



DATA DESERVES TO BE ACCESSIBLE AND SECURED

All too often, what started out as secure data in a centralized system of record becomes insecure data in an un-managed, un-governed data silo.

Why put your data at risk?

Three Signs Your Data Is Vulnerable

1 Data Integration Breaks Your Data Governance

Role and policy based access controls are essential to govern, preserve, and audit data entitlements. If these controls are not managed through the lifecycle of data integration, you introduce unnecessary complexity and risk.

2 Application Developers Burdened With Data Security

It's really hard to secure your data up and down the stack and across multiple data silos. Unfortunately, security is often not tested and maintained in a single data layer, but instead the burden is put on developers to secure data at the application layer for every new application.

3 Unknown, Unmanaged Risks From Insider Threats

Some of the biggest data breaches have occurred because an insider got the keys to the kingdom. Unfortunately, many databases are vulnerable to such attacks because they only have all-or-none data access rather than granular security controls. Data governance and audit become impossible.

If this is your reality, you need MarkLogic – the most secure and trusted NoSQL database.

“Customers expect services that adapt quickly to their needs – and they also expect their information to be kept secure and private. But too often companies have unwittingly compromised security and privacy in an attempt to increase agility.”

— Joe Pasqua, executive vice president of product strategy at MarkLogic

Organizations Trust MarkLogic Security

Large investment banks, major healthcare organizations, and classified government systems around the world run their most demanding, mission-critical systems on MarkLogic. MarkLogic® is the only NoSQL database that is Common Criteria certified. MarkLogic also runs on classified systems in US Intelligence Community, Department of Defense, and Law Enforcement organizations.

With granular access controls, separation of duties, data segmentation, advanced encryption and more, MarkLogic has the features you need to deliver the triad of Confidentiality, Integrity and Availability (CIA). Whether you're an IT executive or security manager, performing security audits and InfoSec, responsible for deploying applications or for ensuring software supply chain safety – MarkLogic provides the data protection you require along with the agility you need for dynamic business operations.



Secure and Accessible Data With MarkLogic

KPMG

KPMG built a MarkLogic-powered application to support client onboarding primarily for the purposes of compliance with regulation, tax, and reporting. The application uses intelligent automation of complex manual processes and maintains a fully traceable, auditable data workflow.

Deutsche Bank

MarkLogic replaced Oracle to be the global trade store for the bank's operational trade data. The first production deployment that integrated over 30 trading systems launched in just six months—all while maintaining secure and consistent transactions.

U.S. Intelligence Agency

MarkLogic anchors a military messaging system featuring advanced alerting and search with 100s of millions of records and 30,000+ users that depends on MarkLogic's granular access controls.

Let MarkLogic Secure Your Data

As the world's best database for integrating data from silos, MarkLogic's database platform is designed to bring all of your data together—and to ensure that data is accessible, secured and governed.

Visit www.marklogic.com