

KuppingerCole Report
**LEADERSHIP
COMPASS**

By **Alexei Balaganski**
January 19, 2021

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

Content

1 Introduction	4
1.1 Market Segment	5
1.2 Delivery Models	6
1.3 Required Capabilities	6
2 Leadership	9
2.1 Overall Leadership	9
2.2 Product Leadership	11
2.3 Innovation Leadership	13
2.4 Market Leadership	16
3 Correlated View	19
3.1 The Market/Product Matrix	19
3.2 The Product/Innovation Matrix	21
3.3 The Innovation/Market Matrix	22
4 Products and Vendors at a Glance	25
5 Product/Vendor Evaluation	28
5.1 AWS Database Services	30
5.2 Axiomatics Dynamic Authorization Suite	33
5.3 comfrote AG SecurDPS Enterprise	36
5.4 DataSunrise	39
5.5 Delphix Dynamic Data Platform	42
5.6 IBM Security Guardium	45
5.7 Imperva Security Platform	48
5.8 Microsoft Azure	51
5.9 Oracle Autonomous Database Cloud	54
5.10 SecuPi Platform	57
5.11 Thales CipherTrust Data Security Platform	60
6 Vendors to Watch	63
6.1 Dataguise	63

6.2 DB CyberTech 63

6.3 IDERA Software 63

6.4 Informatica 64

6.5 McAfee 64

6.6 Mentis Inc. 64

6.7 Mirco Focus 65

6.8 Protegrity 65

6.9 Trustwave 65

7 Related Research 67

Methodology 68

Content of Figures 74

Copyright 75

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 valuable corporate data must be protected against compromises of their integrity and confidentiality without affecting their availability for business processes.

As more and more companies are embracing digital transformation, the challenges of securely storing, processing, and exchanging digital data continue to multiply. With the average cost of a data breach reaching \$4M, just direct financial losses can be catastrophic for many companies, not even considering indirect reputational damages. High-profile “mega-breaches” that expose millions of sensitive data records can easily drive these costs up to hundreds of millions of dollars, but even the victims of smaller ones are now facing increasingly harsh compliance fines.

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 recently approved CPRA (the new Privacy Rights Act will bring California’s legislation much closer to a GDPR equivalent) make no distinction between relational databases, data lakes, or file stores – all data is equally sensitive regardless of the underlying technology stack. Just keeping track of all the digital information is a big problem, but understanding which data is more sensitive according to various policies and regulations and then selecting and enforcing the necessary data protection and governance capabilities is already too much even for the largest businesses.

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. These include, among others, data protection capabilities, fine-grained access controls, activity monitoring, audit, and compliance features as well as other means needed for comprehensive multi-layered protection against external and internal threats. As the amount and variety of digital information managed by organizations continue to grow, the complexity of the IT infrastructure needed to support this digital transformation grows as well.

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

- Denial of service attacks leading to disruption of legitimate access to data.
- 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.

- Unpatched security vulnerabilities or configuration problems in the database software, which may lead to data loss or availability issues.
- Attacks specifically crafted to target databases through application interfaces or APIs, like SQL injections for relational databases and similar exploits for NoSQL and Big Data solutions.
- Sensitive data exposure due to poor data lifecycle management. This includes improperly protected backups, testing or analytical data without proper masking, etc.
- Unsanctioned access to encrypted sensitive data due to improper key management – this is especially critical for cloud environments where encryption is often managed by the cloud service provider.
- Insufficient monitoring and auditing – not only these pose a significant noncompliance risk, but a lack of a tamper-proof audit trail also makes forensic investigations and incident response much more complicated.

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 is not that easy to define unambiguously. Only the largest vendors can afford to dedicate enough resources for developing a solution that covers all or at least several functional areas – most products mentioned in this Leadership Compass tend to focus on one major 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 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 be more fitting. On the other hand, one must always consider the balance between a well-integrated suite from a single vendor and several 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 and semi-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 (mixing on-premises and cloud) 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.

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, a cloud-based data lake, or 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 most 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.

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** – not limited to just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations, and 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** – technologies such as data encryption at rest and in transit as well as enterprise key management, tokenization, static and dynamic data masking, and other methods for protecting data integrity and confidentiality and for ensuring regulatory compliance for sensitive data in cloud environments.
- **Monitoring and analytics** – 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** – 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** – not just basic coarse-grained access controls to database instances, but more sophisticated dynamic policy-based access management based on various data or user

attributes, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.

- **Audit and Compliance** – offering 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.
- **Deployment 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; all these must be supported in on-prem, cloud and hybrid environments.

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

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 this 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.

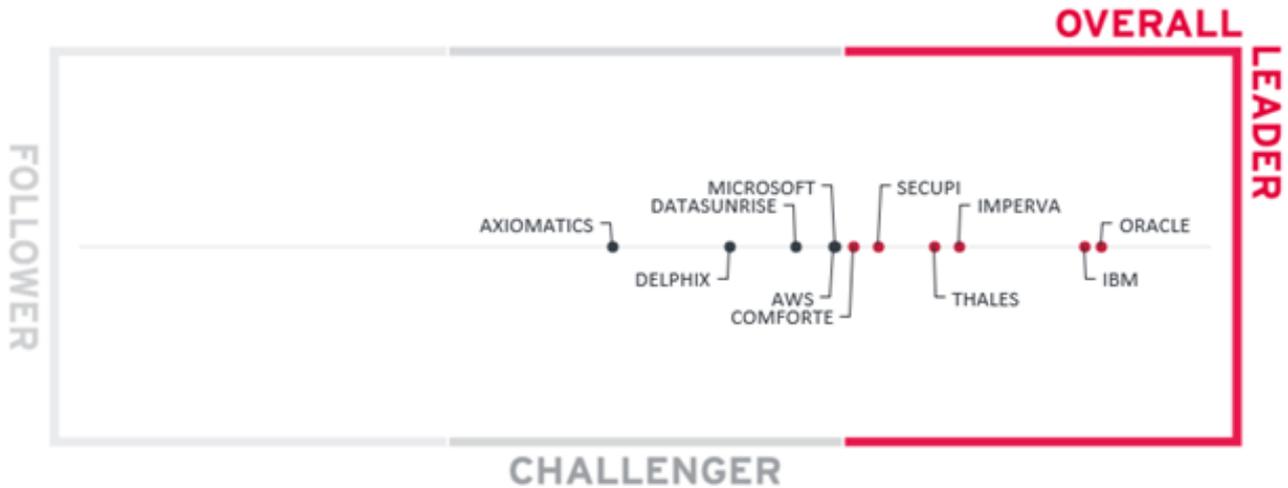


Figure 1: The Overall Leadership rating for the Database and Big Data Security market segment

Compared to the last year’s edition of this Leadership Compass, we can observe notable changes in the overall leadership rating. Oracle and IBM retain their distant leadership just like last year, which reflects both companies’ global market presence, broad ranges of database security solutions, and impressive financial strengths. However, this time, they are joined by three other vendors, which were found among the challengers last year, but managed to transition to Leaders. Comforte AG, Imperva, SecuPi and Thales have substantially improved their respective solutions with additional data protection capabilities, either through acquiring and integrating new technologies into their products or by forming technology partnerships with 3rd party vendors.

All other vendors can be found in the Challengers segment. Lacking the combination of both an exceptionally strong market and product leadership, they are hanging somewhat behind the leaders, but still deliver mature solutions excelling in certain functional areas. Axiomatics and Delphix have already participated in earlier Leadership Compasses, while DataSunrise is a newcomer that was only mentioned as a “Vendor to watch” previously.

AWS and Microsoft are also participating, both having broad portfolios of cloud-native database services (for more information, we recommend checking out KuppingerCole’s Leadership Compass on Enterprise Databases in the Cloud). However, while both companies are large and respectable cloud service providers, databases and database security are not their primary focus. Still, both AWS and Azure clouds offer a broad selection of security tools designed specifically for their own database services.

No vendors appear in the Followers segment of our overall rating.

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):

- comfote AG
- IBM
- Imperva
- Oracle
- SecuPi
- Thales

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

Just like last year, there are the same largest players in the market, offering a wide range of products covering different aspects of database security, that take the first two product leadership positions with a strong lead ahead of the competition. IBM Security Guardium is a data security platform that 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.

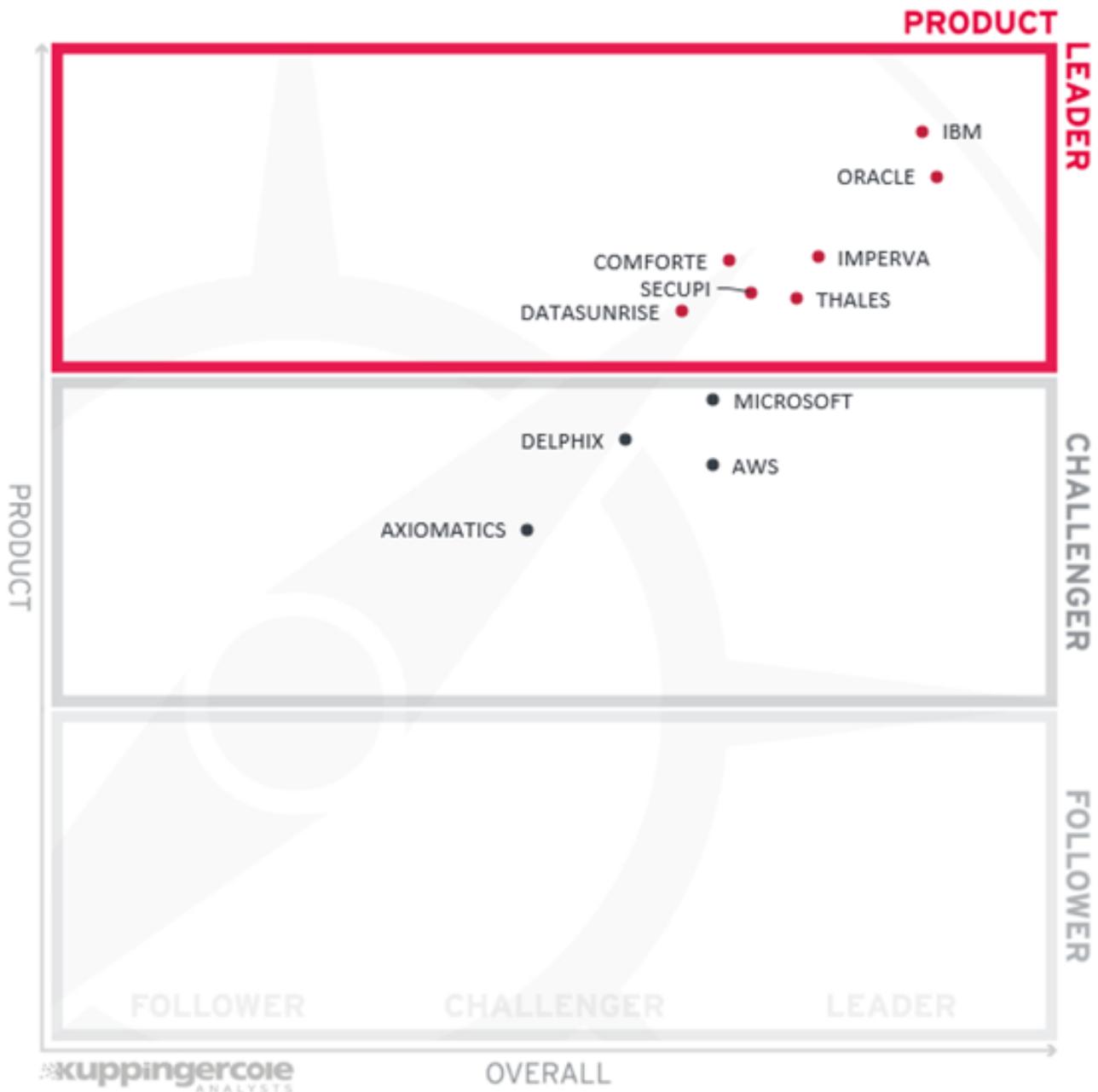


Figure 2: Product Leaders in the Database and Big Data Security segment

Following them we have a tight group of companies that were also present among the leaders last year; in fact, the only notable change is Imperva improving their rating quite substantially, considering the company's strong investments into expanding and better integrating their data protection portfolio during the time since our 2019 edition.

It is joined by comfote AG with its 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; SecuPI – a young but ambitious vendor focusing on data-

centric protection and GDPR/CCPA compliance for databases, big data, and business applications; and Thales with its scalable and unified data security platform combining data discovery and classification, encryption, tokenization, data and masking and centralized key management for on-premises and clouds, across entire IT landscapes.

A newcomer among the leaders is DataSunrise, whose solution combines data discovery, activity monitoring, database firewall, and dynamic data masking capabilities in a single integrated product.

Among the Challengers in product leadership, we can find both AWS and Microsoft with their comprehensive data security portfolios integrated into their cloud service offerings, as well as smaller companies focusing on specific functional areas of database security.

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 we find Axiomatics – a leader in dynamic access control with a specialized ABAC solution for databases and Big Data frameworks.

Again, we have no Followers in the product leadership rating.

Product Leaders are (in alphabetical order):

- comfote AG
- DataSunrise
- 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.

Just like last year, we find both Oracle and IBM among the Leaders. Oracle has continued its highly innovative developments of the Autonomous Database from the previous years into further areas, offering not just several new flavors of autonomous database cloud services that operate without human administrative intervention, but has brought them to on-prem customers as well. Other notable

developments include context-aware database access controls and comprehensive access governance that reduces the attack surface and improves compliance.

IBM has continued to expand the focus of the Guardium platform, adding even more support for unstructured data monitoring in on-prem and cloud stores, as well as the incorporating of the latest technological developments like artificial intelligence and consent management, integrations with cloud-native data stores, and advanced threat prevention.

This time, however, we have additional newcomers among the innovation leaders. Imperva has substantially improved its innovation rating by not just expanding its data protection portfolio with new solutions (like a service designed specifically for cloud databases) but to a significant extent to its recent acquisition of jSonar, which provides a unified, extensible agentless platform for implementing security controls across any type of data repository.

SecuPI delivers a single privacy-focused data protection platform for on-premises and cloud-based applications, which is easy to deploy and to operate thanks to the centralized management of data protection policies. Thanks to its innovative platform-agnostic approach, SecuPi can address security and compliance challenges directly at the application layer, dramatically reducing complexity and improving performance at the cloud scale.

Thales was also able to enter the Leaders segment thanks to a multitude of innovative developments within its data protection portfolio. These include not only a major product consolidation that eliminates functional overlaps with previously acquired competitive products, but continued integration efforts, major simplification of securing complex, heterogeneous data environments, and Live Data Transformation technology that eliminates downtime when encrypting databases or rekeying. Their biggest innovations in 2020 include adding data discovery and classification to their platform and integrating cloud key management within the CipherTrust Manager.

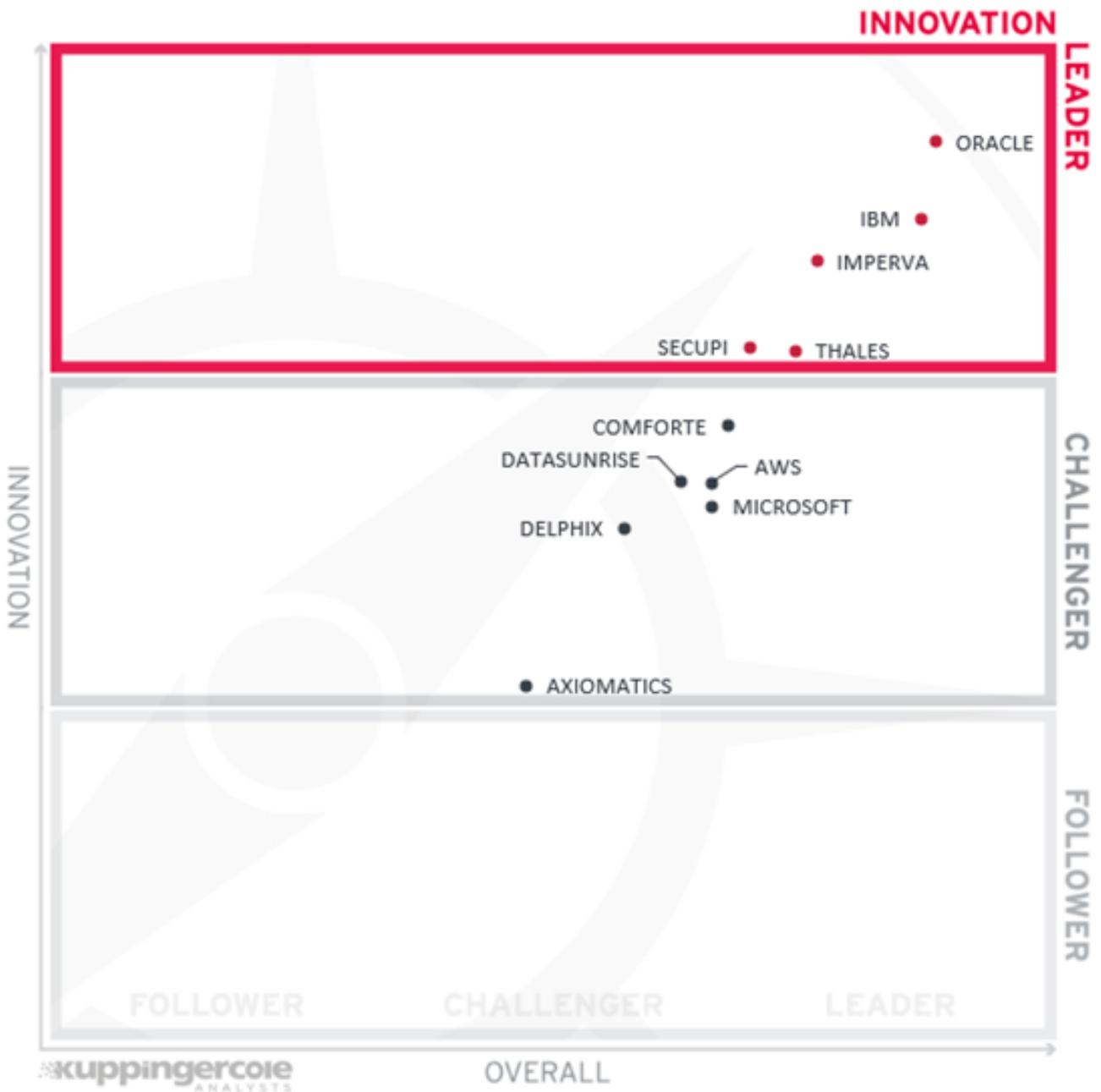


Figure 3: Innovation Leaders in the Database and Big Data Security segment

The rest of the vendors populate the Challengers segment, reflecting their continued investments into delivering new features in their solutions, which, however, are mostly limited to a specific functional area or simply do not represent the respective company’s primary focus.

There are no Followers in this year’s innovation rating as well.

Innovation Leaders are (in alphabetical order):

- IBM

- Imperva
- Oracle
- SecuPi
- Thales

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.

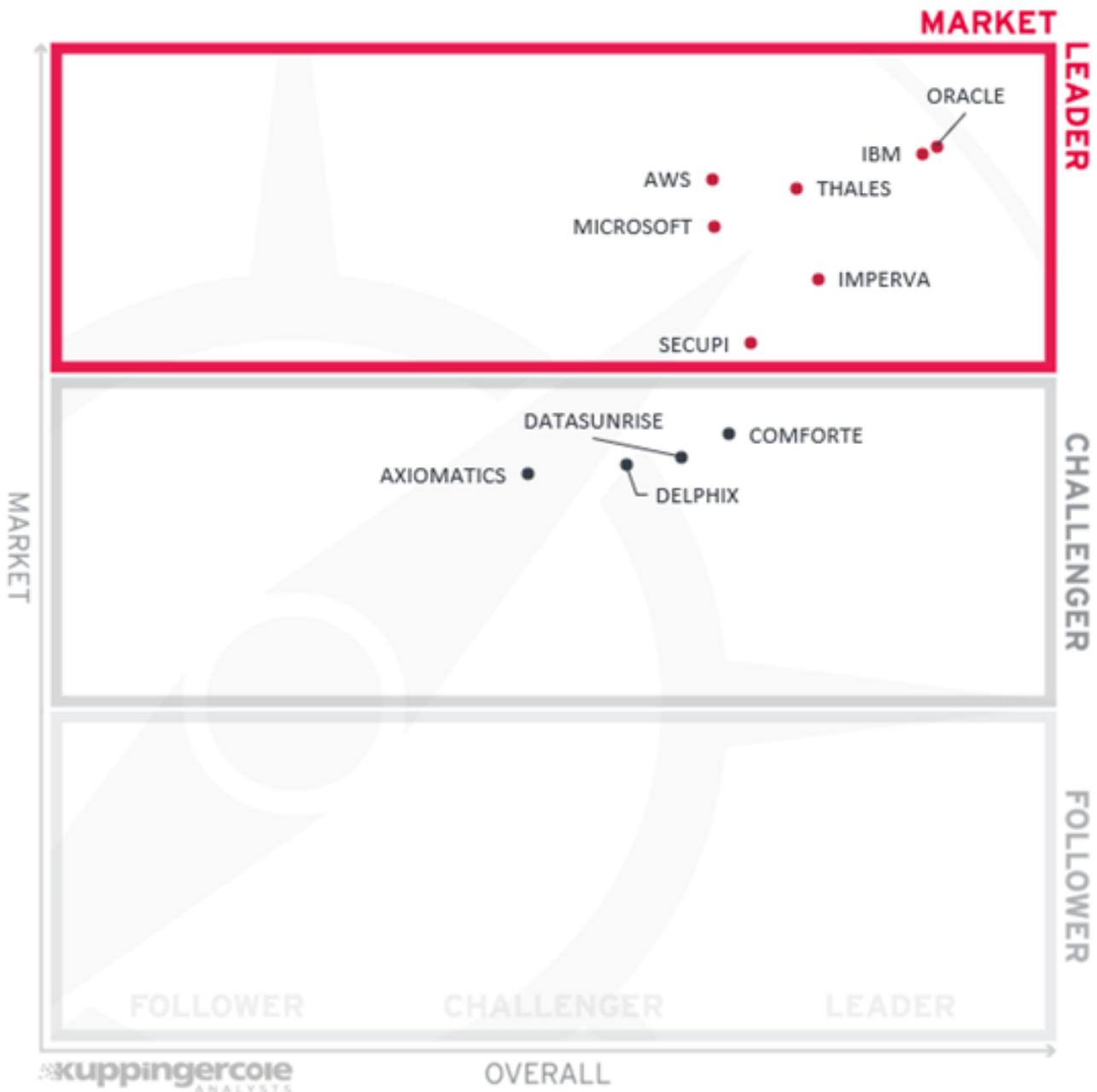


Figure 4: Market Leaders in the Database and Big Data Security market segment

Again, completely unsurprisingly, most market leaders in our rating are large, veteran vendors with massive international presence, large partner networks, and impressive customer bases. These include both database security-oriented vendors like Oracle, IBM, Thales, and Imperva, as well as large cloud service providers like AWS and Microsoft. The only smaller vendor among market leaders is SecuPi, thanks to its close business relationships with major cloud service providers.

All smaller companies are found in the Challengers segment, indicating their relative financial stability and future growth potential. Once again, we have no Followers in our market leadership rating.

Market Leaders are (in alphabetical order):

- AWS
- IBM
- Imperva
- Microsoft
- Oracle
- SecuPi
- 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. 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.

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

Here one can identify 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 once again find the largest well-established vendors including IBM, Oracle, Thales, and Imperva, as well as SecuPi thanks to its prominent presence in the marketplaces of major cloud service providers.

comforte AG and DataSunrise appear in the middle right box, indicating the opposite skew, where strong product capabilities have not yet brought them to a strong market presence. We believe they have a strong potential for improving their market positions in the future.

AWS and Microsoft occupy the top middle segment, highlighting both their massive market presence as leading cloud service providers and the fact that database security is by far not their primary focus area. 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.

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. This time, they are joined by Imperva, SecuPi and Thales, reflective the respective companies' major recent investments into innovative technologies and expansion of their data protection portfolios.

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

All other vendors have landed in the central box, showing a healthy combination of solid product capabilities and a steady, if not perhaps amazing pace of innovation. This is typical for smaller companies or vendors that do not primarily focus on database security alone.

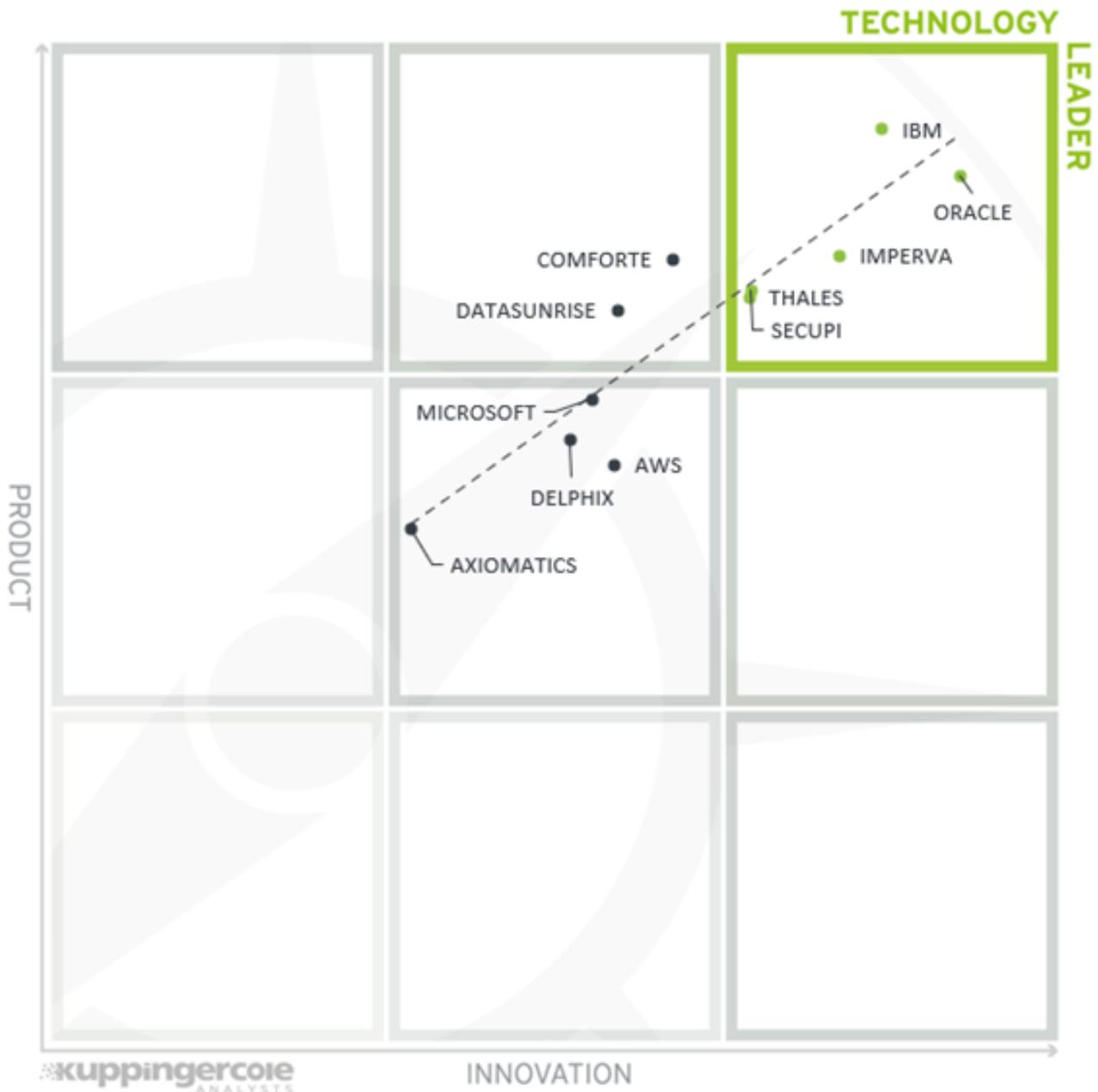


Figure 6: The Product/Innovation Matrix

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, highly innovative vendors have a good chance of improving their market position but often face risks of failure, especially in the case of vendors lacking a strong strategic vision.

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

Among the Big Ones, we again find all the large vendors with strong data protection portfolios, namely IBM, Imperva, Oracle, and Thales – all of them combine well-established market presence with a strong pace of innovation. SecuPi, despite its relatively small size, managed to reach the top segment as well.



Figure 7: The Innovation/Market Matrix

AWS and Microsoft in the top middle box indicate their strong market positions despite not focusing primarily on database security (even though both naturally provide a broad range of security services as a part of their database portfolios).

Comforte AG, DataSunrise and Delphix occupy the central box below the dotted line, indicating their strong performance in innovation, which has not yet translated into larger market shares. Axiomatics has managed to escape the left middle box it has occupied in the previous edition and joins the rest of the vendors in the middle segment.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass document. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, and so on.

It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4. Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in the table below.

Product	Security	Functionality	Interoperability	Usability	Deployment	
AWS Database Services	●	●	●	●	●	
Axiomatics Dynamic Authorization Suite	●	●	●	●	●	
comforte AG SecurDPS Enterprise	●	●	●	●	●	
DataSunrise	●	●	●	●	●	
Delphix Dynamic Data Platform	●	●	●	●	●	
IBM Security Guardium	●	●	●	●	●	
Imperva Security Platform	●	●	●	●	●	
Microsoft Azure	●	●	●	●	●	
Oracle Autonomous Database Cloud	●	●	●	●	●	
SecuPi Platform	●	●	●	●	●	
Thales CipherTrust Data Security Platform	●	●	●	●	●	
Legend		● critical	● weak	● neutral	● positive	● strong positive

Besides, we provide four additional ratings for the vendors. 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	Innovativeness	Market Position	Financial Strength	Ecosystem	
Amazon Web Services	●	●	●	●	
Axiomatics	●	●	●	●	
comforte AG	●	●	●	●	
DataSunrise	●	●	●	●	
Delphix	●	●	●	●	
IBM	●	●	●	●	
Imperva (was acquired by Thoma Bravo)	●	●	●	●	
Microsoft	●	●	●	●	
Oracle	●	●	●	●	
SecuPi	●	●	●	●	
Thales	●	●	●	●	
Legend	● critical	● weak	● neutral	● positive	● strong positive

5 Product/Vendor Evaluation

This section contains a quick one-page rating for database or big data security vendor we have included in this Leadership Compass. For some of the products and services mentioned in this chapter, there are additional KuppingerCole Reports available, providing more detailed information.

Please note that some of the vendors are providing a single product or a platform, while others offer broad portfolios of specialized tools or services. Thus, in our reviews, we focus more on the overall ability of vendors to deliver integrated, reliable, scalable, and convenient solutions for securing their customers' sensitive data.

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, typically by combining several various services into suites or integrated platforms.

This report focuses on the following eight categories:

- Vulnerability assessment – visibility into database infrastructures, discovering known vulnerabilities, analyzing misconfigurations, assessing, and mitigating detected risks.
- Data discovery and classification – finding and assessing sensitive data across multiple siloes, providing a baseline for proper security and compliance policies.
- Data-centric security – data encryption at rest and in transit, tokenization, static and dynamic data masking, other methods for protecting data integrity and confidentiality.
- Monitoring and analytics – visibility into all access and administrative activities, alerting and reporting, advanced real-time analytics
- Threat prevention – protection from cyber-attacks, mitigation of unpatched vulnerabilities, other infrastructure-specific security measures.
- Access Management – fine-grained, dynamic policy-based access management, removing excessive user privileges, managing shared and service accounts, blocking of suspicious user activities.
- Audit and Compliance – centralized auditing and reporting across multiple database environments,

separation of duties, forensic analysis, and compliance audits.

- Deployment and Scalability – ability to withstand high loads, minimize performance overhead, support deployments in high availability configurations.

5.1 AWS Database Services

Amazon Web Services, Inc. (AWS) is a multinational cloud service provider headquartered in Seattle, USA. A subsidiary of the American retail giant Amazon.com, AWS was initially formed to consolidate and standardize the computing infrastructure powering Amazon's online business. In 2006, the AWS platform was launched officially with the vision of offering on-demand access to this infrastructure to customers on a subscription basis, thus essentially making the company the first major player in the cloud computing market.

AWS offers a broad and versatile portfolio of database services for any kind of customer – from small open-source projects to business-critical enterprise. AWS makes a strong focus on providing purpose-built database engines for different data models and diverse use cases. Besides being able to provide cloud infrastructure for just about any existing database, the company offers 15 fully managed database services, not to mention the popular unstructured data storage options like Amazon S3 object storage service and Data Lakes built on top of it.

Amazon Aurora, the company's flagship relational database service, offers a full range of data protection capabilities including encryption at rest and in transit, fine-grained access controls, network isolation with VPC, and a firewall. Protection against internal threats is supported with Database Activity Streams to audit administrative access and generate alerts.

Amazon Macie is a managed, AI-powered data security and privacy service that discovers and protects sensitive unstructured data on the AWS cloud. Currently, it focuses on Amazon S3 buckets across multiple accounts, discovering insufficiently protected buckets with sensitive information and helping fix compliance violations and prevent data breaches. It does not come with remediation capabilities out of the box but integrates with other services like AWS Lambda and AWS Security Hub as a single pane of glass that integrates with existing SIEM solutions. In the end, AWS provides the customers with a multitude of security, privacy, and compliance tools to support their data protection efforts.

Security	● ● ● ● ●
Functionality	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○



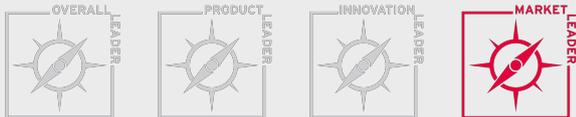
Strengths

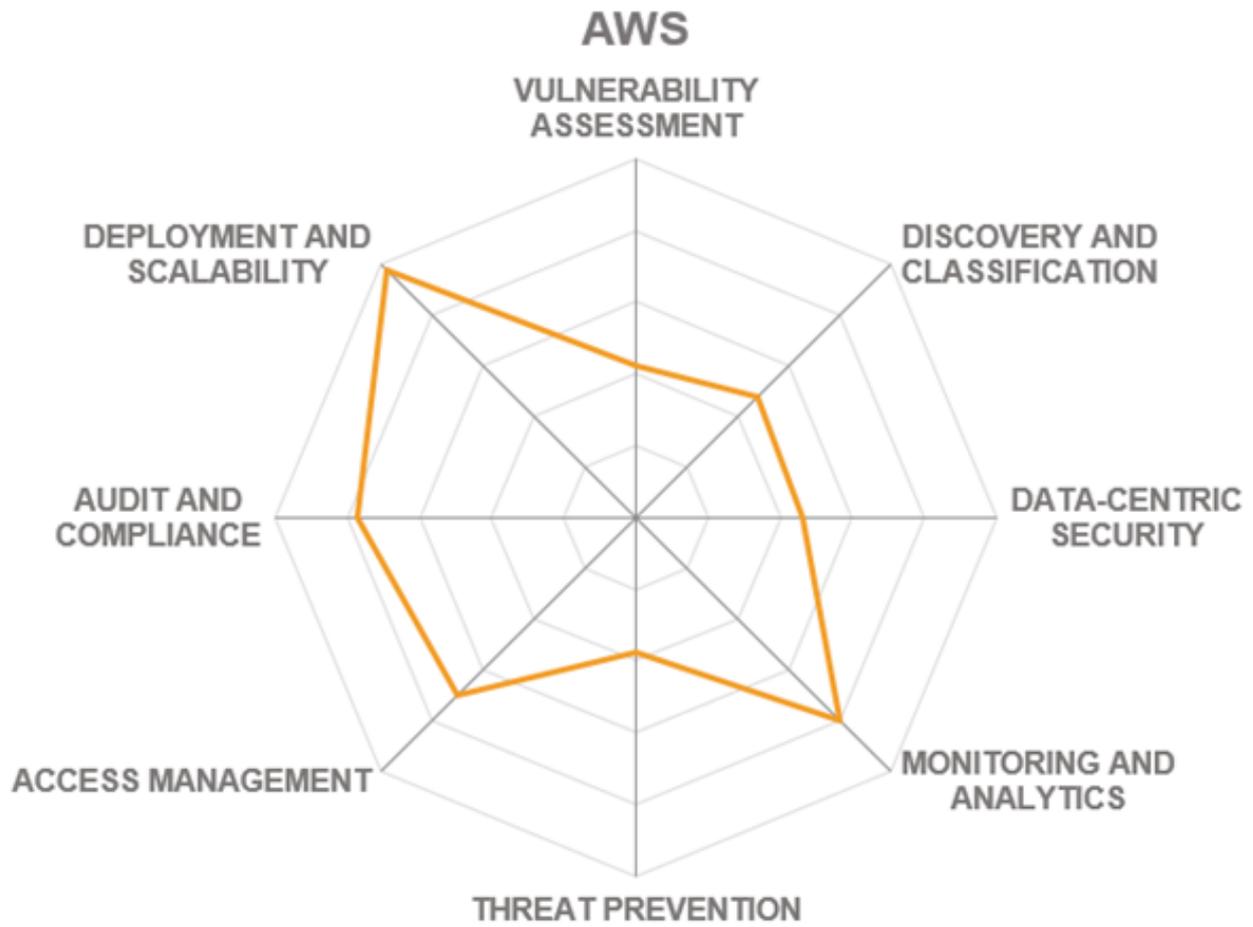
- Broad selection of purpose-built database engines and unstructured storage options.
- Full set of data protection capabilities for relational databases.
- Fully managed data security and privacy for S3 storage.
- Deep integrations with identity management, security analytics, and other AWS services.

Challenges

- Only available in AWS cloud or other platforms hosted on AWS.
- Data protection capabilities can vary substantially between database engines.
- Focuses on managed cloud database services only.

Leader in





5.2 Axiomatics Dynamic Authorization Suite

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.

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. On this foundation, the data protection suite includes Axiomatics Data Access Filter for Multiple Databases 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 solution 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. This allows for centralized management of authorization policies, which are then applied across all connections, regardless of application endpoint. Multiple database types, like Oracle, Microsoft SQL Server, or IBM DB2 are supported, as well as Apache Spark, the analytics engine for big data processing.

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.

Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ○ ○
Deployment	● ● ● ● ○

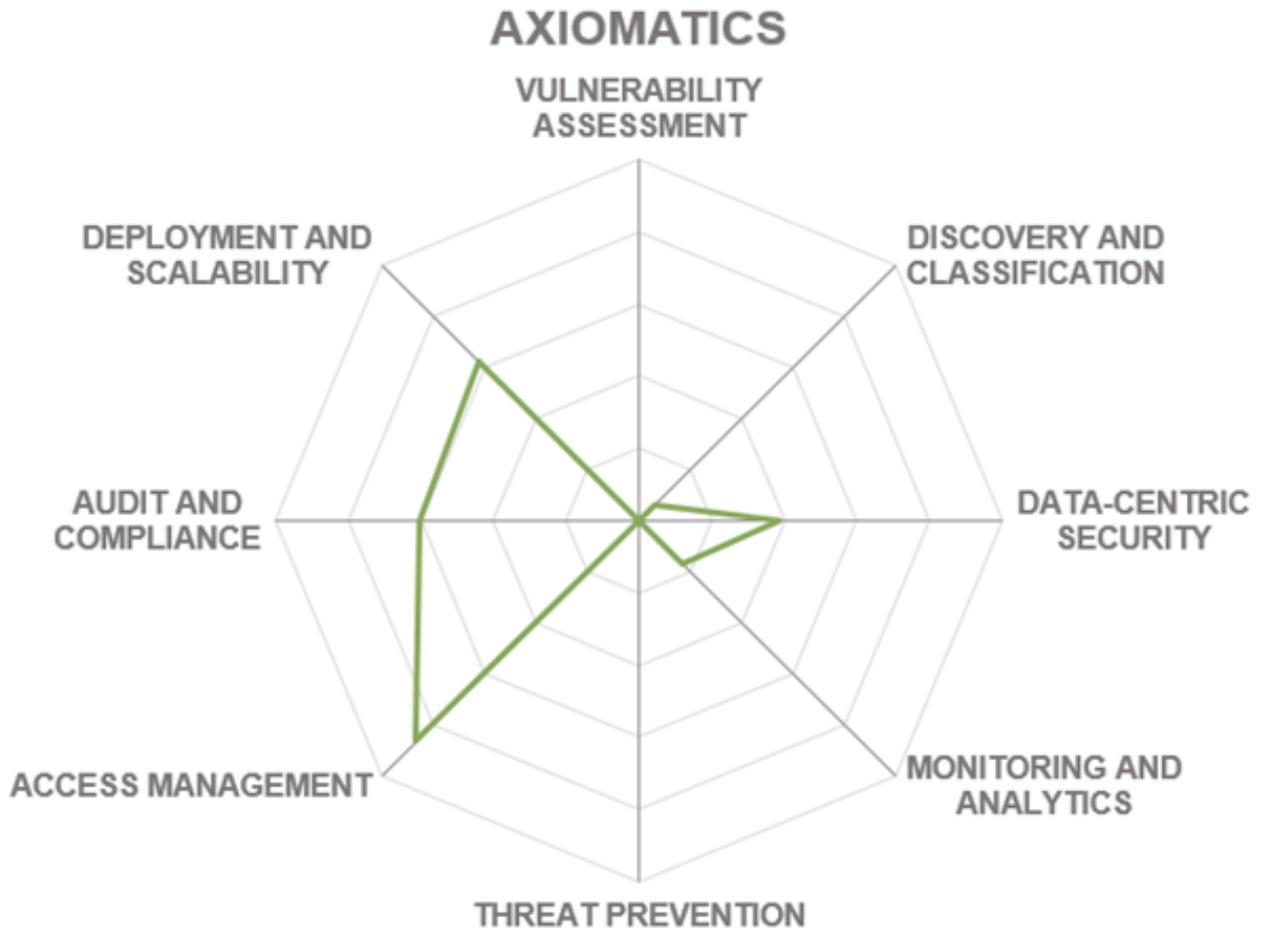


Strengths

- 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.

Challenges

- Quite narrow functional focus compared to other products in the rating.
- Relies on 3rd party components to enforce policies.
- Targeted primarily at large complex enterprise deployments.



5.3 comfote AG SecurDPS Enterprise

comfote AG is a privately held software company specializing in data protection and digital payment 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, comfote'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.

A few years ago, comfote 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.

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. The patented stateless tokenization algorithm supports limitless scaling across heterogeneous environments. Strong focus on regulatory compliance directly addresses PCI DSS and GDPR requirements.

Since our last review in 2019, the company has introduced major improvements to the platform. First, secureDPS Discovery, a new data discovery and classification solution has been introduced, which implements automated, ML-supported identification and analysis of data repositories with sensitive information. By associating discovered data with data subjects, the solution helps produce data lineage and simplify data flow analysis.

Another new component is secureDPS Connect, a security gateway for protecting data in SaaS applications utilizing transparent on-the-fly tokenization, format-preserving encryption, or masking. Combined with the ability to deploy the core protection nodes in Kubernetes clusters, the solution is now fully ready for scalable cloud-native deployments.

Security

Functionality

Interoperability

Usability

Deployment




Strengths

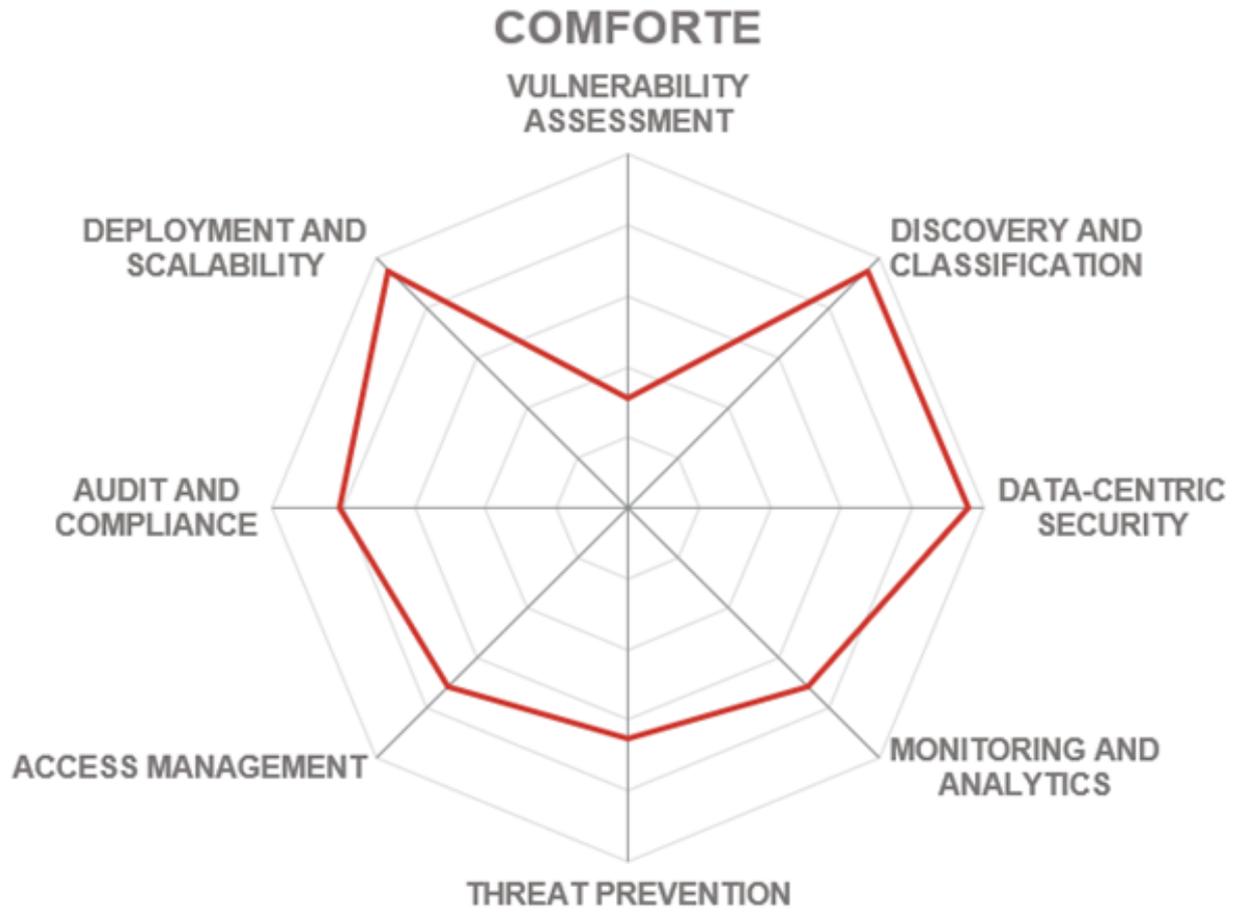
- Unique hardened, scalable, and fault-tolerant architecture for mission-critical use cases.
- Deployment flexibility, hybrid cloud, and as-a-Service scenarios are supported.
- Security Gateway for SaaS applications.
- Broad range of transparent application integration options, support for Big Data and stream processing frameworks.
- Strong focus on maintaining regulatory compliance like PCI DSS and GDPR.

Challenges

- No vulnerability assessment capabilities included.
- Data discovery engine is a 3rd party OEM product.
- Somewhat limited market visibility outside of the financial industry.

Leader in





5.4 DataSunrise

DataSunrise is a security vendor based in Seattle, WA, United States. It was founded in 2015 to develop 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.

DataSunrise Data and Database Security is a cross-platform solution for protecting databases and other types of data stores across on-prem and cloud environments with centralized management and a broad range of capabilities. Implemented as a universal database proxy, the solution is non-intrusive, does not require infrastructure changes, and is certified by major cloud platforms to protect their managed database services.

DataSunrise combines sensitive data discovery, activity monitoring and auditing, threat protection, and data masking to offer a range of security capabilities under unified policy management. A recent addition to the platform is the regulatory compliance manager, an automated compliance engine that greatly simplifies compliance with GDPR, PCI DSS, HIPAA, and other important regulatory frameworks.

Even if DataSunrise cannot offer full feature parity with enterprise-grade capabilities of some of its larger competitors, the solution is notable for combining nearly all aspects of database security covered in this Leadership Compass in one integrated product. With over 30 database engines, big data platforms, and other types of data stores and a strong focus on supporting managed database services, DataSunrise might be a compelling choice for modern cloud-native companies with highly heterogeneous database infrastructures.

Security

Functionality

Interoperability

Usability

Deployment



Data Sunrise

Data and Database Security

Strengths

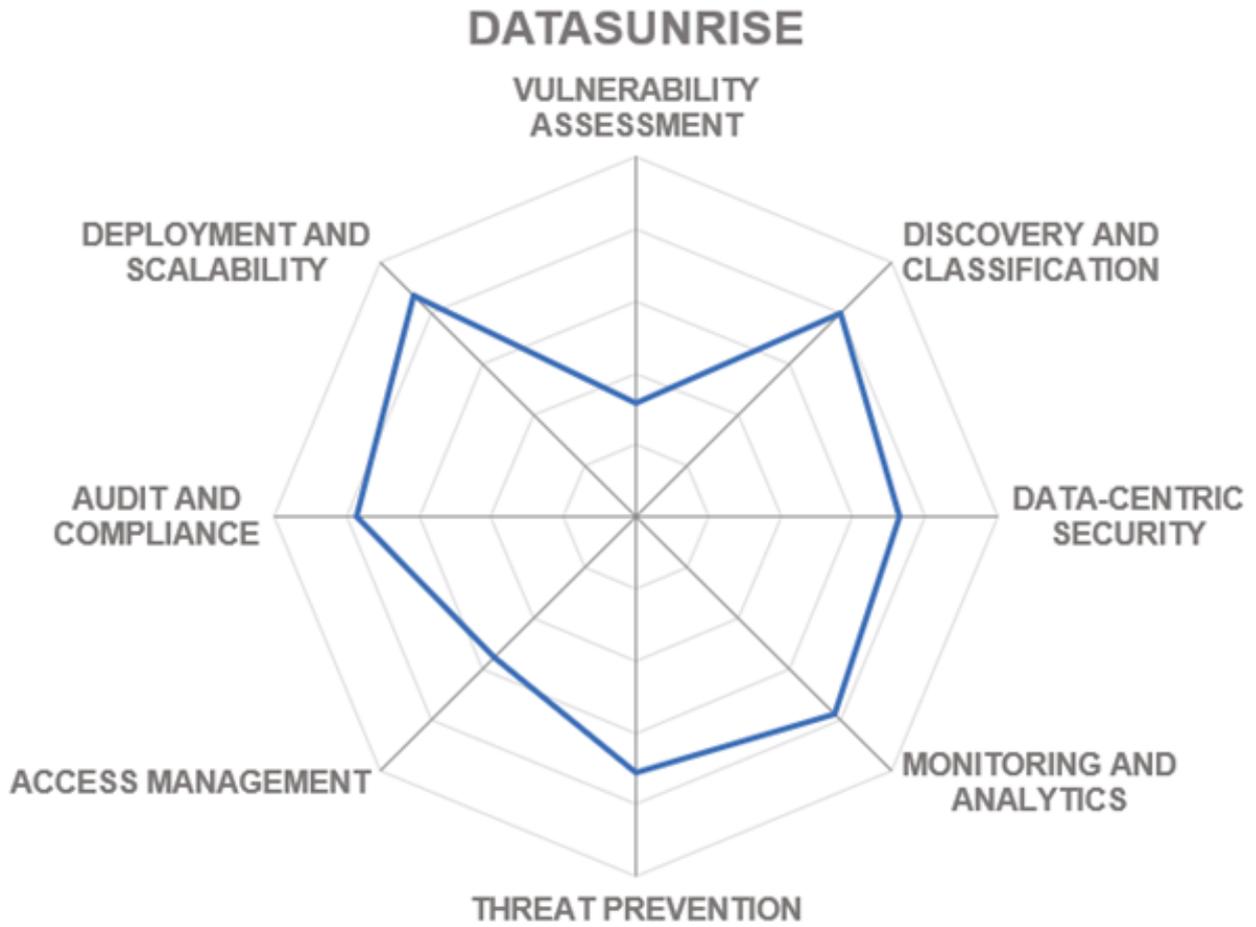
- Tightly integrated multi-functional database security suite covers all major attack surfaces.
- Broad range of supported SQL and NoSQL databases, unstructured data stores.
- Support for multiple cloud databases and storage services simplifies hybrid deployments.
- Database Regulatory Compliance manager automates compliance with major privacy regulations.

Challenges

- Relies on cloud platforms for scalability and HA deployments.
- Targeted as smaller companies, not suitable for enterprise-scale projects.
- Relatively small market presence.

Leader in





5.5 Delphix Dynamic Data Platform

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.

Delphix Dynamic Data Platform is an integrated and fully automated DataOps platform that combines data virtualization and data masking, making corporate data from various sources available across on-premises and cloud environments quickly and securely at the speed and scale needed to support a wide range of use cases: from development and testing to data analytics to cloud migration to disaster recovery. Using the integrated data masking technology, Delphix implements the automatic discovery of sensitive data and its obfuscation by using masking or reversible tokenization as a seamless part of the virtualization process.

Flexible deployment options and a wide range of supported databases and file systems make the Delphix platform a very interesting choice for companies that are planning a deep dive into the DataOps methodology or just looking for a universal tool to address multiple pain points in such areas as DevOps, data analytics, cloud migration, and even disaster recovery. The company provides pre-configured images for deployment on AWS, Azure, and GCP public clouds, and several cloud-based database types are supported as well. Thus, the platform enables transparent data virtualization across hybrid environments, substantially reducing the amount of data that must be replicated into the cloud and automatically enforcing the security and compliance policies.

D E L P H I X

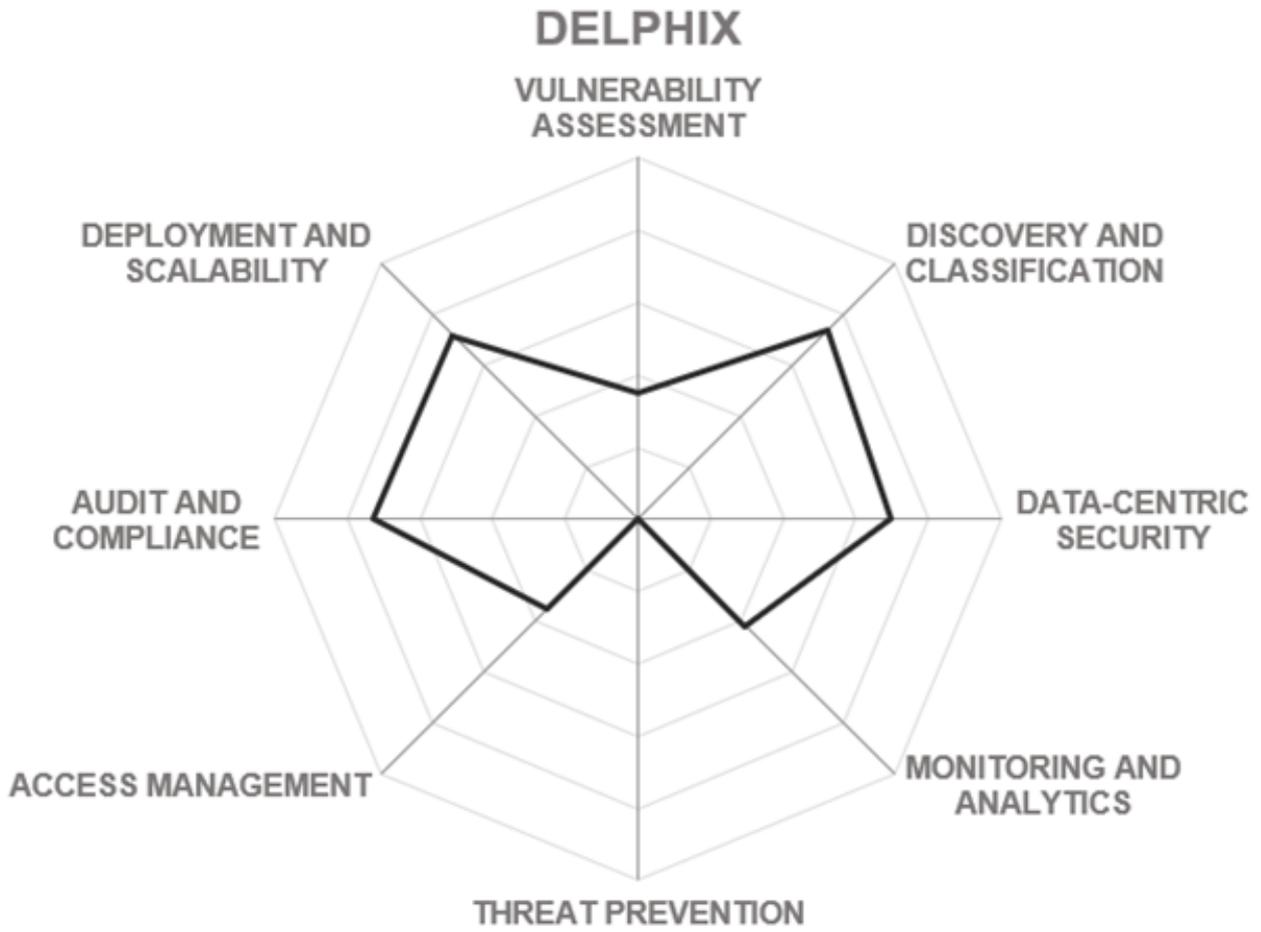
Security	● ● ● ● ○
Functionality	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

Strengths

- 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.
- Fully supports self-service workflows for data consumers.
- Preconfigured for GDPR compliance.

Challenges

- Data protection is not the core focus of the solution.
- Additional storage must be provisioned separately.
- Limited monitoring and analytics functions.



5.6 IBM Security Guardium

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. With over 100 years of history, IBM has evolved from a computing hardware manufacturer towards offering a broad range of software solutions and infrastructure, hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, and information security.

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.

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.

IBM Cloud Pak for Data, the company's modern, cloud-native integrated data management platform, now supports direct integration with Guardium to audit sensitive data in any assets managed by the solution.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●



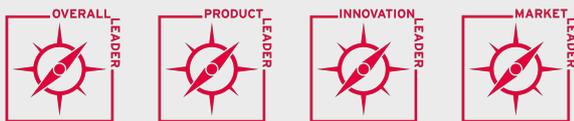
Strengths

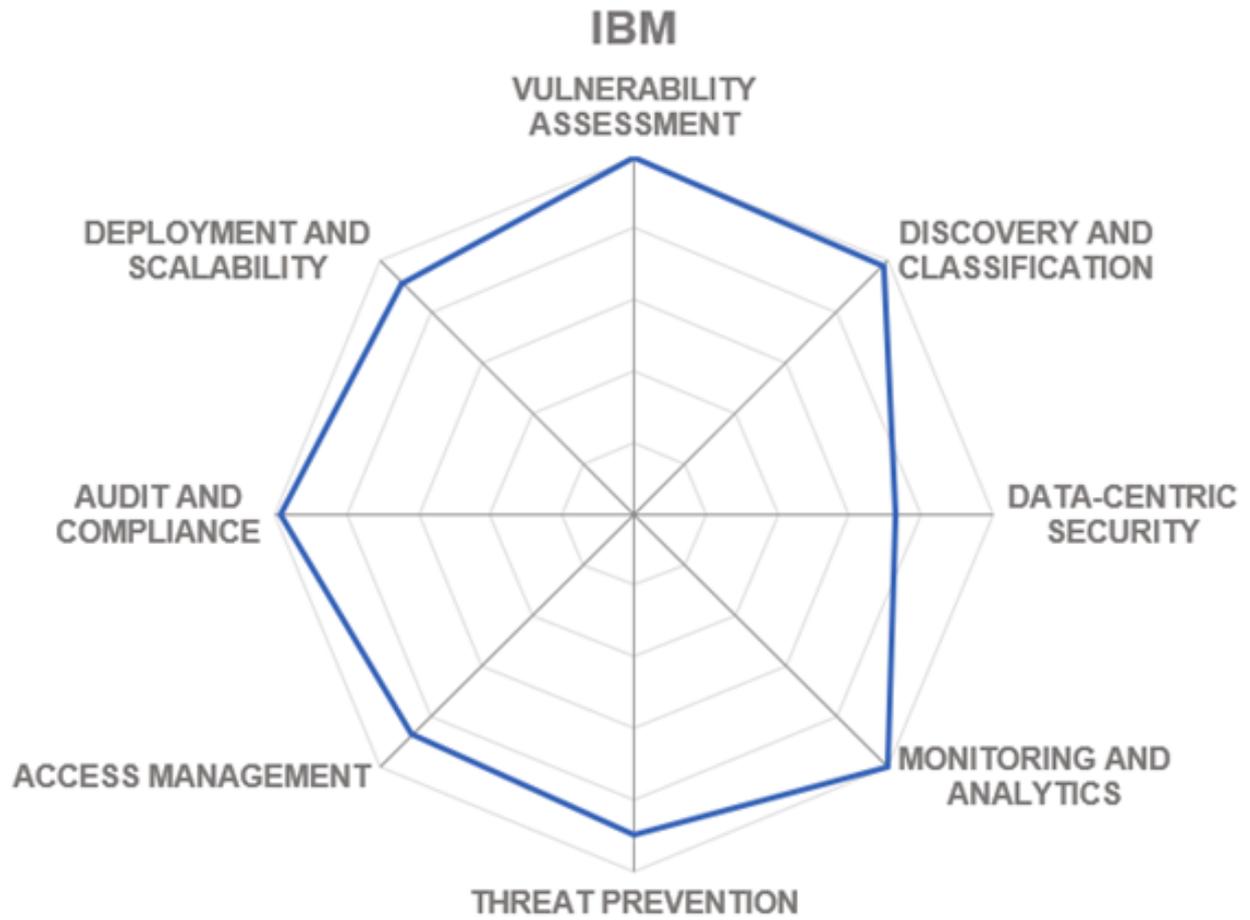
- Full range of security capabilities for structured and unstructured data.
- Support for hybrid multi-cloud environments.
- Advanced Big Data and Cognitive Analytics.
- Integrated ecosystem with IBM's and 3rd party security, identity, and analytics products.
- Massive network of technology partners and resellers.

Challenges

- Setup and operations may be complicated for some customers.
- Data protection capabilities based on 3rd party OEM technology.
- Not quite affordable for smaller organizations.

Leader in





5.7 Imperva Security Platform

Imperva is an American cybersecurity solution company headquartered in San Mateo, California. Since 2002, the company is primarily known for its web application firewall solutions, but from the very start, Imperva's portfolio included 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.

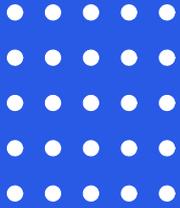
Although Imperva is primarily known as a leading developer of web application security solutions and not immediately recognized as a database security vendor, the company's been focusing on data protection for years: in fact, its motto has long been protecting data and all paths to it.

After the acquisition by Thoma Bravo, a strategic direction for the company has been incorporating all existing products into a single integrated Security platform. Combining data discovery and classification, data monitoring and protection, data risk analytics, database vulnerability assessment, as well as sensitive data masking, the platform addresses nearly all phases of the information protection lifecycle, lacking only in support for encryption and tokenization.

Last year's report has already mentioned Cloud Data Security, a new SaaS-based offering that extends discovery, classification, and analytics capabilities to database assets in the cloud. However, the biggest expansion of Imperva's platform was brought by the recent acquisition of jSonar, creators of the highly innovative agentless security analytics platform designed to be database-agnostic and easily extensible to any kind of structured or unstructured data source. This technology allows Imperva to add support for hundreds of various data stores and environments (on-prem or cloud-native), incorporate new behavior analytics functions, and add database-specific security orchestration (SOAR) into its existing platform.

Delivering on the motto "Protecting data and all paths to it", the company is incorporating all its products into a unified solution that combines data protection, application security, and web and API security. This enables such capabilities as user-to-data tracking that provides full context into transactions that start from the edge via the app to a data source or API data tracking that detects data leaks via APIs.

Security
Functionality
Interoperability
Usability
Deployment



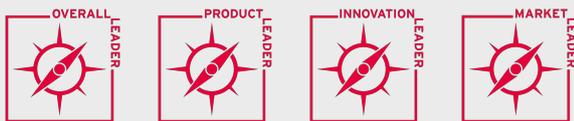
Strengths

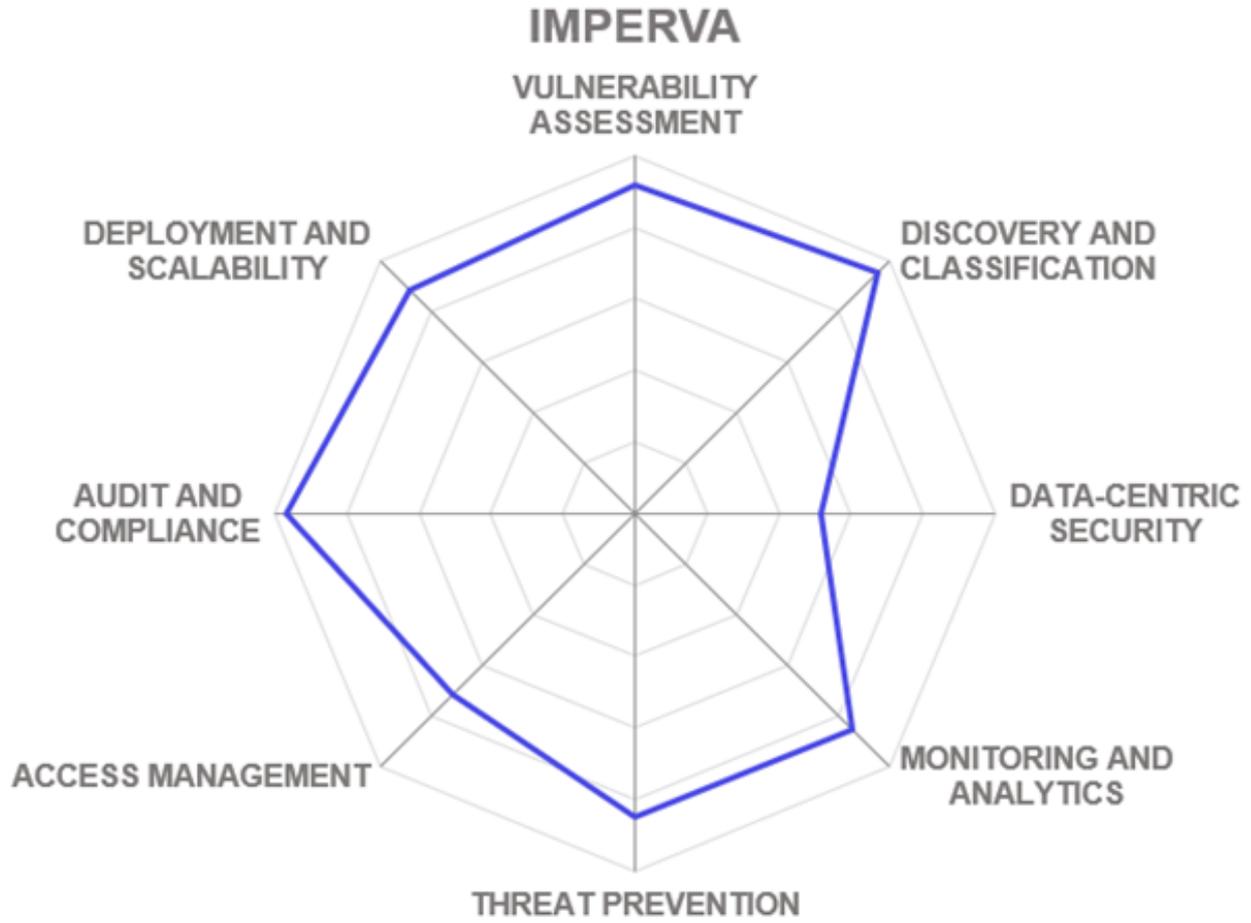
- Integrated platform approach to data protection.
- Nearly full coverage of data protection lifecycle.
- Advanced security intelligence and behavior analytics.
- Strong focus on cloud data protection.
- Extremely broad support of heterogeneous data sources.

Challenges

- Limited visibility in the data security market, especially outside of North America.
- Advanced data protection functionality (encryption, tokenization) available through integrations only.
- SaaS offering not yet available for enterprise customers.

Leader in





5.8 Microsoft Azure

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. Microsoft is the world's largest software vendor and one of the top corporations by market capitalization. The company is also one of the leading cloud service providers, operating the Microsoft Azure cloud platform since 2010.

Microsoft Azure offers a broad portfolio of fully managed database engines for various usage scenarios, including a family of Microsoft's own Azure SQL databases that help customers migrate from their on-premises Microsoft SQL Server databases to the cloud at their own pace. The company offers a choice of hosting SQL workloads on Azure Virtual Machines to maintain full compatibility, modernize existing applications for the cloud with Azure SQL Managed Instances, or become fully cloud-native with serverless Azure SQL Database.

To protect databases in the Azure cloud, Microsoft offers a multilayered approach comprising network security, role-based access management and fine-grained authorization, advanced threat protection, and data encryption and masking. An innovative Always Encrypted feature ensures that sensitive data is only decrypted for immediate processing within applications, thus preventing DB administrators from ever getting access to it. An additional level of security is provided by confidential computing within secure enclaves that act as isolated protected environments for manipulating sensitive data.

Vulnerability assessment, data discovery and classification functions provide additional data feeds for Microsoft's powerful security analytics platform that concentrates the immense amounts of security telemetry collected from endpoints, cloud services, and the Azure Active Directory, providing customers with unified insights into security and compliance postures across their whole enterprises.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○



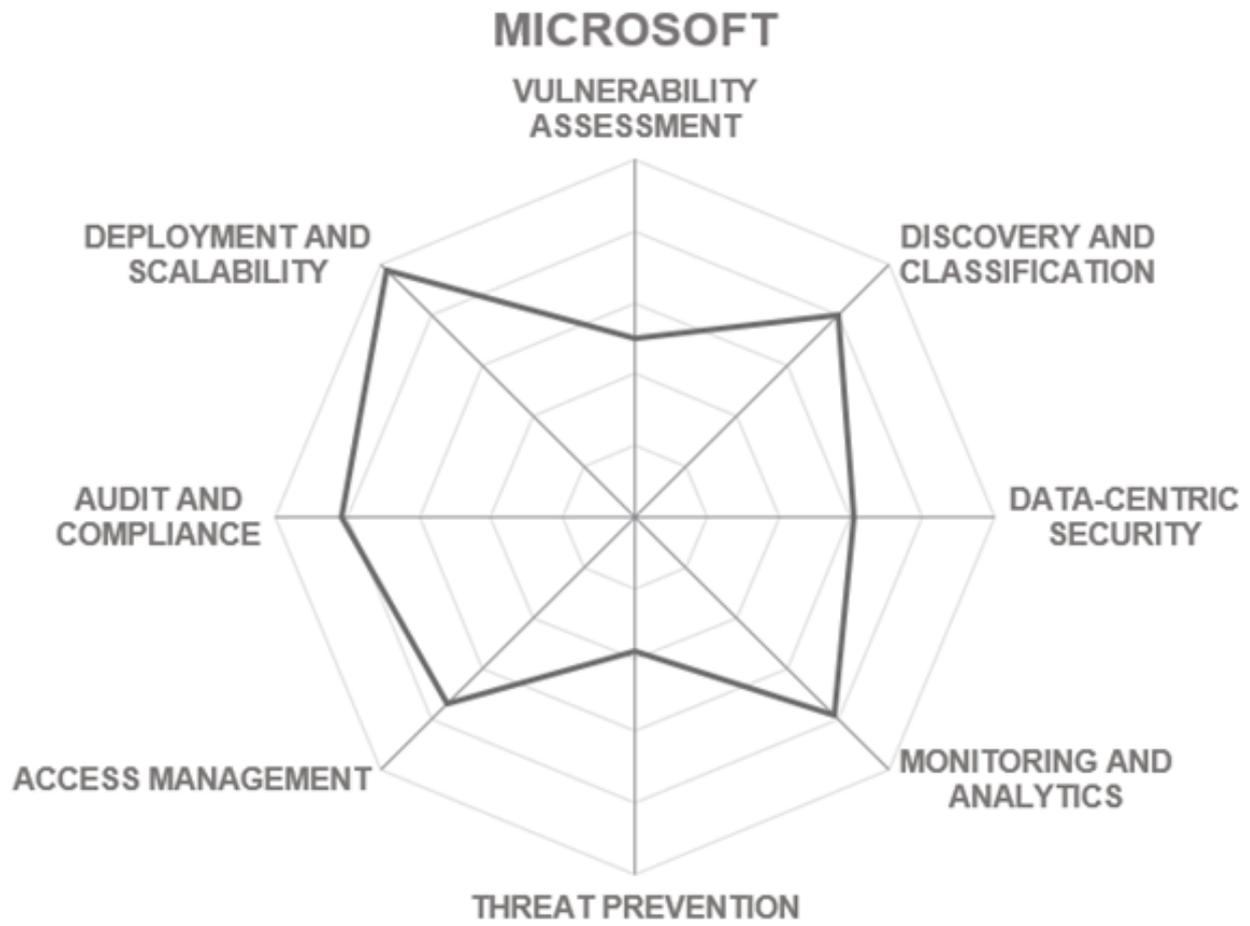
Strengths

- Strong expertise both in database development and cloud platforms.
- Capabilities available for nearly all phases of information protection lifecycle.
- Innovative secure enclave technology for the highest level of isolation.
- Powerful access management and security analytics in Azure cloud.

Challenges

- Most functions are only available in the Azure cloud.
- Protection capabilities vary substantially between supported databases.
- Data discovery and classification not yet in production.

Leader in



5.9 Oracle Autonomous Database Cloud

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.

The breadth of the company's database security portfolio is impressive: with multiple protection and detection products and 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 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.

In 2020, the company has expanded its autonomous offering by introducing new flavors of Autonomous Databases (such as JSON) as well as additional on-prem and cloud-based security services like Data Guard for disaster protection. Perhaps the most notable addition is the Data Safe service for comprehensive database risk assessment, including configuration drift detection, user risk assessment, activity audit, sensitive data discovery and static masking. Besides, Oracle now offers full feature parity for the Autonomous Database both in the cloud and on-premises (including Cloud@Customer managed private cloud services).

It should be noted however 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.



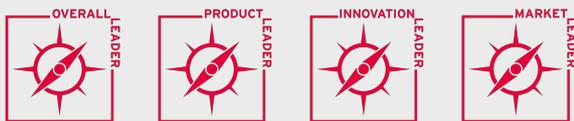
Strengths

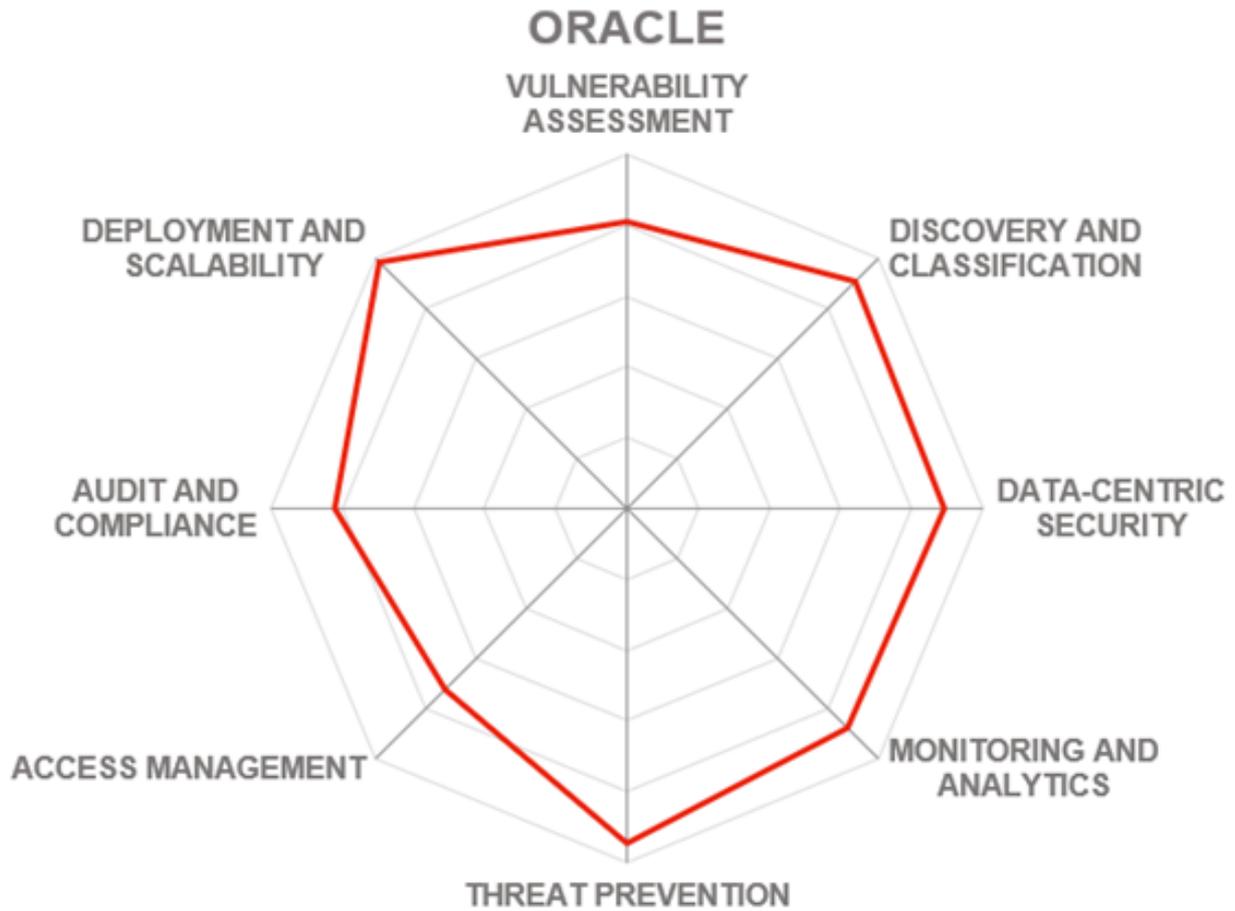
- Autonomous cloud database platform eliminating human administrative access.
- Security capabilities integrated directly into the database core.
- Broad range of tools and services for the whole information protection lifecycle.
- Secure cloud infrastructure adds another layer of protection.
- Comprehensive database and data risk assessment.

Challenges

- Most security tools only support Oracle databases.
- Big Data and NoSQL products are not yet integrated with RDBMS security solutions.
- DBaaS market segment presence still relatively small but growing.

Leader in





5.10 SecuPi Platform

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”.

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 major development platforms like Java or .NET instead of numerous distinct data source types. SecuPi provides exact same column-level encryption or tokenization but completely transparent to the data layer or the application layer for a broad range of databases, big data platforms and other semi-structured data stores, with no code changes or additional API calls needed for existing applications.

Also, 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.

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.

Fine-grained PBAC/ABAC combined with data protection options, 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.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●



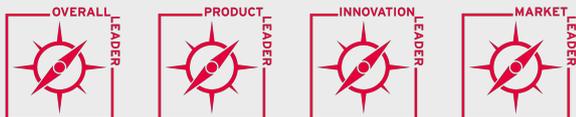
Strengths

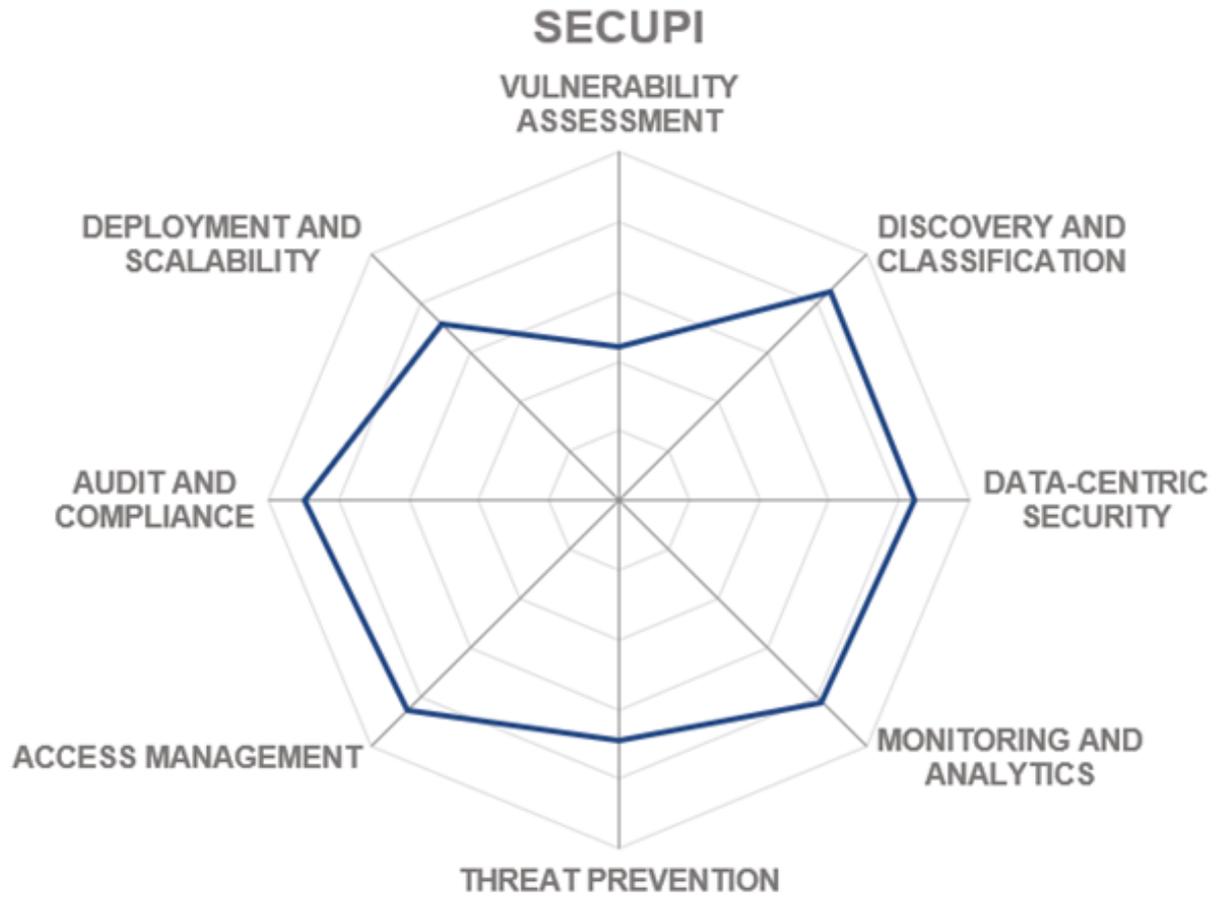
- Integrated data protection and privacy. platform with a strong focus on GDPR/CPRA
- Application-level protection overlays simplify deployment and management.
- User identity context for more fine-grained policies and monitoring.
- Broad support for big data and EDW platforms.

Challenges

- Architecture potentially limits support of less popular or legacy platforms.
- Limited focus on database infrastructure assessment or protection.
- Small market presence compared to competitors.

Leader in





5.11 Thales CipherTrust Data Security Platform

Thales Cloud Protection and Licensing (CPL) is a business line in Thales Group with over 40 years of experience in information security. The company is a veteran player in such areas as hardware security modules (HSM), data encryption, key management, PKI, Identity and Access Management and Software Licensing. Thales Group is an international company headquartered in Paris, France, which provides solutions and services for defense, aerospace, and transportation markets. In 2019, Thales has completed the acquisition of Gemalto, incorporating the technologies of Gemalto and SafeNet, its former major competitors in the data protection market.

Since mid-2019, Thales has been undergoing a reorganization of its internal business structure and consolidation of its SafeNet and Vormetric data protection portfolios, focusing on eliminating duplicate functionality from formerly competing products and integrating all available components into its new CipherTrust Data Security Platform.

The CipherTrust Data Security Platform now provides a full range of data-centric security capabilities, including data discovery and classification, transparent encryption, database and application data protection, data masking, tokenization, access controls, enterprise key management, and cloud key management unified from a single management interface.

Even though the solution focuses primarily on data discovery and data protection through key management, encryption and masking, its unified, ubiquitous approach across all available IT environments enables multiple business-focused use cases beyond just compliance, including reduction of data security complexity, accelerating cloud migrations, and reducing data exposure risks significantly across whole enterprises.

Thales has the broadest ecosystem of partners, and therefore will meet the largest set of use cases. Its new data discovery and classification product is an important addition to the platform. However, their leadership remains with their transparent encryption solution which works on premises, in private and public cloud environments. It supports privileged user access control, Live Data Transformation, is the only encryption vendor with SAP HANA support, works across traditional database, Big Data, and Teradata environments.

Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●



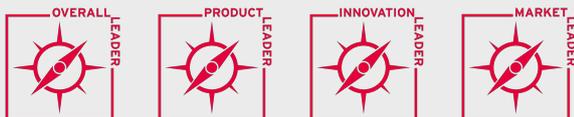
Strengths

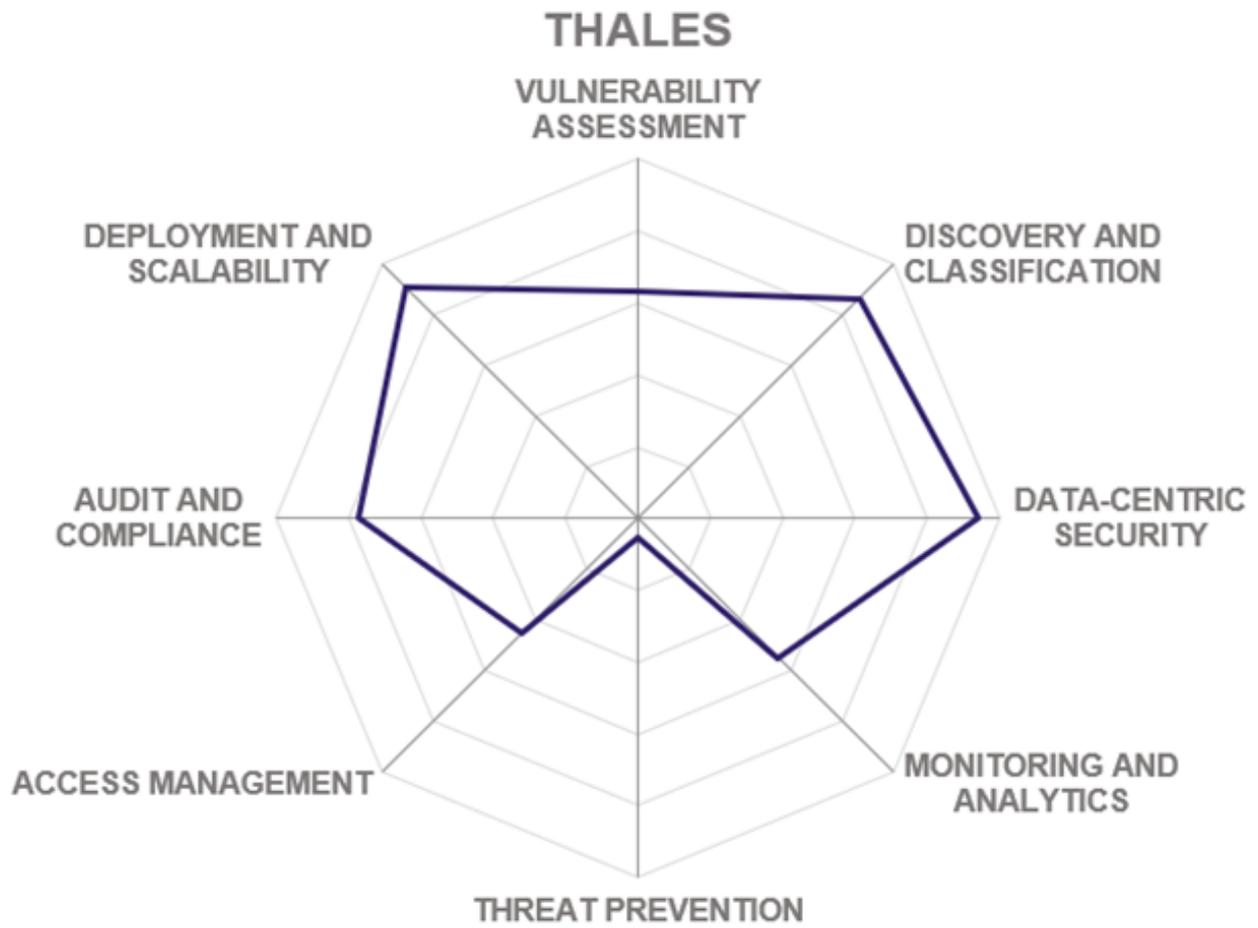
- Comprehensive data discovery and classification, transparent encryption, tokenization, access control and masking capabilities.
- Broadest enterprise key management support including KMIP, TDE, Always Encrypted, and Cloud Key Management
- High-performance thanks to hardware encryption support.
- Centralized management across all environments, even 3rd party products
- Standard APIs for adding encryption support to existing applications.

Challenges

- No threat prevention capabilities included.
- Application-level integrations not transparent, require changes to applications.

Leader in





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 in this chapter. 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 software company headquartered in Fremont, California. 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 DB CyberTech

DB CyberTech is a database security vendor headquartered in San Diego, California. 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.

6.3 IDERA Software

IDERA Software is a database management vendor based in Houston, Texas. Since 2003, the company produces a range of database lifecycle management solutions for DBAs and IT operations teams, including tools for designing databases and data models, monitoring database performance, and protecting database integrity.

IDERA's database protection portfolio includes tools for monitoring and auditing database user activities, managing access permissions, database backup and recovery, as well as centralized management and security across multiple database platforms. The solutions support both popular on-premises database engines and managed database services from major cloud providers.

6.4 Informatica

Informatica is a software development company founded in 1993 and headquartered in Redwood City, California. The company's Intelligent Data Platform is a complete, modular, AI-powered solution for cloud data management and data integration. Data Privacy Management, part of Informatica's portfolio, is a data governance solution that is aimed at bringing together users, processes, and policies across an enterprise and its partners to ensure privacy-compliant and trusted access to sensitive data and to enable the automation of key sensitive data and risk management tasks.

Data Privacy Management provides sensitive data risk management and mitigation tools in a single product with integrations with Informatica's flagship data masking products as well as some third-party data protection products and security information systems. This makes it a strong candidate for any organization looking to improve and customize their risk management capabilities.

6.5 McAfee

McAfee is a veteran American computer security vendor headquartered in Santa Clara, California. Founded in 1987, the company has a long history of 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 several 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.

6.6 Mentis Inc.

MENTIS is a 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 can 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.

6.7 Mirco 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 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.

6.8 Protegrity

Protegrity is a privately held software vendor from Stamford, Connecticut. 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, Illinois. 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 Related Research

[Leadership Compass: Database and Big Data Security – 79015](#)
[Leadership Compass: Enterprise Databases in the Cloud – 70309](#)
[Advisory Note: Database Governance – 70102](#)
[Leadership Brief: Introduction to the Information Protection Life Cycle and Framework – 80370](#)
[Leadership Brief: Data Security and Governance \(DSG\) for Big Data and BI Environments – 80109](#)
[Snapshot: IBM Security 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](#)
[Executive View: Informatica Data Privacy Management – 80276](#)

Methodology

About KuppingerCole's Leadership Compass

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 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.

Types of Leadership

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders:** Product Leaders identify the leading-edge products in the 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 in 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 leadership type, 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 a given 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.

Product rating

KuppingerCole as an analyst company regularly conducts 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 Analysts IT Model. 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 a vendor deals with them.

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.

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.

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 lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

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

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 market position or financial strength, indicating that vendors are very small and have a very low number of customers.

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 in 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 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.

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 chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

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

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

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

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

Figure 5: The Market / Product Matrix

Figure 6: The Product/Innovation Matrix

Figure 7: The Innovation/Market Matrix

Copyright

©2020 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks[™] or registered[®] trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support 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 back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

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