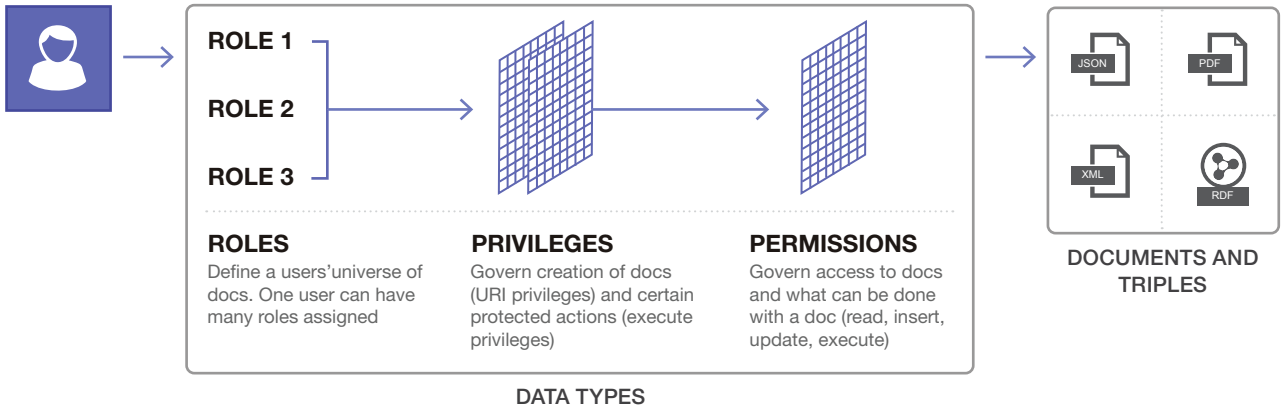
MarkLogic®

DATASHEET

Certified Security

Security is critical to maintaining data integrity and trust. MarkLogic has focused on having enterprise-grade security from the start, and has fine-grained, certified security that is required to manage data and provide a shield against today's cyber threats. It is for this reason that MarkLogic® is chosen to run the most demanding, mission-critical applications at the heart of large investment banks, major healthcare organizations, and classified government systems.

ROLE-BASED ACCESS CONTROL AT THE DOCUMENT LEVEL



Certified, Granular Security

Organizations trust MarkLogic's certified security to ensure their data is safe and to make data governance easier. The risk of not securing data is simply too high, which is why, according to Gartner, investment in IT security will increase by around 39%, to $93 billion, by 2017.

The number, sophistication, and severity of cyber-attacks continues to increase, and a single cyber incident can cost a company $5.4M on average, or $188 per record. Organizations need a database they can trust, and MarkLogic has a proven track record with over a decade of experience running mission-critical applications. MarkLogic is unique, carrying top security certifications that only traditional relational databases have, while also having the flexibility and agility of a NoSQL database.

Key Aspects of MarkLogic's Security

Certified for Mission-Critical Systems

MarkLogic is one of only six vendors that offers a database that is Common Criteria certified, and MarkLogic is the only NoSQL database with the certification. MarkLogic is also installed and operational on government systems that are PL3/ICD 503 and DITSCAP certified and accredited—top level certifications for classified systems in the US Intelligence Community and Department of Defense.

Common Criteria

The National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme (NIAP CCEVS) provides an industry standard database security certification.

MarkLogic®

Role Based Access Control (RBAC)

MarkLogic uses a document model to store data, and each document is governed by specific roles and permissions. This differs from many NoSQL databases that have database-level security for granting all-or-none access. By default, MarkLogic uses a role-based access control (RBAC) security model in which each user is assigned any number of roles, and these roles are associated with any number of privileges and permissions. Privileges govern the creation of documents and execution of functions (URI and execute privileges) and permissions govern what can be done with a document (read, insert, update, execute). Security checks verify the necessary credentials before granting the requested action, and security information is stored in a specific security database in MarkLogic.

Additional Security Models

MarkLogic can also employ other security models for even more granular security, such as Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), or Label-Based Access Control (LBAC). These models further restrict access based on attributes (e.g., social security number, IP address, user's age, or time of day), external policies or policy information stored in document metadata, or simple labels representing "high" or "low" levels of trust.

Authentication and Auditing

To create secure HTTPS connections between browsers and app servers, MarkLogic uses a standard handshake procedure using SSL certificates. To further increase security, MarkLogic supports mutual authentication, so that both the client and the server are authenticated. MarkLogic also supports external authentication using either Lightweight Directory Access Protocol (LDAP) or Kerberos. External Authentication can be setup at system initialization time and can combine Kerberos tickets with LDAP authorization. And, authentication changes are audit events, enabling robust security controls for access to the system. MarkLogic's auditing capability makes it possible to capture security-relevant events to monitor suspicious database activity or to satisfy applicable auditing requirements. Users can audit document access and updates, configuration changes, administrative actions, code execution, and changes to access control.

Governance, Risk, and Compliance

MarkLogic has transactional consistency, high availability, and certified security—all of which play an important role in tracking, controlling, and managing your data environment. And, MarkLogic makes it easy to report to auditors on changes to the environment when needed, and has extensive and detailed logs with non-repudiation. In addtion, MarkLogic has other advanced features such as bitemporal, which makes it possible to query data across two timelines so that you can answer, "what did you know?" and "when did you know it?" Changes to important data can be tracked at a granular level and data queried from the perspective of a particular time.

About MarkLogic

MarkLogic is the world's best database for integrating data from silos, providing an operational and transactional Enterprise NoSQL database platform that integrates data better, faster, with less cost. Visit www.marklogic.com for more information.

MARKLOGIC CORPORATION
999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885 | www.marklogic.com | sales@marklogic.com