TRUSTLOGIX

Why TrustLogix Replaces IBM Guardium DAM

IBM Guardium was built for static, on-prem environments. As your databases move, the infrastructure required to run Guardium grows with them. TrustLogix is built for where your data lives now: a single platform covering on-prem, hybrid, and cloud environments, agentless and cloud-native, with the access enforcement and security context Guardium can't provide on its own.

The problem with IBM Guardium at scale

IBM Guardium is a Data Activity Monitoring tool. It captures database traffic using agents, analyzes access patterns, and detects anomalies. That architecture made sense for static, on-prem environments. In hybrid and cloud environments, it creates a compounding problem.

Guardium's enterprise deployment requires taps, collectors, aggregators, and a Central Manager, all provisioned and managed by the customer. Every new cloud database adds more components. Every component runs on the customer's compute, storage, and network. During a cloud migration, organizations run parallel infrastructure for on-prem and cloud databases simultaneously: the footprint doubles before it shrinks.

Beyond infrastructure, Guardium's logs don't provide sufficient context for incident response. Some organizations are forced to export Guardium logs to a separate enrichment service (Microsoft ADX) before forwarding to their SIEM, adding transit costs, duplicate storage, and another vendor dependency just to get actionable alerts.

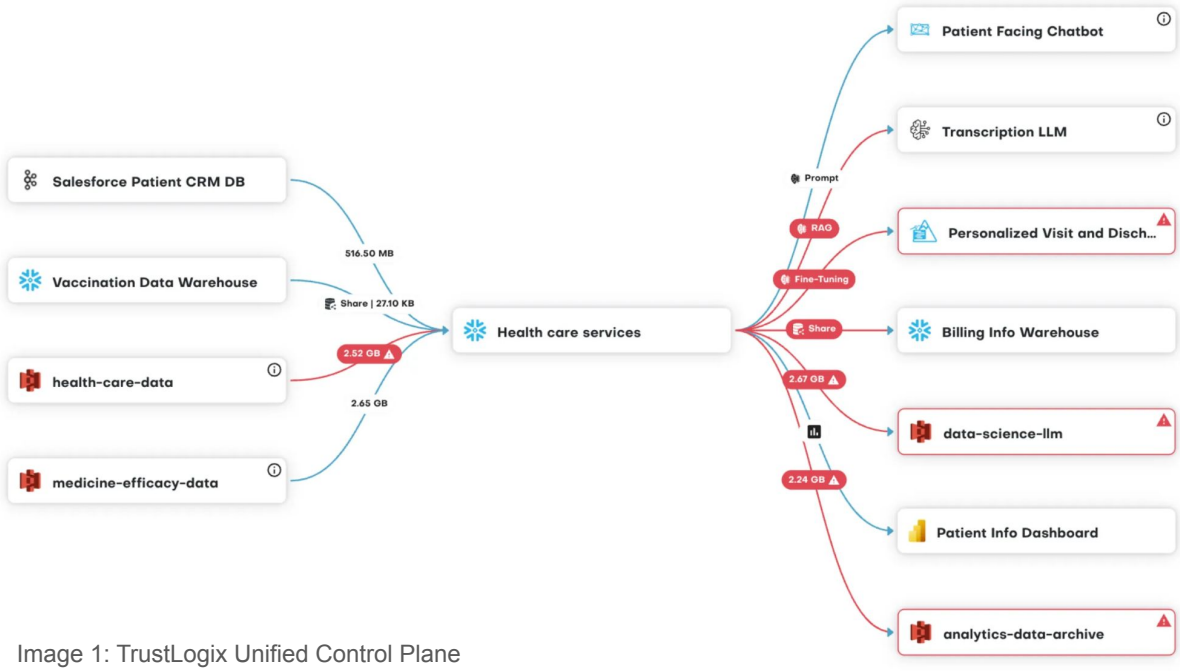

Image 1: TrustLogix Unified Control Plane

How TrustLogix wins

TrustLogix is a cloud-native, agentless data security platform. No taps. No collectors. No customer-managed infrastructure. Deployed as fully SaaS or a single data plane instance in the customer's environment. Adding a new database takes minutes: create a user, and log ingestion begins immediately.

Infrastructure and operational overhead

TrustLogix replaces 12+ customer-managed IBM components with one data plane instance or full SaaS. No provisioning, no patching, no IP white-listing as the environment grows. Identifies data access risks in under 30 minutes.

Total cost

Guardium cost has two components: the license and the cloud infrastructure bill for running all those components continuously. For mid-size enterprise deployments, the infrastructure running cost rivals or exceeds the license cost. TrustLogix eliminates the infrastructure cost entirely for SaaS deployments.

Security context, built in

TrustLogix builds rich context directly into monitoring policies: user, IP address, OS, time, and application are all visible in the risk detail without a separate enrichment layer. No ADX. No additional vendor. SIEM export is a standard output.

Native Snowflake and Databricks support

Guardium does not natively support Snowflake or Databricks. TrustLogix provides native support for Snowflake, Databricks, AWS RDS, Azure Synapse, Amazon Redshift, Google BigQuery, and on-prem databases from a single platform.

Capabilities Guardium doesn't have

Access Analyzer: Visualizes complex role hierarchies to identify and resolve excessive privileges. Guardium has no role analysis capability.

No-code policy builder: Data owners create and manage access control policies without engineering involvement. Guardium requires manual configuration by technical users for every policy.

Purpose-Based Access Control (PBAC): Ensures users access only data relevant to their role, reducing over-permission risk.

Dark data reports: Identifies unused and risky data to reduce compliance exposure.

Real-time data sprawl monitoring: Detects shadow IT risks, unauthorized data movement, and policy violations across cloud and hybrid environments.

Out-of-band architecture: TrustLogix operates with no performance impact on databases and no application changes required. Guardium's tap-based model streams live traffic, sitting in the data path and generating continuous compute cost.

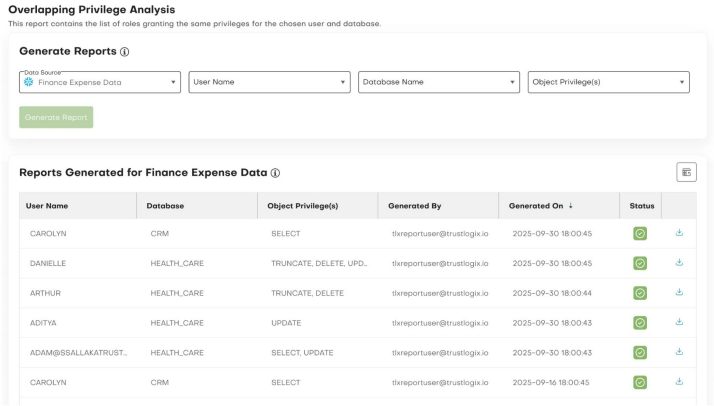

Image 2: TrustLogix Privilege Analysis

	TrustLogix	IBM Guardium
Deployment	Agentless, SaaS or single data plane	Agents, taps, collectors, aggregators, Central Manager
Customer-managed components	1 (optional)	12+
Cloud infrastructure cost	Eliminated (SaaS) or single instance	Ongoing compute, storage, network for all components
Snowflake support	Native	Requires external tooling
Databricks support	Native	Requires external tooling
Log enrichment	Built into monitoring policies	Requires separate enrichment service
No-code policy builder	Yes	No
Access Analyzer	Yes	No
Role analysis	Yes	No
Data sprawl monitoring	Yes	No
Time to first risk detection	Under 30 minutes	Days to weeks

See it for yourself

- Schedule a demo at trustlogix.ai/get-started
- hello@trustlogix.io | trustlogix.ai