Informatica

Solution Brief

Informatica Advanced Masking Solution

Key Benefits

- Ensure the protection of critical information for privacy compliance and security
- Cost-effectively protect business applications and production databases from data breaches without impact
- Improve development, testing, and training quality
- Simplify test data management
- Support big data, cloud, and outsourcing initiatives while protecting sensitive information

Data growth and proliferation challenge organizations to protect themselves from unauthorized use and access. Organizations use data in more locations and for more purposes than ever before. Coupled with the demands of global privacy regulations, organizations must deploy data protection that travels with the data, regardless of how and where it is used. They need data privacy and protection by design, providing a consistent approach to data privacy and protection across the enterprise. Traditional security (e.g., NGFW, VPNs, SEIMs, bulk encryption) provide a first line of defense for virtually all organizations. But, the continued growth of data loss has clearly demonstrated that more is needed, and privacy regulations demand granular control of personal data.

To reduce the risk of data loss that could trigger policy violations or noncompliance of privacy regulations, organizations should protect personal data through anonymization, pseudonymization, and dynamic encryption. Regardless of the environment or data type, data must be protected so that personal and private data of customers and employees is only used in accordance with an organization's security and privacy policies. With data-centric controls, organizations can demonstrate compliance readiness and best practices for safeguarding the use and access of sensitive data.

Protection of Operational Environments

Informatica Dynamic Data Masking (DDM)

Informatica® provides capabilities to control access to sensitive and personal data in use by both mission-critical and line-of-business applications, such as customer service, billing, order management, and customer engagement. Informatica Dynamic Data Masking (DDM) masks or blocks sensitive information to users based on their role, location, and privileges. DDM provides alerts for unauthorized access attempts and includes logs for compliance and audits.

The solution is built on a patented database network in-line proxy, transparently installed between applications and databases. Acting as a database listener, the proxy processes all inbound application requests coming from application screens, canned reports, and development tools. Once they are analyzed or acted on, they are then sent to the database for prompt execution.

With support for relational, big data, and HTML applications, your IT organization can apply sophisticated, flexible data masking rules based on a user's authentication level. Through an intelligent rules engine, you can specify criteria to identify which SQL statements or SQL results should be modified. When there's a match, DDM applies one or more actions (e.g., mask, scramble, hide, rewrite, block, or redirect) to prevent unauthorized users from accessing sensitive information in real time.

Protection of DevOps/Test Environments

Informatica Persistent Data Masking (PDM)

Informatica provides capabilities that reduce the risk of unauthorized data access by masking test or development data sets created from production data, regardless of database, platform, or location. Informatica Persistent Data Masking (PDM) provides sophisticated but flexible masking rules that allow your IT team to apply different types of masking techniques to various data used in testing, training, and other nonproduction environments.

PDM anonymizes personal and sensitive data, such as credit card information, social security numbers, names, addresses, and phone numbers, while preserving the data's format and referential integrity. This is data that testing teams can rely on for accurate and thorough applications testing. And since the data is anonymized, your organization will stay compliant with privacy and security policies.

PDM provides scalability, robustness, and connectivity in traditional databases, Apache Hadoop, and cloud environments. It provides consistent data masking policies across the enterprise with a single audit trail. With comprehensive audit logs and reports, you can track procedures for protecting sensitive data. When privacy policies require validation, PDM simulates masking rules before actual execution. To adhere to privacy policies, PDM defines and reuses data masking rules, with support for in-place and in-streaming masking, which accelerates results for your organization.

Protection of Big Data Environments

Informatica provides a range of data protection capabilities to protect data at rest and data in use for data lakes. With Informatica PDM, organizations can either mask data or encrypt it, depending on the use case. Data masking is used to protect personal and sensitive data when the data needs to be anonymized and there is no need for re-identifying the data. Re-identification may be required for certain conditions, such as in medical research, when a patient's anonymized data indicates an unknown medical condition.

But, in some cases, data may need to be re-identified. Informatica PDM provides pseudonymization of analytic data with a NIST-standard format preserving encryption (FPE) transformation, supporting needs for reversible masking for analytics or privacy needs (e.g., GDPR compliance or for medical or legal research).

About Informatica

Digital transformation changes expectations: better service, faster delivery, with less cost. Businesses must transform to stay relevant and data holds the answers.

As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides you with the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on everything data, we offer the versatility needed to succeed.

We invite you to explore all that Informatica has to offer—and unleash the power of data to drive your next intelligent disruption.

Finally, Informatica DDM can be used to protect big data environments that support operational processes, such as those provided by CRM or ERP applications. Personal and sensitive data is masked based on the role and location of a user to support privacy and use policies.

Key Features

Precision for Data Privacy Laws
Combinations of personal, health, or credit information can be anonymized to comply with complex cross-border privacy laws and regulations.

Powerful Masking and Encryption capabilities
A range of masking and encryption functions are repeatable across systems to ensure that business processes are reliable and precise. Format preservation during encryption ensures that the application data model can stay the same.

Performance
Dynamic Data Masking's high-speed engine ensures no impact on user throughput. Persistent data masking can scale to mask terabytes of data for large testing, outsourcing, or analytic projects.

Role-based Masking
Based on role and location, Dynamic Data Masking accommodates data security and privacy policies that vary based on users' locations (e.g., accessing data in the U.S. vs. Switzerland).

Data Connectivity
Informatica has developed comprehensive integrations and connectors with its long-term heritage in data integration and management.

Monitoring and Compliance Reporting
Data security and privacy professionals can validate that identified sensitive data has been masked to meet security and privacy policies.

Learn more

For more information about the Informatica Advanced Masking Solution, please visit https://www.informatica.com/products/data-security/data-masking.html.

Informatica

Worldwide Headquarters 2100 Seaport Blvd., Redwood City, CA 94063, USA Phone: 650.385.5000, Toll-free in the US: 1.800.653.3871

IN17_1218_03580