

The Three Pillars of Durable Data Security

Presence, Lineage, and AI: why each depends on the others

Every security vendor now claims AI capabilities, and foundation models are becoming interchangeable. The real question is not which vendor has the best model. It is **what the model is running on**. A durable program rests on three elements. Miss one, and the architecture breaks.

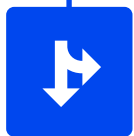


ELEMENT ONE

Endpoint Presence

You cannot secure what you cannot see. The endpoint is where a developer pastes proprietary code into a local AI tool and where an AI agent reads files and redistributes content with no human approving each step. Cloud-only tools miss all of it.

Adoption of endpoint-based AI agents grew **509%** in 2025.



ELEMENT TWO

Data Lineage

The factual record of how information moves: who created it, who touched it, how it was transformed, and where it went. Risk does not live in storage. It lives in movement, and lineage is what reveals the full chain of events.

Two organizations in the same industry, using the same tools, can have **entirely different** data movement patterns. Generic policy misses that; observed lineage reflects it.



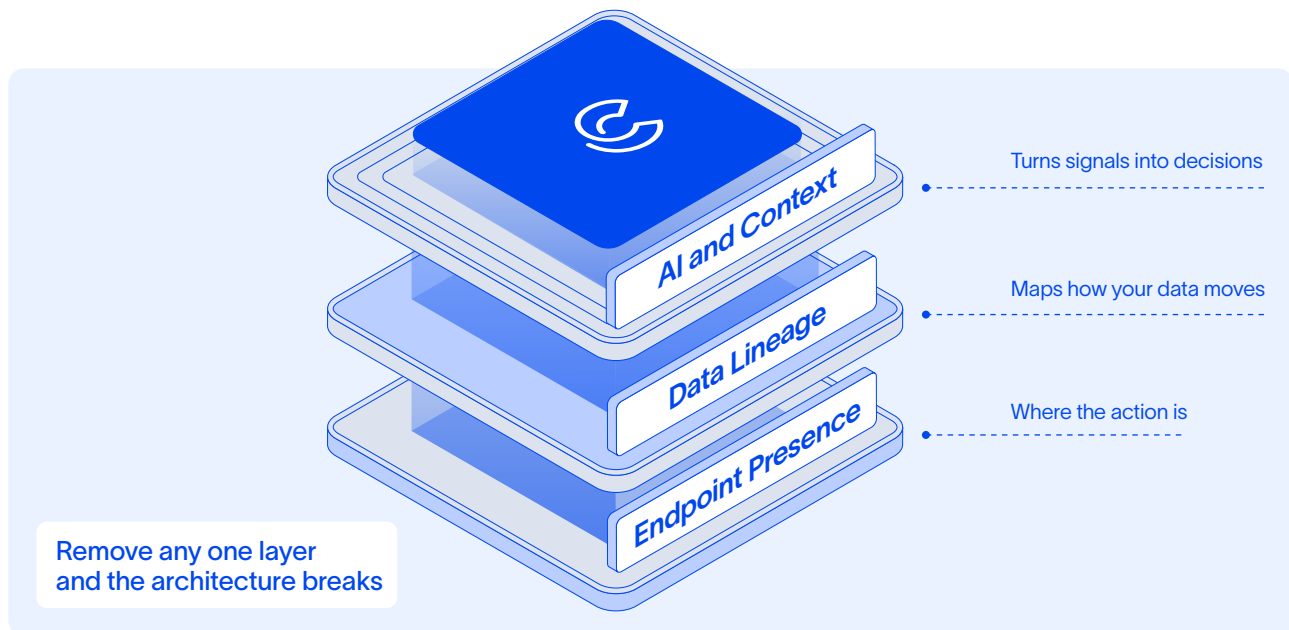
ELEMENT THREE

Contextual AI

Raw telemetry is noise. AI turns presence and lineage into decisions, distinguishing an analyst doing something unusual from an analyst doing something risky, and hardening policy as the environment changes.

AI without presence and lineage gives you a model with **nothing real** to reason over. Context is what separates signal from noise.

One System, Three Dependent Layers

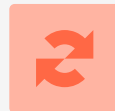


Presence without lineage is data you cannot interpret. Lineage without AI is history you cannot act on. AI without presence and lineage has **nothing real to reason over**. Each layer makes the next one possible.

What the Full Architecture Delivers



Fewer false positives, because context disambiguates signal from noise instead of treating every unusual event as a threat.



Policies that adapt as the environment changes, grounded in observed behavior rather than rules written against a snapshot.



Protection that follows data across endpoints, cloud, SaaS, and AI tools, without new rules for every tool that appears.



A platform that gets more precise over time, because each event observed adds to the lineage and improves the context AI reasons over.

Source: Cyberhaven Labs, AI Adoption Risk Report 2026. Read the full article at cyberhaven.com/blog/three-pillars-data-security

About Cyberhaven

Cyberhaven is the leader in Data Security for the Agentic Enterprise, tracing the full lifecycle of your data and adapting protection as context changes. Protect workflows, not just data. Take action when and where it matters. Proven by the world's most innovative companies. AI changed work. See how Cyberhaven protects it at cyberhaven.com.