KuppingerCole Report

LEADERSHIP COMPASS

by Alexei Balaganski | June 2019

Database and Big Data Security

This Leadership Compass provides an overview of the market for database and big data security solutions along with guidance and recommendations for finding the sensitive data protection and governance products that best meet your requirements. We examine the broad range of technologies involved, vendor product and service functionality, relative market shares, and innovative approaches to implementing consistent and comprehensive data protection across your enterprise.

by **Alexei Balaganski**
ab@kuppingercole.com
June 2019

Leadership Compass
Database and Big Data Security
By KuppingerCole Analysts AG

Content

List of Tables

List of Figures

Related Research

Leadership Compass: Database Security - 70970

Advisory Note: Database Governance – 70102

Leadership Brief: Six Key Actions to Prepare for GDPR – 70340

Snapshot: IBM InfoSphere Guardium – 70632

Executive View: IBM QRadar Security Intelligence Platform – 72515

Executive View: Oracle Autonomous Database – 70964

Executive View: Oracle Database Security Assessment – 70965

Executive View: comforte AG SecurDPS Enterprise – 80007

Executive View: Axiomatics Policy Management Suite – 70895

Executive View: Axiomatics Data Security – 70345

Executive View: Delphix Dynamic Data Platform – 79010

Executive View: Thales Vormetric Application Crypto Suite – 79069

Snapshot: Vormetric Data Security – 70634

1 Introduction

Databases are arguably still the most widespread technology for storing and managing business-critical digital information. Manufacturing process parameters, sensitive financial transactions or confidential customer records - all this most valuable corporate data must be protected against compromises of their integrity and confidentiality without affecting their availability for business processes. The area of database security covers various security controls for the information itself stored and processed in database systems, underlying computing and network infrastructures, as well as applications accessing the data.

However, since the last edition of KuppingerCole's Leadership Compass on Database Security two years ago, a notable change in the direction the market is evolving has become apparent: as the amount and variety of digital information an organization is managing grows, the complexity of the IT infrastructure needed to support this digital transformation grows as well.

Nowadays, most companies end up using various types of databases and other data stores for structured and unstructured information depending on their business requirements. Recently introduced data protection regulations like the European Union's GDPR or California's CCPA make no distinction between relational databases, data lakes or file stores – all data is equally sensitive regardless of the underlying technology stack.

Because of this, we have decided to expand the scope of this year's Leadership Compass to incorporate data protection and governance solutions for NoSQL databases and Big Data frameworks in addition to relational databases we focused on last time.

Among the security risks databases of any kind are potentially exposed to are the following:

- Data corruption or loss through human errors, programming mistakes or sabotage;
- Inappropriate access to sensitive data by administrators or other accounts with excessive privileges;
- Malware, phishing and other types of cyberattacks that compromise legitimate user accounts;
- Security vulnerabilities or configuration problems in the database software, which may lead to data loss or availability issues;
- Denial of service attacks leading to disruption of legitimate access to data;

Consequently, multiple technologies and solutions have been developed to address these risks, as well as provide better activity monitoring and threat detection. Covering all of them in just one product rating would be quite difficult. Furthermore, KuppingerCole has long stressed the importance of a strategic approach to information security.

Therefore, customers are encouraged to look at database and big data security products not as isolated point solutions, but as a part of an overall corporate security strategy based on a multi-layered architecture and unified by centralized management, governance and analytics.

1.1 Market Segment

Because of the broad range of technologies involved in ensuring comprehensive data protection, the scope of this market segment isn't easy to define unambiguously. In fact, only the largest vendors can afford to dedicate enough resources for developing a solution that covers all or at least several functional areas – the majority of products mentioned in this Leadership Compass tend to focus on a single aspect of database security like data encryption, access management or monitoring and audit.

The obvious consequence of this is that when selecting the best solution for your particular requirements, you should not limit your choice to overall leaders of our rating – in fact, a smaller vendor with a lean, but flexible, scalable and agile solution that can quickly address a specific business problem may, in fact, be more fitting. On the other hand, one must always consider the balance between a well-integrated suite from a single vendor and a number of best-of-breed individual tools that require additional effort to make them work together. Individual evaluation criteria used in KuppingerCole's Leadership Compasses will provide you with further guidance in this process.

To make your choice even easier, we are focusing primarily on security solutions for protecting structured data stored in relational or NoSQL databases, as well as in Big Data stores. Secondly, we are not explicitly covering various general aspects of network or physical server security, identity and access management or other areas of information security not specific for databases, although providing these features or offering integrations with other security products may influence our ratings.

Still, we are putting a strong focus on integration into existing security infrastructures to provide consolidated monitoring, analytics, governance or compliance across multiple types of information stores and applications. Most importantly, this includes integrations with SIEM/SoC solutions, existing identity, and access management systems and information security governance technologies.

Solutions offering support for multiple database types as well as extending their coverage to other types of digital information are expected to receive more favorable ratings as opposed to solutions tightly coupled only to a specific database (although we do recognize various benefits of such tight integration as well). The same applies to products supporting multiple deployment scenarios, especially in cloud-based and hybrid infrastructures.

Another crucial area to consider is the development of applications based on the Security and Privacy by Design principles, which have recently become a legal obligation under the EU's General Data Protection Regulation (GDPR) and similar regulations in other geographies. Database and big data security solutions can play an important role in supporting developers in building comprehensive security and privacy-enhancing measures directly into their applications.

Such measures may include transparent data encryption and masking, fine-grained dynamic access management, unified security policies across different environments and so on. We are taking these functions into account when calculating vendor ratings for this report as well.

Despite our effort to cover most aspects of database and big data security in this Leadership Compass, we are not covering the following products:

- Solutions that primarily focus on unstructured data protection having limited or no database-related capabilities
- Security tools that cover general aspects of information security (such as firewalls or antimalware products) but do not offer functionality specifically tailored for data protection
- Compliance or risk management solutions that focus on organizational aspects (checklists, reports, etc.)

1.2 Delivery models

Since most of the solutions covered in our rating are designed to offer comprehensive protection and governance for your data regardless of the IT environment it is currently located – in an on-premises database, in a cloud-based data lake or in a distributed transactional system – the very notion of the delivery model becomes complicated as well.

Certain components of such solutions, especially the ones dealing with monitoring, analytics, auditing, and compliance can be delivered as managed services or directly from the cloud as SaaS, but the majority of other functional areas require deployment close to the data sources, as software agents or database connectors, as network proxies or monitoring taps and so on. Especially with complex Big Data platforms, a security solution may require multiple integration points within the existing infrastructure.

In other words, when it comes to data protection, you can safely assume that a hybrid delivery model is the only viable option.

1.3 Required Capabilities

When evaluating the products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- platform support

We also considered the following key functional areas of database security solutions:

- **Vulnerability assessment** – this includes not just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations and, last but not least, the means for assessing and mitigating these risks.
- **Data discovery and classification** – although classification alone does not provide any protection, it serves as a crucial first step in defining proper security policies for different data depending on their criticality and compliance requirements.
- **Data-centric security** – this includes data encryption at rest and in transit, static and dynamic data masking and other technologies for protecting data integrity and confidentiality.

- **Monitoring and analytics** – these include monitoring of database performance characteristics, as well as complete visibility in all **access** and administrative actions for each instance, including alerting and reporting functions. On top of that, advanced real-time analytics, anomaly detection, and SIEM integration can be provided.
- **Threat prevention** – this includes various methods of protection from cyber-attacks such as denial-of-service or SQL injection, mitigation of unpatched vulnerabilities and other infrastructure-specific security measures.
- **Access Management** – this includes not just basic access controls to database instances, but more sophisticated dynamic policy-based access management, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.
- **Audit and Compliance** – these include advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, as well as tools supporting forensic analysis and compliance audits.
- **Performance and Scalability** – although not a security feature per se, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead and to support deployments in high availability configurations. For certain critical applications, passive monitoring may still be the only viable option.

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help to identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of the pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1 Overall Leadership

Figure 1: The Overall Leadership rating for the Database and Big Data Security market segment

The Overall Leadership rating is a combined view of the three leadership categories: Product Leadership, Innovation Leadership, and Market Leadership. This consolidated view provides an overall impression of our rating of the vendor's offerings in the particular market segment. Notably, some vendors that benefit from a strong market presence may slightly drop in other areas such as innovation, while others show their strength, in the Product Leadership and Innovation Leadership, while having a relatively low market share or lacking a global presence. Therefore, we strongly recommend looking at all leadership categories, the individual analysis of the vendors, and their products to get a comprehensive understanding of the players in this market.

In this year's Overall Leadership rating we observe the same situation as in the previous release: only the two biggest vendors, namely IBM and Oracle, have reached the Leaders segment, which reflects both companies' global market presence, broad ranges of database security solutions and impressive financial strengths.

However, while last time we have positioned IBM slightly in the front, considering the fact that IBM's solutions are database-agnostic, while half of Oracle's portfolio only focuses on Oracle databases, this time the situation has changed. During the last year, Oracle has substantially increased its stake in the database security market, primarily with their innovative Autonomous Database technology stack, as well as numerous improvements in their existing products. Thus, we recognize Oracle as this year's overall leader in Database and Big Data security.

It is worth mentioning that while maintaining database agnosticism, IBM Data Protection has continued to add support for new data sources and has enhanced their capabilities to facilitate secure hybrid multi-cloud. IBM has also added support for unstructured data protection making Guardium a universal platform for data discovery, classification, and protection wherever this data resides.

The rest of the vendors are populating the Challengers segment. Lacking the combination of an exceptionally strong market and product leadership, they are hanging somewhat behind the leaders, but still deliver mature solutions excelling in certain functional areas. We have a mix of companies we had recognized previously - Axiomatics, Imperva and Thales (which has completed the acquisition of Gemalto in early 2019) - and several newcomers like comforte AG, Delphix and SecuPI, each offering excellent solutions in their respective functional areas.

There are no Followers in this rating, indicating the overall maturity of the vendors representing the market in our Leadership Compass.

Unfortunately, several vendors we had in the rating last time were unable to participate this time. You can still find them mentioned in the later chapter "Vendors to Watch". For more technical details about their products, please refer to the previous edition of this Leadership Compass.

Again, we must stress that the leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company's products will be necessary.

Overall Leaders are (in alphabetical order):

- IBM
- Oracle

2.2 Product Leadership

The first of the three specific Leadership ratings is about Product Leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

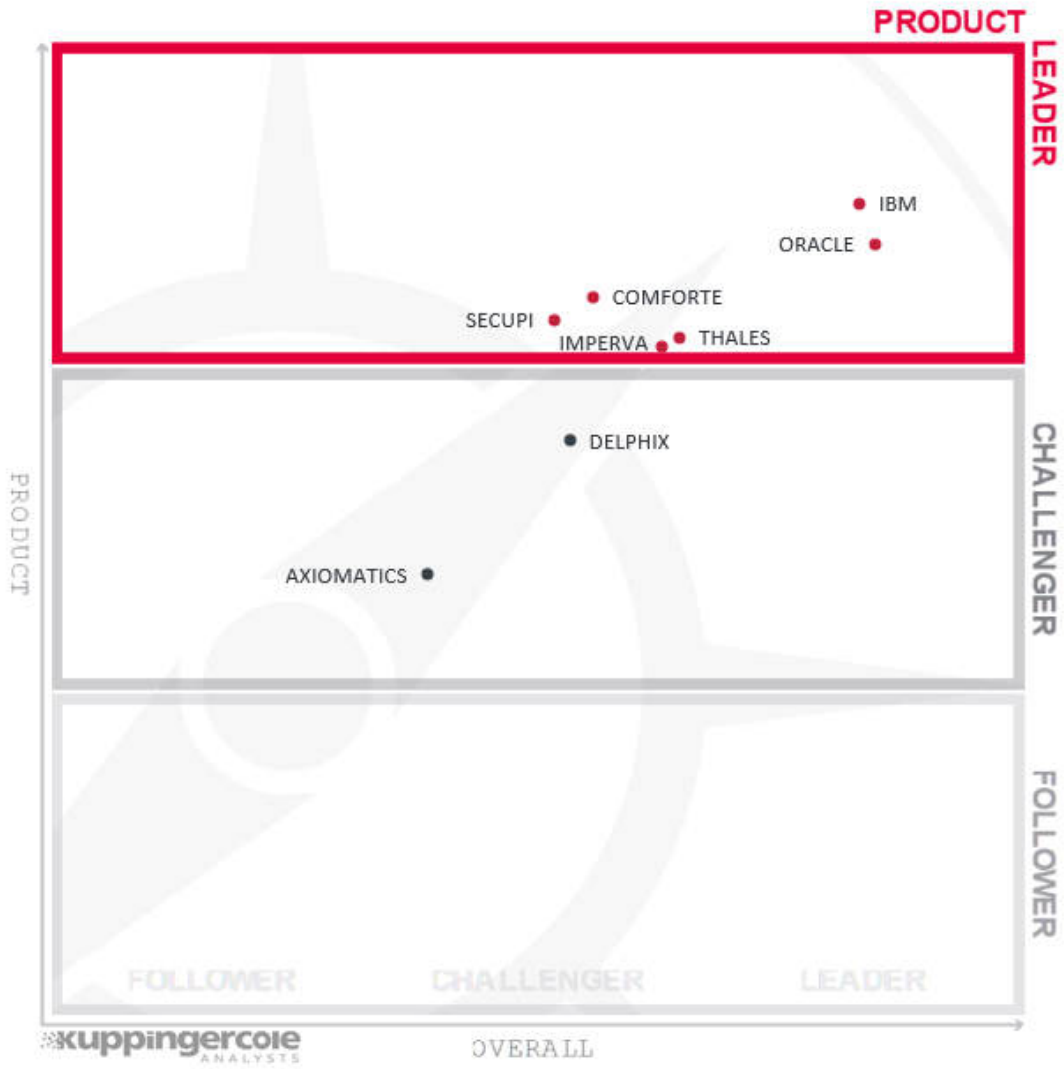


Figure 2: Product Leaders in the Database and Big Data Security segment

In the Product Leadership rating, we look specifically for functional strength of the vendors' solutions. It is worth noting that, with the broad spectrum of functionality we expect from a complete data security solution, it's not easy to achieve a Leader status for a smaller company.

Among the distant leaders are the largest players in the market, offering a wide range of products covering different aspects of database security.

IBM Security Guardium, the company's data security platform provides a full range of data discovery, classification, entitlement reporting, near real-time activity monitoring, and data security analytics across different environments, which has led us to recognize IBM as the Product Leader.

Oracle's impressive database security portfolio includes a comprehensive set of security products and managed services for all aspects of database assessment, protection, and monitoring – landing the company at the close second place.

Following them we can find two newcomers of the rating: comforte AG with their highly scalable and fault-tolerant data masking and tokenization platform that has grown from the company's roots in high performance computing and decade-long experience serving large customers in the financial industry, and SecuPI – a young but ambitious vendor focusing on data-centric protection and GDPR/CCPA compliance for databases, big data and business applications.

Finally, Thales after the recent acquisition of Gemalto and Imperva with a substantial R&D investment from Thoma Bravo have managed to improve their earlier ratings substantially, making it into the Leaders segment as well.

Other vendors with their robust, but less functionally broad solutions are populating the Challengers segment. Delphix is a leading provider of data virtualization solutions for cloud migration, application development, and business analytics scenarios, all with a comprehensive set of data desensitization capabilities. Somewhat behind it we find Axiomatics – a leader in dynamic access control with a specialized ABAC solution for databases and Big Data frameworks.

There are no followers in our product rating.

Product Leaders are (in alphabetical order):

- comforte AG
- IBM
- Imperva
- Oracle
- SecuPI
- Thales

2.3 Innovation Leadership

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging customer requirements they are facing.

Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on supporting leading-edge new features which deliver emerging customer requirements.

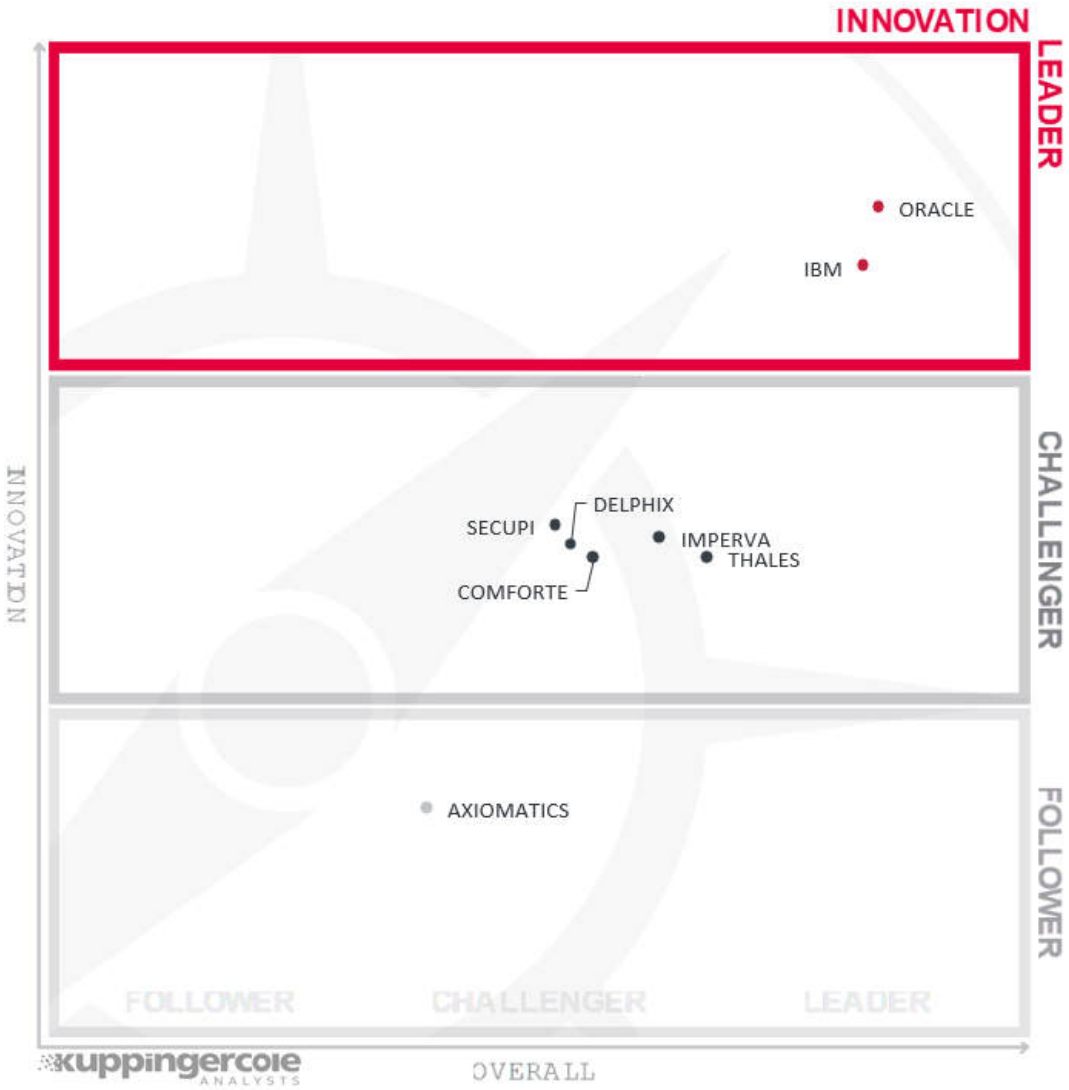


Figure 3: Innovation Leaders in the Database and Big Data Security segment

In this rating, we again observe IBM and Oracle in the Leaders segment, reflecting both companies' sheer development resources which allow them to constantly deliver new features based on innovative technologies.

IBM has continued to expand the focus of the Guardium platform – of note is the added support for unstructured data monitoring in on-prem and cloud stores, as well as the incorporation of the latest technological developments like containerized databases, artificial intelligence and consent management.

Thanks to their recent breakthrough innovations with the Autonomous Database product family, which offers substantial improvements in terms of security, compliance, performance and availability of sensitive data by completely removing human interaction from database operations, Oracle has managed to increase their rating compared to the last edition, landing them at the first place in our innovation chart.

Most other vendors can be found in the Challengers segment, reflecting their continued investments into delivering new innovative features in their solutions, which, however, simply cannot keep up with the behemoths among the leaders.

The only company in the Followers segment is Axiomatics. This does not imply any negative assessment of their solutions, however, rather emphasizing the maturity of their technology and lack of major competitors in their narrow area of the market.

Innovation Leaders are (in alphabetical order):

- IBM
- Oracle

2.4 Market Leadership

Here we look at Market Leadership qualities based on certain market criteria including but not limited to the number of customers, the partner ecosystem, the global reach, and the nature of the response to factors affecting the market outlook. Market Leadership, from our point of view, requires global reach as well as consistent sales and service support with the successful execution of marketing strategy.

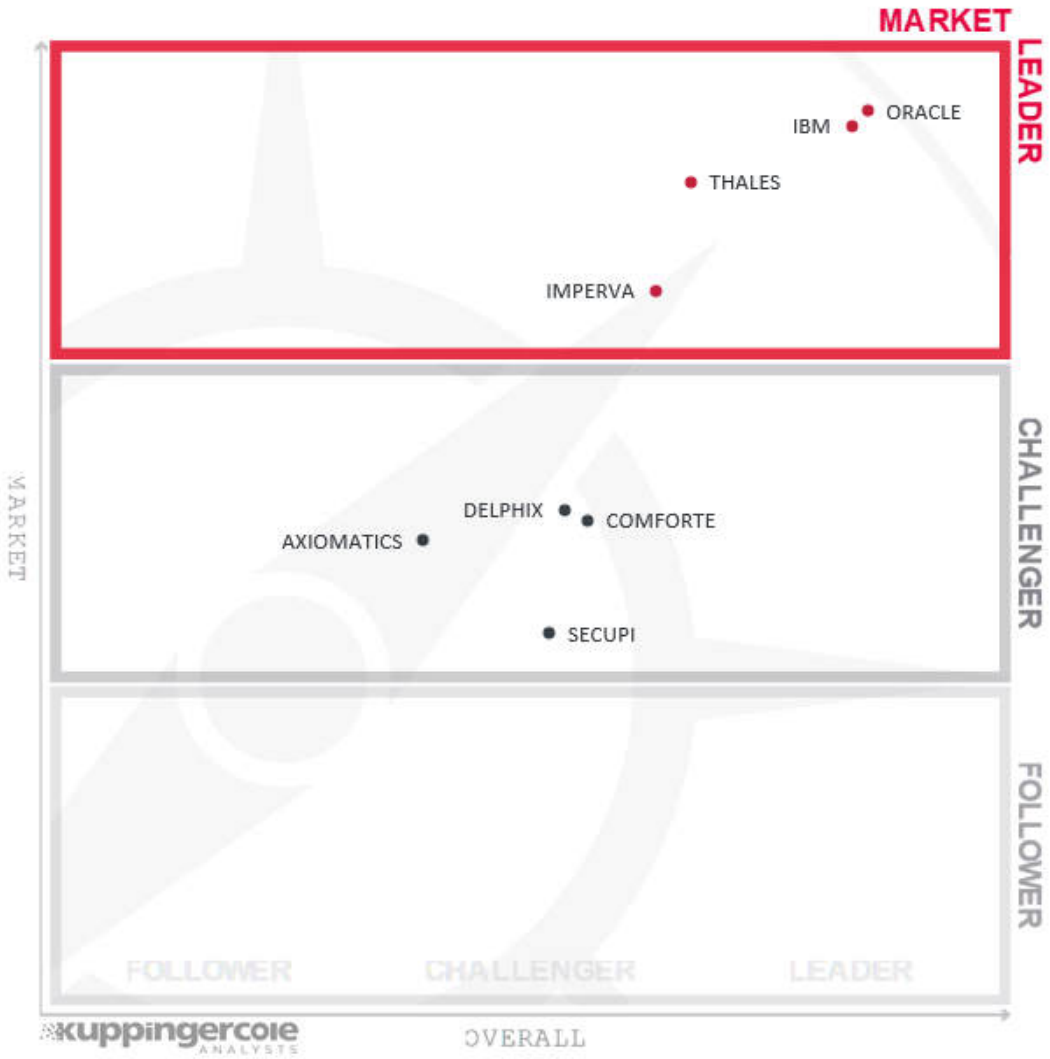


Figure 4: Market Leaders in the Database and Big Data Security segment

Unsurprisingly, among the market leaders, we can observe all large and established vendors like Oracle, IBM, Thales, and Imperva. All these companies are veteran players in the IT market with a massive global presence, large partner networks and impressive numbers of customers (including those outside of the data security market).

All smaller and younger companies are found in the Challengers segment, indicating their relative financial stability and future growth potential.

Market Leaders are (in alphabetical order):

- IBM
- Imperva
- Oracle
- Thales

3 Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we deliver additional analysis that correlates various Leadership categories and delivers an additional level of information and insight.

3.1 The Market/Product Matrix

The first of these correlated views looks at Product Leadership and Market Leadership.

Figure 5: The Market / Product Matrix

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line are often innovative but focused on specific regions.

Among the Market Champions, we can find the usual suspects – the largest well-established vendors including IBM, Oracle, Thales, and Imperva.

comforte AG and SecuPI appear in the middle right box, indicating the opposite skew, where strong product capabilities have not yet brought them to strong market presence. Given both companies' relatively recent entrance to the global database security market, we believe they have a strong potential for improving their market positions in the future.

Axiomatics and Delphix can be found in the middle segment, indicating their relatively narrow functional focus, which corresponds to limited potential for future growth.

3.2 The Product/Innovation Matrix

The second view shows how Product Leadership and Innovation Leadership are correlated. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

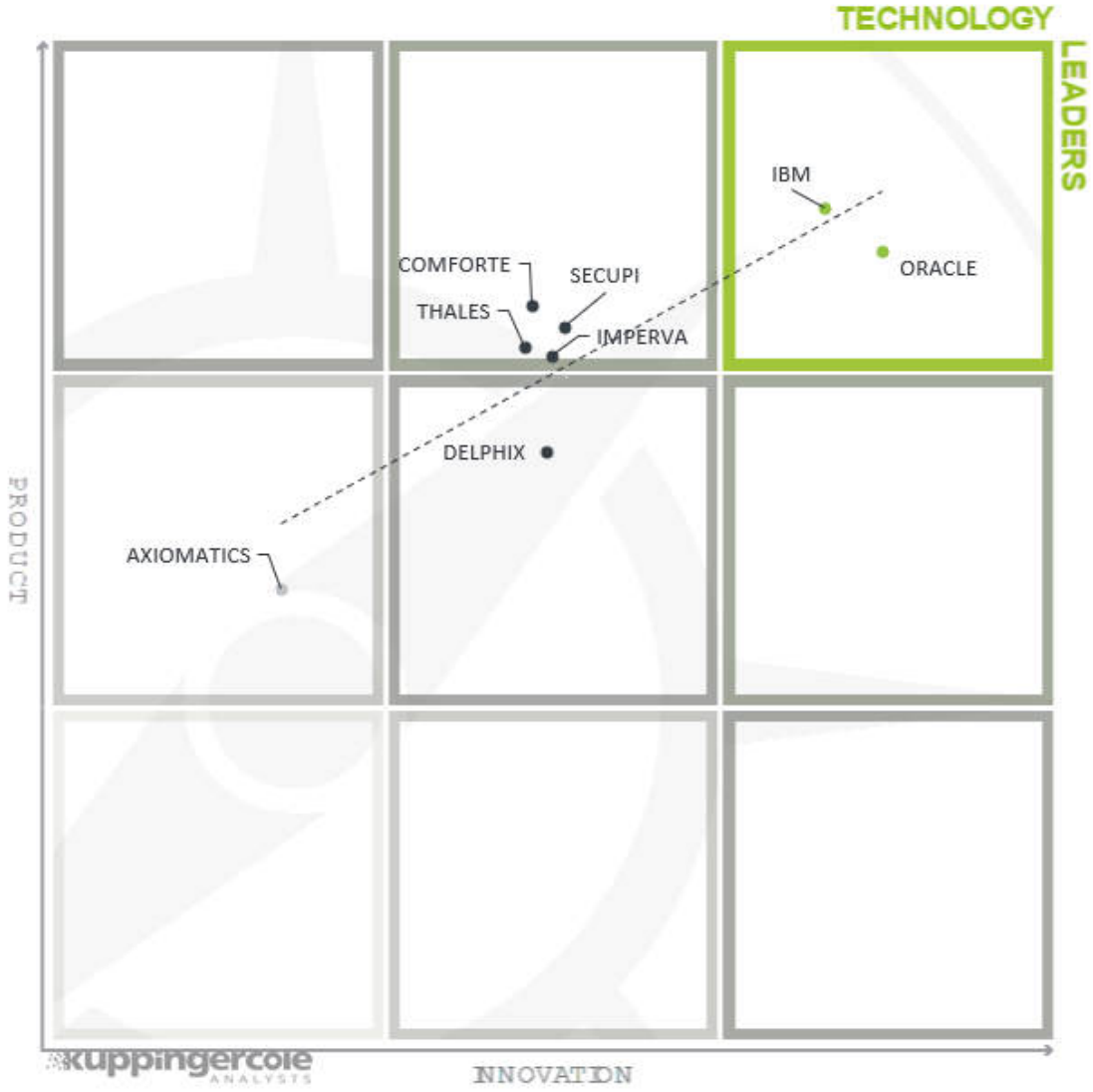


Figure 6: The Product / Innovation Matrix

Here, we see a good correlation between the product and innovation ratings, with most vendors being placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market.

Among Technology Leaders, we again find IBM and Oracle, indicating both vendors' distant leadership in both product and innovation capabilities thanks to their huge resources and decades of experience.

The top middle box contains vendors that are providing good product features but lag behind the leaders in innovation. Here we find comforte AG, SecuPI, Thales and Imperva, indicating their strong positions in the selected functional areas of data security.

Delphix has landed in the middle segment, showing that even with somewhat limited functional focus a vendor can still deliver a healthy amount of innovation.

The only company showing a noticeably lower level of innovation is Axiomatics; still, it has landed in the middle left box, indicating strong product capabilities.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk to their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors that are highly innovative have a good chance of improving their market position but often face risks of failure, especially in the case of vendors with a confused marketing strategy.

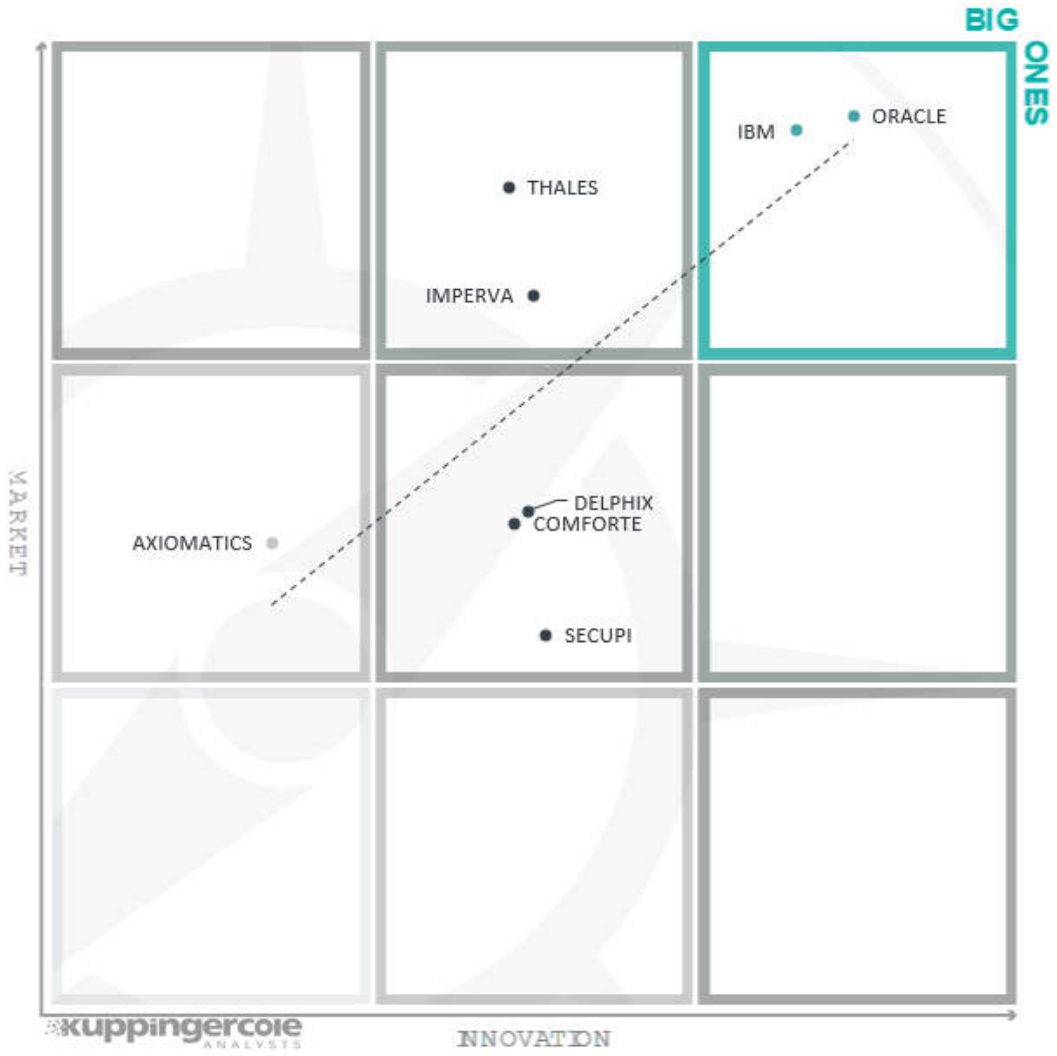


Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market compared to their relatively weak position in the Innovation Leadership rating, while vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.

Again unsurprisingly, we can find IBM and Oracle among the Big Ones – vendors that combine strong market presence with a strong pace of innovation.

Thales and Imperva in the top middle box indicate their strong market positions despite somewhat slower innovation, while comforte AG, Delphix and SecuPI occupy the opposite positions below the dotted line, indicating their strong performance in innovation, which has not yet translated into larger market shares.

Axiomatics can be found in the left middle box, indicating their position as an established player in a small, but mature and "uncrowded" market segment, which inhibits innovation somewhat.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Database and Big Data Security. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in the table below.

Vendor	Security	Functionality	Integration	Interoperability	Usability
AXIOMATICS	positive	neutral	positive	positive	neutral
COMFORTE	strong positive	positive	strong positive	strong positive	positive
DELPHIX	positive	neutral	strong positive	positive	strong positive
IBM	strong positive	strong positive	strong positive	strong positive	strong positive
IMPERVA	strong positive	strong positive	positive	positive	strong positive
ORACLE	strong positive	strong positive	strong positive	strong positive	strong positive
SECUPI	strong positive	positive	strong positive	positive	strong positive
THALES	strong positive	neutral	strong positive	strong positive	positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we also provide four additional ratings for the vendor. These go beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovation	Market Position	Financial Strength	Ecosystem
AXIOMATICS	neutral	positive	positive	neutral
COMFORTE	neutral	positive	strong positive	weak
DELPHIX	positive	strong positive	neutral	weak
IBM	strong positive	strong positive	strong positive	strong positive
IMPERVA	positive	strong positive	positive	strong positive
ORACLE	strong positive	strong positive	strong positive	strong positive
SECUPI	positive	neutral	neutral	weak
THALES	positive	strong positive	strong positive	strong positive

Table 2: Comparative overview of the ratings for vendors

In the area of innovation, we were looking for the service to provide a range of advanced features in our analysis. These advanced features include but are not limited to implementing practical applications of new innovative technologies like machine learning and behavior analytics or introducing new functionality in response to market demand. Where we could not find such features, we rate it as “Critical”.

In the area of market position, we are looking at the visibility of the vendor in the market. This is indicated by factors including the presence of the vendor in more than one continent and the number of organizations using the services. Where the service is only being used by a small number of customers located in one geographical area, we award a “Critical” rating.

In the area of financial strength, a “Weak” or “Critical” rating is given where there is a lack of information about financial strength. This doesn’t imply that the vendor is in a weak or a critical financial situation. This is not intended to be an in-depth financial analysis of the vendor, and it is also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding ecosystem applies to vendors which do not have or have a very limited ecosystem with respect to numbers of partners and their regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that the success and growth of companies in a market segment rely on strong partnerships.

5 Product evaluation

This section contains a quick rating for every product we've included in this report. For some of the products, there are additional KuppingerCole Reports available, providing more detailed information.

In the following analysis, we have provided our ratings for the products and vendors in a series of tables. These ratings represent the aspects described previously in this document. Here is an explanation of the ratings that we have used:

- **Strong Positive:** this rating indicates that, according to our analysis, the product or vendor significantly exceeds the average for the market and our expectations for that aspect.
- **Positive:** this rating indicates that, according to our analysis, the product or vendor exceeds the average for the market and our expectations for that aspect.
- **Neutral:** this rating indicates that, according to our analysis, the product or vendor is average for the market and our expectations for that aspect.
- **Weak:** this rating indicates that, according to our analysis, the product or vendor is less than the average for the market and our expectations in that aspect.
- **Critical:** this is a special rating with a meaning that is explained where it is used. For example, it may mean that there is a lack of information. Where this rating is given, it is important that a customer considering this product look for more information about the aspect.

It is important to note that these ratings are not absolute. They are relative to the market and our expectations. Therefore, a product with a strong positive rating could still be lacking in functionality that a customer may need if the market in general is weak in that area. Equally, in a strong market, a product with a weak rating may provide all the functionality a particular customer would need.

5.1 Axiomatics

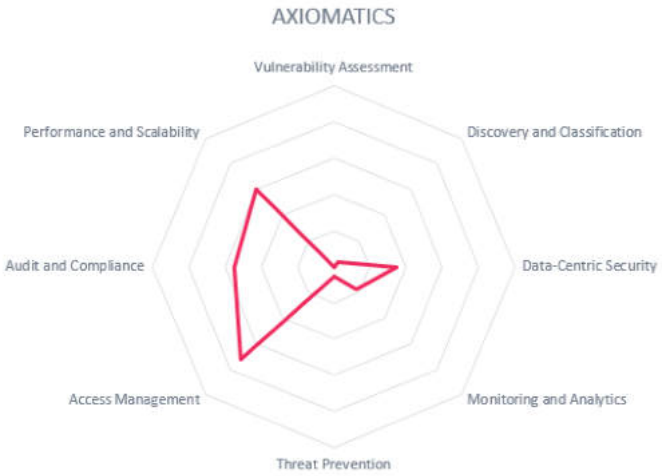
Axiomatics is a privately held company headquartered in Stockholm, Sweden. Founded in 2006, the company is currently a leading provider of dynamic policy-based authorization solutions for applications, databases, and APIs. Despite its relatively small size, Axiomatics serves an impressive number of Fortune 500 companies and government agencies, as well as actively participates in various standardization activities. Axiomatics is a major contributor to the OASIS XACML (eXtensible Access Control Markup Language) standard, and all their solutions are designed to be 100% XACML-compliant.

Strengths	Challenges
• Database-agnostic approach ensures unified policy application across different databases and big data stores • 100% compliance with the XACML standard • Shares the authorization model with other Axiomatics products for applications, APIs, etc.	• Quite narrow functional focus compared to other products in the rating • Relies on 3rd party components to enforce policies

Table 3: Axiomatics major strengths and challenges

The company's flagship data protection solution is the Dynamic Authorization Suite built around the Axiomatics Policy Server, an enterprise-wide universal Attribute-Based Access Control (ABAC) product. Included in the suite are Axiomatics Data Access Filter MD for managing access to sensitive information in relational databases along with SmartGuard for Big Data frameworks and cloud data stores.

Implemented as loosely coupled add-ons or proxies, the suite provides policy-based access control defined in standard XACML, as well as dynamic data masking, filtering and activity monitoring transparently for multiple data sources, which integrates seamlessly with other company's access management solutions for applications, APIs and microservices and other third-party products.



Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	neutral

Table 4: Axiomatics rating

The key features of the solution include dynamic context-aware authorization implemented in a vendor-neutral way, flexible access control to sensitive data based on real-time dynamic data filtering, dynamic data masking and filtering for financial, healthcare, pharmaceutical and other types of personal information, and centralized management of access policies across databases, applications, and APIs.

5.2 comforte AG

comforte AG is a privately held software company specializing in data protection and digital payments solutions based in Wiesbaden, Germany. The company's roots can be traced back to 1998 when its founders came to the market with a connectivity solution for HPE NonStop systems – a fault-tolerant self-healing server platform for critical business applications. Over the years, comforte's offering has evolved into a comprehensive solution for protecting sensitive business data with encryption and tokenization, tailored specifically for critical use cases that do not allow even minimal downtime.

Strengths	Challenges
• Unique hardened, scalable and fault-tolerant architecture for mission-critical use cases • Deployment flexibility, hybrid cloud, and as-a-Service scenarios are supported • Broad range of transparent application integration options, support for Big Data and stream processing frameworks	• Current functionality limited to tokenization and masking (other data protection technologies planned for future) • Somewhat limited market visibility outside of the financial industry

Table 5: Comforte AG major strengths and challenges

A few years ago, comforte AG has entered the data-centric security market with their SecurDPS Enterprise solution that combines the company's patented stateless tokenization algorithm, proven highly scalable and fault-tolerant architecture, flexible access control and policy management, augmented by a broad range of transparent integration options, which allow various existing applications to be quickly included into the enterprise-wide deployment without any changes in infrastructure or code.

Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 6: Comforte AG rating

The platform's decentralized and redundant architecture ensures deployment flexibility in any scenario: hybrid cloud and as-a-Service use cases are supported as well. Patented stateless tokenization algorithm supports limitless scaling across heterogeneous environments. Strong focus on regulatory compliance directly addresses PCI DSS and GDPR requirements.

5.3 Delphix

Delphix is a privately held software development company headquartered in Redwood City, California, USA. It was founded in 2008 with a vision of a dynamic platform for data operators and data consumers within an enterprise to collaborate in a fast, flexible and secure way. With offices across the USA, Europe, Latin America, and Asia, Delphix is currently serving over 300 global enterprise customers including 30% of the Fortune 100 companies.

Strengths	Challenges
• Based on a universal, high-performance and space-efficient data virtualization technology • Support for a broad range of database types and unstructured file systems • Transparent data masking and tokenization capabilities • Preconfigured for GDPR compliance	• Limited data protection capabilities, lack of encryption support • Limited monitoring and analytics functions

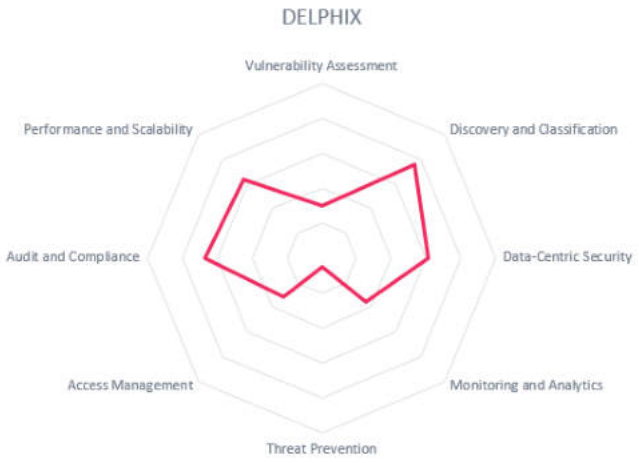
Table 7: Delphix major strengths and challenges

Delphix Dynamic Data Platform is a software-based data virtualization platform – quickly provisioning virtual copies of masked or unmasked data across different IT environments. Delivered as virtual appliances that can be deployed anywhere, the platform offers unified support for on-prem, cloud and hybrid environments.

Using compression, intelligent data block sharing and other optimizations and offering self-service capabilities and API-driven automation functions, the Delphix platform ensures that data consumers can get access to the data they need as quickly and efficiently as possible, enabling numerous usage scenarios: cloud migration, data analytics, DevOps automation of data delivery, test data management, and even disaster recovery.

Security	positive
Functionality	neutral
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 8: Delphix rating



Since the platform is designed to be fully transparent for existing applications and services, this ensures effortless hybrid cloud deployment for new and existing applications. Powerful self-service functions for data consumers enable quick provisioning, refreshing, rewinding, and sharing of data sources in minutes instead of hours, powering the emerging DataOps methodology. Integrated data anonymization features come preconfigured for GDPR compliance.

5.4 IBM

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. IBM offers a broad range of software solutions and infrastructure, hosting and consulting services in numerous market segments. With over 370 thousand employees and market presence in 160 countries, IBM ranks as one of the world's largest companies both in terms of size and profitability.

Strengths	Challenges
• Full range of security capabilities for structured and unstructured data • Support for hybrid multi-cloud environments • Advanced Big Data and Cognitive Analytics • Nearly unlimited scalability • Integrated ecosystem with IBM's and 3rd party security, identity and analytics products • Massive network of technology partners and resellers	• Setup and operations may be complicated for some customers

Table 9: IBM major strengths and challenges

IBM Security, one of the strategic units of the company, provides a comprehensive portfolio including identity and access management, security intelligence and information protection solutions. The product covered in this rating is IBM Security Guardium – a comprehensive data security platform providing a full range of functions, including discovery and classification, entitlement reporting, data protection, activity monitoring, and advanced data security analytics, across different environments: from file systems to databases and big data platforms to hybrid cloud infrastructures.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 10: IBM rating

Among the key features of the Guardium platform are discovery, classification, vulnerability assessment and entitlement reporting across heterogeneous data environments; encryption, data redaction and dynamic masking combined with real-time alerting and automated blocking of malicious access; and activity monitoring and advanced security analytics based on machine learning.

Automated data compliance and audit capabilities with Compliance Accelerators for specific frameworks like PCI, HIPAA, SOX or GDPR ensure that following strict personal data protection guidelines becomes a continuous process, leaving no gaps either for auditors or for malicious actors.

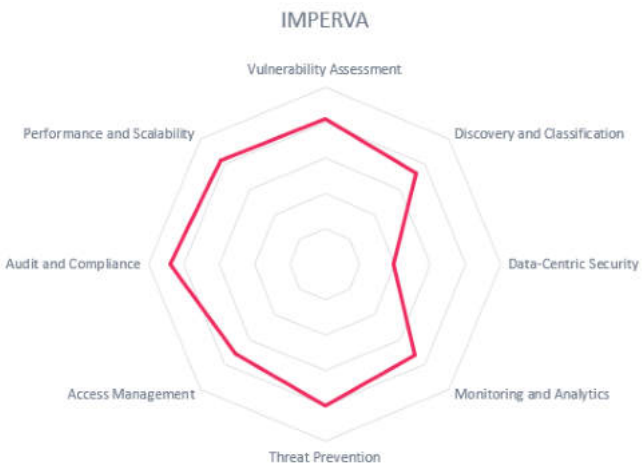
5.5 Imperva

Imperva is an American cybersecurity solution company headquartered in Redwood Shore, California. Back in 2002, the company's first product was a web application firewall, but over the years, Imperva's portfolio has expanded to include several product lines for data security, cloud security, breach prevention, and infrastructure protection as well. In 2019, Imperva was acquired by private equity firm Thoma Bravo, making it a privately held company and providing a substantial boost in R&D. At the same time, major changes in product licensing were announced, which reduced a large number of standalone products towards a short list of convenient packages called FlexProtect Plans.

Strengths	Challenges
• Convenient licensing plans for comprehensive data protection • Multiple collection methods ensure minimal performance overhead • Advanced security intelligence and behavior analytics • Large number of out-of-the-box workflows and compliance reports	• No support for data encryption or dynamic masking

Table 11: Imperva major strengths and challenges

Instead of multiple SecureSphere products for Discovery and Assessment, Activity Monitoring, Database Firewall, as well as CounterBreach for threat protection and Camouflage for masking, Imperva customers only need to subscribe for a single FlexProtect for Data licensing plan to enable full protection of their sensitive data.



Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 12: Imperva rating

The new data protection suite offers all the required capabilities, such as the unified protection across relational databases, data warehouses, Big data platforms, and mainframes; comprehensive activity monitoring, auditing, and forensic investigation, augmented with advanced security analytics based on behavior profiling; pre-defined policies, remediation workflows, and hundreds of compliance reports Integrations with other Imperva's security products ensure that this multi-factored data security can be enforced across endpoints, web applications, and cloud services.

A notable recent addition to Imperva's portfolio is Cloud Data Security, a new offering that extends discovery, classification and analytics capabilities to database assets in the cloud. Delivered as SaaS, the platform can be deployed and configured in hours, delivering actionable insights for prioritizing threat remediations immediately.

5.6 Oracle

Oracle Corporation is an American multinational information technology company headquartered in Redwood Shores, California. Founded back in 1977, the company has a long history of developing database software and technologies; nowadays, however, Oracle's portfolio incorporates a large number of products and services ranging from operating systems and development tools to cloud services and business application suites.

Strengths	Challenges
• Autonomous cloud database platform eliminating human administrative access • Automated provisioning, upgrades, backup and DR, no downtime • Comprehensive product portfolio for all areas of database security • Deep integration with other Oracle's Data Provisioning, Testing and Cloud technologies	• A number of products are available only for Oracle databases • Big Data and NoSQL products are not yet integrated with RDBMS security solutions

Table 13: Oracle major strengths and challenges

The breadth of the company's database security portfolio is impressive: with a number of protection and detection products and a number of managed services covering all aspects of database assessment, protection, monitoring and compliance, Oracle Database Security can address the most complex customer requirements, both on-premises and in the cloud.

The recently introduced Oracle Autonomous Database, which completely automates provisioning, management, tuning and upgrade processes of database instances without any downtime, not just substantially increases security and compliance of sensitive data stored in Oracle databases, but makes a compelling argument for moving this data to the Oracle cloud.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 14: Oracle rating

It's worth noting that a substantial part of the company's security capabilities is still specifically designed for Oracle databases only, which makes Oracle's data protection solutions less suitable for companies using other DB types.
This strategy seems to change slowly however as the company is planning to offer more database-agnostic tools in the future.

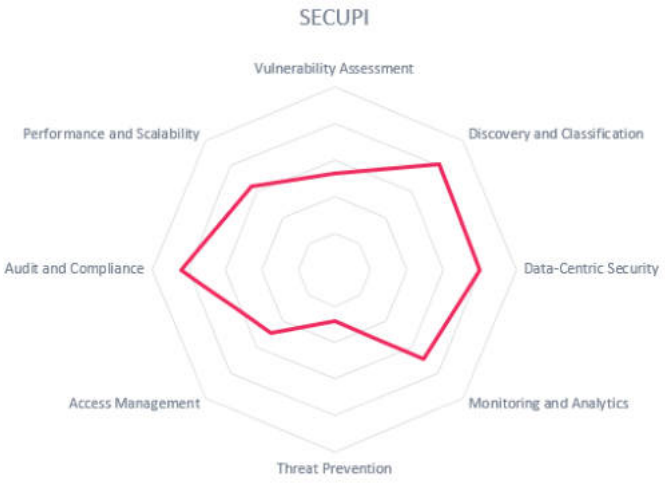
5.7 SecuPI

SecuPI is a privately held data-centric security vendor headquartered in Jersey City, NJ, USA. The company was founded in 2014 by entrepreneurs with a strong background in financial technology, also known for co-inventing the very concept of dynamic data masking. After realizing that data masking alone does not solve modern privacy and compliance problems, the company was established with a vision "to do the things the right way".

Strengths	Challenges
• Integrated data protection and privacy platform with strong focus on GDPR/CCPA • Application-level protection overlays simplify deployment and management • User identity context for more fine-grained policies and monitoring • Broad support for big data and EDW platforms	• Architecture potentially limits support of less popular or legacy platforms • Small market presence compared to competitors

Table 15: SecuPI major strengths and challenges

As opposed to most competitors that encrypt information at the database level, SecuPI's approach is to embed encryption overlays directly into application stacks. Thus, the solution can only focus on supporting a few of major development platforms like Java or .NET instead of numerous distinct data source types. In addition, this approach gives the platform access to real user identities and not to typical service accounts used to connect to databases. With this technology, SecuPI delivers a single privacy-focused data protection platform for on-prem and cloud-based applications, which is easy to deploy and to operate thanks to the centralized management of data protection policies.



Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 16: SecuPI rating

SecuPI software platform brings data-centric security and compliance closer to application owners and business units, enabling sensitive data discovery, classification, anonymization, and minimization across the whole organization, with centralized policy management along with real-time monitoring of all data flows and user activities without any changes in existing applications and network infrastructures.

Built-in controls for user consent management, anonymization and other data subject rights (such as the right to be forgotten) ensure that all existing applications can be made compliant with GDPR and similar regulations quickly and without the need to adapt existing database structures.

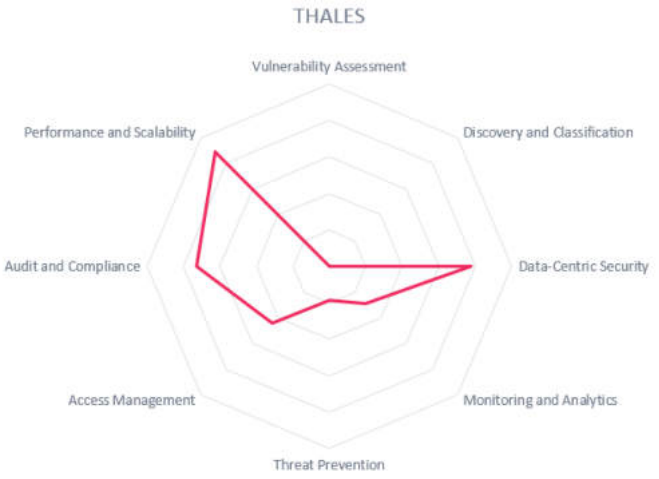
5.8 Thales

Thales is a leading provider of data protection solutions headquartered in Austin, Texas, USA. With over 40 years of experience in information security, the company is a veteran player in such areas like hardware security modules (HSM), data encryption, key management and PKI. The company's modern history began in 2000 when it became a part of Thales Group, an international company based in France, which provides solutions and services for defense, aerospace and transportation markets. In 2019, Thales has completed the acquisition of Gemalto, its largest competitor in the data protection market, thus substantially increasing both its market position and functional capabilities with new services like Authentication and Access Management.

Strengths	Challenges
• Comprehensive transparent encryption, tokenization and masking capabilities • High-performance thanks to hardware encryption support • Centralized management across all environments, even 3rd party products • Standard APIs for adding encryption support to existing applications	• Primary focus on data protection only, no coverage of other functional areas

Table 17: Thales major strengths and challenges

In this rating we focus primarily on the Vormetric Data Security Platform, a unified data protection platform providing customers the flexibility, scale and efficiency to address different security requirements like transparent encryption of the entire database environments, privileged user access controls, granular field-level data protection with encryption, tokenization and data masking, and a single security manager for maximizing value and minimizing the total cost of ownership.



Security	strong positive
Functionality	neutral
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 18: Thales rating

Notable features of the platform include centralized management of encryption keys and policies across all environments and products, application encryption APIs for embedding transparent encryption into existing apps, and dynamic masking with format-preserving tokenization. Live Data Transformation enables in-place encryption of data without the need to move it elsewhere first; this helps reduce maintenance windows for rotating encryption keys or other scenarios like versioned backups. Tight integrations with storage vendors enable innovative capabilities like efficient storage deduplication of transparently encrypted data.

6 Vendors to watch

In addition to the vendors evaluated in detail in this Leadership Compass, there are several companies that for various reasons were unable to participate in the rating but are nevertheless worth mentioning. Some of the vendors below are focusing primarily on other aspects of information security yet show a notable overlap with the topic of our rating. Others have just entered the market as startups with new, yet interesting products worth checking out.

6.1 Dataguise

Dataguise is a privately held company headquartered in Fremont, CA, United States. Founded in 2007, the company provides a sensitive data governance platform to discover, monitor and protect sensitive data on-premises and in the cloud across multiple data environments. Although the company primarily focuses on Big Data infrastructures, supporting all major Hadoop distributions and many Hadoop-as-a-Service providers, their solution supports traditional databases, as well as file servers and SharePoint.

From a single dashboard, customers can get a clear overview of all sensitive information stored across the corporate IT systems, understand which data is being protected and which is at risk of exposure, as well as ensure compliance with industry regulations with a full audit trail and real-time alerts.

6.2 DataSunrise

DataSunrise is a privately held company based in Seattle, WA, United States. It was founded in 2015 with the goal of developing a next-generation data and database security solution for real-time data protection in heterogeneous environments.

The company's solution combines data discovery, activity monitoring, database firewall and dynamic data masking capabilities in a single integrated product. However, the company does not focus on cloud databases only, offering support for a wide range of database and data warehouse vendors. In addition, DataSunrise provides integrations with a number of 3rd party SIEM solutions and other security tools.

6.3 DB CyberTech

DB CyberTech (formerly DB Networks) is privately held database security vendor headquartered in San Diego, CA, United States. Founded in 2009, the company focuses exclusively on database monitoring through non-intrusive deep protocol inspection, database discovery, and artificial intelligence.

By combining network traffic inspection with machine learning and behavioral analysis, DB Networks claims to be able to provide continuous discovery of all databases, analyze interactions between databases and applications and then identify compromised credentials, database-specific attacks and other suspicious activities which reveal data breaches and other advanced cyberattacks.

6.4 McAfee

McAfee is a veteran American computer security vendor headquartered in Santa Clara, California. Founded in 1987, the company has a long history in developing a broad range of endpoint protection, network, and data security solutions. Between 2011 and 2016, McAfee has been a wholly owned subsidiary of Intel. Currently, the company is a joint venture between Intel and an investment company TPG Capital.

In the database security market, McAfee offers a number of products that form the McAfee Database Security Suite providing unified database security across physical, virtual, and cloud environments. The suite provides comprehensive functionality in such areas as database and data discovery, activity monitoring, privileged access control, and intrusion detection – all through a non-intrusive network-based architecture.

6.5 Mentis Inc

MENTIS is a privately held company that provides sensitive information management solutions since 2004. It is headquartered in New York City, USA. The company offers a comprehensive suite of products for various aspects of discovery, management, and protection of critical data across multiple sources, built on top of a common software platform and delivered as a fully integrated yet flexible solution.

With this platform, MENTIS is able to offer business-focused solutions for such common challenges as GDPR compliance, migration to public clouds and sensitive data management for cross-border operations. The company promises quick and simple deployment for most customers with pre-built controls for data masking, monitoring, auditing and reporting for popular enterprise business applications.

6.6 Micro Focus

Micro Focus is a large multinational software vendor and IT consultancy. Originally established in 1976 in Newbury, United Kingdom, nowadays the company has a large global presence and a massive portfolio of products and services for application development and operations management, data management and governance, and, of course, security. In recent years, Micro Focus has grown substantially through a series of acquisitions, and in 2017, it has merged with the HPE's software business.

Voltage SecureData Enterprise, the company's data security platform provides a comprehensive solution for securing sensitive enterprise data through transparent encryption and pseudonymization across multiple database types and Big Data platforms, on premises, in the cloud, and on the edge.

6.7 Microsoft

Microsoft is a multinational technology company headquartered in Redmond, Washington, USA. Founded in 1975, it has risen to dominate the personal computer software market with MS-DOS and Microsoft Windows operating systems. Since then, the company has expanded into multiple markets like desktop and server software, consumer electronics and computer hardware, mobile devices, digital services and, of course, the cloud.

Given their leading position in multiple IT environments – on endpoints, in data centers and in the public cloud, Microsoft has the unique opportunity to collect vast amounts of security-related telemetry and convert it into security insights and threat intelligence.

In the recent years, the company has established itself as a notable security solution provider, and even though they do not yet offer specialized database security products, their portfolio in the areas of information protection and security analytics is worth checking.

Even more interesting are the recent developments in their SQL Server platform, which focus on the concept of Confidential Computing – performing operations on sensitive data within secured enclaves. Combined with the existing encryption capabilities, this technology enables consistent data protection at any stage: at rest, in transit, and in use.

6.8 Protegrity

Protegrity is a privately held software vendor from Stamford, CT, USA. Since 1996, the company has been in the enterprise data protection business. Their solutions implement a variety of technologies, including data encryption, masking, tokenization and monitoring across multiple environments – from mainframes to clouds.

Protegrity Database Protector is a solution for monitoring and securing sensitive information in databases, storage and backup systems with policy-based access controls. Big Data Protector extends this protection to Hadoop-based Big Data platforms – protecting the data both at rest and in transit, as well as in use during various stages of processing.

Protegrity Data Security Gateway provides transparent protection for data moving between multiple devices, without the need to modify any existing applications or services.

6.9 Trustwave

Trustwave is a veteran cybersecurity vendor headquartered in Chicago, IL, United States. Since 1995, the company provides managed security services in such areas as vulnerability management, compliance, and threat protection.

Trustwave DbProtect is a security platform that provides continuous discovery and inventory of relational databases and Big Data stores, agentless assessment of each asset for configuration problems, vulnerabilities, dangerous user rights, and privileges and potential compliance violations and finally enables comprehensive reporting and analytics of security and compliance postures of the organization's database infrastructure.

The solution's distributed architecture can meet the scalability demands of large organizations with thousands of data stores.

7 Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a particular market segment which you should consider for product decisions.

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

7.1 Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in a particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

For every area, we distinguish between three levels of products:

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular areas.
- Challengers: This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag behind in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even the best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

7.2 Product rating

KuppingerCole as an analyst company regularly does evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way vendors deal with them.

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration—integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated.

And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability—interoperability also can have many meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability —accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

[2] https://www.kuppingercole.com/report/cb_apieconomy16122011

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided are of the highest importance. This is because the lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

7.3 Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position – measures the position the vendor has in the market or the relevant market segments. This is an average rating overall markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

7.4 Rating scale for products and vendors

For vendors and product feature areas, we use – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

Strong positive	Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for the market position or financial strength, indicating that vendors are very small and have a very low number of customers.

7.5 Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider graph for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the field of Database and Big Data Security, we look at the following eight areas:

Vulnerability assessment	Discovering known vulnerabilities in database products, providing complete visibility into complex database infrastructures, detecting misconfigurations and the means for assessing and mitigating these risks.
Discovery & Classification	Crucial first step in defining proper security policies for different data depending on their criticality and compliance requirements.
Data-centric Security	Data encryption at rest and in transit (and in use wherever available), static and dynamic data masking and other technologies for protecting data integrity and confidentiality.

Monitoring & Analytics	Monitoring of database performance characteristics, complete visibility for all access and administrative actions for each instance, including alerting and reporting functions, advanced real-time analytics, anomaly detection, and SIEM integration.
Threat Prevention	Various methods of protection from cyber-attacks such as denial-of-service or SQL injection, mitigation of unpatched vulnerabilities and other infrastructure-specific security measures.
Access Management	Access controls for database instances, dynamic policy-based access management, identifying and removing excessive user privileges, managing shared and service accounts, detection, and blocking of suspicious user activities.
Audit & Compliance	Advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, forensic analysis, and compliance audits.
Performance & Scalability	Ability to withstand high loads, minimize performance overhead and to support deployments in high availability configurations.

These spider graphs add an extra level of information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas while being strong in other areas. These might be a good fit if only specific features are required. Given the breadth and complexity of the full scope of database security, only very few largest vendors have enough resources to offer solutions that cover all of the areas; thus, we do not recommend overlooking smaller, more specialized products – often they may provide substantially better return of investment.

7.6 Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack of Market Leadership.
- Denial of participation: Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.

- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

Despite our effort to cover most aspects of database and big data security in this Leadership Compass, we are not planning to review the following products:

- Solutions that primarily focus on unstructured data protection having limited or no database-related capabilities;
- Security tools that cover general aspects of information security (such as firewalls or antimalware products) but do not offer functionality specifically tailored for data protection;
- Compliance or risk management solutions that focus on organizational aspects (checklists, reports, etc.)

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview of vendors not covered and their offerings in the chapter *Vendors to watch*. In that chapter, we also look at some other interesting offerings around the Database and Big Data Security market and in related market segments.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com