imperva
a Thales company

DATASHEET

Mage Static Data Masking

Take the data risk out of development, testing and analysis

Copying data increases vulnerability

As organizations look to leverage the value of the data they hold, copies of production data are often made for non-production environments such as development, test, research and analytics, and outsourcing. Unfortunately, the spread of sensitive production data throughout an organization increases non-compliance and data breach risks.

To mitigate these risks, organizations can reduce the attack surface by eliminating the use of real production data while still providing a realistic alternative for development and test simulations, with a static data masking solution provided jointly by Imperva and Mage.

Remove the threat without crippling the process

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

Using a variety of transformation techniques, real data that contains sensitive information is replaced with fictional yet high-quality realistic data that is functionally and statistically accurate. 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 an SSN of 747-88-9999.

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

- Personal Data covered by privacy regulations such as GDPR, CCRA, and others
- Protected health information (PHI, subject to HIPAA)
- Payment card information (subject to PCI-DSS regulation)
- Intellectual property (subject to ITAR and EAR regulations)

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

Data masking example

Simple and Fast

Mage Data Masking automatically identifies and classifies sensitive and personal data, so you know what sensitive information resides in a database you need to mask. Mage Data Masking makes it easy with a process wizard, and 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 information such as:

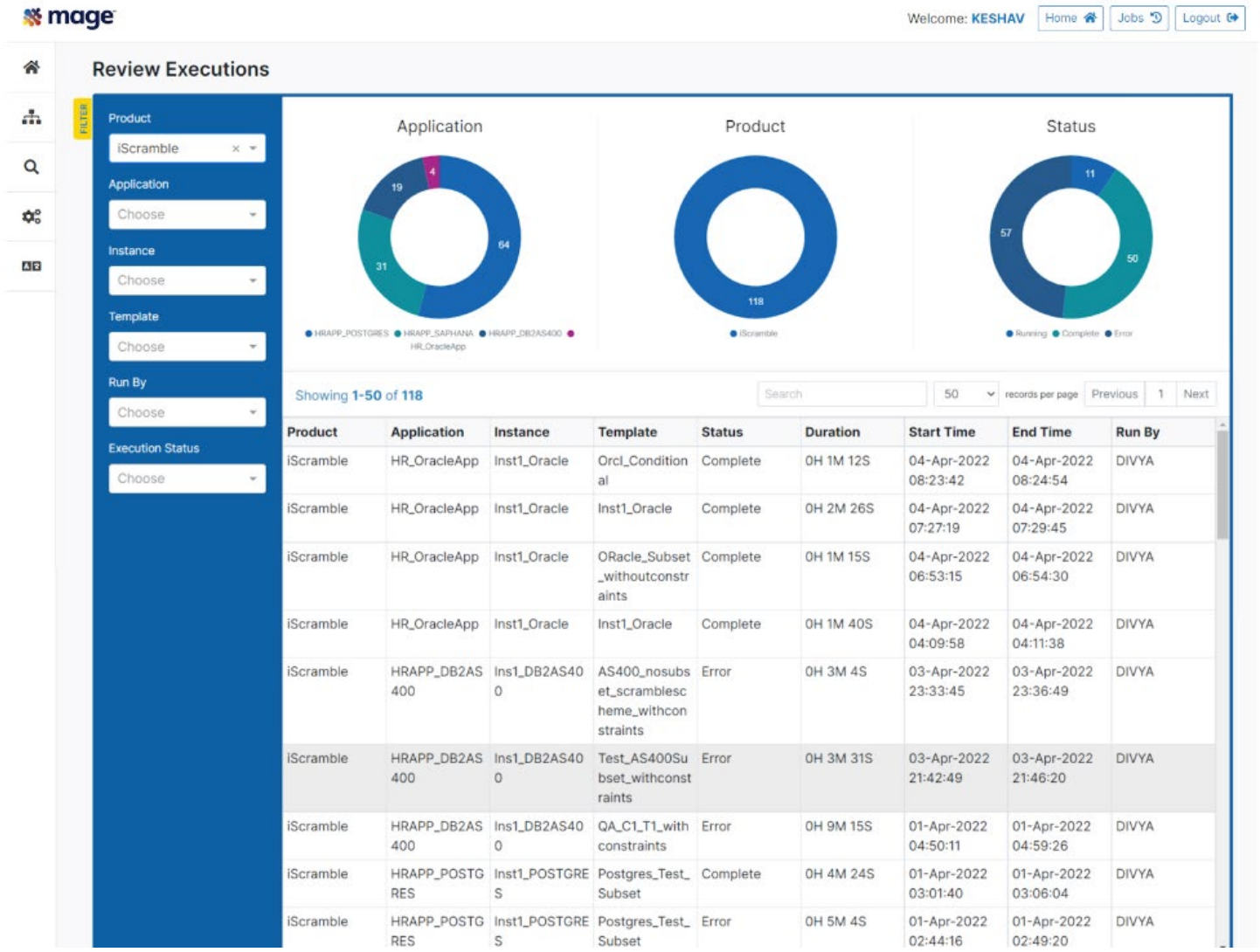
- Credit card numbers
- Birth dates
- Bank card numbers
- Healthcare codes
- Identification numbers (SSN, National ID, etc.)
- Names
- Addresses
- Phone numbers
- Financial fields (salary, hourly rate)
- Email address

Additionally, Mage 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 platforms.

Mage 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.

Meet privacy and regulatory compliance needs enterprise wide

Mage Data Masking will help ensure compliance with data privacy and protection regulations. The centralized management and reporting capability allows you to easily prove the data is anonymized and generate compliance reports. The predefined report templates automate compliance reporting requirements and provide visibility into data use, risk and protection.



Out-of-box templates simplify masking policy development

A flexible architecture allows Mage Data Masking to easily adapt to your enterprise environment. Mage Data Masking can scan and mask large volumes of data quickly and easily. In addition to predefined transformation techniques it provides the flexibility to create custom masking rules that can be integrated with your existing processes and environments. Regardless of whether you need to secure in-house non-production databases or outsourced environments, Mage Data Masking makes it easy for you to identify, classify, and pseudonymize sensitive data, saving you time and money to protect what matters most.

A comprenhensive security, compliance and privacy protection solution

Imperva Data Security Fabric (DSF) is the first data-centric solution that enables security and compliance teams to quickly and easily secure sensitive and personal data no matter where it resides with an integrated, proactive approach to visibility, control and compliance automation. Imperva DSF provides a unifying dashboard that simplifies data governance enterprise-wide.

Imperva Data Security Fabric with Mage Static Data Masking work together to provide data transformation capabilities and ensure data protection in non-production environments across multiple data platforms without the need for any additional architectural changes to systems, networks and applications. Mage is a member of the Imperva Technology Alliance Program.

To learn more visit Imperva.com and read about how Imperva Data Security Fabric can help your organization.