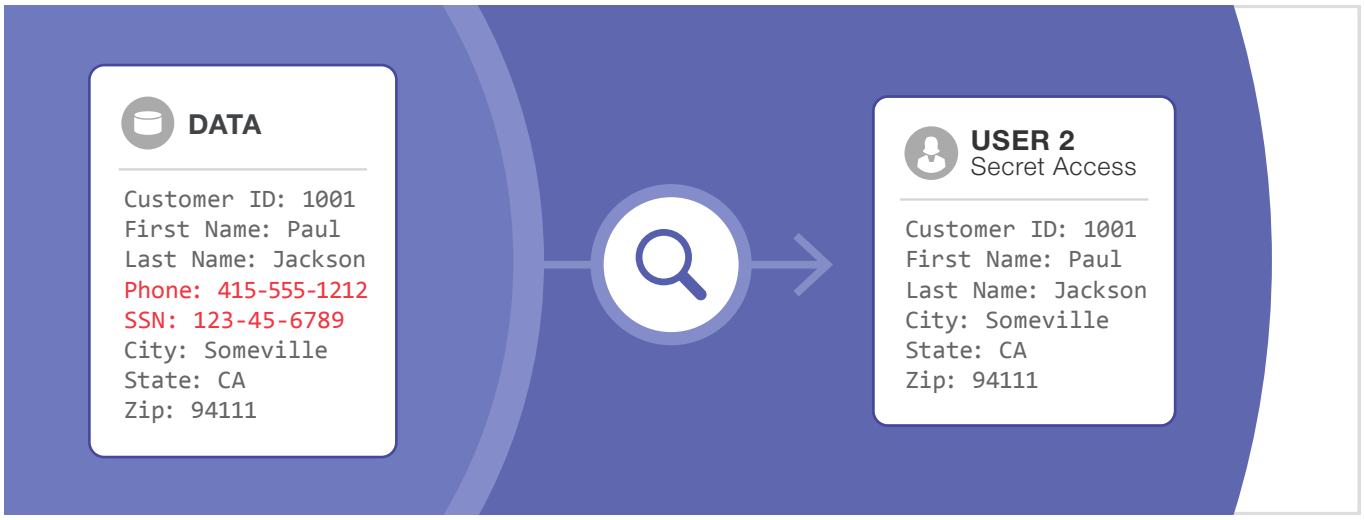
MarkLogic®

DATASHEET

Element Level Security & Redaction

Data security is critical to maintaining data integrity and trust as you seek to share data within and outside your organization. Many databases have all-or-none data access, which is not sufficient to shield against today's cybersecurity threats. MarkLogic® has focused on providing optimal data security from the start, and has granular, certified security that is required for mission-critical use cases. Element Level Security secures your data at the sub-document level when different people search and query the data stored in MarkLogic. Redaction removes or obscures sensitive parts of your data when exporting data out of MarkLogic. As a whole, these features ensure confidentiality, make compliance easier, and improve data governance.

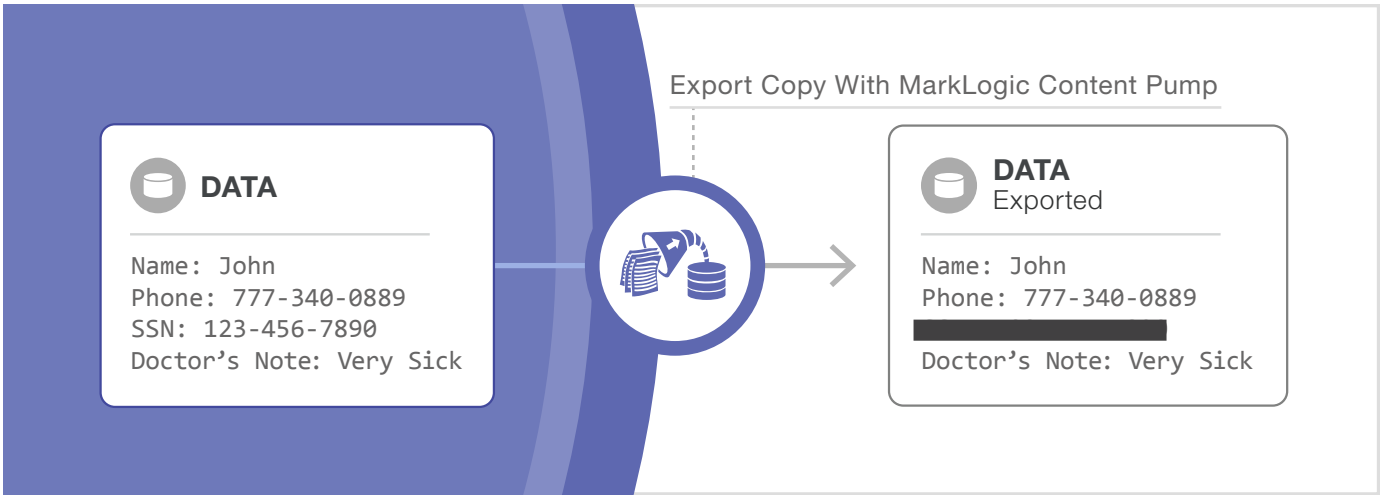


Element Level Security: Granular security at the sub-document level

By default, MarkLogic provides role-based access control at the individual document level. Element Level Security goes a step further by allowing security administrators to apply additional controls to individual parts of a document at the level of *JSON properties* or *XML elements* within documents. It is similar to "cell-level" security in relational databases (except it is not restricted to cells). This means that specific information inside a document may be hidden from a particular user based on the user's role, while still providing access to other information in the document.

- **Based on User Roles** – MarkLogic uses Role Based Access Control (RBAC) at the document and sub-document level. With this level of control, you can allow an administrator to see a person's Social Security Number but not a call center operator
- **Real-Time Protection** – Protect data during real-time operations, including search, queries, and updates
- **Secure Data Regardless of Schema** – Protect sensitive information wherever it happens to appear within the structure of a document using rich, industry-standard, path expressions rather than a rigid specification
- **Secure Using Attributes and Values** – Secure data using attributes of XML elements or values of JSON properties. For example, consider the XML element `<person classification="secret">John</person>` that has the classification attribute `"secret"`. A more restrictive security rule can be applied to any elements that have that attribute
- **Leak-Proof via Advanced Indexing Method** – Content that matches protected paths are hashed and combined with hashed roles and then added to MarkLogic's indexes to ensure no confidential data is plainly stored in the indexes

MarkLogic®



Redaction: Export controls to avoid sharing sensitive data

Redaction addresses privacy concerns by making it possible to remove or mask information when importing, exporting, or copying data into and outside of MarkLogic. This prevents leakage of sensitive information to unauthorized users. For example, redaction is often required when providing data for analysis by data scientists, or when a developer needs production data but should not have access to real credit card data or personally identifiable information. Overall, redaction helps avoid privacy violations and reduces risk while not preventing secure data sharing.

- **Based on Rules and Policies** – To implement, a MarkLogic security administrator creates redaction policies that contain rules defining which sensitive information should be redacted, and then chooses which policy to apply when running an export. Administrators can combine built-in or custom rules into policies to match different target needs
- **Utilizes Built-in Functions** – Includes built-in functions for different types of redaction:
  - Concealing: Hide elements and/or their values (or properties and/or their values in the case of JSON)
  - Masking: Change the data using *random masking* (the value varies with each instance), *deterministic masking* (the same value is applied every time), or *dictionary masking* (the value is applied from a specified dictionary)
  - Patterns: Change the data using a pattern such as Social Security Number, U.S. phone number, email, IPv4, or Regex
  - Custom: Use server-side JavaScript or XQuery functions to apply unique rules (e.g., redact the name if the person is less than 18 years old)
- **Fully Auditable** – All rules and actions taken by users are logged, ensuring all export activity can be audited later on
- **Performs In Batch at Scale** – Redaction is designed to be used when running large bulk exports. And, by utilizing the MarkLogic Content Pump (mlcp), it is faster and more secure than solutions implemented at the application layer

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