Knowledge Brief

Quadrant Knowledge Solutions

K2view is a Leader in SPARK Matrix™: Data Masking, Q3 2023

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix: Data Masking, Q3 2023"

K2view is a Leader in SPARK Matrix™: Data Masking, Q3 2023

Quadrant Knowledge Solutions defines data masking as a process to replace organizational data with structurally similar and authentic data. The goal is to protect sensitive data while providing a functional substitute. Data masking techniques can include substituting portions of datasets and reorganizing and scrambling the data, among others.

It is a pivotal tool for enterprises aiming to fortify their data security infrastructure. Organizations can significantly diminish vulnerabilities to unauthorized access and potential data breaches by systematically obfuscating sensitive data. This methodology aligns with stringent data protection regulations and optimizes operational workflows, expediting data-driven analytics and reporting. Data masking emerges as a more cost-efficient and streamlined solution than traditional encryption, adeptly countering external cyber threats and insider risks, if any. Furthermore, it facilitates a secure data-sharing paradigm, allowing developers to understand a better-safeguarded ecosystem without compromising the production data.

The evolution of data masking is rooted in the need to protect sensitive data while ensuring its usability, especially in non-production environments. Initially, the most security-conscious organizations developed in-house tools and methods to safeguard data against breaches. As the technology evolved, it became evident that specialized data masking tools could identify and protect sensitive data fields more effectively than many internal processes. This shift democratized data protection, allowing organizations of all sizes to safeguard sensitive information more efficiently.

Over time, data masking has developed to address various challenges, such as ensuring data remains meaningful for application logic and maintaining its appearance of authenticity. Organizations now recognize the benefits of purchasing specialized data masking tools over maintaining their internal tools. Currently, with the increase in sophisticated data masking solutions, businesses can seamlessly adapt to their ever-evolving data protection needs and environments.

The data masking market is being propelled by advances such as more sophisticated masking algorithms, automation capabilities, cloud-based delivery models, support for new unstructured data types, metadata protection, integration

with data quality tools, and the rise of masking-as-a-service providers. These technologies enable a wider range of industries to implement advanced data masking programs by making masking faster, more flexible, and applicable to diverse data types. The evolution of masking technologies allows organizations to better secure sensitive data in compliance with rising privacy regulations while maintaining data usability for secondary purposes like testing and analytics.

Advancements in data masking revolve around the seamless incorporation of data masking tools with cloud platforms, databases, and DevOps pipelines, ensuring data privacy across various stages of the data lifecycle. AI and ML innovations enable automated, intelligent, and scalable data masking capabilities. Technologies such as automated sensitive data discovery, format-preserving masking, context-aware masking, dynamic real-time masking, and continuous data monitoring drive speed, accuracy, utility, and ease of implementation. These advancements make data masking smarter and more broadly applicable across diverse industries and use cases. It is a major technological driver spurring adoption and expanding the market. Furthermore, as organizations increasingly migrate to multi-cloud and hybrid cloud environments, there's a trend toward centralized data masking solutions that can work across diverse platforms.

Vendors are harnessing AI/ML technologies to create advanced automated data masking platforms. Services such as Google Cloud's Sensitive Data Protection offer comprehensive solutions that intelligently identify and protect sensitive data across structured and unstructured sources. These platforms integrate seamlessly with data pipelines, employ sophisticated obfuscation methods such as masking and tokenization, and ensure data utility preservation. Their scalable cloud services, dynamic real-time masking capabilities, and interoperable features make them indispensable for modern enterprises aiming for robust data protection without compromising data value.

In conclusion, data masking is rapidly evolving into an intelligent, automated, and seamlessly integrated data protection technique to proactively secure sensitive information across the entire data lifecycle in alignment with compliance needs. As enterprises handle vast amounts of sensitive information, the demand for sophisticated and automated data masking solutions is rising. By leveraging AI/ML technologies, vendors are offering scalable and dynamic platforms that integrate seamlessly across diverse data environments.

The research includes detailed competition analysis and vendor evaluation with the proprietary SPARK Matrix analysis. The SPARK Matrix includes ranking and positioning of the leading Data Masking vendors with a global impact, including - This study mainly includes an analysis of the following key vendors: Accelario, Axiomatics, BMC Software, Broadcom, Comforte AG, DataSunrise, Delphix, EPI-USE Labs, IBM, Imperva, Informatica, K2View, Mage Data, Microsoft, Oracle, Privacy Analytics, SAP, SecuPi, Solix Technologies, and Thales Cloud Security.

Market Trends

The data masking market is driven by rising data volumes and stringent privacy regulations. It is rapidly adopting new technologies such as cloud services, automation, and AI to enable more scalable and fine-grained data protection. Key trends include adopting cloud-based masking services, automated sensitive data discovery and policy engines, synthetic masked data generation using machine learning (ML), support for diverse emerging data types, and multi-layered masking combining tokenization, encryption, & dynamic masking.

- Sensitive data discovery entails locating data that needs to be protected against compromising circumstances. Advanced ML classifiers can be trained to identify different data types, such as credit cards, SSNs, and medical records, across structured and unstructured sources. With more data, these models get better over time. Auto-discovery of sensitive data fields helps recommend appropriate masking techniques tailored to each data type. This reduces reliance on inefficient manual data scanning, especially for unstructured data sources.

- The use of sophisticated algorithms to generate realistic but fake masked data that retains the formats, patterns, and statistics of the original data will continue to grow. Techniques such as shuffling, substitution, and data modeling are used to build fake data that mirrors production data as closely as possible.

- The data masking market is seeing a rise in cloud-based software-as-a-service (SaaS) solutions from vendors. Cloud masking offers faster time-to-value with minimal upfront costs compared to on-premise solutions. Businesses can get started with data masking quickly without lengthy installations. Cloud masking also enables easier scaling to handle spikes in masking workloads.

- Specialized data masking tools now allow streamlined integration with mainstream databases, applications, and IT processes. They provide pre-built connectors and templates to simplify connecting masking engines with various platforms, such as SQL Server, Oracle, and SAP. Automated discovery capabilities analyze database schemas and suggest ready masking rule sets for rapid implementation. API-

based integrations allow embedding masking functions within CI/CD pipelines and DevOps workflows.

- Emerging techniques such as generative adversarial networks (GANs) are being leveraged to synthesize high-fidelity, representative masked data. GANs can learn data distributions and generate new masked data, preserving correlations and statistical properties of original data. This enables the creation of large-scale synthetic data mirrors for analytics and AI.

SPARK Matrix™ Analysis of of Data Masking Market

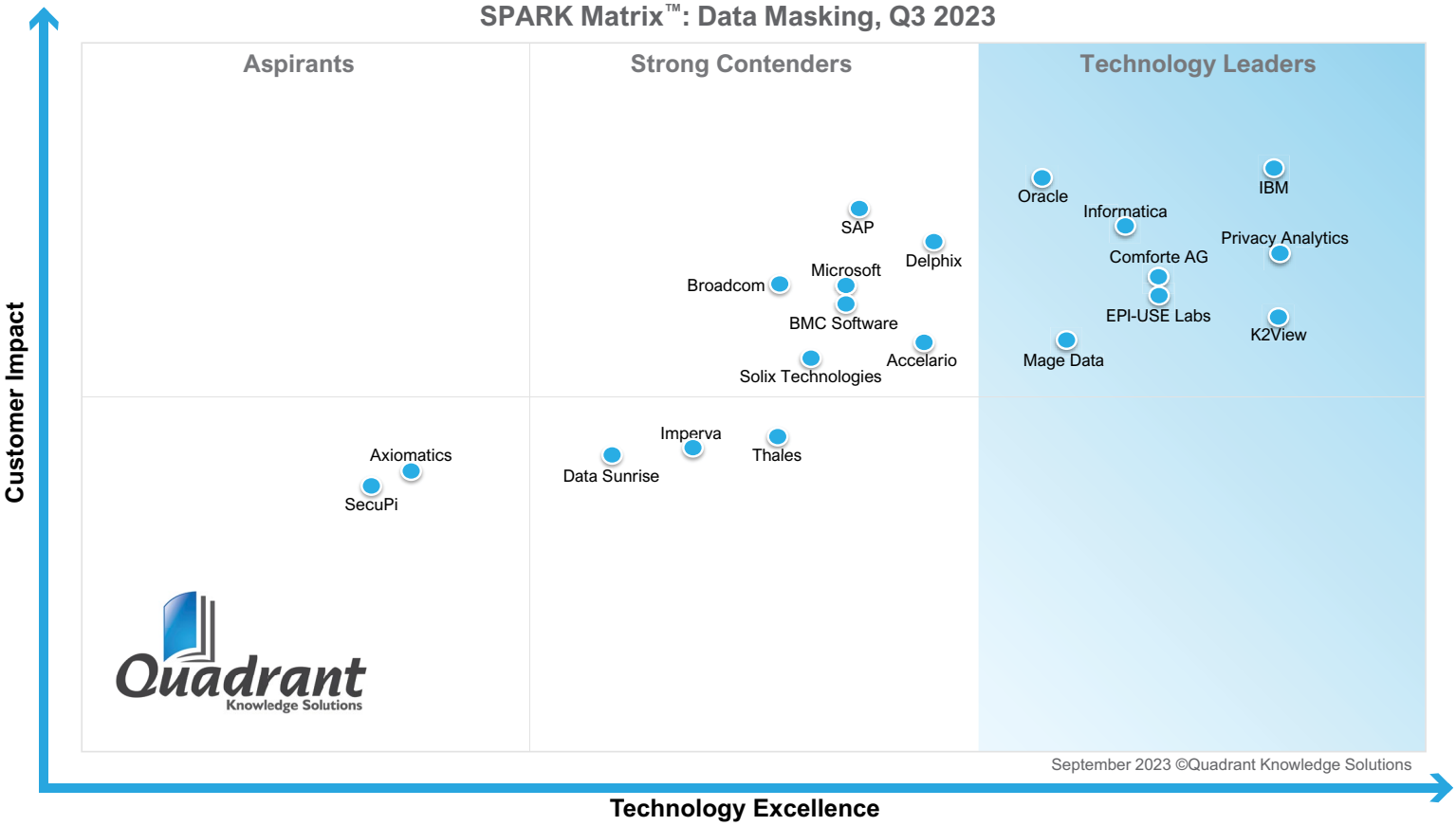
Quadrant Knowledge Solutions conducted an in-depth analysis of the major Data Masking vendors by evaluating their product portfolio, market presence, and customer value proposition. The Data Masking market research provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on primary research, including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Data Masking market.

Technology Excellence	Weightage	Customer Impact	Weightage
Governance, Security & Compliance	20%	Product Strategy & Performance	20%
Data Masking Technique	15%	Market Presence	20%
Deployment Architecture	10%	Proven Record	15%
Platform Coverage	10%	Ease of Deployment & Use	15%
Competitive Differentiation	10%	Customer Service Excellence	15%
Reporting & Auditing Functionality	10%	Unique Value Proposition	15%
Vision & Roadmap	8%		

According to the SPARK Matrix analysis of the global Data Masking market, K2view, with its comprehensive technology for Data Masking, has received strong ratings across the parameters of technology excellence and customer impact and has been positioned amongst the technology leaders in the 2023 Data Masking.

According to Saurabh Raj, Research Analyst at Quadrant Knowledge Solutions. “K2view offers a robust and comprehensive data masking solution that addresses the challenges of modern hybrid environments. Leveraging patented micro-database technology, their platform fragments and secures data at the lowest granularity while maintaining referential integrity across systems. K2view’s scalable architecture, encryption capabilities, and support for synthetic test data generation position them well to gain market share. Their product roadmap includes a fully cloud-native delivery, deeper automation, and advanced synthetic data masking.”

Figure: 2023 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Data Masking, Q3 2023



K2view

URL: https://www.K2view.com/

Founded in 2009 and headquartered in Yokneam, Israel, K2view offers unified data masking solutions for enterprises to protect data at rest, in use, and in transit for production, testing, and analytics environments. K2view's key features and functionalities include customizable and configurable masking, referential integrity, CI/CD integration, in-flight data integration, and structured, unstructured, dynamic, and static data masking.

K2view's data masking platform offers a unique approach to data protection by focusing on business entities by providing instant data ingestion and masking, supporting static and dynamic data masking. The platform also includes features such as on-the-fly and unstructured data masking, micro-database management, and integration with other data management tools. This comprehensive solution ensures efficient and secure handling of sensitive data, making it suitable for compliance, development, testing, and analytics.

Analyst Perspective

The following is the analysis of K2view's capabilities in the data masking market:

- K2view's data masking feature provides a comprehensive solution for data protection, offering built-in configurable masking that simplifies the process without coding. It includes a graphical tool for data transformation and orchestration, allowing data engineers to integrate, cleanse, and mask data quickly. The solution supports various functions for masking personally identifiable information (PII), including blurring, scrambling, synthetic substitution, hashing, encryption, and tokenization, and can be applied at any stage of data handling. K2view's patented micro-database ensures referential integrity across multiple environments, and its unique approach to data management fragments data according to business entity instances, enabling integration with CI/CD pipelines.

- The platform offers dynamic data masking, which selectively obscures, transforms, and blocks sensitive data based on user roles and privileges. It supports real-time and batch data tokenization and detokenization and the ability to create synthetic structured and unstructured substitute data types. K2view's in-flight data integration and masking feature eliminates the need for cumbersome batch processes and staging areas, ensuring protection for structured and unstructured data, such as images, PDFs, and text files. The versatile and customizable capabilities of K2view's data masking solution provide a robust tool for preserving data integrity and security across various systems and formats.

- Its solution is a part of its Data Product Platform, which organizes fragmented data from disparate systems into specific schemas such as customer, order, device, or other business entities. This approach streamlines data management and ensures security through data masking, which encrypts or obscures sensitive information. By integrating with various systems, providing real-time updates, ensuring compliance with regulations, and enhancing accessibility, K2view offers a comprehensive and flexible solution that addresses modern data management challenges.

- K2view's approach to data masking extends to structured and unstructured data, providing robust protection for various types of information. For unstructured data, such as images, PDFs, and text files, K2view offers both static and dynamic masking capabilities. This includes the ability to replace real photos with synthetic ones, use optical character recognition (OCR) to detect content for intelligent masking, and synthetically generate digital versions of items such as receipts, checks, and contracts for testing purposes. The emphasis on unstructured data masking addresses the critical need to secure sensitive information within non-traditional data formats, ensuring compliance with regulations and enhancing cybersecurity.

- The company's architecture is designed for massive-scale enterprise deployments, utilizing a multi-threaded and distributed runtime structure. By leveraging distributed storage systems such as Casandra and Azure Blob Storage, K2view stores Micro-DBs generated from

data sources, all of which are masked before access. This ensures inherent high availability and disaster recovery capabilities. K2view's platform can be configured across multiple nodes spread over various data centers and geographies to support billions of daily inbound queries for masked data, which can be executed in milliseconds.

- A key differentiator of the solution is its security priority across its products, employing multiple mechanisms to protect customer data. This includes encryption at all stages (in transit, at rest, and when exposed), unique encryption for every business entity, and a patented security module that encrypts every micro-database with its 256-bit key. The platform can operate within secure networks, including firewalls and VPNs, and integrate with customer corporate identity providers such as SAML and AD to ensure authorized access. K2view's approach to data security also includes a Time to Leave (TTL) function, enabling the deletion of masked records after a predefined period.

- Built on a distributed and scalable architecture, K2view's platform supports 24/7 operation with high resiliency and built-in data replication. It ensures high availability and survivability of both data and services. The platform is horizontally scalable, requiring simple maintenance, enabling automated deployments, and providing transparency for monitoring. It also offers built-in migration capabilities and preserves referential integrity and the formatting of masked data across systems.

- K2view's platform leverages parallel and in-memory processing for maximum performance. Its parallel, distributed processing enables data to be processed, masked, and provisioned quickly. This ensures positive customer experiences and meets or exceeds business expectations. The platform's massive-scale architecture benefits from linear scalability and split-second response times, making it suitable for deployment on commodity hardware, either on-premises or in the cloud.

- The platform offers an integration layer, supporting connectivity to multiple source/target systems through various methods, such

as JDBC, API, data streaming, data messaging, CDC, and ETL/ batch. Different integration methods can be used for structured and unstructured sources, and more than one per source. The platform also provides a no-code/low-code data masking framework with built-in functions, accelerating time to value. It enhances the sophistication of data masking through native Java customization, catering to unique customer-specific requirements.

- Some top use cases of K2view include Customer 360, which provides a complete, compliant, and real-time view of the customer to operational systems, such as CRM, a self-service portal, interactive voice response (IVR), field services, and others. It also provides use cases such as test data management, data privacy, data tokenization, data preparation & delivery into data lakes & warehouses, and data security.

- K2view has a significant geographical presence in North America, Latin America, Europe, the Middle East, and Africa, followed by Asia-Pacific. The company holds a strong customer base, including leading brands, across industry verticals, such as banking, insurance, healthcare, telecommunications, tourism, and the government & public sectors.

- K2view's key challenges include the growing competition from well-established and emerging vendors with innovative technology offerings. The company may focus on catering to mid-market to small enterprise needs and supporting more use cases. With its sophisticated technology offerings and comprehensive functional capabilities, K2view is well-positioned to expand its share in the data masking market in the near future.

- K2view's technology roadmap for data masking emphasizes a transition to a fully cloud-native platform by enabling global management by authorized users, with hybrid/on-prem options available. It also plans to introduce new types of synthetic data creation for artificial substitutions of official documents, like driver's licenses and passports, from multiple countries. Integration with a data catalog will enable the visual and operational mapping of a customer's database architecture in the near future. This will include

the capability to automatically discover, mark, and mask PII fields through a graphical user interface (GUI). Furthermore, a future no-code GUI will allow K2view administrators to set user permissions to view data either as masked or unmasked based on predefined rules, further enhancing the data management process.