KuppingerCole Report

LEADERSHIP COMPASS

by Alexei Balaganski | March 2017

Database Security

Database security is a broad section of information security that concerns itself with protecting databases against compromises of their integrity, confidentiality and availability. It 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.

by **Alexei Balaganski**
ab@kuppingercole.com
March 2017

Leadership Compass
Database Security
By KuppingerCole

KuppingerCole Leadership Compass
Database Security
Report No.: **70970**

Content

Content Tables

Table of Figures

Related Research

Leadership Compass: Enterprise Key and Certificate Management – 70961

Advisory Note: Database Governance – 70102

Executive View: Axiomatics – Beyond Database Security – 71270

Vendor Report: SafeNet – 70876

Snapshot: GreenSQL Unified Database Security – 70588

Snapshot: IBM InfoSphere Guardium V 9.0 – 70632

Executive View: Oracle Database Vault – 70899

Executive View: Oracle Audit Vault and Database Firewall – 70890

Snapshot: Vormetric Data Security – 70634

1 Management Summary

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

Among security risks databases are potentially exposed to are the following:

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

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

In this Leadership Compass, however, we are focusing on a relatively narrow segment of database security solutions to avoid comparing functionally distinct products and to exclude market segments already covered in other KuppingerCole's reports.

First and foremost, we are focusing primarily on security solutions for protecting traditional relational database management systems (RDBMS), which are still by far the most widespread type of databases used by enterprises; however, solutions that extend their protection to NoSQL databases as well are going to be rated higher. Secondly, we are not explicitly covering various general aspects of network or physical server security, identity and access management or other areas of information security not specific for databases, although providing these features or offering integrations with other security products may influence our ratings.

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

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

Another crucial area to consider is development of applications based on the Security and Privacy by Design principles, which are soon going to become a legal obligation under the EU's upcoming General Data Protection Regulation (GDPR). Database 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.

These are the key functional areas of database security solutions we are looking for in this rating:

- **Vulnerability assessment** – this includes not just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations and, last but not least, the means for assessing and mitigating these risks.

- **Data discovery and classification** – although classification alone does not provide any protection, it serves as a crucial first step in defining proper security policies for different data depending on their criticality and compliance requirements.

- **Data protection** – this includes data encryption at rest and in transit, static and dynamic data masking and other technologies for protecting data integrity and confidentiality.

- **Monitoring and analytics** – this includes monitoring of database performance characteristics, as well as complete visibility in all access and administrative actions for each instance, including alerting and reporting functions. On top of that, advanced real-time analytics, anomaly detection and SIEM integration can be provided.

- **Threat prevention** – this includes various methods of protection from cyber-attacks such as denial-of-service or SQL injection, mitigation of unpatched vulnerabilities and other database-specific security measures.

- **Access Management** – this includes not just basic access controls to database instances, but more sophisticated dynamic policy-based access management, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.

- **Audit and Compliance** – this includes advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, as well as tools supporting forensic analysis and compliance audits.

- **Performance and Scalability** – although not a security feature per se, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead and to support deployments in high availability configurations. For certain critical applications, passive monitoring may still be the only viable option.

Below you will find a short summary of our findings including the diagrams showing vendors' positions on KuppingerCole Leadership scales.

1.1 Overall Leadership

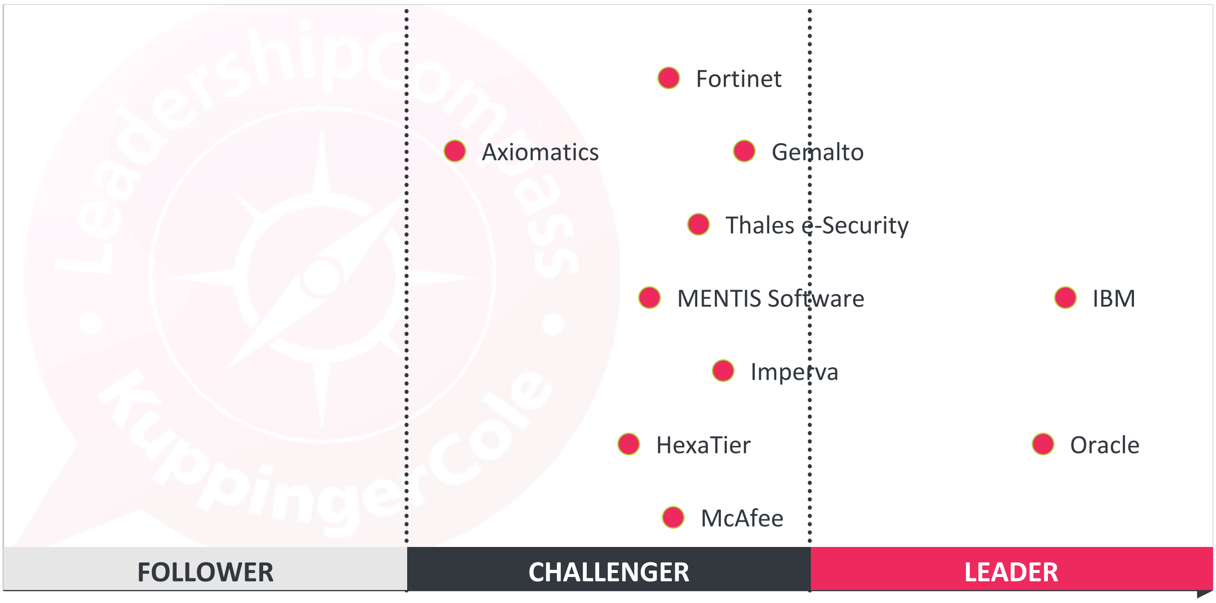


Figure 1: Overall Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

In the Overall Leadership rating, we find IBM and Oracle among the Leaders, which is completely unsurprising, considering both companies' global market presence, broad ranges of database security solutions and impressive financial strengths. However, the fact that IBM's solutions are database-agnostic, while a half of Oracle's portfolio only focuses on Oracle databases has influenced KuppingerCole's decision to position IBM as the overall leader in Database Security.

The rest of the vendors are populating the Challengers segment. Lacking the combination of exceptionally strong market and product leadership, they are hanging somewhat behind the leaders, but still deliver mature solutions exceling in certain functional areas. The segment includes both large veteran players with massive customer reach like Imperva, Gemalto, Thales e-Security, McAfee and Fortinet and smaller but impressively innovative companies like HexaTier, MENTIS Software and Axiomatics.

There are no Followers in this rating, indicating overall maturity of the vendors representing the market in our Leadership Compass. Still, there is a number of smaller companies or startups with innovative products entering the market, worth mentioning outside of our rating. These companies are briefly covered in the chapter 14 "Vendors to watch".

1.2 Product Leadership

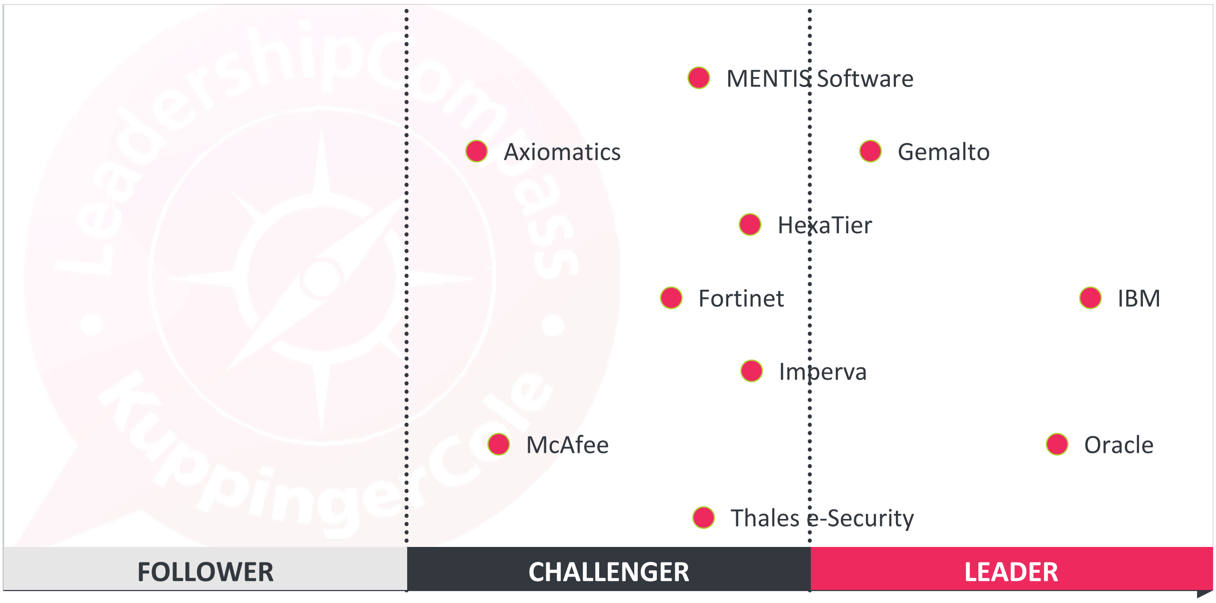


Figure 2: Product Leaders in the Database Security segment [Note: There is only a horizontal axis; Vendors to the right are positioned better]

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

Only the largest players in the market, which offer a wide range of products covering different aspects of database security can be found among the leaders. IBM Security Guardium, the company's data security platform provides a full range of data discovery, protection and 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. With the strong focus on Oracle databases only that has led us to reduce the company's overall rating somewhat, Oracle is positioned on the close second place. Somewhat behind them we find Gemalto with their unified data protection suite backed by a massive technology ecosystem.

Other vendors with their robust, but less functionally broad solutions covering at least several major functional areas of database security are populating the Challenger segment. Leading the group are Imperva with their portfolio combining strong database protection and monitoring with advanced security analytics, HexaTier with an innovative cloud-ready integrated database security suite, Thales e-Security with their recently acquired Vormetric encryption, data masking and key management platform and Fortinet with hardware appliances for database security, vulnerability management and compliance.

Somewhat behind we find several vendors with strong focus in single functional area only, namely McAfee with a portfolio strongly focusing on database activity monitoring, vulnerability management and virtual patching and Axiomatics – a leader in dynamic access control with a specialized ABAC solution for databases.

There are no Followers in our product rating.

1.3 Market Leadership

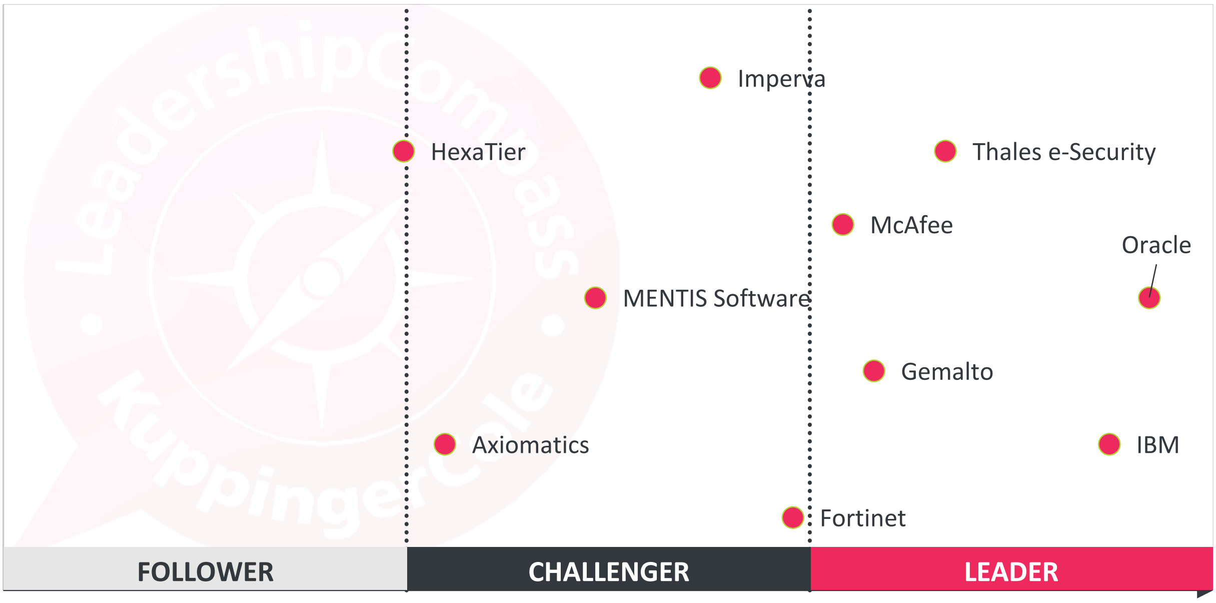


Figure 3: Market Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

KuppingerCole's Market Leadership rating is based on the number of customers, strength of partner networks, and global market presence.

Among the market leaders, we can observe Oracle, IBM, Thales e-Security (with their Vormetric portfolio), Gemalto (with SafeNet Data Protection suite) and McAfee. All these companies are veteran players in the IT market with massive global presence, large partner networks and impressive numbers of customers.

Other vendors are positioned in the Challenger segment. Leading here are Fortinet, which barely missed the leaders segment, and Imperva, whose recent financial results were not particularly impressive.

Somewhat behind we find MENTIS Software, which, despite offering an innovative and well-integrated suite of database security product, has not yet been able to win enough customers to compete with market leaders.

Axiomatics, despite being one of the leading providers of general-purpose access control solutions, is only just entering the database security market with their Data Access Filter with a handful of active deployments. We expect this number to grow in the near future.

HexaTier just barely avoids slipping into the Followers segment of the rating because several factors like limited presence outside of the US market and the size of their partner ecosystem. Given their unique focus on protecting Databases-as-a-Service in the cloud, the company desperately needs to have more partnerships with cloud service providers. However, the recent news about HexaTier's acquisition by the Chinese technology giant Huawei indicate that the company's market presence may dramatically increase quite soon.

1.4 Innovation Leadership

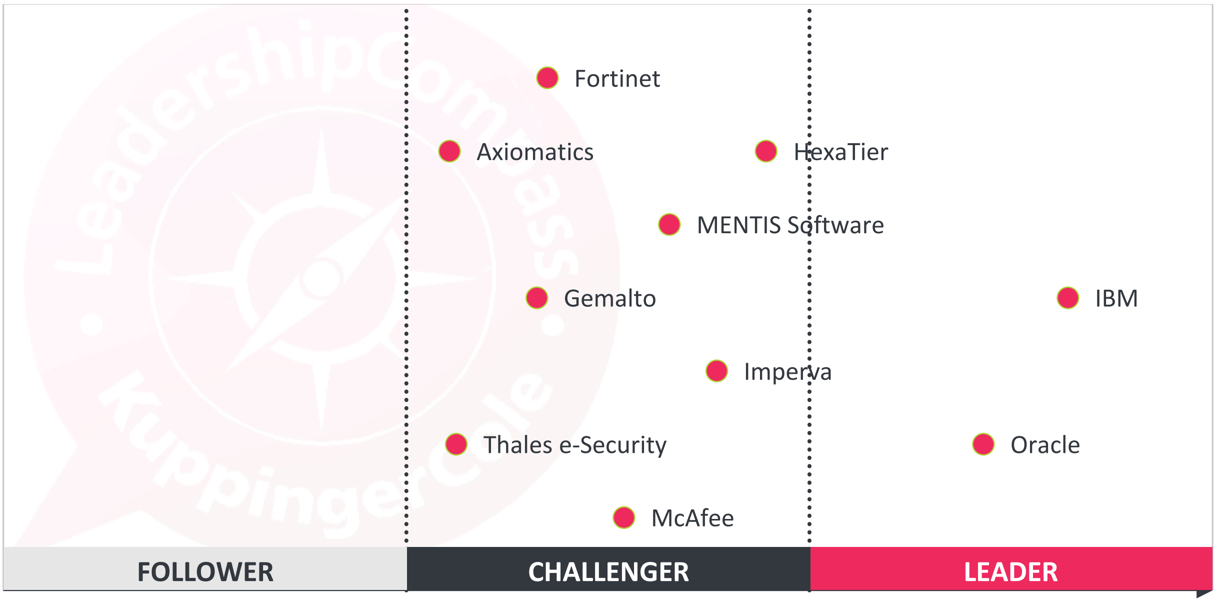


Figure 4: Innovation Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

Finally, there is the Innovation Leadership rating, where we are looking specifically at the vendor's ability to deliver new ideas or emerging technologies for a particular market segment. Innovation leaders are shaping the future of the market by coming up with innovative features that will eventually become standard for all their competitors.

In this rating, we again observe IBM and Oracle in the Leaders segment, reflecting both companies' sheer development resources which allow them to constantly deliver new features based on innovative technologies. Worth noting here is IBM's strong focus on advanced analytics and Oracle's unique hybrid cloud management and privileged user control capabilities.

Most other vendors can be found among the Challengers. HexaTier's unique focus on protecting cloud databases with a unified easy to use solution and Imperva's unified security intelligence platform for behavior and endpoint analytics warrant their higher ratings.

Following them are MENTIS Software with their a la carte approach towards designing a data security suite, Fortinet's hardware appliances with impressive out-of-the-box capabilities, McAfee with a real-time non-intrusive architecture for database protection and Gemalto with its unified data protection suite.

Thales e-Security with their innovative application and cloud encryption capabilities and Axiomatics with a unique application of ABAC to database access management conclude the Challengers list.

Again, there are no Followers in our innovation rating.

Please note that these ratings provide just a high-level comparison of the products we have tested. Depending on your specific requirements, vendors generally not recognized as the Leaders may still be the best choice. We recommend that you always perform a thorough product selection and evaluation process for your specific projects.

2 Methodology

KuppingerCole Leadership Compass is a tool that provides a synopsis of a particular IT market segment and identifies the leaders in this segment. It is the compass that assists you in identifying the vendors and products that you should consider when making the best solution decisions for your company.

It is recommended that the information provided in this Leadership Compass be augmented with local analysis. Customers should always define their specific requirements and analyse in greater detail solutions to those needs. Picking a vendor for a specific customer scenario is beyond the scope of this report A more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features is always required. KuppingerCole Advisory Services provide such customer-specific assessments.

We look at four types of leaders:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products largely deliver what we expect from products in that market segment. They are mature.
- **Market Leaders**: Market Leaders are vendors that 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 that are driving new ideas, devices, or methods in the market segment. They provide several of the most innovative and forthcoming features we hope to see in the this segment.
- **Overall Leaders**: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

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

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in specific 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 best choice for specific use cases and customer requirements but are of limited value in other situations.

In addition, we have defined a series of tables and charts which

- **Provide individual correlations,** for instance, between the rating for innovation and the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path from established vendors, but also established vendors which no longer lead in innovation. These tables provide additional viewpoints on the vendors and should be considered when picking vendors for RFIs (Request for Information), long lists, etc. in the vendor/product selection process.
- **Add additional views** by comparing the product rating to other feature areas. This is important because not all customers need the same product, depending on their current situation and specific requirements. Based on these additional matrices, customers can evaluate which vendor fits best to their current needs but also is promising regarding its overall capabilities. The latter is important given that a product not only should address a pressing challenge but become a sustainable solution. It is a question of helping now, but also of being good enough for the next steps and future requirements. Here these additional matrices come into play.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view of vendors and their products.

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

3 Product Rating

KuppingerCole as an analyst company regularly performs evaluations of products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview of our perception of the products/services 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/services:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security – the security measure indicates the degree of security features incorporated within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (**Scenario: Understanding Identity and Access Management - 70129**). It provides a mature approach to security assessment and a model for product security; a key requirement for evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization are identified as weaknesses in security. Security vulnerabilities to known hacks are also rated as weaknesses. The security rating is based on the severity of such weaknesses and the way in which the product vendor accommodates them.

Functionality – this is measured in relation to three factors:

- vendor promises
- status of the industry
- expected functionality

In mature market segments, the status of the industry and KuppingerCole expectations 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 the market segment. When vendors fail to meet customer's expectations in a market segment, lower ratings will result, unless a product provides additional features, or uses another approach, that provides additional customer benefits.

Integration — integration is measured by the degree to which a vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent in which products interoperate. The level of integration a product exhibits is uncovered by analyzing the configuration effort required to deploy, operate and manage the product. The degree of integration is then directly related to this effort. For example: if each product maintains its own identity record for each user, it is not well integrated; if products use multiple databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single account allows the administrator to manage all aspects of the product suite, then a better level of integration has been achieved.

Interoperability — interoperability refers 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 equipped their products or technologies to work with other products or standards that are important in the market segment. Extensibility is a component of this and measured by the degree to which a vendor allows its technologies and products to be extended for wider use by its customers. Extensibility is given equal status to interoperability 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; the future is one in which programmatic access through a well-documented and secure set of APIs is expected.

Usability — accessibility refers to the degree to which the vendor enables accessibility to its technologies and products by various user groups. Typically, at least two aspects of usability must be addressed – the end user view and the administrator view. While good documentation is the basis for adequate accessibility, we have strong expectations regarding well integrated user interfaces and a high degree of consistency across user interfaces, particularly across different products from a single vendor. We also expect vendors to follow common, established approaches to user interface design rather than creating their own UI conventions.

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

- **People Participation**—Human participation in systems at any level is the highest area of cost and causal factor of failure for any IT endeavor.
- **Level 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.
- **Level of Identity and Security Exposure to Failure**—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to increased manual intervention with its attendant mistakes and decreased customer satisfaction with breakdowns in their business processes. It also creates openings for malicious attacks and system failure.

When KuppingerCole evaluates a set of technologies or products from a vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of utmost importance because the lack of excellence in any or all of these areas will inevitably lead to identity and security shortcomings and poor infrastructure.

4 Vendor Rating

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

- Level of Innovation
- Market position
- Financial strength
- Ecosystem

Level of Innovation – this is measured as the capability to drive innovation in a direction which aligns with the direction of the particular market segment in question. Innovation has no value in 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 where applicable. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness. Innovativeness, despite being part of the vendor rating, looks at the innovativeness in the particular market segment analyzed in this KuppingerCole Leadership Compass.

Market position – measures the position of the vendor in the market or in relevant market segments. This is an average rating over all 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. Again, while being part of the vendor rating, market position evaluates the vendor's position in the particular market segment analyzed in this KuppingerCole Leadership Compass. Note: a very large vendor might not be a Market Leader in the particular market segment in question, but may enjoy a higher overall market position.

Financial strength – KuppingerCole doesn't consider size to be of value by itself but financial strength is an important factor for customers when selecting a solution. In general, publicly available financial information is an important factor for this rating. Companies which are venture-financed are rated lower because they are more likely to become an acquisition target, with potential risk for customers adopting their product as a solution.

Ecosystem – this dimension looks at the ecosystem of the vendor for the market segment covered in this Leadership Compass document. It focuses on the partner base of a vendor and the approach they have taken in acting as a "good citizen" in heterogeneous IT environments.

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.

5 Vendor Coverage

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

However, there might be vendors which don't appear in this document for various reasons:

- **Limited market visibility**: There might be vendors and products/services 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 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 report will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole report.

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

For this KuppingerCole Leadership Compass, we have identified a number of key vendors with mature solutions covering various aspects of database security and with a substantial market presence. In addition, smaller companies that offer innovative, but niche products, are listed in the chapter 14 of this report classified as "vendors to watch".

6 Market Segment

One of the biggest challenges modern enterprises are facing is the evolution towards connected businesses. To survive in the fiercely competitive environments, businesses strive to be as agile as possible, to continuously adopt new business models and establish new communication channels with their partners and customers. For more and more companies, digital data, not physical products or services, has become their most valuable asset or even the largest source of income.

Unfortunately, the infamous Digital Transformation does not only enable a whole range of business prospects, it also exposes the company's "crown jewels" to new security risks. Since those digital assets are nowadays often located somewhere in the cloud, with an increasing number of people and devices accessing them anywhere at any time, the traditional notion of security perimeter ceases to exist, and the data becomes even more vulnerable to new sophisticated cyberattacks.

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

Among security risks databases are potentially exposed to are the following:

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

In this Leadership Compass, we are focusing on a relatively narrow segment of database security solutions, namely on security solutions for protecting relational database management systems (RDBMS) from database-specific threats and risks. We are not focusing on 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.

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

These are the key functional areas of database security solutions we are looking for in this rating:

- **Vulnerability assessment** – this includes not just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations and, last but not least, the means for assessing and mitigating these risks.
- **Data discovery and classification** – although classification alone does not provide any protection, it serves as a crucial first step in defining proper security policies for different data depending on their criticality and compliance requirements.
- **Data protection** – this includes data encryption at rest and in transit, static and dynamic data masking and other technologies for protecting data integrity and confidentiality.
- **Monitoring and analytics** – this includes monitoring of database performance characteristics, as well as complete visibility in all access and administrative actions for each instance, including alerting and reporting functions. On top of that, advanced real-time analytics, anomaly detection and SIEM integration can be provided.
- **Threat prevention** – this includes various methods of protection from cyber-attacks such as denial-of-service or SQL injection, mitigation of unpatched vulnerabilities and other database-specific security measures.
- **Access Management** – this includes not just basic access controls to database instances, but more sophisticated dynamic policy-based access management, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.
- **Audit and Compliance** – this includes advanced auditing mechanisms beyond native capabilities, centralized auditing and reporting across multiple database environments, enforcing separation of duties, as well as tools supporting forensic analysis and compliance audits.
- **Performance and Scalability** – although not a security feature per se, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead and to support deployments in high availability configurations. For certain critical applications, passive monitoring may still be the only viable option.

7 Specific Features Analyzed

When evaluating the products, there are a number of specific elements we look at besides looking at the more general aspects of:

- Overall functionality
- Size of the company
- Number of customers
- Number of developers
- Partner ecosystem
- Licensing models
- Platform support

7.1 Vulnerability assessment

Here we consider how the product helps identify known security holes in database infrastructures. This isn't limited just to discovering known vulnerabilities in database products, but also providing complete visibility into complex database infrastructures, detecting misconfigurations and, last but not least, the means for assessing and mitigating these risks. So, we are looking for means for enforcing security best practices:

- Database infrastructure discovery;
- Vulnerability scanning and risk assessment;
- Identifying misconfigurations, excessive access rights and weak credentials;
- Vulnerability mitigation, such as virtual patching.

7.2 Data discovery and classification

Here we analyze how products are able to automatically identify sensitive information, classify it according to internal business requirements as well as country- and industry-specific compliance regulations. Although classification alone does not provide any protection, it serves as a crucial first step for defining proper security policies.

- Automated sensitive data discovery across whole infrastructures;
- Classification of data by business criticality and by compliance regulations;
- Management of security policies based on discovery results.

7.3 Data protection

This area covers various technologies for protecting data integrity and confidentiality both within the database, in transit and during information processing. These technologies include:

- Data encryption at rest;
- Data encryption in transit;
- Data tokenization, static and dynamic masking;
- Application encryption methods;
- Other methods of data integrity protection.

7.4 Monitoring and analytics

This includes 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.

- Activity monitoring for data access and administrative actions;
- Real-time analytics and anomaly detection;
- Real-time alerting and reporting;
- Integration with SIEM solutions.

7.5 Threat prevention

Here, we are looking at various methods of protection from cyber-attacks such as denial-of-service or SQL injection and other database-specific security measures:

- General cyber-threat prevention techniques like intrusion detection systems;
- Database-specific threat detection (for example, SQL injection);
- Protocol analysis to detect and prevent database exploits;
- Automated blocking of malicious requests;
- Connection controls to prevent denial of service.

7.6 Access Management

This includes not just basic access controls to database instances, but more sophisticated dynamic policy-based access management, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.

- Dynamic policy-based access management with additional contextual information;
- Identify real user identities behind shared or service accounts;
- Identifying and removing excessive user privileges;
- User behavior analytics, detection and blocking of suspicious user activities;

7.7 Audit and Compliance

This includes 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.

- Expand and improve native auditing capabilities;
- Centralized auditing across multiple database environments;
- Enforcing separation of duties;
- Forensic investigation support;
- Compliance reporting.

8 Market Leaders

Based on our evaluation we have identified several Leaders in the Database Security market segment. The Market Leaders are shown in the figure below.

We expect Market Leaders to be Leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered market Leaders. The same holds true for the vendor's partner ecosystem – without a global scale in the partner ecosystem, we don't rate a vendor as a Market Leader.

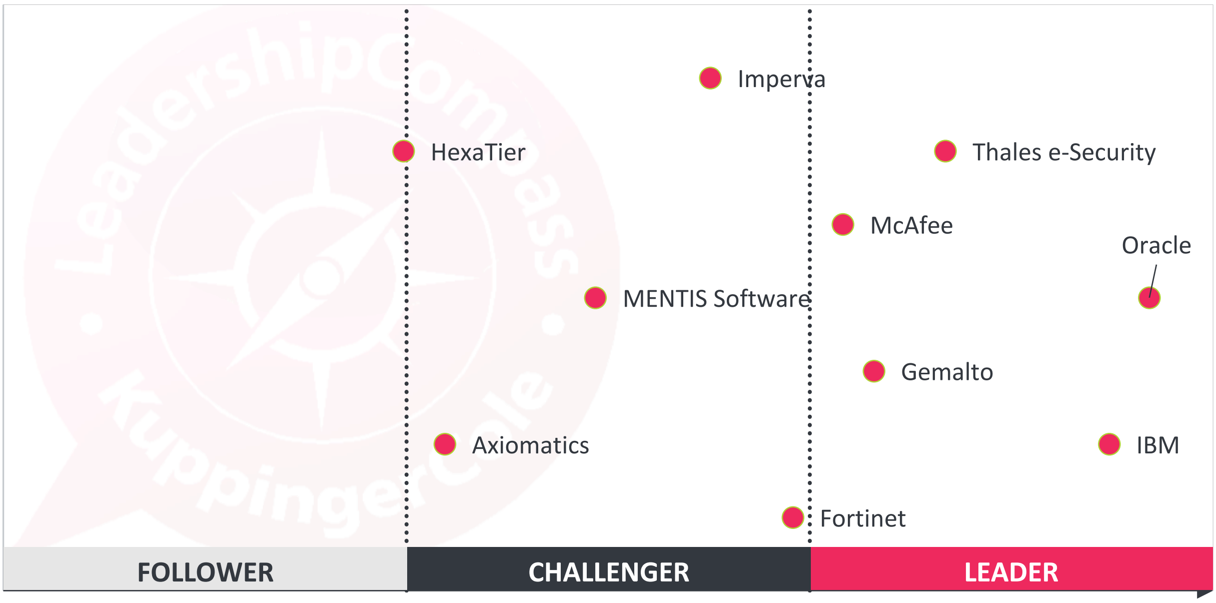


Figure 5: Market Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

Among the market leaders, we can observe Oracle, IBM, Thales e-Security (with their Vormetric portfolio), Gemalto (with SafeNet Data Protection suite) and McAfee. All these companies are veteran players in the IT market with massive global presence, large partner networks and impressive numbers of customers.

Other vendors are positioned in the Challenger segment. Leading here are Fortinet, which barely missed the leaders segment, and Imperva, whose recent financial results were not particularly impressive.

Somewhat behind we find MENTIS Software, which, despite offering an innovative and well-integrated suite of database security product, has not yet been able to win enough customers to compete with market leaders.

Axiomatics, despite being one of the leading providers of general-purpose access control solutions, is only just entering the database security market with their Data Access Filter with a handful of active deployments. We expect this number to grow in the near future.

HexaTier just barely avoids slipping into the Followers segment of the rating because several factors like limited presence outside of the US market and the size of their partner ecosystem. Given their unique focus on protecting Databases-as-a-Service in the cloud, the company desperately needs to have more partnerships with cloud service providers. However, the recent news about HexaTier's acquisition by the Chinese technology giant Huawei indicate that the company's market presence may dramatically increase quite soon.

Market Leaders (in alphabetical order):

- Gemalto
- IBM
- McAfee
- Oracle
- Thales e-Security

9 Product Leaders

The second view we provide is about Product Leadership. This view is mainly based on the analysis of product features and the overall capabilities of the various products.

The Product Leadership rating focuses on the functional strength and overall completeness of vendors' products. This rating shows a number of vendors with very similar ratings which indicates very strong competition in an evolving market.

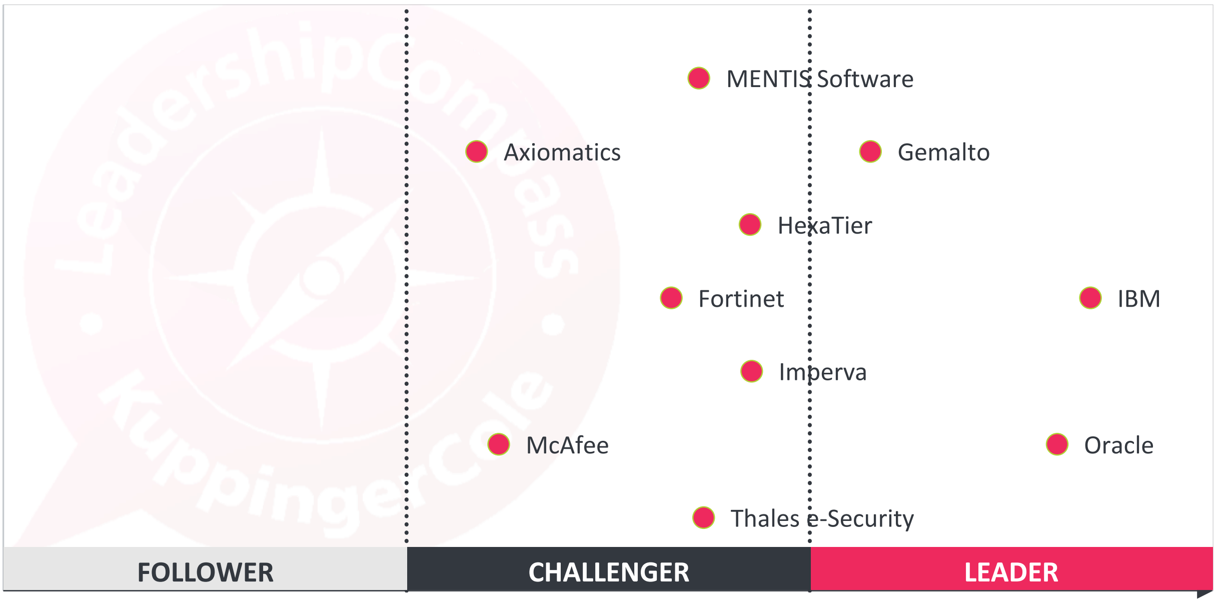


Figure 6: Product Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

Only the largest players in the market, which offer a wide range of products covering different aspects of database security, namely IBM and Oracle, can be found among the leaders. IBM Security Guardium, the company's data security platform provides a full range of data discovery, protection and 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 products and managed services for all aspects of database assessment, protection and monitoring. With the strong focus on Oracle databases only that has led us to reduce the company's overall rating somewhat, Oracle is positioned on the close second place. Somewhat behind them we find Gemalto with their unified data protection suite backed by a massive technology ecosystem.

Other vendors with their robust, but less functionally broad solutions covering at least several major functional areas of database security are populating the Challenger segment. Leading the group are Imperva with their portfolio combining strong database protection and monitoring with advanced security analytics, HexaTier with an innovative cloud-ready integrated database security suite, Thales e-Security with their recently acquired Vormetric encryption, data masking and key management platform and Fortinet with hardware appliances for database security, vulnerability management and compliance.

Somewhat behind we find several vendors with strong focus in single functional area only, namely Axiomatics – a leader in dynamic access control with a specialized ABAC solution for databases, and McAfee, with a portfolio strongly focusing on database activity monitoring, vulnerability management and virtual patching.

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

Again, when selecting a product, it is important to look at the specific features and map them to the customer requirements. There are examples where products which are not "feature Leaders" are nevertheless a better fit for specific customer scenarios.

Product Leaders (in alphabetical order):

- Gemalto
- IBM
- Oracle

10 Innovation Leaders

The third view we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what is required from vendors to continue to provide new functionality to meet their customers' needs. Hence an analysis of a vendor's record of innovation is often as important as the current features of their product/service.

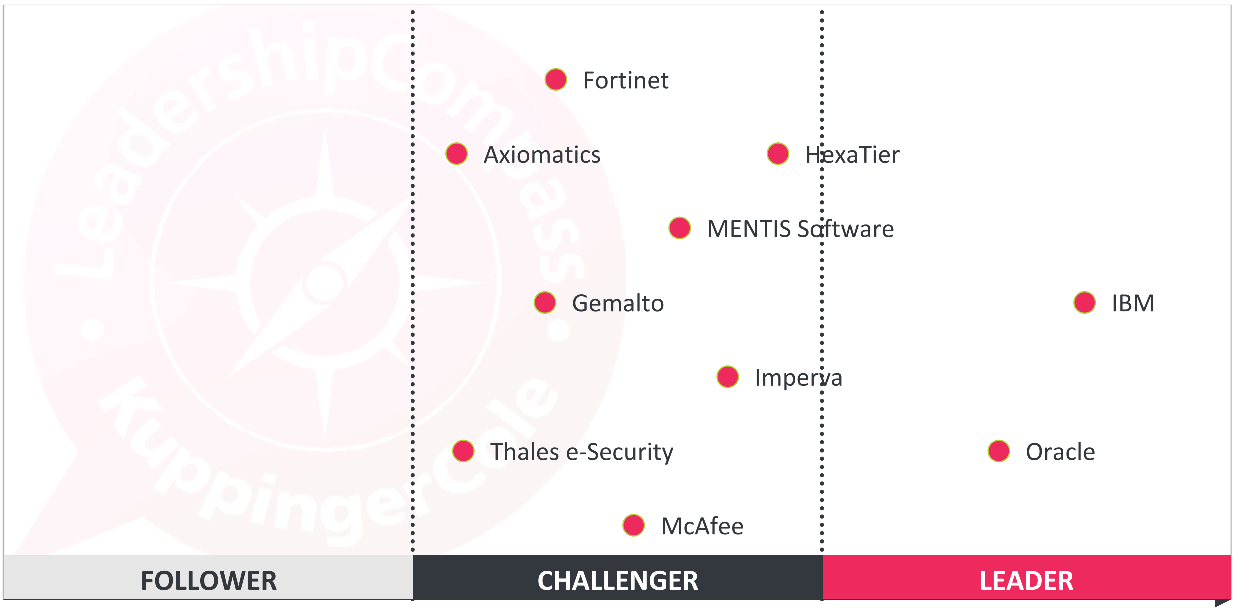


Figure 7: Innovation Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

In this rating, we again observe IBM and Oracle in the Leaders segment, reflecting both companies' sheer development resources which allow them to constantly deliver new features based on innovative technologies. Worth noting here is IBM's strong focus on advanced analytics and Oracle's unique hybrid cloud management and privileged user control capabilities.

Most other vendors can be found among the Challengers. HexaTier's unique focus on protecting cloud databases with a unified easy to use solution and Imperva's unified security intelligence platform for behavior and endpoint analytics warrant their higher ratings.

Following them are MENTIS Software with their a la carte approach towards designing a data security suite, Fortinet's hardware appliances with impressive out-of-the-box capabilities, McAfee with a real-time non-intrusive architecture for database protection and Gemalto with its unified data protection suite.

Thales e-Security with their innovative application and cloud encryption capabilities and Axiomatics with a unique application of ABAC to database access management conclude the Challengers list.

Innovation Leaders (in alphabetical order):

- IBM
- Oracle

11 Product Evaluation

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

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

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

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

Each vendor evaluation also includes a spider chart showing our assessment of the performance of the product evaluated against the 5 aspects described in chapter 7.

11.1 Axiomatics

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

Strengths/Opportunities	Weaknesses/Threats
● Database-agnostic approach ensures unified policy application across different databases ● 100% compliance with the XACML standard ● Shares the authorization model with other Axiomatics products for applications, APIs, etc.	● Very narrow functional focus compared to other products in the rating ● Just a few active customer deployments of the database security solution

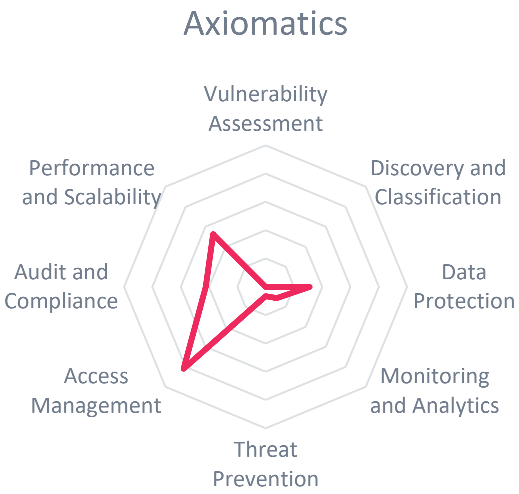
Table 1: Axiomatics major strengths and weaknesses

The company's flagship product is Axiomatics Policy Server, an enterprise-wide universal Attribute-Based Access Control (ABAC) solution. In the area of database security, the company offers **Axiomatics Data Access Filter MD**, a specialized ABAC solution for managing access to sensitive information in databases.

Implemented as an SQL proxy service, the solution provides policy-based access control defined in standard XACML, as well as dynamic data masking, filtering and activity monitoring transparently for multiple database types.

Security	positive
Functionality	weak
Integration	positive
Interoperability	positive
Usability	weak

Table 2: Axiomatics rating



The key features of the product include:

- Multiple database type support, including Microsoft SQL Server, Oracle, IBM DB2 and Teradata
- Dynamic context-aware authorization for data held in the databases
- Flexible access control to sensitive data based on real-time dynamic data filtering
- Dynamic data masking and filtering for financial, healthcare and other types of personal information
- Real-time data unmasking for authorized users (for example, transparent decryption)
- Centralized management of access policies across databases, applications and APIs

11.2 Fortinet

Fortinet is an American publicly traded cybersecurity company headquartered in Sunnyvale, California. Founded in 2000, the company is focusing primarily on network security solutions like firewalls, antimalware, intrusion prevention and web security. One of the largest network security vendors by revenue, Fortinet offers a broad range of specialized security gateways and appliances, which provide comprehensive cyberthreat protection with centralized management and reporting.

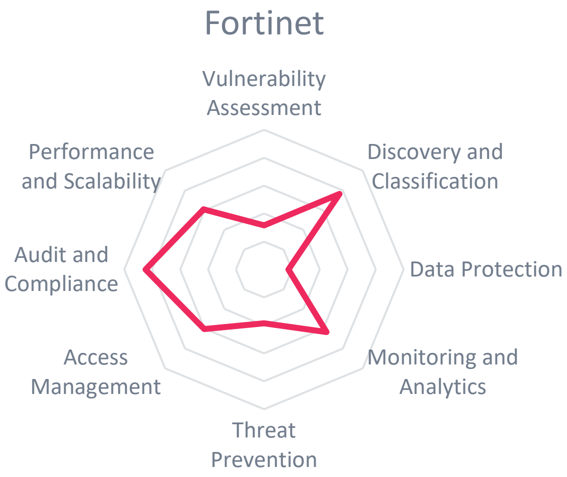
Strengths/Opportunities	Weaknesses/Threats
● Delivered as preconfigured hardware appliances: easy to deploy and manage ● Rich discovery and classification functions ● Powerful out-of-the-box support for compliance frameworks ● Deep integration and unified management with other Fortinet's security products	● Very limited data protection functionality ● Threat prevention only when combined with other Fortinet's products ● No support for cloud deployments

Table 3: Fortinet major strengths and weaknesses

The company's database security solution is **FortiDB** database security software, which is available both as a family of specialized hardware appliances and as software deployment for physical and virtualized environments. By combining several monitoring technologies (native audit, network sniffer and local agents), FortiDB aims to deliver the most comprehensive database vulnerability management, auditing and compliance with minimal performance impact.

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

Table 4: Fortinet rating



The key features provided by FortiDB appliances are:

- Database discovery and vulnerability management using a number of different collection methods;
- Monitoring of privileged and application users utilizing advanced user behavior analytics;
- Powerful policy management with out-of-the box support for DDL, DCL, SOX and PCI;
- Rich alerting and reporting capabilities with predefined reports for audit, compliance and forensic investigations; integrations with popular SIEM solutions;
- Policy-based intrusion prevention to block suspicious activities automatically.

11.3 Gemalto

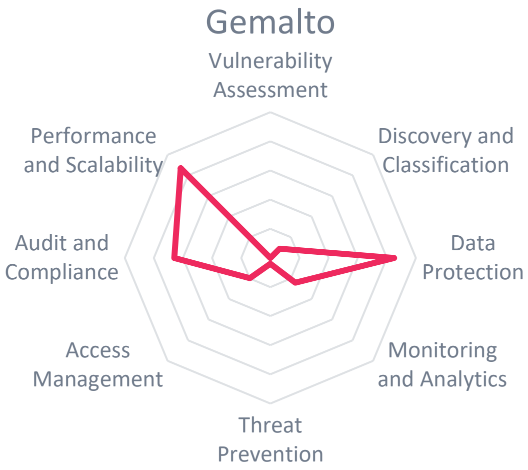
Gemalto is an international digital security company headquartered in Amsterdam, Netherlands. Established in 2006 after a merger of two rival smart card manufacturers, the company has grown into the world's leading provider of SIM cards, as well as a broad range of other security-related products, software applications and managed services.

Strengths/Opportunities	Weaknesses/Threats
● Unified data protection on multiple levels ● Centralized key management and single point of administration ● One of the largest ecosystems of technology partners, broad support for applications, database types, environments ● Support for all major cloud providers ● Comprehensive auditing capabilities	● Functional focus on data encryption only, no coverage of other areas reviewed ● Limited database support for tokenization solution ● No MSP or cloud service offerings available yet (planned for future releases)

Table 5: Gemalto major strengths and weaknesses

After acquiring SafeNet, one of the largest suppliers of encryption technology, in 2014, Gemalto is currently offering a broad range of **SafeNet Data Protection** solutions for various environments across the enterprise, all united by the common cryptography foundation and a single point of management. Depending on their requirements, customers may combine

The company strongly emphasizes their solution's high performance and scalability, enabling companies to process large amounts of data across multiple locations transparently for existing applications.



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

Table 6: Gemalto rating

Major features provided by Gemalto's SafeNet Database protection solutions include:

- SafeNet ProtectDB provides transparent column- or table-level encryption for SQL databases;
- SafeNet Tokenization provides application-level tokenization and masking for sensitive data;
- Safenet ProtectApp allows embedding encryption into existing applications easily and efficiently;
- SafeNet ProtectFile supports file system-level encryption for entire databases and Big Data stacks;
- A large ecosystem of technology integrations enables uniform application of data encryption across on-premises, virtualized and cloud-based infrastructures, including all notable cloud providers.

11.4 HexaTier

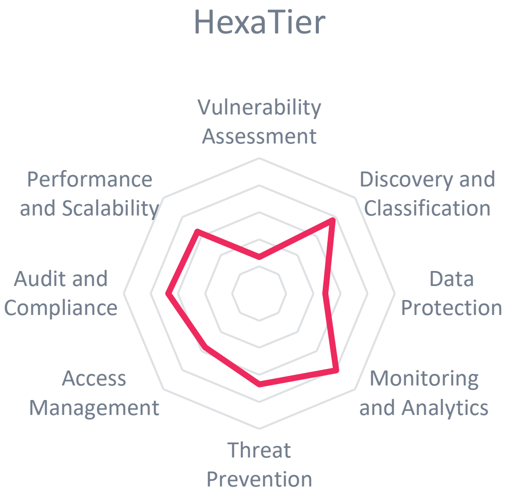
HexaTier is an Israeli security start-up specializing in protecting Database-as-a-Service (DBaaS) deployments. Established in 2009, the company has its roots in the Open Source GreenSQL project, a popular database security solution for small and medium businesses. Over the years, GreenSQL has evolved into a unified database security platform combining data discovery, dynamic data masking and activity monitoring based on a reverse proxy technology.

Strengths/Opportunities	Weaknesses/Threats
● Reverse proxy technology for protecting databases in the cloud ● Multiple functional areas integrated in a single product ● Extends on-premises AD to the cloud with the Database Authentication Proxy ● Designed for SMBs with a focus on ease of deployment and operation	● Limited number of supported database types ● No infrastructure discovery functionality ● Market presence still too low (expected to improve under new ownership)

Table 7: HexaTier major strengths and weaknesses

In 2016, the company has rebranded as **HexaTier**, reflecting its new focus on providing security and compliance for databases in the cloud. The company delivers a scalable and agile solution, using a software-based approach that is easy to install, operate, and maintain. At the end of 2016, HexaTier was acquired by Huawei, a leading Chinese ICT solutions provider. Under new ownership, the company is expected to significantly improve its market presence, which has been the company's biggest challenge.

HexaTier's product can boast the highest degree of integration, delivering database threat protection, activity monitoring, sensitive data discovery and dynamic data masking in a single package aimed at small and medium businesses.



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

Table 8: HexaTier rating

The key features provided by HexaTier are:

- Focus on protecting Database as a Service platforms in the cloud;
- Automated discovery and classification of sensitive data according to compliance regulations;
- Transparent dynamic Data Masking based on an agentless non-intrusive technology;
- Database firewall and access control for real-time detection and prevention of cyber-attacks;
- Database Activity Monitoring of all activities down to the column level, alerting and reporting.

11.5 IBM

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

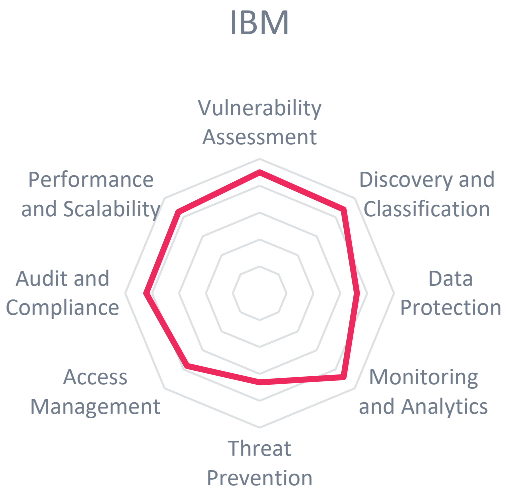
Strengths/Opportunities	Weaknesses/Threats
● Full range of data security capabilities beyond just databases ● Advanced Big Data and Cognitive Analytics ● Nearly unlimited scalability ● Bidirectional integration with QRadar SIEM ● Massive network of technology partners and resellers	● Setup may be complicated for some customers ● Issues with version upgrades

Table 9: IBM major strengths and weaknesses

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

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

Table 10: IBM rating



The key features provided by Guardium 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 for complete protection of sensitive data;
- Activity monitoring and advanced security analytics based on machine learning, with optional bidirectional integration to QRadar Security Intelligence Platform;
- Centralized audit repository for enterprise-wide compliance reporting, performance optimization, investigations and forensics;
- Automated data compliance and audit capabilities with Compliance Accelerators for regulations like PCI, HIPAA, SOX or GDPR.

11.6 Imperva

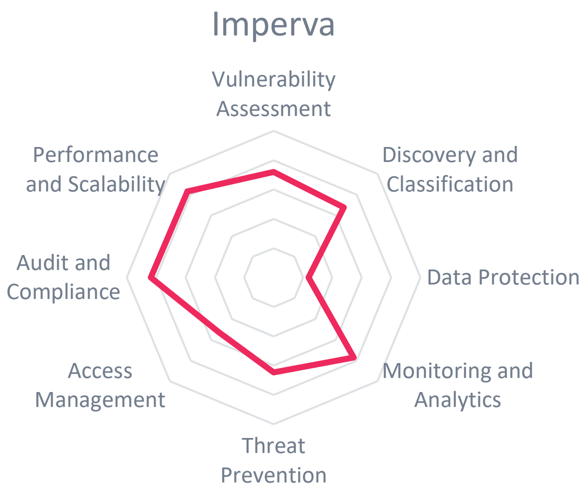
Imperva is an American publicly traded cyber security solution company headquartered in Redwood Shore, California. Back in 2002, the company's first product was a web application firewall, but over the years and after a series of strategic acquisitions, Imperva's portfolio has expanded to include several product lines for data security, cloud security, breach prevention and infrastructure protection as well.

In February 2017, Imperva has acquired the technology and most of the team of Camouflage Software, a company specializing in data masking. This acquisition has allowed the company to incorporate static data masking into its database security portfolio.

Strengths/Opportunities	Weaknesses/Threats
● Unified database protection across multiple platforms and environments ● Multiple collection methods ensure minimal performance overhead ● Advanced security intelligence and behavior analytics ● Large number of out-of-the-box workflows and compliance reports	● Multiple products must be deployed for comprehensive database security ● No support for data encryption or dynamic masking

Table 11: Imperva major strengths and weaknesses

When it comes to database security, we cannot identify a single product providing all necessary functionality. Instead, we are covering several solutions including **SecureSphere Database Security**, which handles data discovery, activity monitoring, threat protection, audit and reporting; **Camouflage Data Masking**, which implements static masking of sensitive data; and **CounterBreach**, which provides unified security intelligence, behavior analytics and identification of compromised endpoints.



Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	strong positive

Table 12: Imperva rating

The key features provided by Imperva's data security solutions are:

- Unified protection across relational databases, data warehouses, Big data platforms and mainframes;
- Comprehensive activity monitoring, auditing and forensic investigation, augmented with advanced security analytics based on behavior profiling;
- Pre-defined policies, remediation workflows, and hundreds of compliance reports simplify administration of security and compliance activities;
- Integration with other Imperva's security products to provide unified multi-factored data security across endpoints, web applications and cloud services.

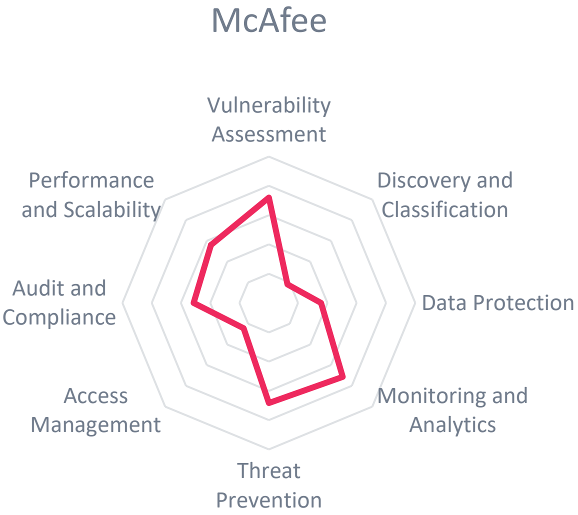
11.7 McAfee

McAfee (currently a part of Intel Security group) is a veteran American computer security vendor headquartered in Santa Clara, California. Founded in 1987, the company has a long history in developing a broad range of endpoint protection, network and data security solutions. Since 2011, McAfee has been a wholly owned subsidiary of Intel; however, a strategic deal with TPG Capital has been recently announced, which will convert Intel Security into a joint venture between TPG and Intel under the original McAfee brand.

Strengths/Opportunities	Weaknesses/Threats
● Comprehensive database discovery, assessment and threat protection capabilities ● Non-intrusive architecture minimizes performance overhead ● Integrates with other McAfee products to provide centralized security management	● No data classification and access management functions ● Data protection capabilities available only with 3rd party products

Table 13: McAfee major strengths and weaknesses

In the database security market, McAfee offers a number of products including McAfee Database Activity Monitoring, McAfee Virtual Patching for Databases, and McAfee Vulnerability Manager for Databases. Together, they form the **McAfee Database Security Suite** providing unified database security across physical, virtual, and cloud environments.



Security	neutral
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	neutral

Table 14: McAfee rating

The key features provided by the suite are:

- Automated discovery of all databases within any environment and identification of sensitive information contained in them;
- Twice as many vulnerability checks as the competition, including detection of insecure PL/SQL code and weak passwords;
- Advanced database activity monitoring with features like deep memory analysis of SQL execution plans, local privileged user access and intrusion protection;
- Non-intrusive architecture ensures that real-time threat detection and prevention does not cause any downtime;
- Integration with McAfee ePolicy Orchestrator enables centralized security management.

11.8 MENTIS Software

MENTIS Software is a privately held security software vendor headquartered in New York, USA. Founded in 2004 with a focus on sensitive information management solutions, the company offers a comprehensive suite of products for various aspects of discovery, management and protection of critical data across multiple sources. Although each product is offered independently, all MENTIS' solutions are built upon a common software platform and can be easily integrated into a single suite.

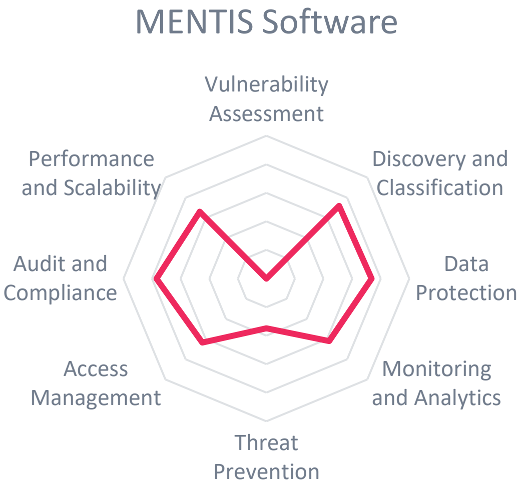
Strengths/Opportunities	Weaknesses/Threats
● A la carte licensing approach: independent products in an integrated suite ● Strong focus on all aspects of data discovery and protection ● Innovative scanning and masking technologies	● No database assessment or threat prevention capabilities ● 3rd party integrations are quite rudimentary ● Limited market presence outside of the US

Table 15: MENTIS Software major strengths and weaknesses

The MENTIS Suite comprises the following products: **iDiscover** for automated high-performance discovery of sensitive information in databases and other environments; **iMask** for dynamic data masking; **iScramble** for static masking of non-production data; **iMonitor** for monitoring database activity and analyzing applications accessing those databases; **iProtect** for fine-grained database access control; and **iRetire** for automating data retention policies.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 16: MENTIS Software rating



The key features provided by the MENTIS suite are:

- A complete and integrated solution that flexibly adapts to individual customer requirements;
- Industry leading scan capability that goes beyond dictionary search, to pattern match, relationship match, and master data match;
- Conditional and location-aware data masking to specify permissible data access based on geographical location of the user;
- Distributed monitoring architecture ensures near real-time results with no performance overhead;
- Intuitive and easy to use interface; quick deployment (typically measured in weeks).

11.9 Oracle

Oracle Corporation is an American multinational information technology company headquartered in Redwood Shores, California. Founded back in 1997, the company has a long history of developing database management products, as well as enterprise software and cloud solutions. Oracle is the second largest software vendor worldwide by revenue.

Strengths/Opportunities	Weaknesses/Threats
● Comprehensive product portfolio for all areas of database security ● Deep integration with other Oracle's Data Provisioning, Testing and Cloud technologies ● Multiple compliance management and reporting tools and services ● Hybrid Cloud Management for seamless operations across different environments	● A number of products are available only for Oracle databases

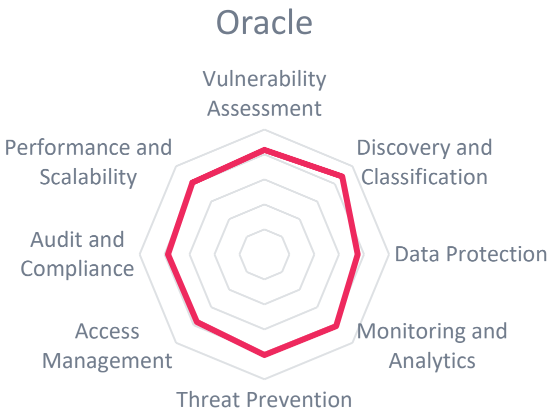
Table 17: Oracle major strengths and weaknesses

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

It's worth noting that some of these products are specifically designed for Oracle databases, which makes Oracle's data protection solutions less suitable for companies using other types of databases. Other products, such as auditing, monitoring and test data management solutions, support multiple database types.

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

Table 18: Oracle rating



Key products of the Database Security suite are:

- Oracle Key Vault for centralized management of encryption keys;
- Oracle Audit Vault and Database Firewall for controlling SQL Injection, detecting anomalies, and supporting forensic analysis;
- Oracle Database Vault for enforcing trusted path access to data and controlling privileged users;
- Oracle Advanced Security for encryption and redaction of sensitive data;
- Oracle Data Masking and Subsetting for targeted archiving and static masking of sensitive data for nonproduction purposes;
- Oracle Label Security to enable multi-tenant use of data tables at the data row level.

11.10 Thales e-Security

Thales e-Security is a leading provider of data protection solutions headquartered in Plantation, Florida, USA. With over 40 years of experience in information security, the company is a veteran player in such areas like hardware security modules (HSM), key management and PKI. The company's modern history began in 2000, when it became a part of Thales Group, an international company based in France, which provides solutions and services for defense, aerospace and transportation markets.

In 2016, Thales has acquired Vormetric, another leading vendor of data protection and cloud security solutions with a long experience in transparent encryption, tokenization and data masking. Starting January 2017, the new fully integrated product portfolio is available to customers, retaining the Vormetric brand name.

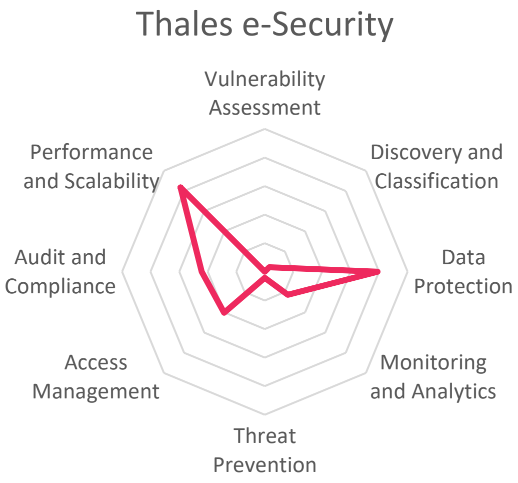
Strengths/Opportunities	**Weaknesses/Threats**
● Comprehensive transparent encryption, tokenization and masking capabilities ● High performance thanks to hardware encryption support ● Centralized management across all environments, even 3rd party products ● Standard APIs for adding encryption support to existing applications	● Functional focus on data protection only, no coverage of other areas reviewed ● Static masking functionality still quite rudimentary

Table 19: Thales e-Security major strengths and weaknesses

The solution covered in our rating is the **Vormetric Data Security Platform**, a unified data protection platform providing customers the flexibility, scale and efficiency to address different security requirements like transparent encryption of the entire database environments, privileged user access controls, granular field-level data protection with encryption, tokenization and data masking, and a single security manager for maximizing value and minimizing the total cost of ownership.

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

Table 20: Thales e-Security rating



Notable features provided by the platform are:

- Centralized management of encryption keys and policies across all environments and products (including 3rd party solutions);
- Application encryption APIs for embedding transparent encryption into existing apps;
- Tokenization and dynamic masking with format-preserving tokenization with or without a token vault;
- Live Data Transformation to reduce maintenance windows needed for deploying encryption, rotating keys or creating versioned backups.

12 Products at a Glance

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

12.1 Ratings at a glance

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

Service	Security	Functionality	Integration	Interoperability	Usability
Axiomatics	positive	weak	positive	positive	weak
Fortinet	positive	neutral	strong positive	neutral	strong positive
Gemalto	strong positive	neutral	strong positive	strong positive	positive
HexaTier	positive	positive	strong positive	neutral	strong positive
IBM	strong positive	strong positive	strong positive	strong positive	strong positive
Imperva	positive	positive	positive	neutral	strong positive
McAfee	neutral	positive	positive	neutral	neutral
MENTIS Software	positive	positive	strong positive	neutral	positive
Oracle	strong positive	strong positive	strong positive	strong positive	strong positive
Thales e-Security	strong positive	neutral	strong positive	positive	neutral

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

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

Company	Innovation	Market Position	Financial Strength	Ecosystem
Axiomatics	neutral	weak	neutral	neutral
Fortinet	neutral	positive	strong positive	positive
Gemalto	neutral	strong positive	strong positive	strong positive
HexaTier	positive	neutral	weak	weak
IBM	strong positive	strong positive	strong positive	strong positive
Imperva	positive	positive	neutral	positive
McAfee	positive	strong positive	strong positive	positive
MENTIS Software	positive	neutral	positive	neutral
Oracle	strong positive	strong positive	strong positive	strong positive
Thales e-Security	neutral	strong positive	strong positive	strong positive

Table 2: Comparative overview of the ratings for the vendors

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

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

In the area of financial strength, a "Weak" or "Critical" rating is given where there is a lack of information about financial strength. This doesn't imply that the vendor is in a weak or a critical financial situation. This is not intended to be an in depth financial analysis of the vendor; and it is also possible that vendors with better ratings might fail and disappear from the market. In the case of a cloud service provider financial failure or withdrawal from the market could create a major problem for a business that depended upon that provider for its business-critical IT services.

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

12.2 The Market/Product Matrix

Furthermore, we've compared the position of vendors regarding combinations of our three major areas of analysis, i.e. Market Leadership, Product Leadership, and Innovation Leadership. This analysis provides additional information. In this diagram, vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "over-performers" when comparing Market Leadership and Product Leadership.

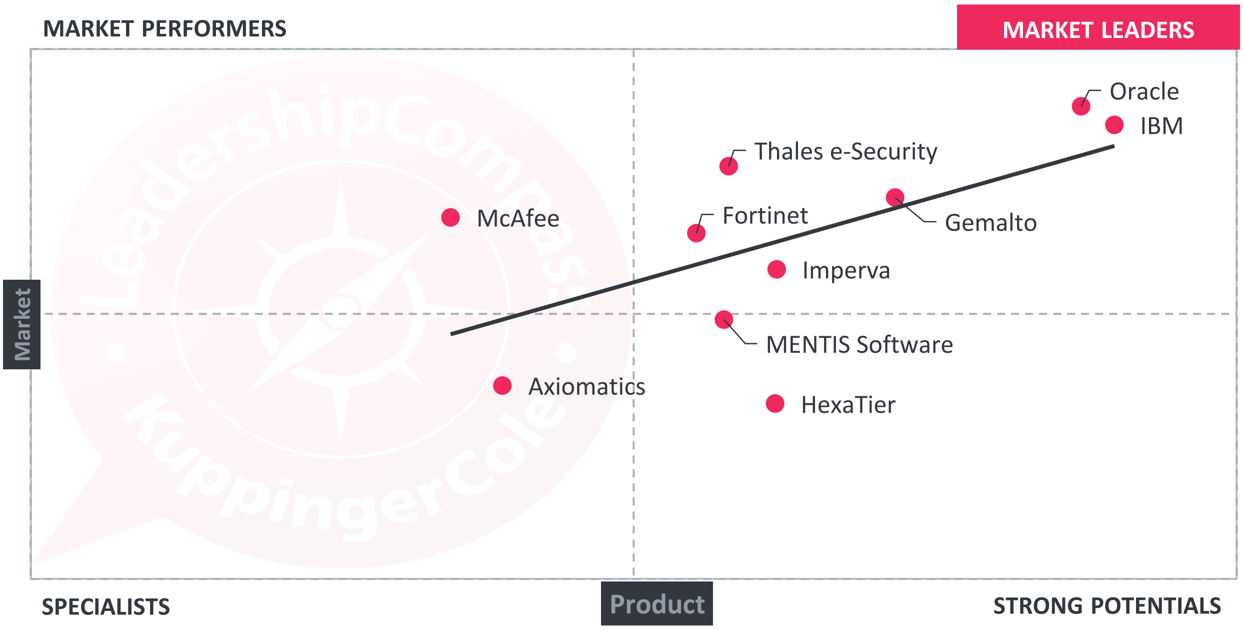


Figure 8: The Market/Product Matrix

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

We've defined four segments of vendors to help in classifying them:

Market Leaders: This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

Strong Potentials: This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be because of various reasons, like a regional focus by the vendors or the fact that they are niche vendors in that particular market segment.

Market Performers: Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically, such vendors have a strong, established customer base due to other market segments they are active in.

Specialists: In this segment, we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.

In the Market Leaders segment, we see IBM and Oracle dominating the ratings both in product and market leadership, followed by Gemalto. The position of Thales e-Security so high above the line indicates that company managed to win a strong market position despite certain shortcomings in their product. This is quite reasonable, having in mind the recent merger that opened Vormetric products to the large Thales' partner network. Imperva, on the other hand, is positioned below the line, indicating their less than stellar financial results last year.

In the Strong Potentials segment, we observe Mentis Software and HexaTier, which, despite offering product suites with impressive functionality and degree of integration, are unable to win a substantial market presence yet, perhaps because of their limited partner ecosystems. Still, with the recent news of HexaTier being acquired by Huawei and MENTIS' continued push towards European markets, both companies have good chances to improve their market positions in the near future.

In the Market Performers segment, we can see McAfee. The company has a large established customer base due to other market segments it operates in, yet its database security solution, while robust and able to address many customer's demands, is not as functionally complete as our rating's Product Leaders.

Finally, Axiomatics has slipped into the Specialists segment, owing this to the fact that their database security product is focused on solving a specific challenge and is yet to win a substantial number of customers.

12.3 The Product/Innovation Matrix

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

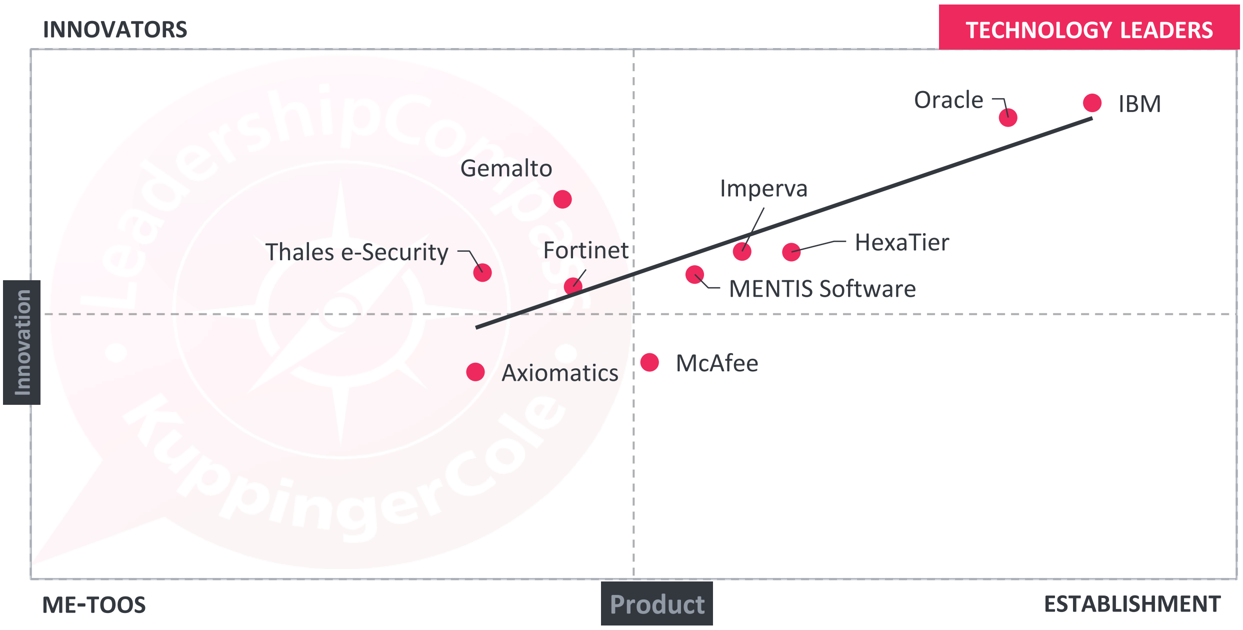


Figure 9: The Product/Innovation Matrix

Again, we've defined four segments of vendors. These are

Technology Leaders: This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

Establishment: In this segment, we typically find vendors that have a relatively good position in the market, but don't perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

Innovators: Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit especially for specific customer requirements.

Me-toos: This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to provide specialized point solutions. However, in most cases this is more about delivering what others have already created.

In the Technology Leaders section, we again find IBM and Oracle as undisputed leaders. Both companies are veteran players in the market that manage to maintain their degree on innovation for decades, constantly updating their mature and full-featured products with new features and incorporating cutting-edge technologies.

This time, they are joined by Imperva, HexaTier and MENTIS Software. Imperva owes this to a broad portfolio that combines solid data protection functionality with innovative security intelligence and behavior analytics. HexaTier, being a pioneer in database firewall technology, has recently reinvented itself as a provider of DBaaS security solutions in the cloud. MENTIS Software continues its long history of innovation in the field of data discovery and masking in a single integrated platform.

In the Innovators section, we find Gemalto, Fortinet and Thales e-Security. All three are known for solution suites that, while not as functionally broad as our product leaders', nevertheless implement various innovative technologies.

In the Establishment section, the only company present is McAfee. Despite having a solid and mature product with comprehensive functionality in several areas covered in this review, the company's solution still relies on integrations with partners in other key areas like encryption or access management.

Finally, Axiomatics with their highly specialized product has slipped into the Me-toos section of the chart.

Please note that low innovation rating does not imply that the quality of the respective vendors' solutions is somehow unsatisfactory – this just means that the companies are focusing on specific functional areas and unorthodox approaches and indeed represent the aforementioned exceptions for the segment definition.

12.4 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 for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position but might also fail, especially in the case of smaller vendors.

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

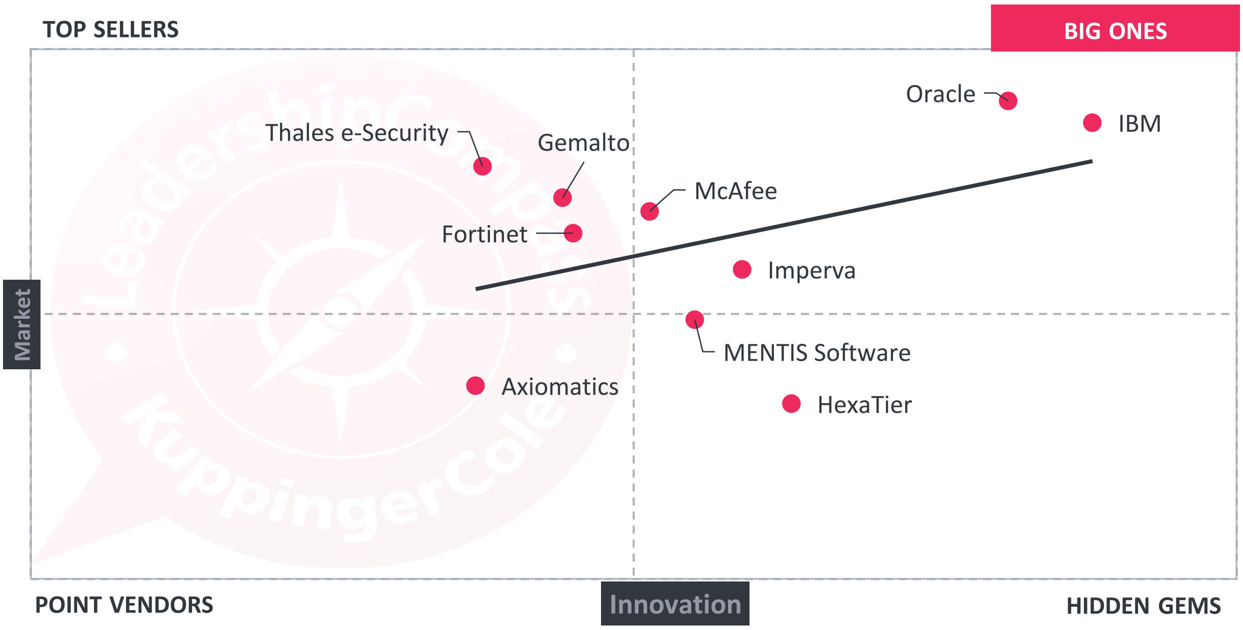


Figure 10: The Innovation/Market Matrix

The four segments we have defined here are

Big Ones: These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

Top Sellers: In this segment, we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of “customer customers”, i.e. a loyal and powerful group of contacts in the customer organizations.

Hidden Gems: Here we find vendors which are more innovative than would be expected given their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless, this group is always worth a look due to their specific position in the market.

Point Vendors: In this segment, we find vendors which typically either have point solutions or which are targeting specific groups of customers like SMBs with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being among the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Again, Oracle and IBM are found in the “Big Ones” segment, joined this time by Imperva. All three companies demonstrate impressive market positions, while maintaining steady innovation in their product portfolios.

In the Top Sellers segment, we find Fortinet, McAfee, Thales e-Security and Gemalto. All these companies enjoy substantial market shares compared to their innovativeness ratings. This may be caused by the specifics of their chosen functional areas or otherwise by strong partner networks and loyal customer bases in other markets.

Hexatier and MENTIS software can be found in the Hidden Gems segment. Both companies show strong innovation in their solutions, yet both have not yet found appropriate market recognition, perhaps due to a low number of partners.

Finally, the only company in the Point Vendors section is Axiomatics. Although a well-known leader in the market for dynamic access management solutions in general, the company can currently offer only a functionally limited product in the area of database security, which is yet to find a substantial number of customers.

13 Overall Leadership

Finally, we've put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 11.

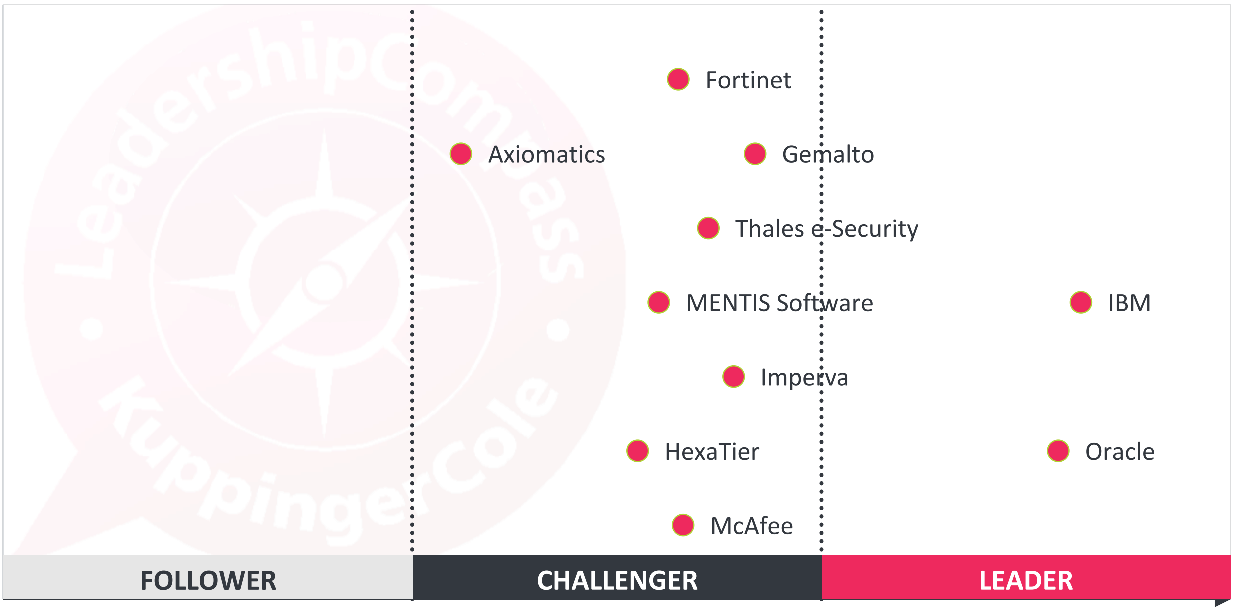


Figure 11: The Overall Leadership rating for the Database Security segment

In the Overall Leadership rating, we find IBM and Oracle among the Leaders, which is completely unsurprising, considering both companies' global market presence, broad ranges of database security solutions and impressive financial strengths. However, the fact that IBM's solutions are database-agnostic, while a substantial portion of Oracle's portfolio only focuses on Oracle databases has influenced KuppingerCole's decision to position IBM as the overall leader in Database Security.

The rest of the vendors are populating the Challengers segment. Lacking the combination of exceptionally strong market and product leadership, they are hanging somewhat behind the leaders, but still deliver mature solutions exceling in certain functional areas. The segment includes both large veteran players with massive customer reach like Imperva, Gemalto, Thales e-Security, McAfee and Fortinet and smaller but impressively innovative companies like HexaTier, MENTIS Software and Axiomatics.

There are no Followers in this rating, indicating overall maturity of the vendors representing the market in our Leadership Compass. Still, there is a number of smaller companies or startups with innovative products entering the market, worth mentioning outside of our rating. These companies are presented in the next chapter.

14 Vendors to Watch

In addition to the vendors evaluated in this Leadership Compass, there are several companies that are nevertheless worth mentioning outside of our rating. Some of these vendors 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 watching.

14.1 Dataguise

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

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

14.2 DataSunrise

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

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

14.3 DB Networks

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

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

14.4 Trustwave

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

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

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

15 Copyright

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.

The Future of Information Security – Today

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

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

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

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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