Best Practices for Dynamic Data Masking

Securing Production Applications and Databases in Real-Time
Table of Contents

Executive Summary ......................................................... 2

The Need for Dynamic Data Masking ................................. 2

Introduction to Dynamic Data Masking ............................... 3

Dynamic Data Masking Compared To Other Security Technologies ................................................. 4

Dynamic Data Masking Best Practices .................................. 5

A Complete Dynamic Data Masking Solution ....................... 6

Informatica Dynamic Data Masking in Action ...................... 7

  Protecting Production Environments ................................. 7
  Minimizing Outsourcing Risks ........................................... 7
  Securing Generic Accounts .............................................. 7

Conclusion ................................................................. 8
Executive Summary

Sensitive data, such as financial records and personal employee or customer information, needs to be protected, both to safeguard it from unauthorized eyes and to comply with a growing number of privacy regulations around the world. At the same time, enterprise environments are becoming ever more heterogeneous and complex, requiring increasing cost and effort to monitor and protect the data they contain. Dynamic Data Masking (DDM) cost-effectively adds an extra layer of data security by customizing the level of data masking, scrambling, or blocking at the individual level. With DDM, IT organizations can give authorized users the appropriate level of data access without changing a single line of code or the database.

The Need for Dynamic Data Masking

PCI-DSS, GLBA, BASEL II, the EU Personal Data Protection Directive, HIPAA, and other privacy regulations were created in response to a growing problem: exposure and theft of sensitive and personal information. These regulations require organizations to limit data access based on the user's business function. However, applying this across the board is difficult, especially in environments that include external users and outsourced and part-time employees.

For example:

- An organization using PeopleSoft to manage human resources needs to give administrators and consultants the amount of access necessary to perform HR tasks, but limit full details to privileged users.
- A large bank needs to anonymize account information in its database environment in order to protect customer privacy without interfering with the day-to-day work of its designers, consultants, contractors, developers, and DBAs.
- A business-critical legacy application risks the security of a major insurance company's confidential client policy and financial data because it includes only the most basic user rights management features.

In most cases, restricting access to sensitive information within packaged and home-grown applications and development and DBA tools is excessively costly and time-consuming. Many database access monitoring (DAM) solutions can audit user access and help to identify data breaches after they occur, but cannot anonymize sensitive information to prevent it from being compromised in the first place. Other technologies require massive application changes, cause unacceptable performance problems, and cannot secure all the many types of personal information that need protection.

A different means of security is necessary; one that can provide stricter rules, more accurate audits, and more granular access control while still remaining transparent to users. Dynamic Data Masking — a term coined by Gartner in its report titled “Cool Vendors in Application Security, 2010” — is the solution.
Introduction to Dynamic Data Masking

Dynamic Data Masking is the process of uniquely masking, scrambling, hiding, auditing, or blocking data access at the individual user level. A DDM solution is proxy software that sits on a single server at the junction of business applications, reporting and development tools, and databases.

As application requests travel through the DDM layer, the solution screens them in real-time and masks sensitive data based on user role, responsibility, and other IT-defined rules. It can also apply row level or column level security as well as restricting the number of rows returned in response to a query. In this way, DDM ensures that business users, external users, part-time employees, business partners, IT teams, and outsourced consultants can access sensitive data in the exact amount and level of security necessary to do their jobs, but no more.

In this graphic illustrating how DDM works, three users are accessing an internal payroll system. On the left is the HR manager, who is authorized to see detailed personal information such as names, account information, and salaries in full. In the center is a part-time payroll employee, who is only authorized to see data in masked form in order to perform administrative tasks. On the right is a developer, DBA, or production support staffer, who requires information in the appropriate format for IT purposes and will receive it from the DDM solution with the values scrambled to comply with privacy protection regulations.
Dynamic Data Masking Compared To Other Security Technologies

Encryption can be deployed in a variety of infrastructure components. However, while end-layer encryption is transparent to the user, it doesn’t protect the data at the application layer. At the same time, application-layer encryption requires complete decryption before the data can be used, creating an opportunity for unauthorized access. It also requires source code or database changes, making it difficult and expensive to use with common packaged applications.

Storage encryption provides no application privacy, as it only protects data at rest. Data is decrypted to be read and presented by business applications and tools, leaving it completely exposed while in use.

Tokenization, which replaces sensitive data with fictionalized data in a database, can protect credit card numbers, but it cannot anonymize names, addresses, and other non-referential information. Tokenization also requires costly, time-consuming database and source code changes.

Database Access Management, which creates a detailed audit of when personal information has been accessed and by whom, can also provide basic SQL request blocking, but not at the level necessary for enterprise business applications that process hundreds of SQL requests per second.

By comparison, DDM uses in-line SQL proxies to work at the database protocol level, rendering it completely transparent. Calling applications see the DDM solution as a source database, while databases see it as an application. As a result, DDM works across all packaged and custom applications, reporting, and development tools with no need to change the database or access the application source code.
Dynamic Data Masking Best Practices

Following the best practices in this step-by-step process will allow an organization to install, test, and deploy a DDM implementation in just days:

1. Classify data into three categories to determine which data needs protection:
   - Highly sensitive data (credit card numbers, passport numbers, last names, addresses, account numbers, Social Security numbers, etc.)
   - Moderately sensitive data (first names, dates of birth, financial records, etc.)
   - Non-sensitive data

2. Identify applications that use private data. Any application that includes personally identifiable information (PII) is a candidate for a DDM initiative. Prioritize applications that have the largest amount of sensitive data and the greatest number of users.

3. Define acceptance scenarios. How will your DDM implementation determine what needs to be masked and for whom? In this step, you will determine which applications, reports, and batch processes need to be secured, which fields should be masked, the criteria for data masking, and the processes that need to be configured so they always receive unmasked data.

4. Map the data by running the scenarios through the DDM solution’s logging and auditing mode.

5. Develop masking rules and test them to verify they work on all relevant screens in applicable applications and tools.

6. Test application functionality. The DDM implementation is useless if it affects other application functions or breaks referential integrity. To protect performance, consider limiting the number of masks for each application.

7. Audit the process. The ability to track who accessed masked data and when is critical for compliance purposes, especially for companies that use both internal and outsourced employees.

8. Extend data masking rules from production into clone, backup, and training environments to increase data security throughout the enterprise.
A Complete Dynamic Data Masking Solution

Informatica Dynamic Data Masking is the first DDM product on the market. It is an application and database vendor agnostic solution for enterprise customers who need fast real-time data masking and database access monitoring with minimal impact on network performance. Informatica DDM can be installed and configured in as little as five minutes, integrating seamlessly with popular enterprise business applications including Siebel, PeopleSoft, SAP, Oracle Apps ERP Suite, Clarify, Cognos, and many others.

The Informatica approach masks data in real-time based on the end user’s network privileges, working seamlessly with existing ActiveDirectory, LDAP, and Identity Access Management software to ensure that each user’s individual network login triggers the appropriate data masking rules for the type of information he or she is authorized to access. This verification process scales easily to additional databases as the number of end users grows, yet happens in as little as 0.15 milliseconds — a delay so brief as to have no noticeable impact on network resources.

Informatica DDM uses multiple methods of masking, scrambling, and blocking data, either individually or in combinations as an organization’s security needs demand:
• data substitution - replaces a value with fictional data
• truncating, scrambling, hiding, or nullifying - replaces a value with NULL or *****
• randomization - replaces a value with random data
• skewing - alters numeric data by shifting it randomly
• character substring masking - creates a custom mask for specific data
• limiting rows returned - provides only a small subset of available responses
• masking based on other referential information - alters only some responses based on predefined rules (for example, masking the names of VIPs while leaving others visible)

In addition, Informatica DDM includes the ability to monitor, log, report on, and create audit trails for end user level access. This simplifies compliance with data privacy regulations and internal reporting needs while dramatically decreasing the risk of a data breach.

Informatica Dynamic Data Masking in Action

These three examples illustrate how Informatica Dynamic Data Masking protects privacy quickly and smoothly in real-time across business applications and production databases:

Protecting Production Environments

Customers of one of the world’s largest telecom companies expect a high level of service. That means the telecom’s developers, DBAs, application designers, and consultants need unlimited access to production applications and databases in order to resolve critical problems quickly. However, multiple privacy laws forbid production support staff from having access to customer addresses, credit card numbers, and other sensitive personal information. Using Informatica DDM, the telecom now completely masks or scrambles sensitive data in real-time so IT can identify and resolve problems quickly without risking customer privacy. In addition, the telecom now maintains a full audit trail for data management and compliance.

Minimizing Outsourcing Risks

A large global manufacturing company relies on thousands of outsourced and offshore employees who access production data using application screens, packaged reports, and development and DBA tools. Today, the manufacturer uses Informatica DDM to identify those employees in order to mask and scramble all sensitive data in real-time as they access it. This helps the organization retain tight control over its most valuable asset — information — while meeting legal and regulatory requirements to protect personally identifiable data.

Securing Generic Accounts

An organization realized that although having generic login accounts like “Billing” or “Apps” made it easier for developers and DBAs to access and monitor production databases and business applications, they also made business-critical systems and sensitive data far too easily accessible. However, these generic accounts were necessary to run crucial operational reports. The organization closed the security loophole by using Informatica DDM to set up audit and security enforcement rules. Now database logins from generic accounts are blocked with alert messages telling users to log in with their own dedicated accounts, while data processing jobs continue to run unhindered. The DDM solution also provides a detailed audit trail for compliance purposes.
Conclusion

In today’s hypercompetitive marketplace, data security and fast performance can not be mutually exclusive. With Dynamic Data Masking, organizations can quickly scale up to protect sensitive and private information in real-time — without tying IT up with costly, time-consuming application and database changes that can impact productivity, and, what’s more, without interfering with employees’ ability to fulfill their responsibilities.

The first true DDM solution on the market, Informatica Dynamic Data Masking, was not only recognized in Gartner’s “Cool Vendors” report in 2010, it was a 2011 SC Magazine Awards finalist for innovation in information security. Leveraging Informatica’s flexible, highly scalable data integration architecture, its technology has already been proven in some of the world’s largest companies and most complex IT environments.

Informatica Dynamic Data Masking and Informatica’s industry-leading Persistent Data Masking (for non-production environments) comprise the company’s total privacy protection solution, designed to secure data and guarantee regulatory compliance end-to-end across the IT environment, from development and testing to the most demanding production business applications. Using these Informatica products to implement best practices for data masking can help your organization ensure that sensitive data is restricted to authorized users on a need-to-know basis.
Learn More

Learn more about the Informatica Platform. Visit us at www.informatica.com or call +1 650-385-5000 (1-800-653-3871 in the U.S.).

About Informatica

Informatica Corporation (NASDAQ: INFA) is the world’s number one independent provider of data integration software. Organizations around the world rely on Informatica to gain a competitive advantage with timely, relevant and trustworthy data for their top business imperatives. Worldwide, over 4,440 enterprises depend on Informatica for data integration, data quality and big data solutions to access, integrate and trust their information assets residing on-premise and in the Cloud. For more information, call +1 650-385-5000 (1-800-653-3871 in the U.S.), or visit www.informatica.com. Connect with Informatica at http://www.facebook.com/InformaticaCorporation, http://www.linkedin.com/company/informatica and http://twitter.com/InformaticaCorp.