IMPERVA

Imperva Camouflage Data Masking

DATASHEET

> *Data masking is a technology aimed at preventing the abuse of sensitive data by providing users fictitious yet realistic data instead of real and sensitive data while maintaining their ability to carry out business processes.*
>
> GARTNER, MARKET GUIDE FOR DATA MASKING, 6 FEBRUARY 2017

Unlock the Power of Data while Limiting Security Risk

Today, ongoing data provisioning creates significant risk within less secure organizations. A greater number of data copies in non-production environments, coupled with widespread access to that data, increase the risk of data breaches from both external attacks and insider threats. While external attacks are often sensationalized, the real threat to sensitive data is from insiders. The harsh reality is that in most cases users had authorized access to the data they stole.

On the other hand, companies are using data to support regular and on-going activities, such as application development, research and analysis, testing, and outsourcing. With the growth of data copies and of access to sensitive data, the biggest challenge remains to be securing these non-production environments while enabling various data users to complete mission critical work.

Imperva Camouflage Data Masking

Imperva Camouflage Data Masking enables organizations to safely use data for critical business processes without exposing sensitive information. It mitigates the risk of data breach and non-compliance by de-identifying sensitive data in non-production environments. Camouflage Data Masking replaces sensitive data with fictional but realistic values that maintain referential integrity, enabling data driven business processes to operate normally.

Camouflage Data Masking Benefits

- Use production data safely and freely in non-production environments, such as testing/QA, application development, training, and outsourcing.
- Gain visibility into where and what sensitive data is
- Enable data-driven business processes without exposing sensitive data
- Deploy an enterprise scalable data masking process
- Comply with data privacy and protection regulations such as PCI, HIPAA, GDPR

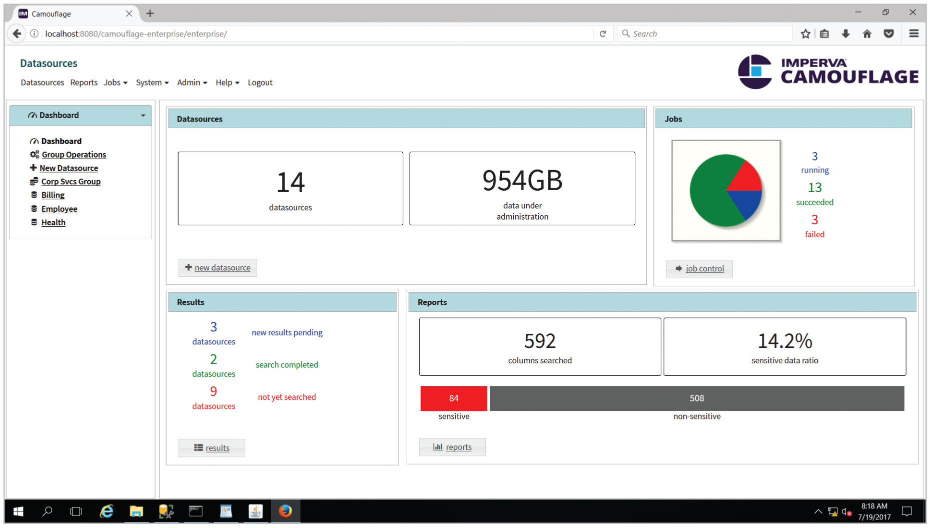
Know Where Your Sensitive Data Lives

Camouflage Data Masking identifies and classifies sensitive data, so you know what sensitive information resides in your enterprise databases. The challenge of data classification often lies in the complex mix of legacy, homegrown, and third-party applications that run in your business. Camouflage Data Masking makes it easy to uncover sensitive data. The out-of-box predefined pattern templates accelerate your masking progress by quickly locating and identifying a wide range of sensitive data, including but not limited to:

- 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)

On the other hand, automated discovery of sensitive data shortens deployment times, enabling you to complete your masking project in days, not weeks or months.

Understanding the nature of your sensitive data and the context in which it resides enables you to put appropriate data privacy and security controls in place. In addition, Camouflage Data Masking analyzes sensitive data relationships by using heuristics and statistical analysis. By automating the identification of data relationships, Camouflage Data Masking significantly reduces the manual effort and enables a more efficient sensitive data analysis process, allowing you to detect and audit changes to the sensitive data landscape over time.



> *Security and risk management leaders should ensure that data masking is part of their organizations' security and compliance technology portfolio and look for new opportunities to reduce data exposure.*
>
> GARTNER, HOW DATA MASKING IS EVOLVING TO PROTECT DATA FROM INSIDERS AND OUTSIDERS, 28 NOVEMBER 2016

Enable Data-Driven Business without Exposing Sensitive Data

Camouflage Data Masking enables test, application development, training, and business processes while preventing access to sensitive information. It removes sensitive data in non-production environments by replacing it with fictional but realistic values that maintain statistical and operational accuracy. For example, the original data contains a record of Adam Smith who is 60 years old, and his SSN is 123-44-5555. After the data is masked, it might become Tom White, 56 years old, with a SSN of 747-88-9999 (see Figure 1).

ORIGINAL DATA			
NAME	SSN	AGE	GENDER
Adam Smith	123-44-5555	60	Male
Jenny Park	987-65-4321	28	Female

MASKED DATA			
NAME	SSN	AGE	GENDER
Tom White	747-88-9999	56	Male
Amy Kim	747-88-9998	24	Female

Figure 1. Data Masking Example

By masking data used in non-production databases, Camouflage Data Masking reduces the volume of sensitive data and creates fully functional and realistic data. The masked data retains its realism without disclosing its original properties, meaning even if unwanted users do gain access, they won't be getting any confidential information. Additionally, Camouflage Data Masking can easily be integrated across multiple database types and applications while maintaining relational integrity. It ensures consistency in how sensitive elements are masked and maintains critical data relationships within and across different databases, platforms, and over time.

Meet Regulatory Compliance

Organizations need to not only protect sensitive information, but also demonstrate compliance with applicable regulations in a cost-effective manner. Camouflage Data Masking can help ensure compliance with data privacy and protection regulations. For example, the new EU General Data Protection Regulation (GDPR) requires organizations practice data minimization, which means one can only collect

Data masking can protect many forms of sensitive data, including (but not limited to):

- Personally identifiable information (PII, subject to GDPR)
- Protected health information (PHI, subject to HIPAA)
- Payment card information (subject to PCI-DSS regulation)
- Intellectual property (subject to ITAR and EAR regulations)

and use enough data required for a specific purpose. Additionally, data collected for one purpose cannot be used for another purpose. Camouflage Data Masking helps organizations meet these obligations and enable additional use of the collected data, as it pseudonymizes personal data.

The centralized management and reporting capability of Camouflage Data Masking allow you to track any data changes and generate compliance reports over time. The predefined report templates automate compliance reporting requirements and provide visibility into data use, risk and protection.

Scale for Enterprise

Camouflage Data Masking is designed to effectively mask sensitive data regardless of the complexity of the database environment. It supports common enterprise databases and multiple platforms, across Windows, Mac, and Linux. An open architecture allows Camouflage to easily adapt to your enterprise environment. It is also easy to deploy, manage, and maintain, enabling a repeatable masking process.

Camouflage Data Masking can scan and mask large volumes of data quickly and easily. In addition to predefined transformation techniques, Camouflage Data Masking provides the flexibility to create custom masking rules that can be integrated with your existing processes and environments.

On top of that, it has no impact on the production system performance. Camouflage is a static data masking solution that permanently protects data at rest. Hence, there is no risk of corrupting the production data. Regardless of whether you need to secure in-house non-production databases or outsourced environments, Camouflage Data Masking makes it easy for you to identify, classify, and pseudonymize sensitive data, saving you time and money to protect what matters most.