

MENTIS



# Dynamic Data Masking

## iMask™ Data Sheet

Minimize exposure of sensitive data in production environments



[info@mentisinc.com](mailto:info@mentisinc.com)

[www.mentisinc.com](http://www.mentisinc.com)

# Mask Seamlessly

Static Data Masking. Dynamic Data Masking. Conditional and Location-Aware.

The MENTIS family of data masking products seamlessly and consistently mask non-production, production, and pre-production environments.

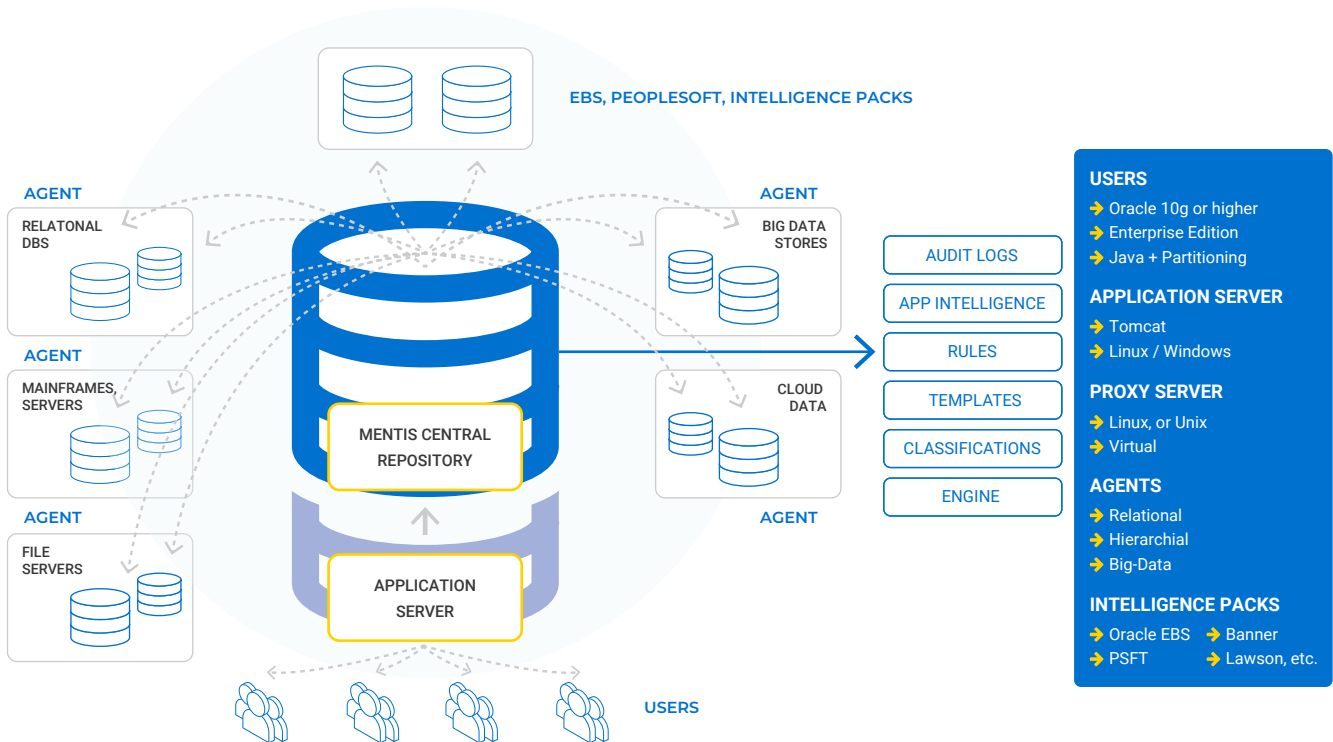
Production environments: **iMASK™** is the dynamic data masking solution that secures sensitive data in production environments.

It substitutes real data with fictitious or concealed data in unauthorized views and reports, without changing your production data.








First launched in 2008, **iMASK™** is the only enterprise-class product on the market where IT and Compliance can determine who sees either “masked” or “unmasked” production data. **iMASK™** protects sensitive data with authorization rules for connections that are made directly to the database. It also provides protection at the application level through responsibilities.

With **iMASK™**, you have all of the compliance safeguards you need, but without the performance penalty or the need to re-engineer or retrofit your applications.

## MENTIS Architecture

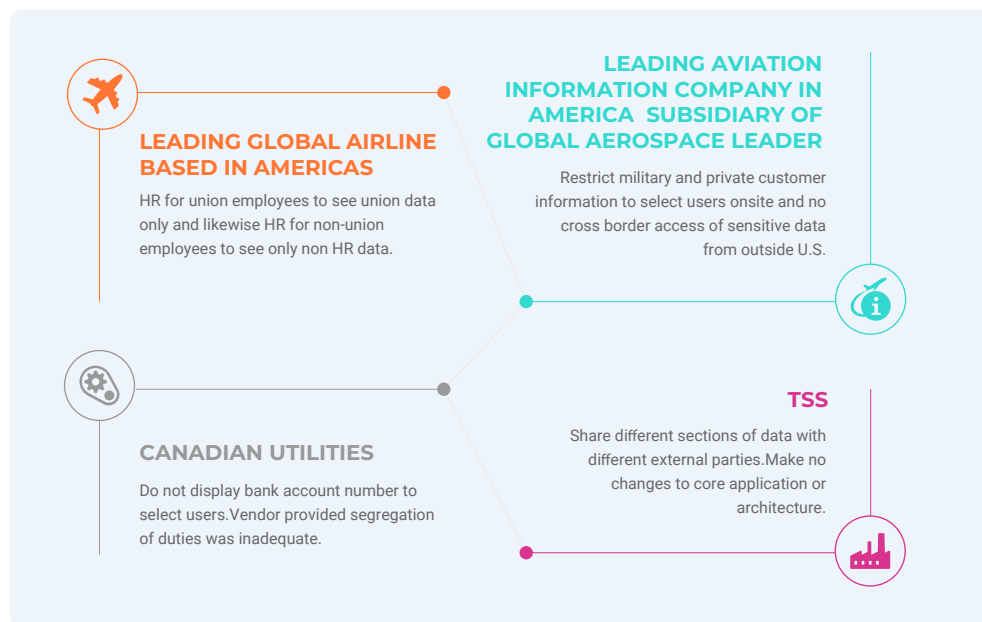


# iMask™

	PRODUCT FEATURES	CUSTOMER BENEFITS
	Take iDiscover™ templates with data classifications and sensitive data locations as input. Find and map ALL sensitive data within application and across data sources for referential integrity.	<ul style="list-style-type: none"> <li>Prevent application fails from finding ALL sensitive data locations and consistently mask the same for referential integrity</li> </ul>
	Display and/or report masked data to unauthorized users accessing sensitive data from programs (DB level masking) or accessing data in application forms, pages (application level masking) or at a putty terminal level (which DBAs use for running scripts). Protect sensitive data access in cloud applications with proxy-based servers.	<ul style="list-style-type: none"> <li>Consistent and comprehensive dynamic data masking to prevent display of sensitive data irrespective of mode of access;</li> <li>No changes in application or database coding.</li> </ul>
	Conditional data masking to specify user/role-based access to sensitive data. Location-Aware™ data masking to specify permissible data access based on geographical location of the user.	<ul style="list-style-type: none"> <li>Conditional and location-aware dynamic data masking are unique solution in the industry to meet BOTH business and compliance needs. Please see table on use cases.</li> </ul>
	Mask across structured data sources in an enterprise. Examples DBMS - Oracle, SQL Server, Sybase, DB2, My SQL, IMS; Unique no architecture using no proxies or man in the middle approach.	<ul style="list-style-type: none"> <li>Single, dynamic data masking solution that covers all well-known data sources;</li> <li>Minimal overhead in application response to display or report masked data.</li> </ul>
	File server masking for unstructured data in documents (Excel, PDF, text files etc) . Flexible approach to allow static data masking (point in time masking of files replicating files to all users) or dynamic data masking (automated masking and run time determination of access permission to original/masked files).	<ul style="list-style-type: none"> <li>Secure sensitive data in unstructured formats such as documents;</li> <li>Use same data classification and masking protocols as in structured data;</li> <li>Flexible implementation to suit requirements.</li> </ul>
	For managing point in time differences of test data, specialized testing or UAT environments, use a combination of iScramble™ and iMask™ for effectiveness.	<ul style="list-style-type: none"> <li>Unique benefit from MENTIS to treat masking requirements, specialized environments, and point-in-time differences.</li> </ul>
	Enterprise sensitive data intelligence in the form of templates that have a single repository of all metadata.	<ul style="list-style-type: none"> <li>Seamless lifecycle solution from discovery to masking, monitoring and retirement.</li> </ul>

## iMask Use Cases

iMask™ is an advanced dynamic data masking solution that was visualized years ago but is especially relevant today where BOTH compliance requirements and business operating models need to be met. The table below lists just some uses of iMask™ by reputable global enterprise, and MENTIS Customers



# About MENTIS

**iMask™** is part of a complete enterprise sensitive data security software suite from MENTIS.

**iDiscover™** finds ALL sensitive data locations and user access across all data sources. The templates from iDiscover™ are used by downstream applications for masking, monitoring and retirement across non-production, production and pre-production environments.

# Non - Production

**iDiscover™** Find ALL sensitive data across all sources and metadata based on data classifications and sophisticated search.

**iScramble™** Static data masking that supports 54 different masking methods, with full referential integrity and high performance scrambling across heterogeneous databases and unstructured data.

**iSubset™** Creates subsets of production data for masking.

# Production

**iDiscover™** Find ALL sensitive data across all sources and metadata based on data classifications and sophisticated search.

**iMask™** Dynamic data masking for databases and applications with unique role based, conditional and location-aware masking.

**Monitor™** For continuous monitoring of connections and statements of sensitive data access by authorized users. Both iMask™ and iMonitor™ have minimal latency.

**iProtect™** Offers intrusion protection at the database level as additional security.

**iRetire™** A tokenization solution for retiring sensitive data in production.

# Pre-Production

MENTIS' unique shared enterprise sensitive data intelligence and integrated architecture combines both static (**iScramble™**) and dynamic (**iMask™**) data masking.

Code scan at preproduction for any changes in sensitive data access can be embedded as security acceptance testing as part of pre-deployment checks and approval.