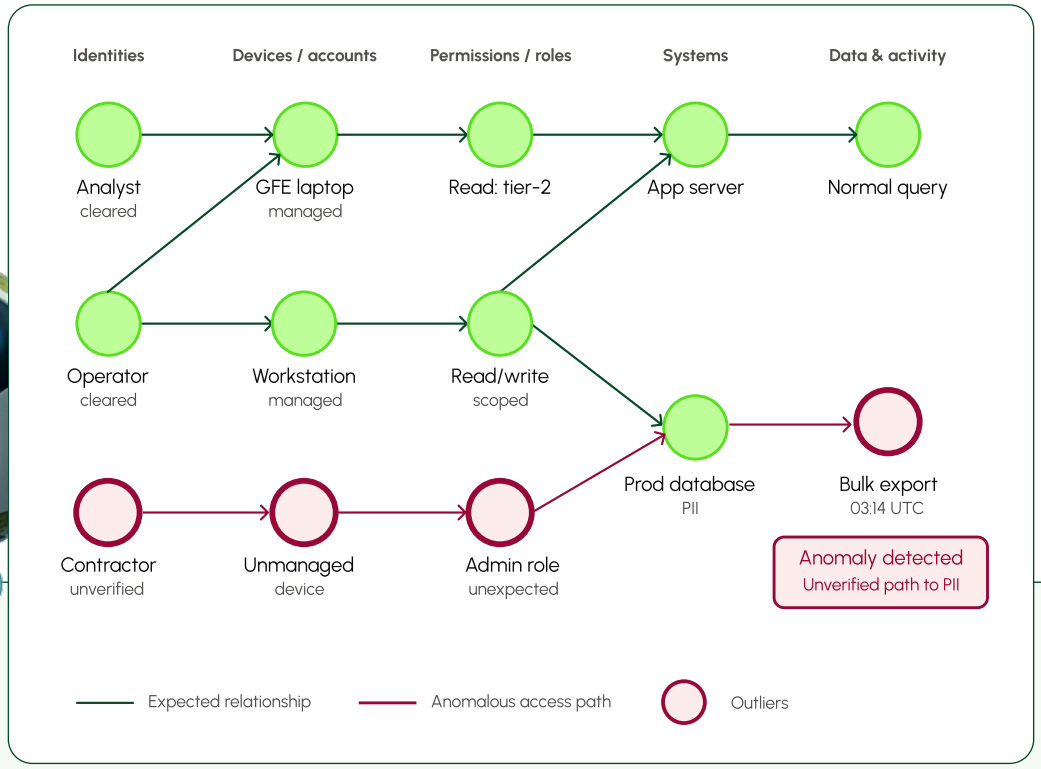
Zero Trust Overview

Preserving Trust, Provenance & Traceability for Zero Trust

Zero Trust is a data problem. NIST SP 800-207 and the CISA Zero Trust Maturity Model ask agencies to verify every user, device, and request continuously — possible only when the relationships among identities, assets, permissions, systems, and activity are connected and governed in one place. Arango models that environment as one governed knowledge graph.

Agencies can enforce least privilege, detect anomalies, and keep every output traceable to source, turning Zero Trust from a policy document into an operational, auditable capability built into the data layer itself.

Zero Trust is a data problem. The graph shows the access path that shouldn't exist.



Modeling users, devices, credentials, permissions, systems and activity as one governed graph lets analysts see (and continuously monitor) least-privilege violations and lateral-movement paths that siloed logs never connect.

The Arango role in Zero Trust:

Preserve Trust

Prove Provenance

Trace Every Answer

Mapping to the CISA Zero Trust Maturity Model

Platform capabilities map to the five pillars of the CISA Zero Trust Maturity Model, plus continuous verification.

Identity
Resolve fragmented identifiers into one authoritative entity per person or account, then enforce role- and attribute-based access control.

Devices
Model device-to-account-to-activity relationships to flag unmanaged or unexpected devices before they reach sensitive systems.

Applications & Data
Enforce field-level authorization in the engine itself, backed by governed lineage and citations for every output.

Visibility & Analytics
Run graph analytics to detect anomalies, lateral movement, and outlier access paths that siloed logs never connect.

Governance
Express policy as data on the graph, backed by immutable audit and explainable query plans for every action.

Continuous Verification
Support NIST SP 800-207 continuous verification of every user, device, and request against the current governed graph.

The five CISA pillars

Identity **Devices** **Applications & Data** **Visibility & Analytics** **Governance**

The Arango Role in Zero Trust

Trust is not a feature bolted on top — it's a property of the data foundation itself. Four capabilities make Arango-grounded analytics and AI defensible in a Zero Trust environment.

Preserve Trust
Least-privilege access is enforced in the engine — RBAC/ABAC at document, edge, and field level.

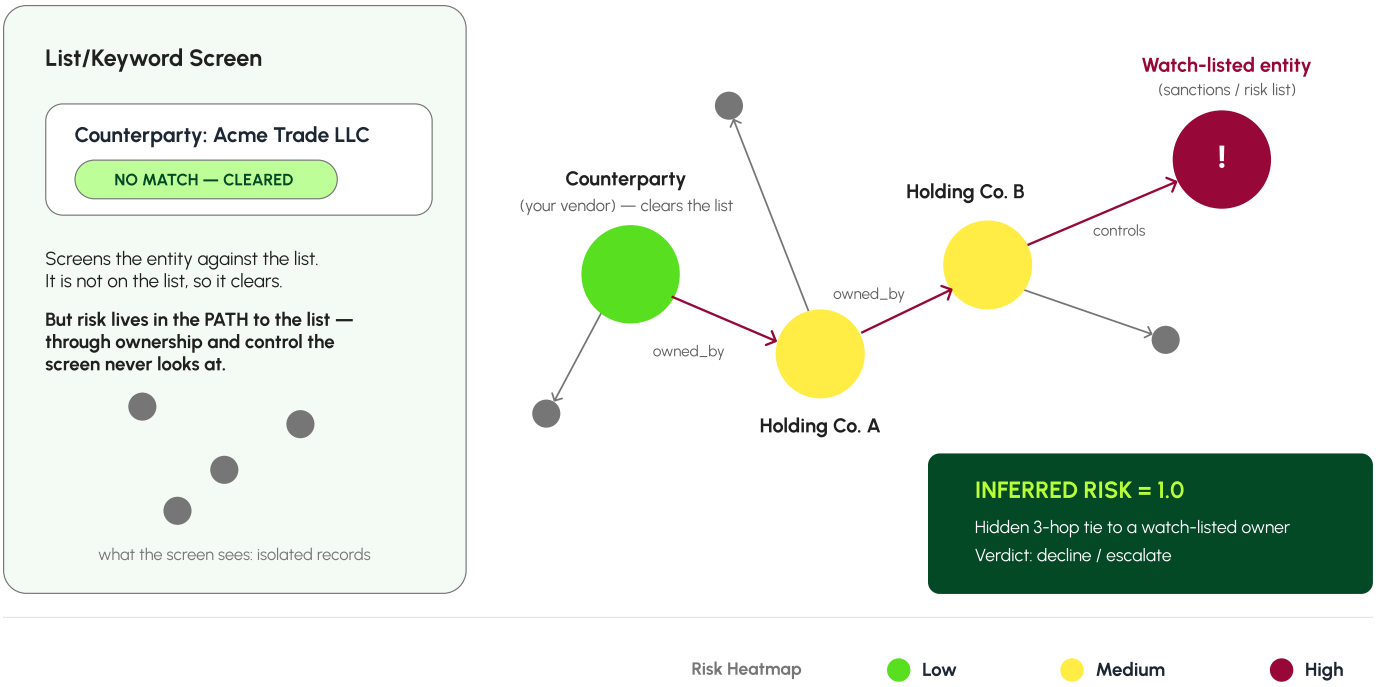
Prove Provenance
Lineage is captured at write and query time, so every output traces to source records.

Trace Every Answer
Explainable query plans, citations, and immutable audit logs support continuous monitoring.

From one governed graph to a defensible answer

Preserve → **Prove** → **Trace**

Knowledge Graphs Surface the Risk a List Search Cannot See



A keyword/list screen clears the vendor. The knowledge graph follows ownership and control across multiple hops, multiplies risk along the path, and surfaces the concealed tie to a watch-listed entity with the exact, auditable path that produced the score.

Platform Context

Zero Trust runs on the same governed graph as Intelligence Analysis and Supply Chain Risk Management. Users, assets, organizations, systems, permissions, and events are modeled as native relationships in one engine, with graph, vector, geospatial, and machine learning running against the same governed data — no bolt-on stores to sync, so anomaly findings stay consistent and explainable across every mission use case.

Operational Impact

A watchlist tells you who is on it; Arango's knowledge graph tells you who is one relationship away — surfacing transitive risk and hidden access paths for insider-threat and fraud analysis.

Built and Certified for the Most Rigorous Requirements

Arango is built and certified for the most rigorous federal security and compliance requirements agencies face today.

Certified & Audited

SOC 2 Type 2, HIPAA compliance, and NIST SP 800-218 secure development, verified by annual penetration testing.

Access Control Built In

RBAC and ABAC enforced at document, edge, and field level, with LDAP/AD and SSO integration.

Encrypted End to End

AES-256 encryption at rest, in transit, and in encrypted backups, with detailed exportable audit logs.

Supports Your Mission ATO

Maps to NIST SP 800-207, NIST SP 800-53 control families, and self-managed, air-gapped deployment options.

Trusted by These Organizations and Many Others

U.S. AIR FORCE · NIH National Institutes of Health · SARONIC · accenture · Deloitte. · BABEL STREET

Ready to make Zero Trust operational, not just policy?

Schedule a demo and see how Arango maps to your mission's Zero Trust maturity model.

arango.ai federal@arangodb.com