IMPERVA®

Imperva Camouflage Data Masking

Reduce the risk of non-compliance and sensitive data theft

Sensitive data is embedded deep within many business processes; it is the foundational element in Human Relations, sales, and strategic analysis systems. The business can not function without enabling access to this information. The problem is that this information is equally valuable to the bad guys – hackers, disgruntled or misguided insiders and competitors. Compliance regulations recognize the value of some of your sensitive data, including personally identifiable information, but your organization has vast amounts of sensitive information that is not subject to regulation. Your challenge is to protect all of the sensitive information and demonstrate compliance with the applicable regulation in a cost-effective manner that fits your business's processes and resources.

The Imperva data security portfolio is purpose-built to provide you with security and compliance capabilities that meet address a broad range of use cases across databases, files, user activity, Big Data and cloud-based systems. The Imperva Camouflage Data Masking solution will reduce your risk profile by replacing sensitive data with realistic fictional data. The fictional data maintains referential integrity and is statistically accurate enabling testing, analysis and business processes to operate normally. The primary use of this masking is for data in non-production systems, including test and development systems or data warehouses and analytical data stores. Another set of candidates for data masking is business enablers that require data to leave the country or company control, such as off-shore teams or outsourced systems. The Imperva Camouflage Data Masking solution will not only protect data from theft, it will help ensure compliance with regulations and international policies dictating data privacy and transport.

- Discover and document sensitive data and data relationships across the enterprise
- Reduce the volume of sensitive data in non-production systems
- Facilitate data transport for out sourcing or compliance with international privacy regulations
- Enable use of production data in development and testing without putting sensitive data at risk
- Track changes and generate compliance reports at each data refresh
- Prevent sensitive data loss from non-production systems

Data Masking: A baseline data security measure

Like other traditional security tools developed to address a specific challenge, data masking is evolving beyond the traditional use case in application development and testing to become a strategic element in an integrated security infrastructure. The Gartner Market Guide for Data-Centric Audit and Protection categorizes data masking as a key data protection capability that should be part of an organization's data security governance "shortlist".[1] The reason is simple: data masking prevents access to sensitive data while enabling testing, analysis, and business processes.

When evaluating data masking, you will likely investigate both dynamic and static masking. Static data masking is primarily used on non-production databases and is permanent; dynamic masking is used on production databases and is temporary. While each masking serves a purpose, static data masking is significantly easier and faster to deploy and manage long-term. Static masking has no impact on the production system performance; there is no risk of corrupting the production

[1] Gartner Report: G00276042; Market Guide for Data-Centric Audit and Protection, December 15, 2015,

data. The Imperva Camouflage Data Masking solution is a static data masking tool that permanently protects data and reduces exposure to compliance requirements.

Data Masking Best Practices

Designing a sustainable static data masking solution requires an understanding of the source data and the dependencies on that data set across the organization. This understanding will drive the masking policies and integration of masking into the existing IT and business processes. The resulting framework supports a repeatable process that minimizes resource requirements, reduces risk and improves compliance with regulatory requirements.

Discover: Retrieve and analyze sensitive data

The goal of the Discover phase is to identify data that needs to be masked in order to provide sufficient protection without compromising data utility. This stage involves documentation of requirements and education on the implications of masking necessary for the creation of configurations during the Policy stage of the Data Masking Best Practice. Automated discovery of sensitive data is a key factor in minimizing deployment times and long-term success.

Assess and Classify: Establish context for sensitive data

The Access and Classify phase are intended to establish criteria that will aid in determining how to mask the data. Including the codification of the contextual information determined during the Discover phase, the sensitivity of various data, its intended use(s), the transformation requirements and any inter-database dependencies.

Set Policy: Create data masking configurations

The goal of the Policy phase is to create data masking configurations based upon customer-specific functional masking requirements defined in prior phases. Including plans and requirements for integrating data masking configurations into the overall data refresh process for non-production environments. This phase also provides an opportunity to develop data masking schedules and establish appropriate change management processes. Data masking software that is easy-to-use, flexible and scalable is critical for accommodating varying and often complex requirements.

Deploy: Integrate data masking in the existing processes

The Deploy phase is intended to transition data masking into the refresh process for non-production environments taking the overall business process(es) into account. This phase entails executing configurations constructed during the Policy phase. Report automation and pre- and post-run scripts options support a wide range of ancillary processes and requirements.

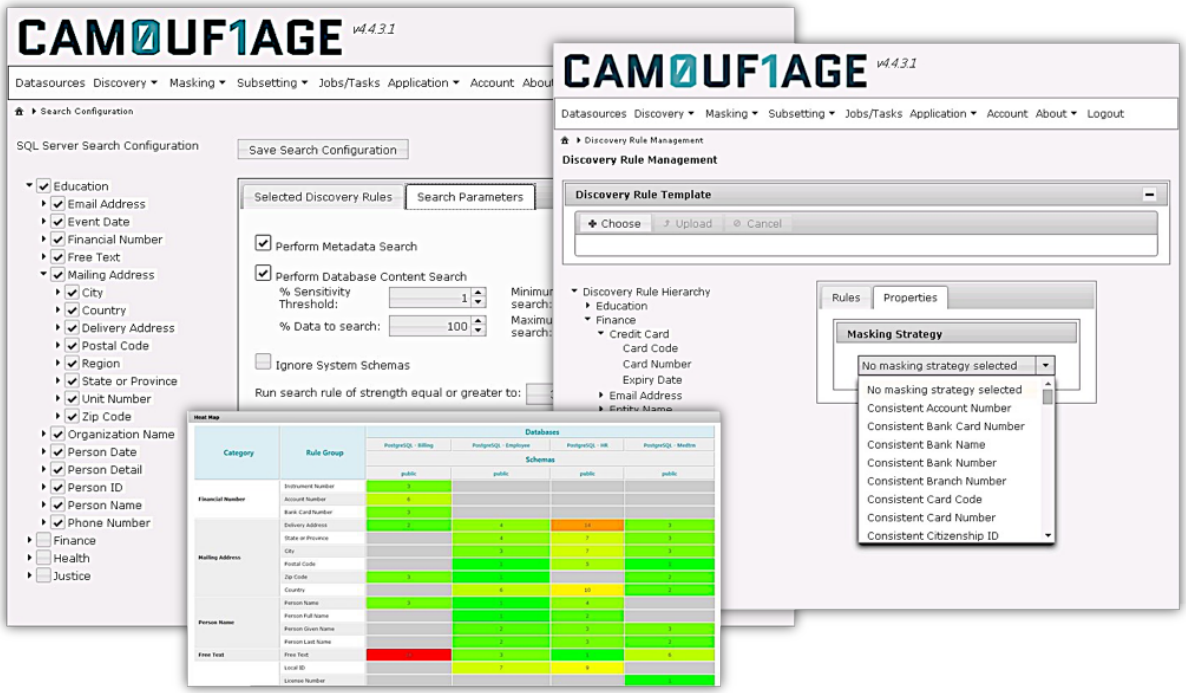
Manage and Report: Adapt to changing requirements and provide visibility

The Manage and Report phase is where the “fit and value” of the solution will become clear. This phase includes change management, job maintenance, configuration updates and compliance reports about data relationships, masking techniques, and masked database structures.

Data Masking Simplified

Some data masking vendors will have you believe it takes years and millions of dollars to implement a data masking solution. This presumption simply is not true. The Imperva Camouflage Data Masking solution implementations can be running in weeks or months from start to finish, even for the largest Fortune 500 organizations. The solution provides ease of use, scalability, and end-to-end functionality that ensure rapid adoption and long-term value.

All data masking functions including data discovery, data masking, management and reporting are performed from the Imperva Camouflage Workbench user interface, resulting in a shorter learning curve. This efficient centralized management contrasts starkly with other solutions that utilize disparate user interfaces for different functionality.



Intelligently identify, classify and analyze sensitive data and data relationships

The challenge of data discovery often lies in the complex mix of legacy, homegrown and third-party applications that run your organization. Sometimes the original developers of legacy applications have moved on, and adequate documentation is non-existent. Many times commercial software is a proprietary “black box". Regardless of whether you need to secure in-house or commercial off-the-shelf applications, Imperva Camouflage makes it easy to identify sensitive data. Organizations that understand the nature of their sensitive data and the context in which it resides can then take measures to put appropriate data privacy and security controls in place.

How data discovery works

Intelligent discovery algorithms and a high-performance architecture allow Imperva Camouflage to scan billions of data points for sensitive data and data relationships throughout an enterprise, greatly reducing the need for manual effort and enabling a more agile and efficient process. Using the predefined pattern templates and any customer specified custom rules Imperva locates and identifies a wide range of sensitive data, including:

- Credit card numbers
- Birth dates
- Bank card numbers
- Healthcare codes
- Identification numbers
- Social security numbers / National Id
- Names
- Addresses
- Phone numbers
- Financial fields (salary, hourly rate)

Imperva Camouflage uses heuristics and statistical analysis to identify sensitive data relationships. Comparing the results with historical results stored in the centralized repository to detect and audit changes to the sensitive data landscape. Data analysis tools and reports provide risk managers and the business stakeholders with the visibility to thoroughly assess sensitive data risk and derive actionable insights for improving the organization’s data security posture.

Understand your sensitive data landscape

By automating the identification of data relationships, the manual effort required is significantly reduced, enabling a more agile and efficient sensitive data analysis process. It also yields data profiles that are snapshots of database information at a particular point in time. A Functional Masking Document may be generated directly from the data profile.

The comprehensive overview report of the Discovery Run provides an easy to understand, and actionable dashboard-style report with graphs, tables, and recommendations that are ideal for sharing with business stakeholders.

Efficiently set policy, configure masking rules and data relationships

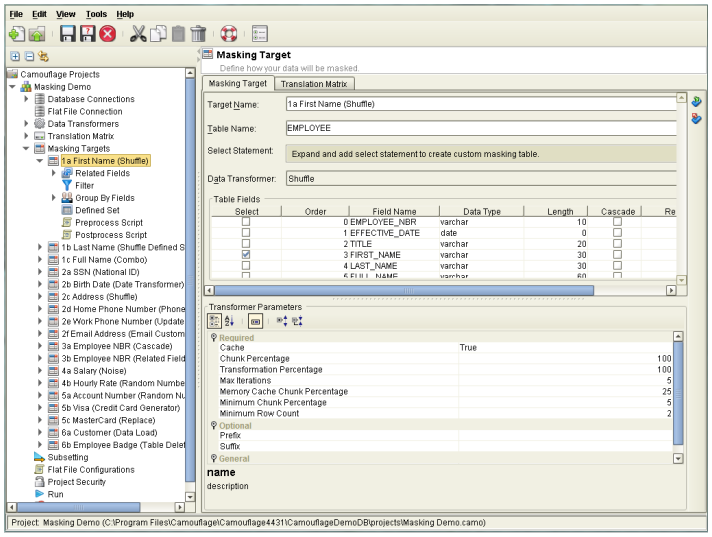
Using Imperva Camouflage to create realistic and fully functional data required for use in nonproduction environments reduces the overall amount of data subject to compliance with privacy legislation and organizational policies. It also eliminates the corresponding risk associated with data loss in the event of a breach.

The centralized Workbench console utilizes a number of predefined templates, data transformers, and click-to-configure options that streamline every aspect of a data masking project, including:

- Data discovery
- Project definition
- Database and flat file/main frame connectivity
- Translation Matrix (Inter-database dependency management)
- Masking targets
- Data transformation
- Project execution (real-time or batch)
- Pre- and post- process scripts
- Sub setting and ETL masking
- Reporting
- Project security
- System and project preferences

Click-to-Configure Masking Capabilities and Functionality

Database driven configuration - When configuring an Imperva Camouflage project, the values defined and selected during the configuration process are retrieved directly from the database or flat file.



Relational Integrity - If primary key/foreign key relationships are defined at the database level, Imperva Camouflage can automatically update all foreign keys when masking a primary key field. When key/foreign key relationships are defined at the application level, the related fields can be configured within Imperva Camouflage to correctly update associated key fields to maintain relational integrity. The Database Translation Matrix allows users to maintain consistent data relationships across different applications and across time.

Realistic Fictional Data - By masking data used in production databases, Imperva Camouflage allows the creation of fully functional and realistic data. Once masked, the data retains its realism without disclosing its original properties.

Key Data Transformers - The data transformers provide the data masking logic. Imperva includes multiple transformers, covering a multitude of transformation needs.

Robust Scripting Capability – In addition to the out-of-the-box transformers, Imperva Camouflage provides the ability to transform data by writing custom scripts. The custom scripts operate alone or in conjunction with one of the pre-defined transformers. Scripts are written using the Groovy scripting language that allows for significant flexibility in creating custom masking functions.

External Data Sources – In addition to the default project connection, other data connections can be configured for use in retrieving external update values.

Enhanced Masking – Imperva Camouflage provides support for advanced and complex masking requirements with advanced filtered data masking (sub setting) and data grouping.

Centralized Management and Reporting

The centralized management and reporting capability of Imperva Camouflage reduces the time required to create and manage data masking projects. Predefined report templates automate compliance reporting requirements and provide visibility into data use, risk, and protection.

Command Line API for Batch Processing – Imperva Camouflage is enterprise friendly, supporting command line execution of tasks for integration with automated IT and database scripts. The integration of the masking process with the process for the refreshment of data in the non-production systems ensures consistent application of compliance and security policies.

Reusable Project Files - All masking actions are stored in a Imperva Camouflage project file for future use, modification, and processing. This file is XML-based, allowing for easy migration of project files between operating systems.

Consistent Masking – Imperva Camouflage provides the ability to create mapping tables that store the original key values as they existed in the database before masking, along with the new key values. Activation of this feature is completely optional (i.e. Imperva does not require these tables in any way) and these tables can also be secured or removed by a database administrator as appropriate.

Multithreaded Database Updates - At runtime, the database refresh can be updated using a configurable number of threads to optimize performance in a given environment.

Project Security – Imperva Camouflage provides a layered security mechanism for protecting the project file as well as the six primary configuration sections within the project. Independent security enablement of each section and the project provide flexibility to match your internal governance policies.

Visibility and Reporting – Pre-defined reports include: Before and After Report, Project Configuration Report, Impacted Object Report, Historical Project Run Report. Automatic report generation is a preference setting within each masking project. In addition to the predefined reports, there are a number of interactive tools and progress monitors that improve the overall user experience and task efficiency.

Summary

Imperva Camouflage Data Masking reduces the amount of sensitive data stored within your environment while maintaining the integrity and validity of the information for use in supporting business processes and test environments. The smaller sensitive data footprint translates into hard savings when you consider the potential risk and security requirements that non-masked data in these systems would pose.

To Learn more visit Imperva.com or call +1 (866) 926-4678