kuppingercole
ANALYSTS

Data Security Platforms

Alexei Balaganski

April 11, 2023

LEADERSHIP
COMPASS
2023

This report provides an overview of the Data Security Platforms market, along with guidance and recommendations for finding the sensitive data protection and governance products that meet your specific requirements. We examine the broad range of technologies involved, vendor product and service functionality, relative market shares, and innovative approaches to implementing consistent and comprehensive data protection across your enterprise, on-premises and in the cloud.

Contents

Introduction / Executive Summary

This Leadership Compass on Data Security Platforms is already the fourth update to our previous coverage of database security solutions that started over 5 years ago. Previous editions of this rating were released under the title “Database and Big Data Security”, but we believe that the updated title better reflects the current market trends and recognizes changes in messaging of many vendors.

We still recognize database security as a broad section of information security that concerns itself with protecting databases (or more generally, any location where structured digital data is stored) against compromises of their integrity, confidentiality, and availability. This functional area covers various security controls for the information itself stored and processed in database systems, underlying computing and network infrastructures, as well as applications accessing the data.

However, as computing and storage technologies continue to improve, and modern applications embrace distributed, heterogeneous, cloud-native architectures, the very notion of a database is changing as well. The concept of Big Data has already almost completely disappeared – from the modern business perspective, it is all just “data”, regardless of the underlying storage technology.

Following this trend, we have chosen to update the title of this Leadership Compass to align it better with both customer expectations and the strategic vision of vendors in this market segment. We do feel however that the full convergence between traditionally separate security solutions for structured and unstructured data is yet to be observed, and thus we continue to focus primarily on securing structured data stores in this Leadership Compass.

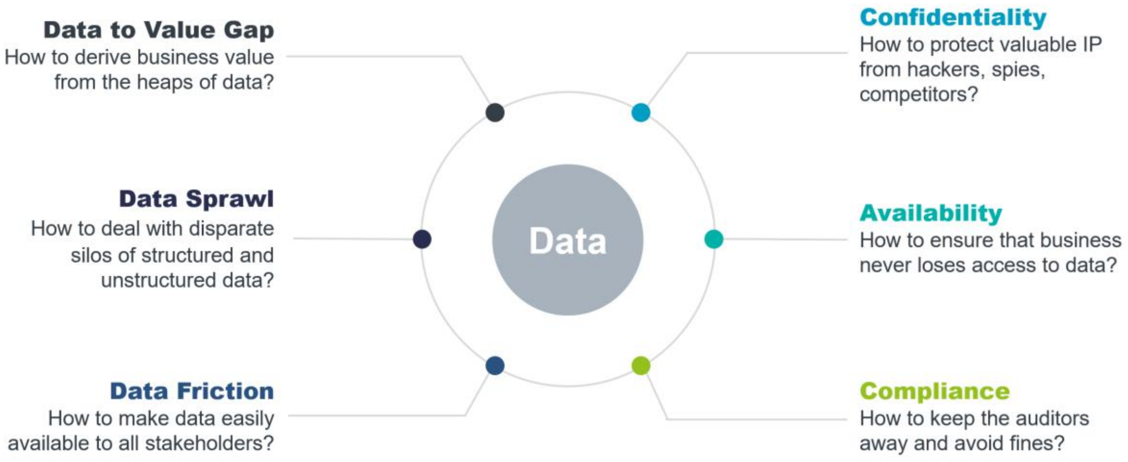

Data to Value Gap
How to derive business value from the heaps of data?
Confidentiality
How to protect valuable IP from hackers, spies, competitors?
Data Sprawl
How to deal with disparate silos of structured and unstructured data?
Data
Availability
How to ensure that business never loses access to data?
Data Friction
How to make data easily available to all stakeholders?
Compliance
How to keep the auditors away and avoid fines?

Figure 1: Data challenges the businesses are facing nowadays.

As more and more companies are embracing digital transformation, the challenges of securely storing, processing, and exchanging digital data continue to multiply. With the average cost of a data breach exceeding $4.35M globally (and over $9M in the United States, according to Statista), just direct financial losses can be catastrophic for many companies, not even considering indirect reputational damages. High-profile “mega-breaches” that expose millions of sensitive data records can easily drive these costs up to hundreds of millions of dollars, but even the victims of smaller ones are now facing increasingly harsh compliance fines.

One of the revelations that businesses, that have recently suffered a costly data breach, finally come to is that not all data is the new oil or their “crown jewels”. In fact, some of the data they have collected turned out to be a dangerous liability that can cause massive problems when not handled properly. Often it simply looks like much of the data companies hold has no intrinsic value, since this value is only generated when data is moving or transforming, creating insights, analytics, statistics, etc. – that is, it serves a tangible purpose for a certain business process. A data security platform must be able to sustain these processes, not introduce additional roadblocks.

One can say that, just like an ideal database, an ideal data security solution is one that does its job and does not get in the way. Businesses are begrudgingly dealing with compliance and privacy issues because of the regulations, but data security is very difficult to sell as a business enabler. Most customers do not **really** want a data security platform; they just want their data to be safe everywhere, at all times, and for any kind of data. They even want this for data in use, even if not all of them really understand the vast complexity of such a solution.

Nowadays, most companies end up using various types of data stores for structured and unstructured information, depending on their business requirements. Data protection regulations like the European Union’s GDPR, California’s CPRA or numerous other country- or state-level laws make no distinction between relational databases, data lakes, or file stores – all data is equally sensitive regardless of the underlying technology stack. Just keeping track of all the digital information is a big problem, but understanding which data is more sensitive according to various policies and regulations and then selecting and enforcing the necessary data protection and governance capabilities is already too much even for the largest businesses.

The area of data security covers various security controls for the information itself stored and processed in database systems, underlying computing and network infrastructures, as well as applications accessing the data. These include, among others, data protection capabilities, fine-grained access controls, activity monitoring, audit, and compliance features as well as other means needed for comprehensive multi-layered protection against external and internal threats. As the amount and variety of digital information managed by organizations continues to grow, the complexity of the IT infrastructure needed to support this digital transformation grows as well.

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

- Denial of service attacks leading to disruption of legitimate access to data.
- Data corruption or loss through human errors, programming mistakes, or sabotage.
- Inappropriate access to sensitive data by administrators or other accounts with excessive privileges.

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

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

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

Ultimately, data security will not be solved until we somehow fully bridge the gap between protecting structured and unstructured data. As mentioned earlier, for customers, there is only “just data”, and the rest of the complexity should not be their concern. The same applies to “at rest” versus “in transit” versus “in use” - the distinction between these states is not as clear-cut anymore.

A working solution for this challenge would completely revolutionize the data security market. However, it has not happened yet and will probably not happen within the next few years.

Highlights

- Data Security Platform is a recently emerged term that better represents the customer demands for a universal data protection solution that “just works without getting in the way”, regardless of the data format, platform, or location.
- While vendors are also eagerly adopting the new name for their existing products, truly universal platforms that can bridge the divide between securing structured and unstructured data are yet to be seen.
- The whole data security market continues to transform. Some of the vendors covered in our previous Leadership Compass have been acquired, transitioned to private ownership, or rebranded and completely reinvented their entire portfolios. Even the

large veteran vendors feel the pressure to evolve to meet the changing customer needs.
- A healthy mixture of traditional security vendors, companies that just entered the market, and innovative startups indicates that the market is still far from maturity, and everyone has an opportunity to gain recognition, especially among the innovation leaders.
- Even though this Leadership Compass recognizes several highly rated overall leaders, it is worth stressing that no single data security solution currently exists that can address every possible use case and customer requirement. Studying the capabilities of every vendor and product presented here is strongly recommended.
- The Overall Leaders in Data Security Platforms are (in alphabetical order) comforte AG, IBM, Imperva, Mage Data, Oracle, SecuPi, and Thales Group.

Market Segment

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

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

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

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

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

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

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

Delivery Models

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

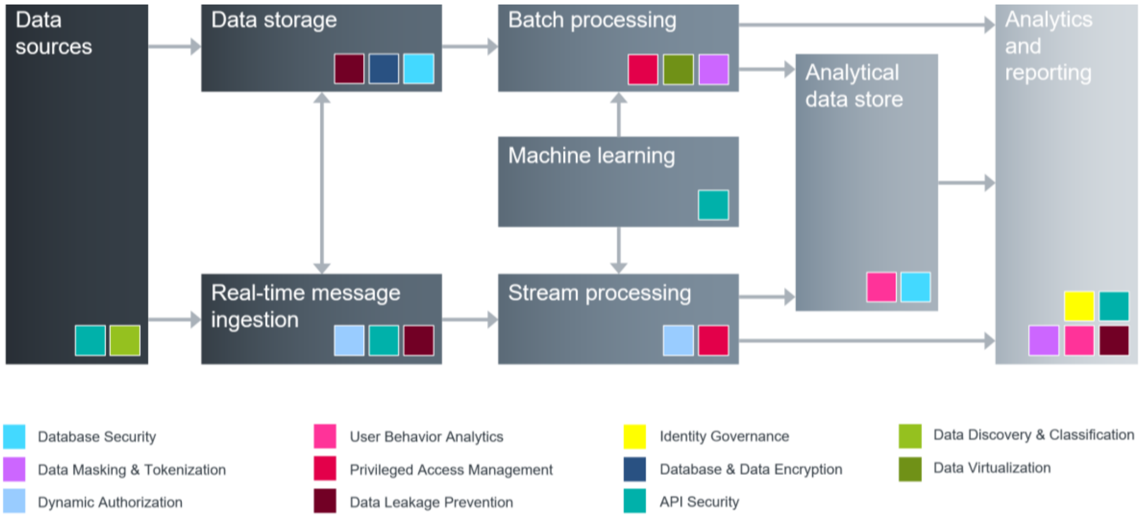


Figure 1: Data movement and transformations, which must be covered by data security controls.

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

In our research, we favor solutions that offer customers a choice of multiple deployment options for different usage scenarios, as well as enough flexibility to mix and match them, migrate to different deployment models, and expand to support new data types and platforms without major efforts.

In the end, the only thing that really is important for businesses is that their valuable and sensitive data is protected reliably and consistently across as many environments, platforms, and operational models as possible.

Required Capabilities

When evaluating the products, besides looking at the overall aspects of the solutions and their respective vendors, like overall functionality and platform support, size of the company and its partner ecosystem, number of customers, licensing models, etc., we also consider the following key functional areas of database security solutions:

Vulnerability assessment – this includes not just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations and, finally, 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, in transit, and in use, 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. Moreover, advanced real-time analytics, anomaly detection, and SIEM integration can be provided.

Attack 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.

In this Leadership Compass, a strong emphasis is placed on implementing database security across heterogeneous environments. Following the latest trends with regard to increasing adoption of cloud-native distributed application models and a growing demand for cloud migration projects, we are also placing a strong emphasis on supporting cloud-based and hybrid deployments and integrating with existing cloud-native identity and security services.

Key criteria we're looking for include:

- Unified support for multiple relational and NoSQL data platforms.
- Comprehensive support for popular Big Data frameworks.
- Support for hybrid deployments across on-premises and cloud infrastructures or managed database services.
- Centralized management, analytics, and audit across multiple data stores.

A strong focus is placed 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.

Combined with functional criteria listed above, these requirements form a two-dimensional evaluation approach that ensures that solutions that excel both in delivering a broad range of security features and in supporting multiple data formats and models will have substantially higher chances to be recognized as leaders.

Optional Capabilities

As much as we would love to include unstructured data protection under the required capabilities, it is unfortunately still too early to expect consistent delivery of these functions from the majority of the vendors. Many "traditional" security companies are rooted in structured data protection technologies and are only beginning to expand their coverage to unstructured data stores.

Solutions that have historically focused on securing unstructured data have been covered in a separate KuppingerCole publication: Market Compass on Data Governance Platforms. Some of the capabilities of those solutions are already finding their way into integrated data security platforms, either through acquisitions, OEM partnerships, and integrations or simply through organic convergent evolution. However, it will take another few years for these fully integrated platforms to reach maturity.

Among the less revolutionary but still notable optional features, we can mention the following:

- Flexible support for different deployment scenarios, such as local agents, network proxies, passive monitoring, etc. to address numerous (and often radically different from the architecture perspective) use cases.

- Support for protecting cloud databases, data lakes, object stores and other -aaS solutions.
- Implementing vendor- and product-neutral security technologies such as encryption instead of relying on built-in vendor-specific implementations.
- Practically unlimited and elastic scalability and minimal performance impact.
- Flexibility and user-friendliness of the management console.
- Ability to integrate into existing Data Fabrics – providing consistent security and compliance across data management, quality, integration, analytics, utilization and other layers of modern business data landscapes.
- Consistent implementation of privacy-enhancing technologies not just for the external data under protection, but within the data security platforms themselves.

Leadership

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

The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right.

Overall Leadership

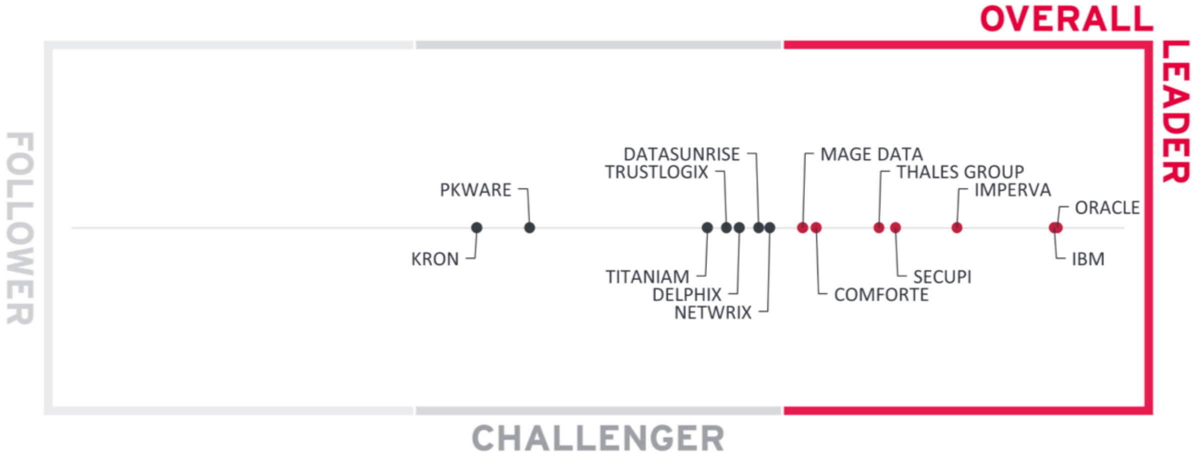


Figure 3: The Overall Leaders in the Data Security Platforms market

Quite unsurprisingly, we mostly observe the same vendors among the overall leaders as in the previous edition of this Leadership Compass. Oracle and IBM still retain their distant leadership, which reflects both companies' global market presence, broad ranges of database security solutions, and impressive financial strengths.

They are followed by Imperva, Thales Group, SecuPi, and comforte AG, just like last time as well. The only newcomer among the leaders is Mage Data, which was only mentioned as a vendor to watch in the previous edition. Formerly known as Mentis, the company has undergone extensive rebranding and portfolio restructuring, emerging as a solid competitor to the established leaders.

The rest of the vendors populate the Challenger segment. Delphix and DataSunrise have retained their positions from the last time, and the rest of the vendors are newcomers, ranging from extremely innovative startups like Titaniam to veteran vendors that only recently ventured into the data security market like Netwrix and PKWARE.

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

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

The Overall Leaders are (in alphabetical order):

- comforte AG
- IBM
- Imperva
- Mage Data
- Oracle
- SecuPi
- Thales Group

Product Leadership

The first of the three specific Leadership ratings is about Product leadership. This view is mainly based on the analysis of the overall capabilities of the various products or services. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

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

Just like last time, there are the same largest players in the market, offering a wide range of products covering different aspects of database security, that take the first two product leadership positions with a strong lead ahead of the competition. IBM Security Guardium is a data security platform that provides a full range of data discovery, classification, entitlement reporting, near real-time activity monitoring, and data security analytics across different environments, which has led us to recognize IBM as the Product Leader.

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

Imperva has managed to improve its position since the previous review, and following it, we have the aforementioned newcomer – Mage Data. After the rebranding in 2022, the company not only has transformed its go-to-market strategy and substantially grown its partner network but came up with a unified data platform combining security and privacy capabilities.

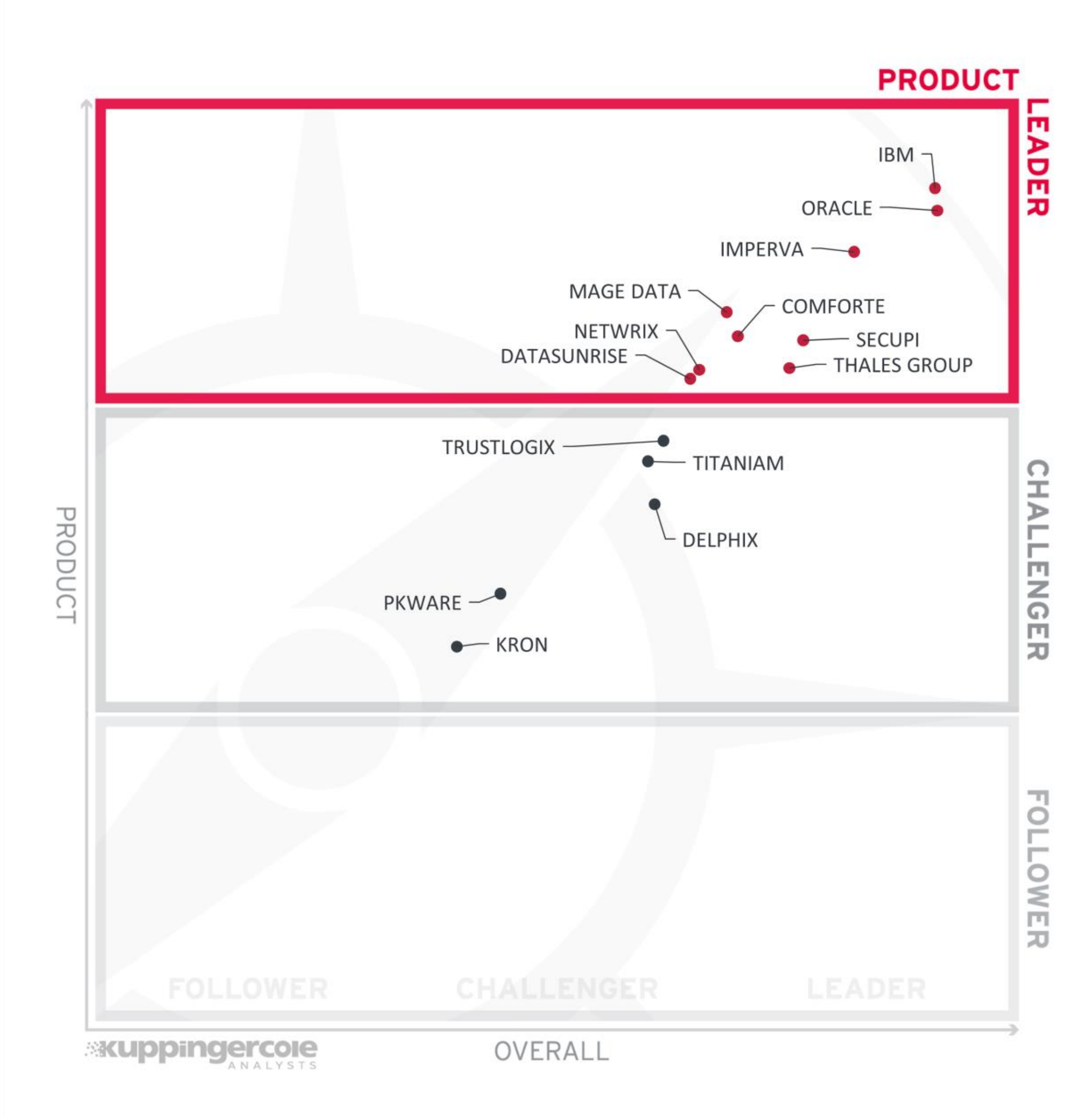


Figure 4: The Product Leaders in the Data Security Platforms market

Joining them again are comforte AG with its highly scalable and fault-tolerant data masking and tokenization solution which has grown into a full-fledged data security platform; SecuPi – an ambitious vendor focusing on data-centric protection and compliance for data and business applications; and Thales Group with its scalable and unified data security platform combining discovery and classification, data protection, and key management for on-premises and clouds, across entire IT landscapes.

Closing the group of the Leaders are Netwrix, a relative newcomer to this market, which has nevertheless managed to build a substantial data security portfolio through acquisitions, and DataSunrise, whose solution combines data discovery, activity monitoring, database firewall, vulnerability assessment, and dynamic and static data masking capabilities in a single integrated product.

The rest of the vendors can be found among the Challengers. Most of them are too specialized, focusing on a single aspect of data security or compliance, to compete with more universal solutions. Still, no company has slipped into the Followers segment, and most of the challengers have a tangible opportunity to become a leader in the future.

The Product Leaders are (in alphabetical order):

- comforte AG
- DataSunrise
- IBM
- Imperva
- Mage Data
- Netwrix
- Oracle
- SecuPi
- Thales Group

Innovation Leadership

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

The vertical axis shows the amount of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

Just like last time, the top three places are occupied by veteran data security vendors. Oracle, IBM, and Imperva continued to demonstrate that even after decades of development, it is still possible to keep up with the evolving market and deliver new innovative capabilities at a steady pace.

All three companies follow their unique paths, with Oracle focusing on incorporating advanced security controls directly into their database products, IBM focusing on expanding the coverage of heterogeneous data platforms and offering new, business-friendly services to a broader customer base, and Imperva on weaving their security capabilities into a single Data Security Fabric, leveraging their broad coverage that comes from their 20-year history as the only pureplay cybersecurity company of the three.

Joining them, however, is another newcomer – Titaniam, with its surprisingly innovative security platform that enables data encryption in-use for a variety of data platforms and use cases, enabling search and analytics without decryption and without the limitations of homomorphic methods.

SecuPi, comforte AG, Trustlogix, Thales Group, Mage Data, DataSunrise, and Netwrix can also be found among the innovation leaders, showing how surprisingly diverse and interesting the data security market is, with numerous opportunities for both established vendors and startups to deliver breakthrough new capabilities.

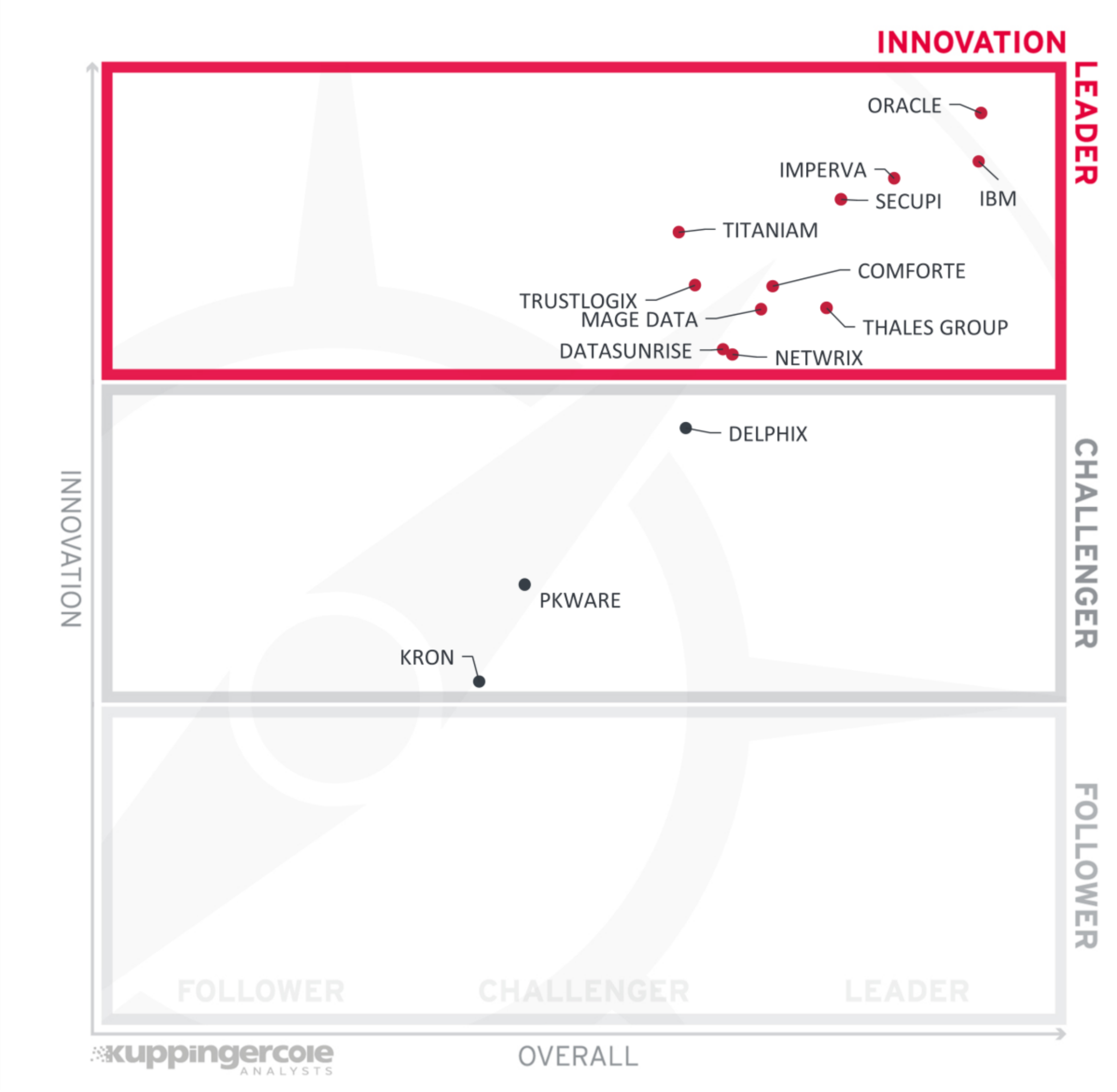


Figure 5: The Innovation Leaders in the Data Security Platforms market

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

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

The Innovation Leaders are (in alphabetical order):

- comforte AG
- DataSunrise
- IBM
- Imperva
- Mage Data
- Netwrix
- Oracle
- SecuPi
- Thales Group
- Titaniam
- Trustlogix

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, the size of deployments and services, the size and geography of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

The vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

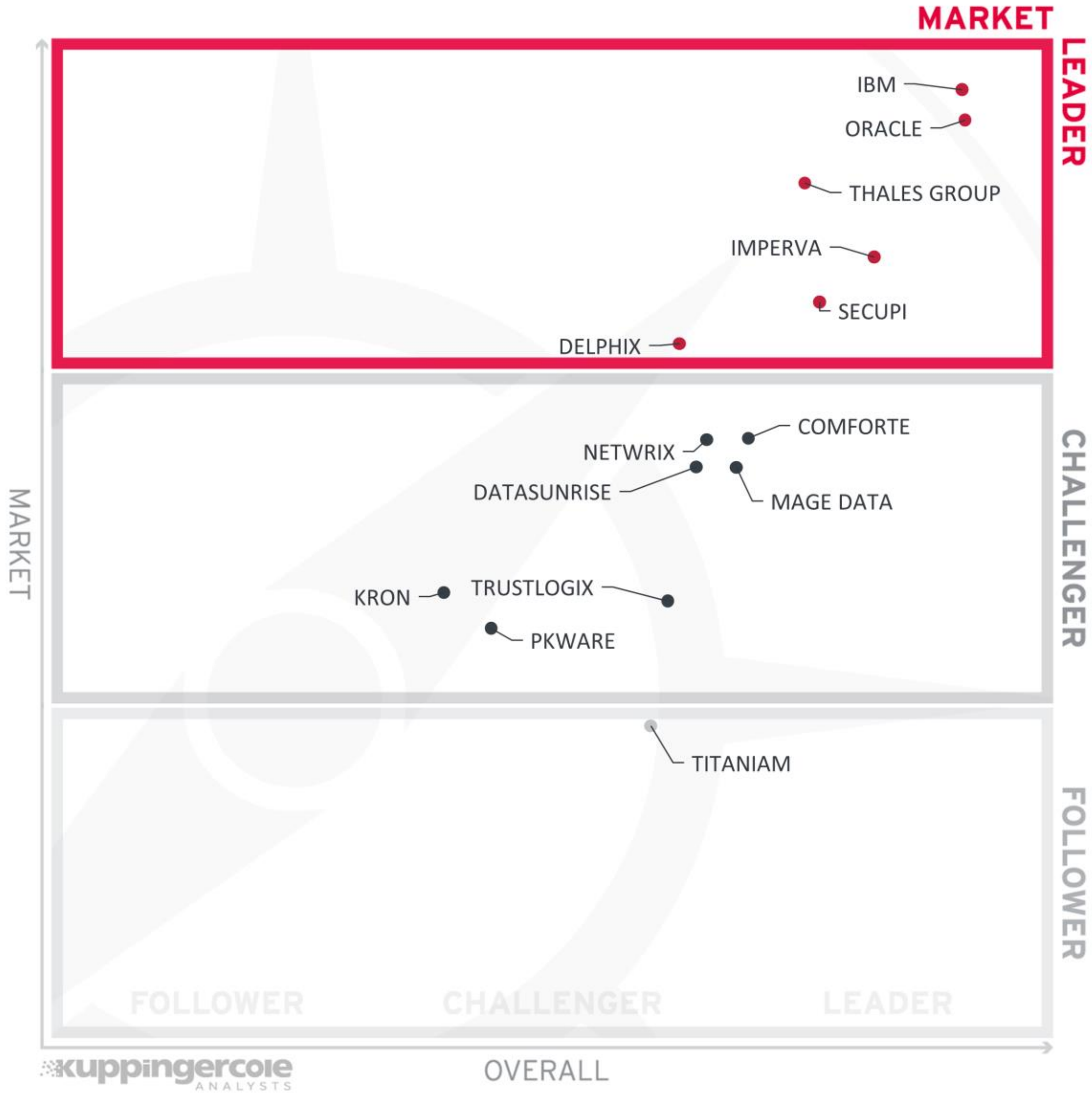


Figure 6: The Market Leaders in the Data Security Platforms market

Again, completely unsurprisingly, most market leaders in our rating are large, veteran vendors with massive international presence, large partner networks, and impressive customer bases. These include vendors like Oracle, IBM, Thales, and Imperva. The only smaller vendors among market leaders are SecuPi, thanks to its close business relationships with major cloud service providers, and Delphix that has recently substantially expanded its market ecosystem through strategic partnerships.

Most other participants of the rating can be found populating the Challengers segment, reflecting their relative financial stability and future growth potential.

The only vendor recognized as a Follower is Titaniam, a startup in the early growth stage, still relying on venture capital to develop their future market presence.

The Market Leaders are (in alphabetical order):

- Delphix
- IBM
- Imperva
- Oracle
- SecuPi
- Thales Group

Correlated View

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

The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership. The vertical axis represents the market position plotted against product strength rating on the horizontal axis.

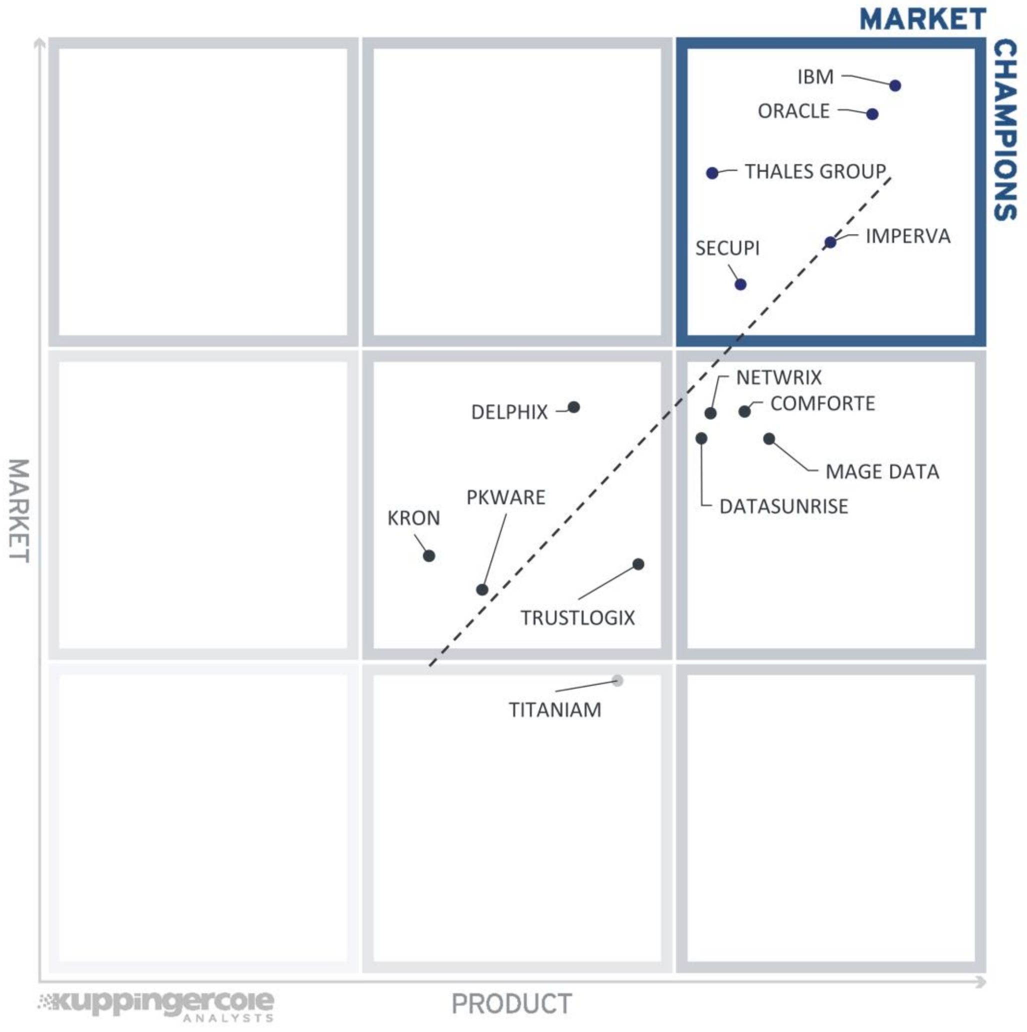


Figure 7: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership. It comes as no surprise that these are mainly large vendors, while vendors below the line are often innovative but focused on specific functional or geographical areas.

Among the Market Champions, we once again find the largest well-established vendors including IBM, Oracle, Thales Group, and Imperva, as well as SecuPi thanks to its prominent presence in the marketplaces of major cloud service providers.

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

Only Titaniam can be found in the bottom middle segment, reflecting how early their journey towards winning the market position their products deserve truly is.

The rest of the vendors occupy the central box, indicating their relatively narrow functional or market focus, which corresponds to a somewhat limited potential for future growth.

The Product/Innovation Matrix

The vertical axis represents the product strength rating plotted against innovation on the horizontal axis.

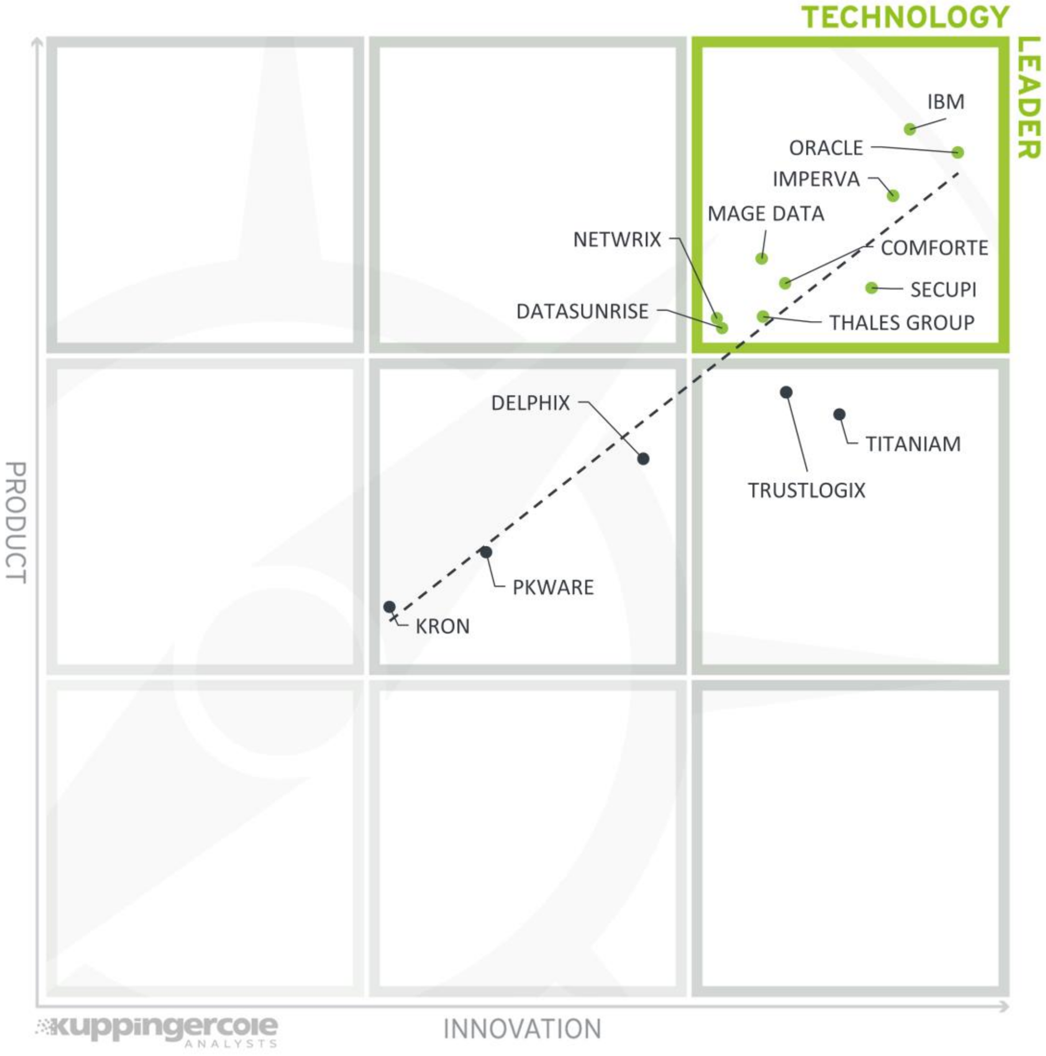


Figure 8: The Product/Innovation Matrix

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

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

Among Technology Leaders, we again find IBM and Oracle, indicating both vendors' distant leadership in both product and innovation capabilities thanks to their huge resources and decades of experience. They are joined by Imperva, Mage Data, Comforte, SecuPi, Thales, Netwrix, and DataSunrise reflective of the respective companies' major recent investments into innovative technologies and expansion of their data protection portfolios.

In the right middle box, we can see Titaniam and Trustlogix, showing that their highly innovative technologies are still being actively transformed into product portfolios.

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

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. The vertical axis represents the market position rating plotted against innovation on the horizontal axis.

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. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

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

Compared to the last edition, the group of the Big Ones has not changed at all, we can see the same vendors occupying the top right corner of the chart. These include all the large vendors with strong data protection portfolios, namely IBM, Imperva, Oracle, and Thales Group – all of them combine a well–established market presence with a strong pace of innovation. SecuPi, despite its relatively small size, managed to reach the top segment as well.

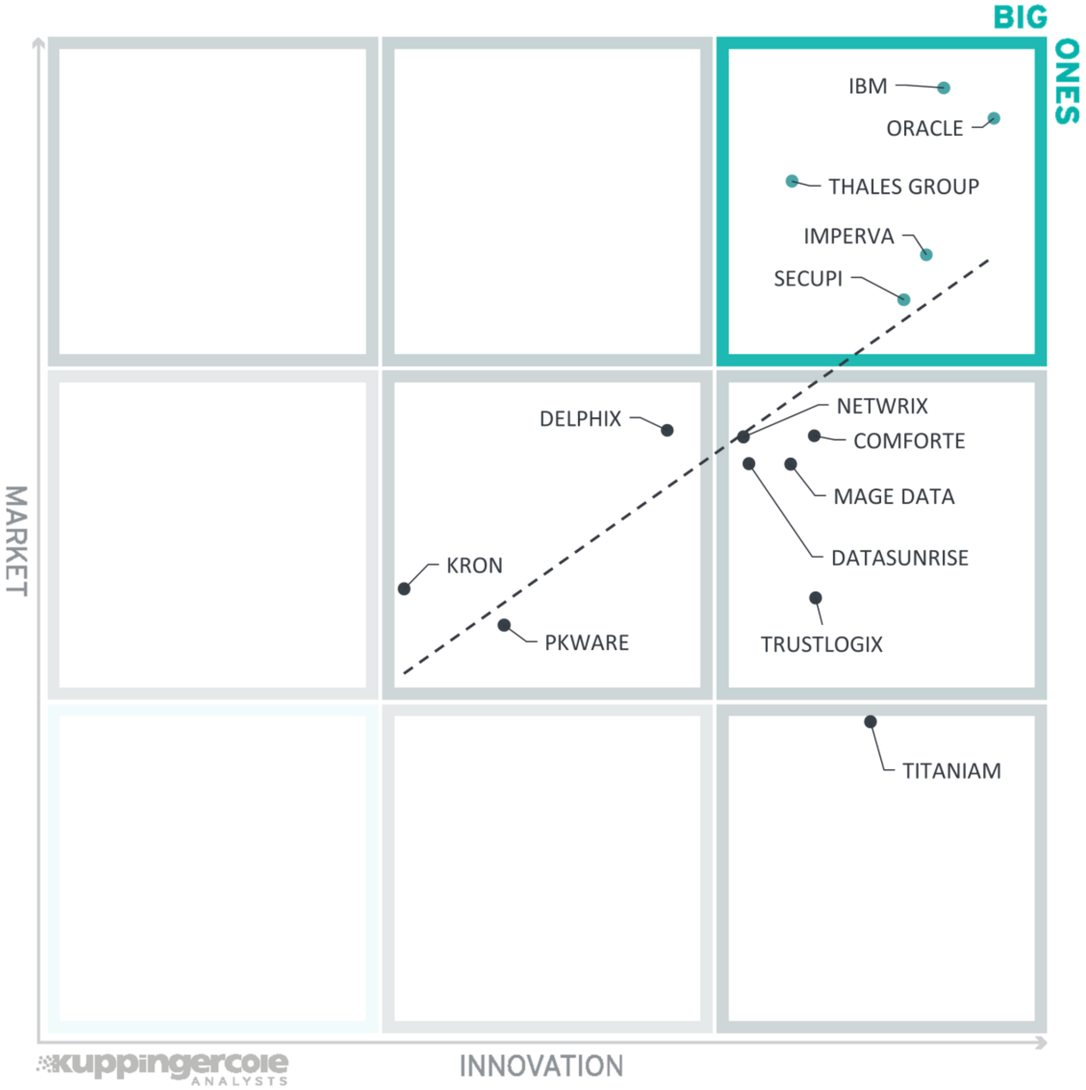


Figure 9: The Innovation/Market Matrix

Comforte AG, DataSunrise, Mage Data, Netwrix, and Trustlogix can be seen in the middle right box, indicating their strong innovation potential that has not yet transformed into corresponding market shares.

Even more so is Titaniam, in the lower right box – its highly innovative technology is still at the early stage of reaching the appropriate customer audience.

Finally, in the middle box we find the remaining vendors, who, as already mentioned earlier, demonstrate average results – perhaps focusing their primary investments in other market segments.

Products and Vendors at a Glance

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

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
comforte AG	strong positive	strong positive	strong positive	strong positive	positive
DataSunrise	strong positive	strong positive	strong positive	strong positive	positive
Delphix	positive	positive	strong positive	positive	strong positive
IBM	strong positive	strong positive	strong positive	strong positive	strong positive
Imperva	strong positive	strong positive	strong positive	strong positive	strong positive
Kron	positive	neutral	positive	neutral	positive
Mage Data	strong positive	positive	strong positive	positive	strong positive
Netwrix	strong positive	positive	strong positive	strong positive	strong positive
Oracle	strong positive	strong positive	strong positive	strong positive	strong positive
PKWARE	positive	positive	positive	positive	neutral
SecuPi	strong positive	strong positive	strong positive	strong positive	strong positive
Thales Group	strong positive	positive	strong positive	strong positive	strong positive
Titaniam	positive	positive	strong positive	positive	positive
TrustLogix	strong positive	positive	positive	positive	strong positive

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

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
comforte AG	positive	positive	strong positive	neutral
DataSunrise	positive	positive	neutral	positive
Delphix	positive	positive	positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
Imperva	strong positive	positive	positive	strong positive
Kron	weak	neutral	neutral	neutral
Mage Data	positive	neutral	neutral	positive
Netwrix	positive	positive	positive	positive
Oracle	strong positive	strong positive	strong positive	strong positive
PKWARE	neutral	weak	neutral	neutral
SecuPi	strong positive	positive	strong positive	positive
Thales Group	positive	strong positive	strong positive	strong positive
Titaniam	strong positive	weak	weak	weak
TrustLogix	strong positive	weak	weak	positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

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

Vulnerability assessment – not limited to just discovering known vulnerabilities in database products, but providing complete visibility into complex database infrastructures, detecting misconfigurations, and the means for assessing and mitigating these risks.

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

Data protection – technologies such as data encryption at rest, in transit, and in use, as well as enterprise key management, tokenization, static and dynamic data masking, and other methods for protecting data integrity and confidentiality and for ensuring regulatory compliance for sensitive data in cloud environments.

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

Attack prevention – various methods of protection from cyber-attacks such as denial-of-service or SQL injection, mitigation of unpatched vulnerabilities, and other infrastructure-specific security measures.

Access Management – not just basic coarse-grained access controls to database instances, but more sophisticated dynamic policy-based access management based on various data or user attributes, identifying and removing excessive user privileges, managing shared and service accounts, as well as detection and blocking of suspicious user activities.

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

Deployment and Scalability – although not a security feature per se, it is a crucial requirement for all database security solutions to be able to withstand high loads, minimize performance overhead, and to support deployments in high availability configurations; all these must be supported in on-premises, cloud, and hybrid environments.

These spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some products may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific use cases must be addressed. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations across complex, heterogeneous IT environments.

Comforte AG – Data Security Platform

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

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

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

Since our last review, comforte AG has not just significantly grown its market footprint and financial strength but invested a lot of effort into turning their capable but still fairly specialized solution into a full-featured data security platform, reflecting the rebranding of its flagship product. Previously used 3rd-party classification technology has been natively incorporated into the platform, providing continuous data inventory, augmenting policy design, and enabling automated enforcement.

The coverage of supported data platforms has been substantially increased as well, now providing integrations with relational and NoSQL databases, data warehouses and cloud-native data stores, business applications and APIs. Thanks to dedicated partnerships with vendors like Snowflake, comforte AG now offers substantially reduced deployment times for such scenarios.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Table 3: comforte AG's rating

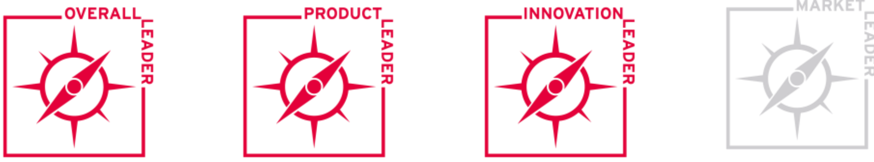
Strengths

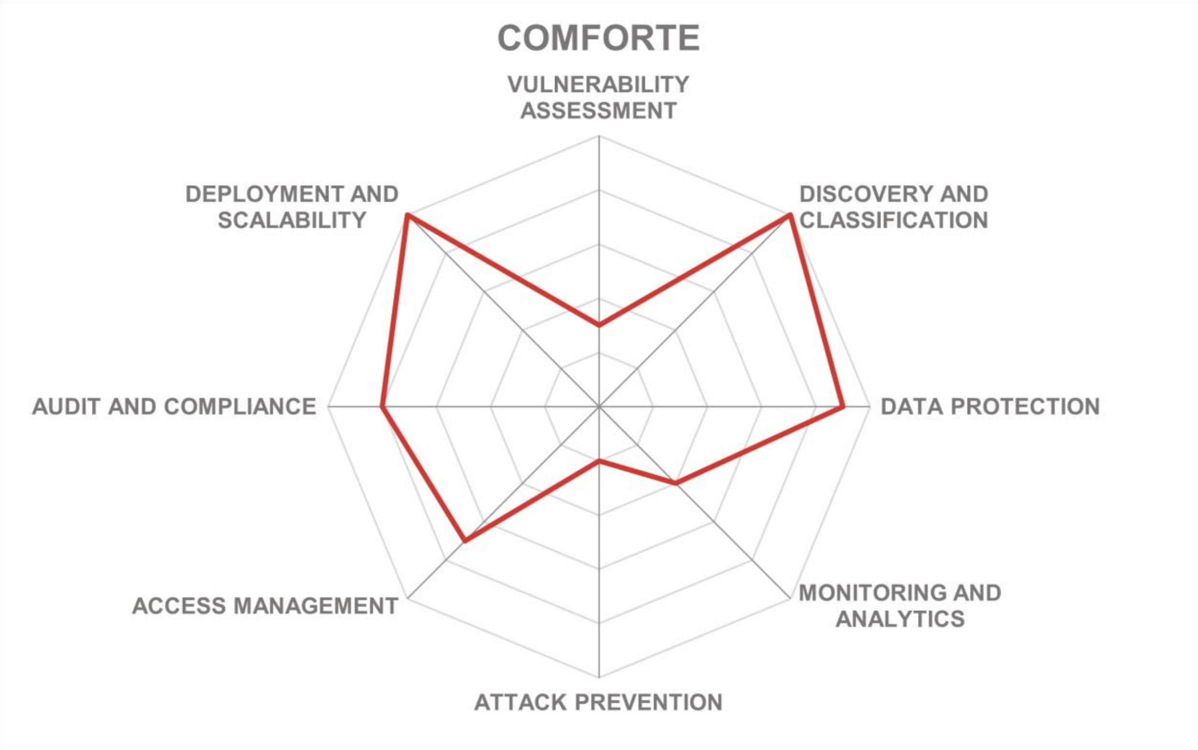
- Unique hardened, scalable, and fault-tolerant architecture for mission-critical use cases.
- Deployment speed and flexibility with hybrid cloud, and as-a-Service scenarios.
- Consistent protection at rest, in motion, and in use for structured and semi-structured data.
- Broad range of integration options for business apps and data flows.
- Strong focus on maintaining regulatory compliance like PCI DSS and GDPR.

Challenges

- No vulnerability assessment capabilities are included in the platform.
- The “single pane of glass” strategic vision is still a work in progress.
- Growing but still fairly limited recognition outside the financial industry.

Leader in





DataSunrise – Database and Data Security

DataSunrise is a security vendor based in Seattle, WA, United States. It was founded in 2015 to develop a next-generation data and database security solution for real-time data protection in heterogeneous environments. The company's solution combines data discovery, activity monitoring, database firewall, vulnerability assessment, and dynamic and static data masking capabilities in a single integrated product. However, the company does not focus on cloud databases only, offering support for a wide range of database and data warehouse vendors.

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

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

Since our last review, DataSunrise has been steadily growing both in market presence, especially outside the US, and in capabilities. The integration with Elastic Kibana provides substantial improvements in analytics. Besides adding support for more specialized database engines like Neo4j or ScyllaDB, the company has most notably expanded its cloud unstructured data handling by adding support for Azure and GCP in addition to AWS. Thus, the company is now serving all major public clouds directly from their marketplaces.

The solution is notable for combining nearly all aspects of database security covered in this Leadership Compass in one integrated product. DataSunrise might be a compelling choice for modern cloud-native companies with highly heterogeneous database infrastructures.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Table 4: DataSunrise's rating

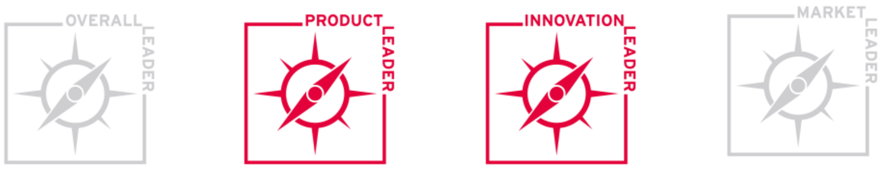
Strengths

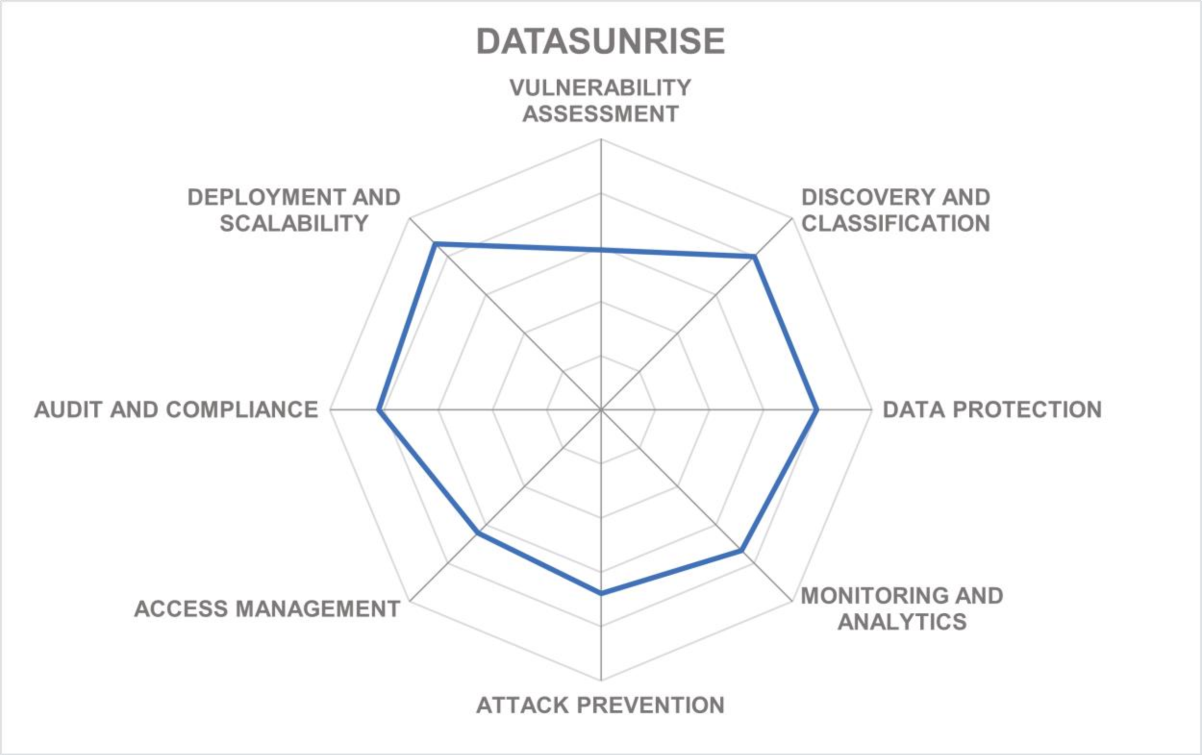
- The tightly integrated multi-functional database security suite covers all major attack surfaces.
- Broad range of supported SQL and NoSQL databases, unstructured data stores.
- Support for multiple cloud databases and storage services simplifies hybrid deployments.
- Available on and implements support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

Challenges

- Relies on cloud platforms for scalability and HA deployments.
- Targeted at smaller companies, less suitable for enterprise-scale projects.
- Vulnerability assessment is limited to recommendations, does not do remediation.

Leader in





Delphix – DevOps Data Platform

Delphix is a privately held software development company headquartered in Redwood City, California, USA. It was founded in 2008 with a vision of a dynamic platform for data operators and data consumers within an enterprise to collaborate in a fast, flexible, and secure way. With offices across the USA, Europe, Latin America, and Asia, Delphix is currently serving over 25% of the Fortune 100 companies. CIOs, CSIOs, leaders of application development, testing, and QA use Delphix to accelerate innovation while protecting data privacy and security across the application lifecycle.

Delphix DevOps Data Platform is an integrated and fully automated DevOps platform that combines data virtualization and data masking, making corporate data from various sources available across on-premises and cloud environments quickly and securely at the speed and scale needed to support a wide range of use cases: from development and testing to data analytics to cloud migration to disaster recovery.

Using the integrated data masking technology, Delphix implements the automatic discovery of sensitive data and its obfuscation by using masking or reversible tokenization as a seamless part of the virtualization process. Flexible deployment options and a wide range of supported databases and file systems make the Delphix platform a very interesting choice for companies that are planning a deep dive into the DevOps methodology or just looking for a universal tool to address multiple pain points in such areas as modernization to the multi-cloud, agile, DevOps, CICD, data analytics, SRE and disaster recovery. Delphix brings APIs and other data capabilities to areas across the application lifecycle including AI model training, to reduce the mean time to recovery for SRE teams that need to develop, test, and deploy fixes.

The company provides pre-configured images for deployment on all public clouds, and several cloud-based database types are supported as well. Thus, the platform enables transparent data virtualization across hybrid environments, substantially reducing the amount of data that must be replicated into the cloud and automatically enforcing the security and compliance policies. It is now fully automated to maintain continuous compliance, not just with virtualized copies but physical data sources as well.

Since our previous review, the company has continued to develop and adapt its platform for the changing market requirements. Notably, the scalability and automation capabilities have been substantially improved to support the data appetite of even the largest enterprises. With this API-first approach, Delphix is now targeting test data management as the primary use case for its solution.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 5: Delphix’s rating

Strengths

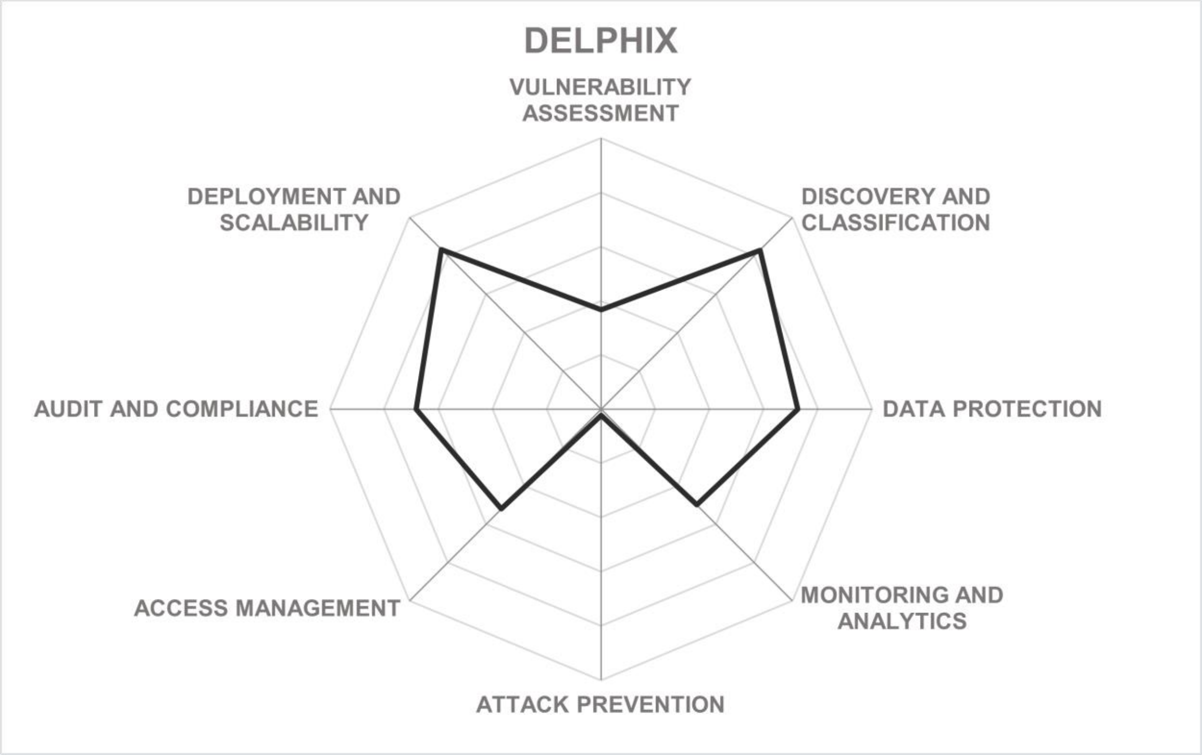
- Based on a universal, high-performance, and space-efficient data virtualization technology.
- Support for a broad range of database types and unstructured file systems.
- Transparent data masking and tokenization capabilities.
- Fully supports self-service workflows for data consumers.
- Pre-configured for popular regulatory compliance frameworks.

Challenges

- Data protection is not the core focus of the solution.
- Primarily focused on large enterprise customers.
- Limited monitoring and analytics functions.

Leader in

OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER



IBM Security – Guardium

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

IBM Security Guardium provides a comprehensive data security platform providing a full range of functions, including discovery and classification, entitlement reporting, data protection, activity monitoring, and advanced data security analytics, across different environments: from file systems to databases and big data platforms to hybrid cloud infrastructures.

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

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

IBM Security Guardium Insights is a recent addition to the Guardium family, a containerized, hybrid multi-cloud hub for data security visibility, which can either work together with Guardium Data Protection or on its own through agentless streaming directly from DBaaS sources. For customers, it offers advanced data risk visualization, protection, and remediation capabilities with much less administrative effort than a traditional Guardium deployment.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 6: IBM Security's rating

Strengths

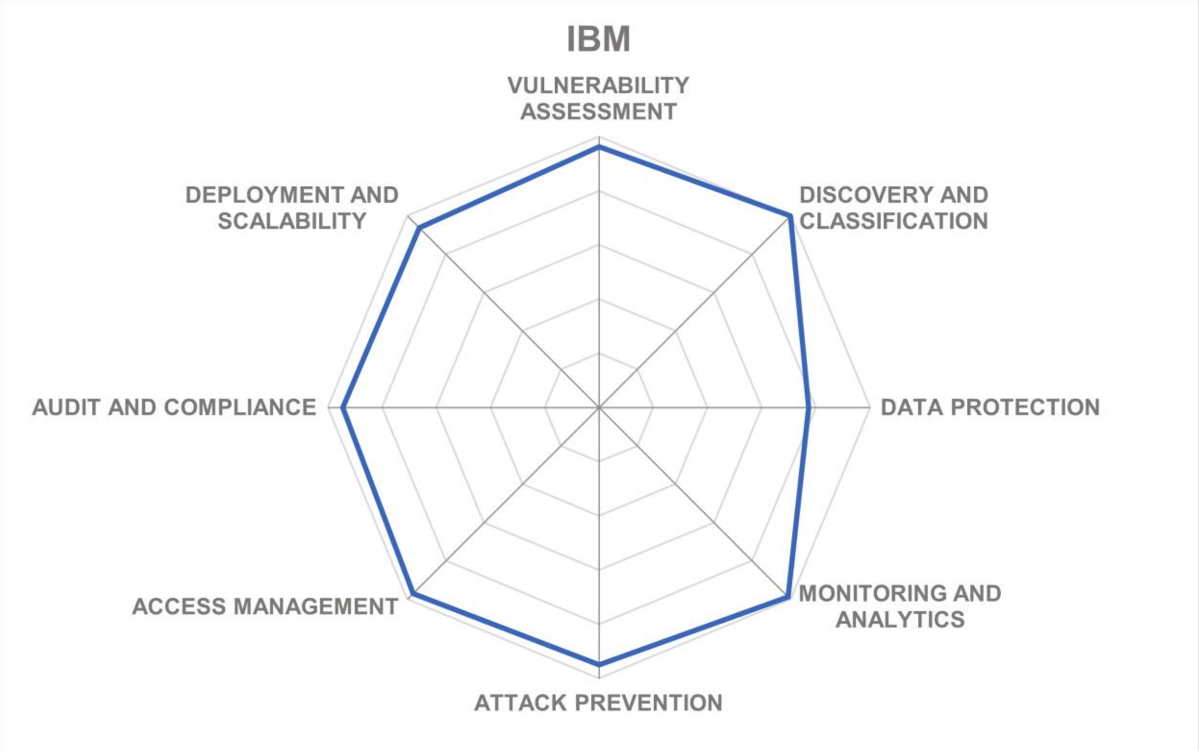
- Full range of security capabilities for structured and unstructured data.
- Support for hybrid multi-cloud environments.
- Modern containerized, multi-cloud architecture aligned with IBM Cloud Paks.
- Advanced Big Data and Cognitive Analytics.
- Integrated ecosystem with IBM's and 3rd party security,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

Challenges

- Setup and operations may be complicated for some customers with complex use cases.
- Data classification and encryption capabilities are based on 3rd party OEM technologies.
- Integrates two separate products with different architectures, feature parity is still a work in progress.

Leader in

OVERALL LEADER PRODUCT LEADER INNOVATION LEADER MARKET LEADER



Imperva – Data Security Fabric

Imperva is an American cybersecurity solution company headquartered in San Mateo, California. Founded in 2002, the company offers a broad portfolio of security solutions. In 2019, Imperva was acquired by private equity firm Thoma Bravo, making it a privately held company and providing a substantial boost in R&D.

While Imperva is widely recognized as a web application firewall solution provider, the company has also been offering comprehensive security for networks, applications, APIs, and data for more than a decade. In fact, its motto has long been “protecting data and all paths to it”.

A recent strategic product transformation at Imperva has been incorporating their flagship data security products into a single integrated security platform by combining data discovery and classification, data monitoring and protection, data risk analytics, and database vulnerability assessment capabilities. Aligned with this, Imperva has extended its Technology Alliance Program (TAP) to enable data security customers to directly obtain products, support, and services for data masking, encryption, tokenization, key management, and other advanced solutions.

The biggest expansion of Imperva’s platform was brought by the 2020 acquisition of jSonar, creators of the highly innovative agentless security analytics platform designed to be database-agnostic and easily extensible to any kind of structured or unstructured data source. This technology allows Imperva to add support for hundreds of various data stores and environments (on-premises or cloud-native), incorporate new behavior analytics functions, and add database-specific security orchestration (SOAR) into its existing platform.

Two years after the acquisition, the integration was finalized, and the company introduced Imperva Data Security Fabric - a modern, hybrid data security platform with the widest coverage for structured, semi-structured, and unstructured data. The new DSF represents Imperva’s migration from traditional agent-based gateways towards cloud-native or agentless architectures.

These allow for unlimited scalability, massive reduction of the infrastructure footprint, and unified visibility, control, and automation across all environments. DSF elevates security insights for customers by enriching log data with application context through seamless integration across Imperva's data and application security platforms.

A recent launch of what Imperva is calling their DSF Kit delivers Terraform support for multi-cloud orchestration. Global financial institutions are already trusting and adopting Imperva's new solution providing data security to all their clouds. Imperva's upcoming releases featuring an elastic, cloud-native architecture with micro-services integration highlight their commitment to delivering scalable and robust security solutions.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 7: Imperva's rating

Strengths

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

Challenges

- Advanced data protection functions (encryption, tokenization, and enterprise key management) are offered through third-party integrations.
- The Cloud-native version of the platform is still in development and only available as a limited release.
- Despite the potential of the solution, there is limited awareness beyond the US market, and it needs more go-to-market investments.

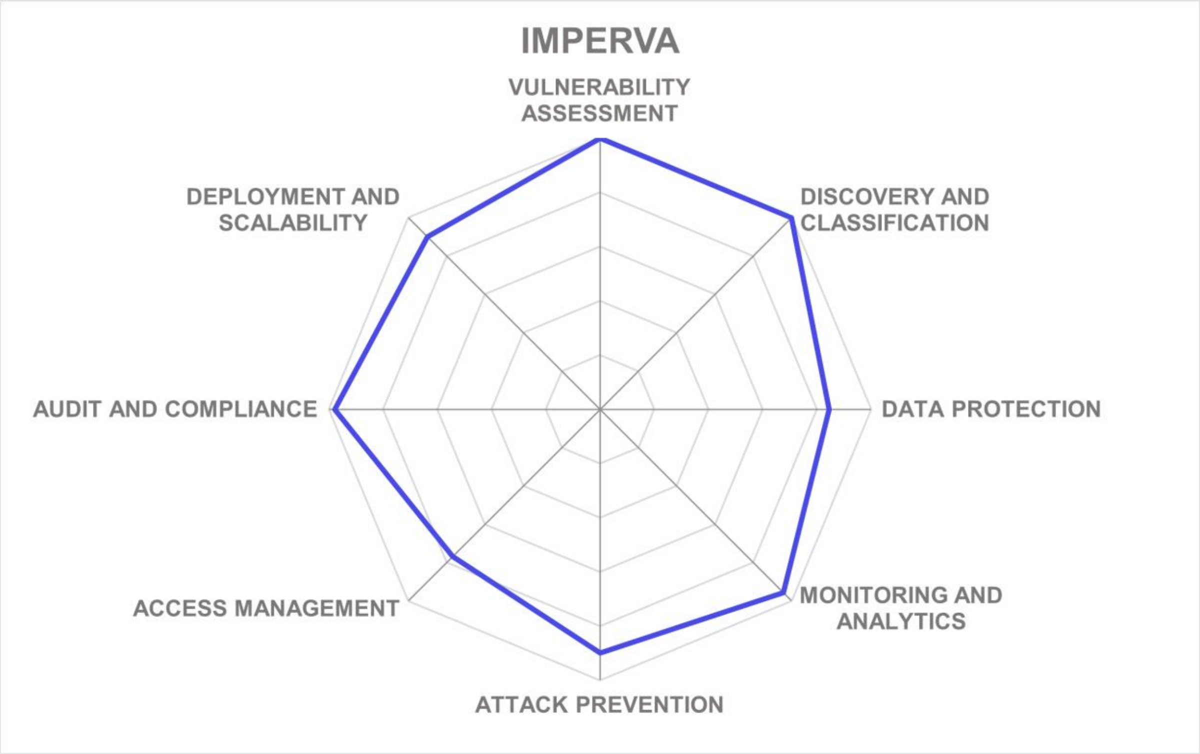
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


IMPERVA
VULNERABILITY ASSESSMENT
DISCOVERY AND CLASSIFICATION
DATA PROTECTION
MONITORING AND ANALYTICS
ATTACK PREVENTION
ACCESS MANAGEMENT
AUDIT AND COMPLIANCE
DEPLOYMENT AND SCALABILITY

Kron – Data Security

Kron Technologies is a public vendor of privileged access management and data security solutions. Founded in 2007 in Istanbul, Turkey, the company currently operates from several offices, including a US one in Jersey City, New Jersey.

Perhaps primarily known for its Ironsphere and Single Connect brands of PAM tools, Kron also offers a portfolio of infrastructure management and operation products for the telecommunications industry, as well as a number of data management and security solutions.

Database Access Manager is implemented as a module for the company's comprehensive privileged access management platform but can be licensed independently. Deployed as a SQL proxy, it transparently performs full monitoring and analytics of all database-related activities.

This way, the platform can provide a full range of access management capabilities: single sign-on and multi-factor authentication, discovery and onboarding of local privileged accounts in databases, activity monitoring and compliance analytics.

In addition, the product utilizes the same technology to manage database access from a single point and provides role-based masking rules to restrict access to sensitive data. A range of connectors for relational databases like Oracle or MS SQL, NoSQL databases like CouchBase and Cassandra, as well as cloud data platforms like Teradata is offered out of the box, with the commitment to develop custom connectors for more exotic data sources on customer request.

Overall, the solution might not be able to compete head-to-head with more sophisticated platforms from other vendors, but it does benefit from the fact that it is a part of a much bigger access management platform – with quick deployments, comprehensive IAM capabilities and a single audit trail across heterogeneous IT systems. The product might be especially appealing to small and medium-sized businesses without enough resources to operate PAM and data security independently.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Positive

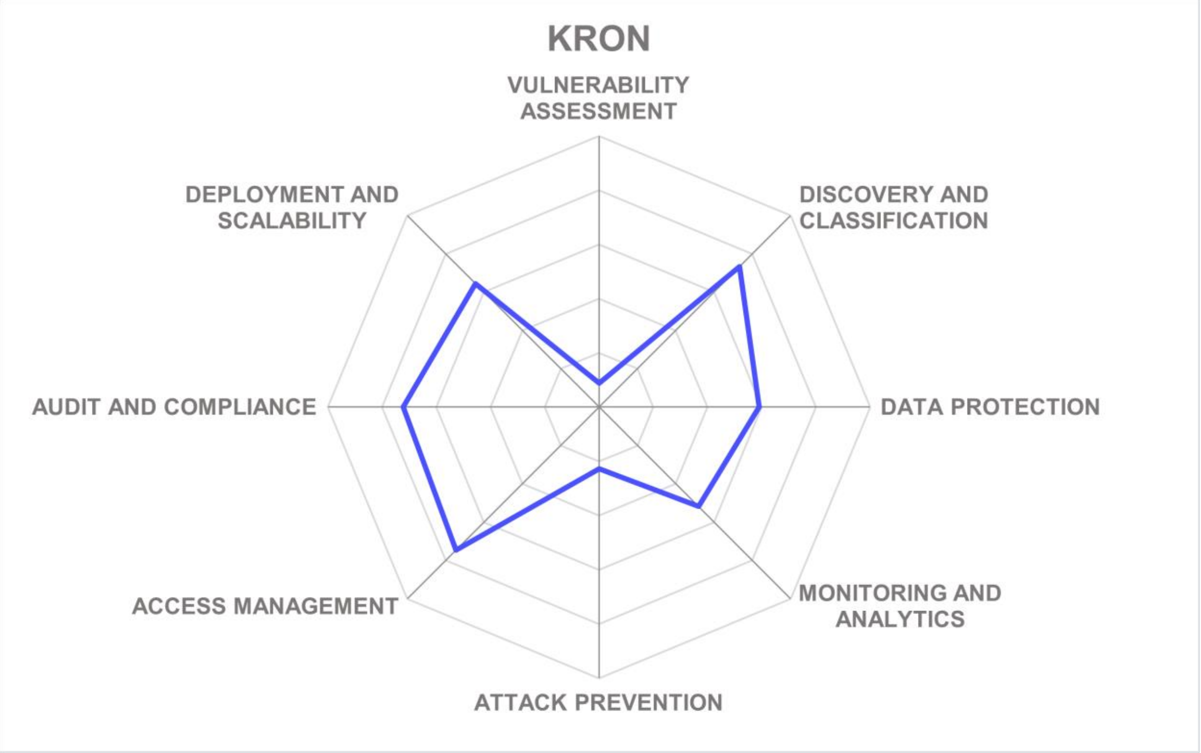
Table 8: Kron's rating

Strengths

- Part of a much bigger “next-generation PAM” platform with unified access management extended to data platforms.
- Support for major relational and NoSQL databases, and Big Data frameworks.
- Strong IAM capabilities, such as account auto-discovery, real user identification, SSO, MFA, etc.
- Comprehensive discovery and data masking capabilities.
- Comprehensive activity monitoring, audit, and compliance features.
- Good UI design for enhanced user experience.

Challenges

- Fairly specialized solution focusing on access management and data masking.
- Does not offer any vulnerability management or attack prevention functions.
- Fairly small visibility outside of the company’s PAM market focus.



Mage Data – Data Security and Privacy Platform

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

Formerly known as Mentis, the company has undergone a major internal transformation and rebranding between 2019 and 2022, re-emerging with a new name, new strategy and vision, and a completely redesigned product portfolio to empower organizations with a data-centric, platform-agnostic approach to better utilizing sensitive or regulated data in a secure, privacy compliant, and responsible way.

The platform's core capabilities include data discovery, analysis and classification, static and dynamic masking, data minimization, activity monitoring, and access control. It is a single integrated solution that has all the modules mentioned above seamlessly communicating with each other. The platform is built with the end user in mind and can be easily managed by a handful of people for the entire enterprise.

Mage Data historical focus has been on Test Data Management (TDM) related capabilities and providing protected but still very usable data sets for DevOps, data analytics and application testing purposes. The platform provides a number of privacy-enhancing technologies to ensure that protected data retains its value for analytics, application testing and other business use cases.

In addition to anonymization or pseudonymization of existing sensitive information, it can also produce completely synthetic yet realistic data for non-production and testing environments. Data Subject Request automation to meet the requirements of GDPR and similar frameworks is also a part of the platform to ensure compliance with privacy regulations.

Mage Data offers an integrated solution for secure digital transformation for businesses migrating their data to the cloud. Not only does the platform help customers to monitor and secure the entire data lifecycle across on-premises and the cloud, but it ensures that the migration itself does not expose the business to additional risks and ensures its continued compliance during the transitional period.

Mage is utilized extensively by global enterprises that are also large Oracle and IBM shops for providing Test Data Management, Static and Dynamic Data Masking, Data Protection, and other capabilities for both structured and semi-structured data formats, as well as unstructured document and other file formats. Many of these capabilities are also available through third-party vendors reselling them to fill gaps in their product suites.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

mage

Table 9: Mage Data's rating

Strengths

- Integrated platform covering most aspects of data security and compliance.
- Broad range of built-in privacy-enhancing capabilities with flexible delivery options.
- Comprehensive coverage of on-premises and cloud platforms, from SaaS services to legacy apps and files.
- Easy to use with modern, convenient UI.
- Strong partner ecosystem, technology partnerships with leading security vendors

Challenges

- Fairly limited attack prevention and infrastructure assessment capabilities.
- Large-scale deployments require an existing data platform for the data layer.
- Relatively small but rapidly growing global customer base.

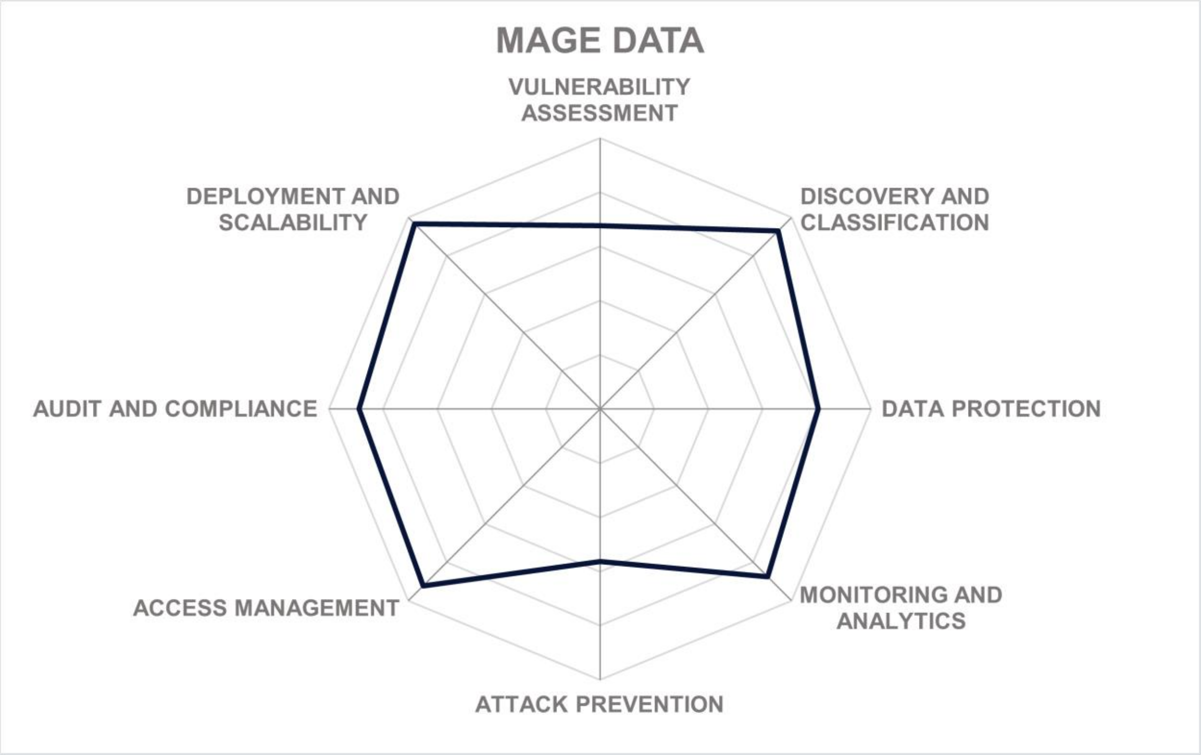
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


MAGE DATA
VULNERABILITY ASSESSMENT
DISCOVERY AND CLASSIFICATION
DATA PROTECTION
MONITORING AND ANALYTICS
ATTACK PREVENTION
ACCESS MANAGEMENT
AUDIT AND COMPLIANCE
DEPLOYMENT AND SCALABILITY

Netwrix – Data Security Portfolio

Netwrix is a private American security software vendor currently headquartered in Frisco, Texas. Founded in 2006, the company has a long history of acquisitions, including the merger with Stealthbits, a cybersecurity vendor specializing in data protection, in early 2021. Since that time, the company can essentially offer its customers two independent data security solutions.

One is based on Netwrix's own technology, including Netwrix Auditor, the company's flagship product focusing on monitoring and mitigating malicious changes in IT infrastructure, augmented by Netwrix Data Classification to perform sensitive data discovery and analysis. This offering is targeted toward small and medium-sized businesses, with a stronger focus on easy deployment, out-of-the-box functionality, and deeper compliance expertise.

In parallel, the Netwrix StealthAUDIT platform acquired from Stealthbits is also available, offering enterprise-level scalability, high configurability, and deeper security expertise to large enterprise customers. Although both platforms have substantial functional overlap, Netwrix has no plan to merge them into a single platform, opting instead for more shared modules and feature parity.

Both platforms are notable for their broad coverage of various structured and unstructured data platforms, both on-premises and in the cloud. In fact, both were also reviewed in detail in KuppingerCole's Market Compass on Data Governance Platforms, showcasing their strong focus on securing unstructured data, and enforcing regulatory compliance.

Another important highlight is the fact that the company offers a broad range of other security tools, which form a strong ecosystem with numerous integrations, cross-correlation, common analytics and reporting capabilities, etc.

Correlating data security-related findings with, for example, user behavior analytics and Active Directory audit helps unlock new insights into the overall security posture of the entire organization.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 10: Netwrix's rating

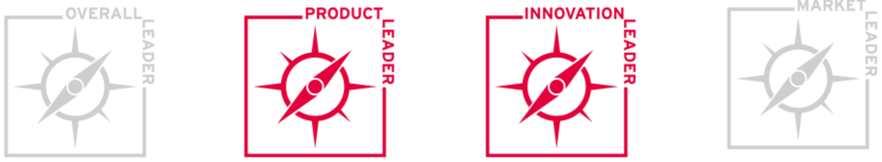
Strengths

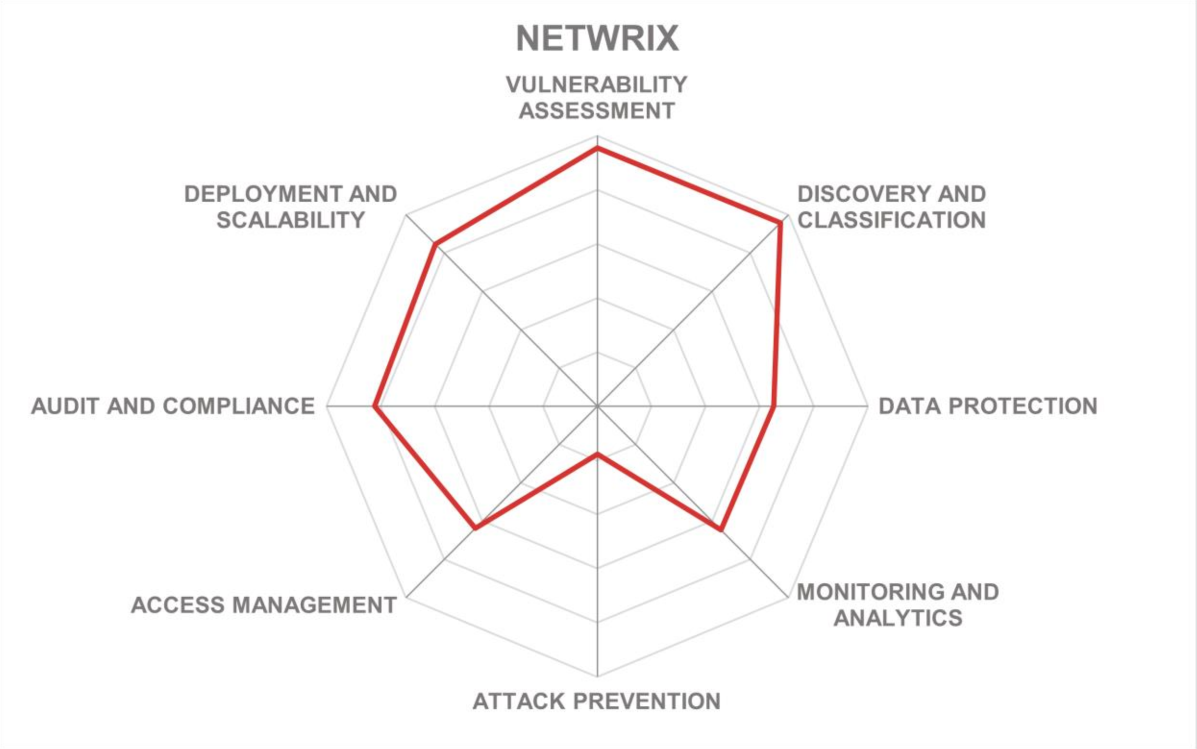
- Broad target platform coverage, including structured and unstructured data sources.
- Highly accurate data classification.
- Visibility and analytics across heterogeneous environments.
- Part of an impressive integrated security ecosystem (IAM, SIEM, SOAR, DLP, ITSM, etc.).
- Ability to address the entire market from SMBs all the way to large enterprises.

Challenges

- By design, different user experiences are offered to enterprise and SMB customers.
- Netwrix data security offering is an on-premises solution; the SaaS offering does not yet include database security.
- A truly integrated IAM-DAG solution is still a work in progress.

Leader in





Oracle – Autonomous Database and Supporting Services

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

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

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

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

More recently, the company continued to deliver innovative features of its flagship database, implementing support for additional data models, multi-cloud authentication, integrated blockchain, improving performance and support for modern distributed architectures, as well as adding more security and compliance controls either directly into the DB core or to the services designed around it. Notably, Oracle has also invested a lot into MySQL, its second database engine with services like HeatWave that combines the familiar developer experience with enterprise-grade scalability and performance for analytical workloads. All these developments ensure that sensitive data can always reside within a single database, consistently protected against security and compliance risks, eliminating the risks related to ETL processes, especially in the cloud.

It should be noted however that a substantial part of the company's security capabilities is still specifically designed for Oracle and MySQL databases only, which makes Oracle's data protection solutions less suitable for companies using other platforms.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 11: Oracle's rating

Strengths

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

Challenges

- Most capabilities are only available for Oracle or MySQL databases.
- Some advanced security functions are only supported in the Oracle Cloud (or its partners).
- Big Data and NoSQL products are not yet integrated with RDBMS security solutions.

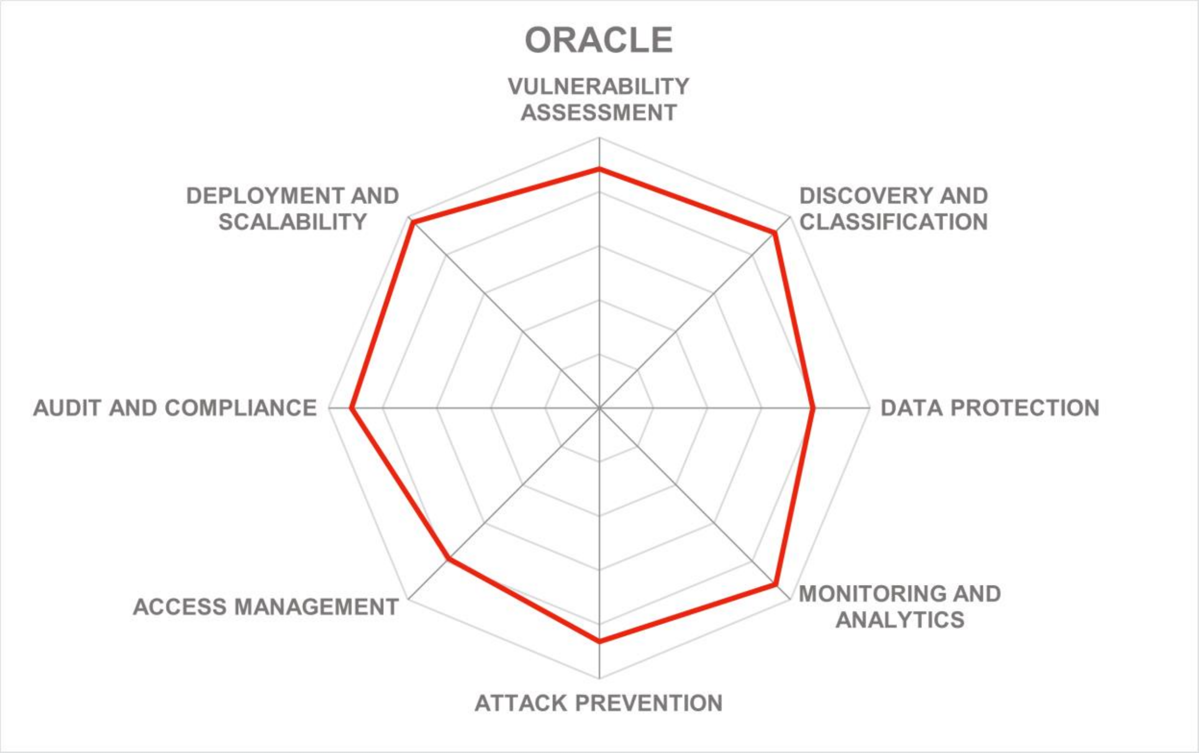
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER



PKWARE – PK Protect

PKWARE is an enterprise data protection software company that provides discovery, classification, masking, and encryption solutions, along with data compression software, used by organizations in financial services, manufacturing, military, healthcare, and government. Founded in 1986 and headquartered in Milwaukee, Wisconsin, it is perhaps best known for bringing to the market the popular ZIP archive standard.

However, since the early 2010s, the company's focus has shifted towards data protection. In 2020, PKWARE acquired Dataguise, a company known for its sensitive data governance platform to discover, monitor, and protect sensitive data on-premises and in the cloud across multiple data environments.

The same year, PKWARE itself was purchased by a private equity firm Thompson Street Capital Partners. Rebranded in 2021, the PK Protect Suite combines all former products into a unified solution for protecting sensitive data through discovery, classification, masking, redaction, and encryption.

A notable differentiator of the company's solution is its two-pronged approach – securing sensitive data not just in data stores, but on endpoints that access these stores as well. Using agents deployed on endpoint devices, PK Protect Endpoint Manager automatically applies the same discovery and protection capabilities on endpoints as the Data Store Manager does for data stores, all while minimizing user disruption. When the entire suite is deployed across endpoints as well as databases, servers, and cloud, customers can be sure that their sensitive data is always protected, no matter where it lives and moves.

The PK Protect suite comprises individual modules responsible for data discovery, classification, masking, encryption, and privacy. Among the numerous offered capabilities, the very broad range of supported data stores is especially notable, ranging from databases and cloud data platforms to file servers and even mainframes. Discovery and classification are optimized for both speed and flexibility, ensuring that even the largest repositories can be handled quickly and exactly according to business requirements.

In addition to a strong focus on maintaining regulatory compliance with frameworks like GDPR, CCPA or HIPAA, PK Protect includes a specialized privacy module for handling DSA requests, automating the redaction processes needed for implementing the "right to be forgotten", analyzing the impact of data breaches, and enforcing multiple privacy-enhancing technologies in real time.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Neutral

PKWARE

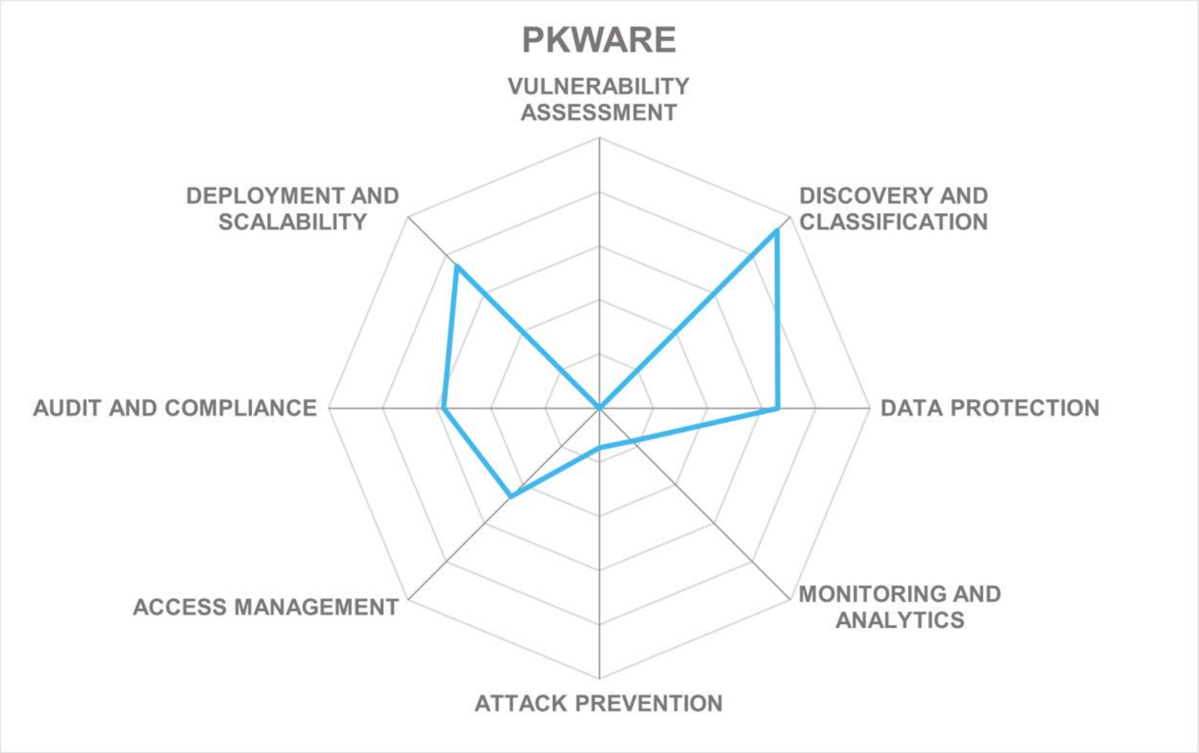
Table 12: PKWARE's rating

Strengths

- Very broad target platform support, including relational and NoSQL databases, data warehouses, Hadoop platforms, object stores, file servers, and endpoints.
- Two-pronged approach towards data protection – both in data stores and on endpoints.
- Fast discovery processing of very large data repositories.
- Flexible choice of classification processes, from manual to AI-powered to third-party integrations.
- Broad selection of privacy-enhancing technologies to enforce regulatory compliance.

Challenges

- Quite specialized solution, lacking vulnerability assessment or attack prevention capabilities.
- No single unified UI for all products is available.
- Very limited market presence.



SecuPi – Data Security Platform

SecuPi is a privately held data-centric security vendor headquartered in Jersey City, NJ, USA. The company was founded in 2014 by entrepreneurs with a strong background in financial technology, also known for co-inventing the very concept of dynamic data masking. However, realizing later that data masking alone does not solve modern privacy and compliance problems, they set out to address the challenge in a more sophisticated way.

As opposed to most competitors that protect information at the database level using database agents or gateways which makes it a challenge to identify the end user hiding behind anonymous service accounts, SecuPi's approach is to embed overlays with no code changes directly into application stacks to collect the context attributes as well as the data request. It also includes gateways for controlling direct DB tools and analytics environments.

The SecuPi overlays support all major development platforms like Java or .NET. SecuPi also provides the exact same column-level FPE encryption or tokenization but completely transparently to the data layer or the application layer. This is applicable for a broad range of databases, big data platforms and other semi-structured data stores, with no code changes or additional API calls needed for existing applications. Also, this approach gives the platform access to real user identities and not to typical service accounts used to connect to databases. With this technology, SecuPi delivers a single privacy-focused data protection platform for on-premises and cloud-based applications, which is easy to deploy and to operate thanks to the centralized management of data protection policies.

SecuPi software platform brings data-centric security and compliance closer to application owners and business units, enabling sensitive data discovery, classification, anonymization, and minimization across the whole organization, with centralized policy management along with real-time monitoring of all data flows and user activities. Fine-grained PBAC/ABAC combined with data protection options, built-in controls for user consent management, anonymization, and other data subject rights (such as the right to be forgotten) ensure that all existing applications can be made compliant with GDPR and similar regulations quickly and without the need to adapt existing database structures.

Since our last review, SecuPi has substantially grown both internally and regarding its market presence, focusing its messaging on the notion of fighting against fragmentation of the data protection market.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 13: SecuPi's rating

Strengths

- Integrated data protection and privacy platform with a strong focus on regulatory compliance and de-identification of critical data in the cloud.
- Full coverage for the data protection lifecycle.
- Application-level protection overlays simplify deployment and management.
- Broad support for big data and cloud analytics platforms.
- Secure privileged access to databases with SSO and Passwordless

Challenges

- Architecture potentially limits the support of legacy platforms.
- Not focusing on database infrastructure assessment.
- Potential buyers might not initially require all available capabilities.

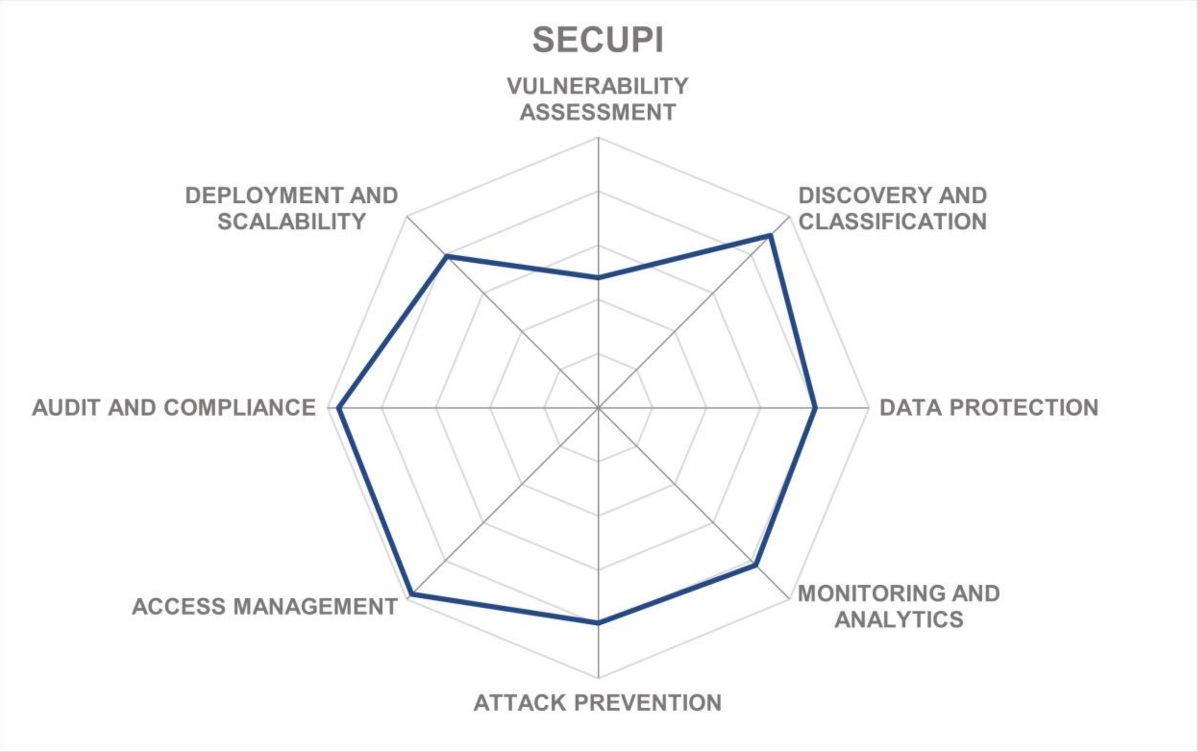
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER



Thales Group – CipherTrust Data Security Platform

Thales Group is an international company headquartered in Paris, France, which provides solutions and services for defense, and aerospace markets. In 2019, Thales completed the acquisition of Gemalto, incorporating the technologies of Gemalto and SafeNet, its former major competitors in the data protection market.

Thales Cloud Protection and Licensing (CPL) is a business line in the Digital Identity & Security global business unit of Thales Group with over 40 years of experience in information security. The company is a veteran player in such areas as hardware security modules (HSM), data encryption, key management, PKI, Identity and Access Management, and Software Licensing.

The CipherTrust Data Security Platform represents the results of the consolidation of the former SafeNet and Vormetric data protection portfolios. It provides a full range of data-centric security capabilities, including data discovery and classification, transparent encryption, database and application data protection, data masking, tokenization, access controls, enterprise key management, and cloud key management unified from a single management interface.

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

Thales has the broadest ecosystem of technology partners, and therefore will meet the largest set of use cases. Its new data discovery and classification product is an important addition to the platform. However, their strongest focus remains with their transparent encryption and key management solutions that work on premises, in private and public cloud environments. It supports privileged user access control, Live Data Transformation, and works across traditional database, Big Data, and Teradata environments. Thales is also well positioned in the Cloud Sovereignty space with deployments in France and Germany.

The platform provides a single pane of glass to simplify operations across all capabilities and environments, as well as unified policy management, administration, and maintenance operations. 100% CLI and API coverage makes a wide range of integration, DevOps and DevSecOps scenarios possible.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 14: Thales Group’s rating

Strengths

- Comprehensive data discovery and classification, transparent encryption, tokenization, access control and masking capabilities.
- Broadest enterprise key management support including KMIP, TDE, Always Encrypted, and Cloud Key Management.
- High-performance thanks to hardware encryption support.
- Centralized management across all environments, even third-party products.
- Standard APIs for adding encryption support to existing applications.
- A Free Community Edition of the platform is available, limited only in deployment size.

Challenges

- Does not offer attack prevention capabilities.
- Some advanced use cases are only possible with third-party integrations.
- Some application-level integrations are not transparent, require code changes.

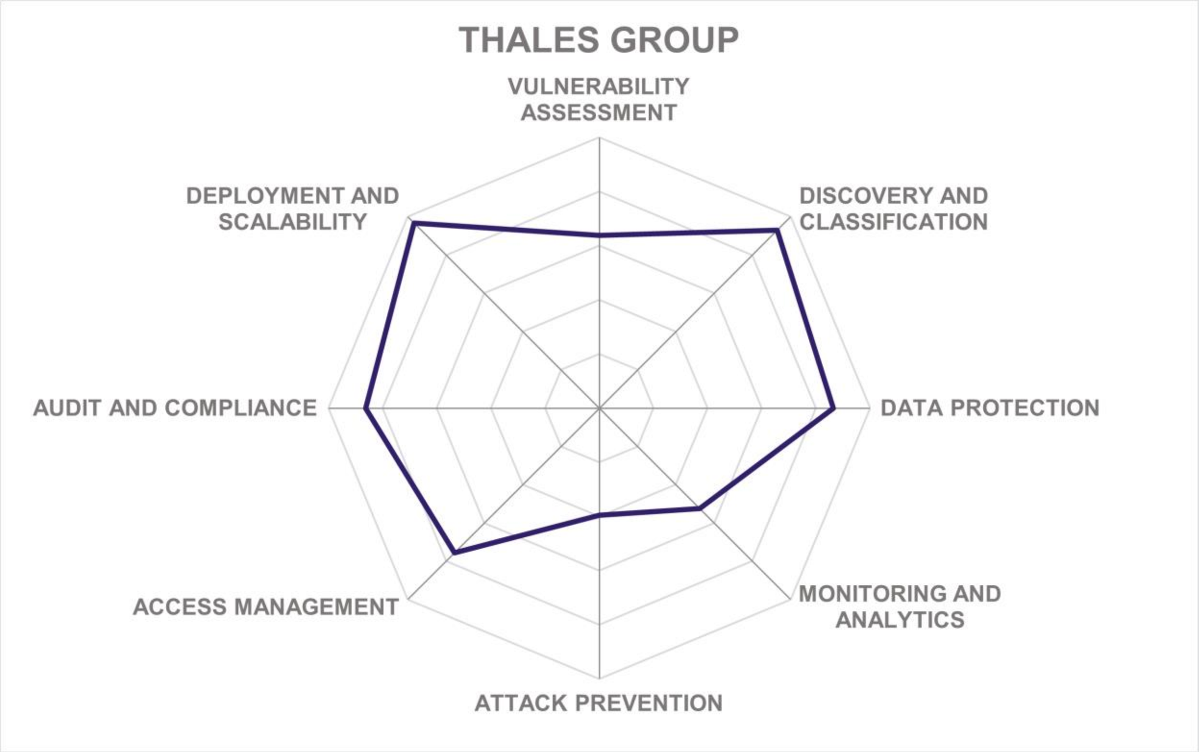
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER



Titaniam – Data Security Platform

Titaniam is an American data protection startup headquartered in San Jose, California with an additional office in Chennai, India. Founded in 2019, the company has pioneered an innovative high-performance encryption-in-use technology that enables customers to work on sensitive data without decryption and ensures that this data can only be released to an external party in a privacy-preserving format.

Based on this universal platform that supports many structured and unstructured data sources, Titaniam offers an entire portfolio of individual products that can be selected and combined for different use cases – cloud or on-premises, inline or API-based, modern or legacy. Together they enable portable, composable, always-on data security, when data remains encrypted even in use across heterogeneous platforms with customer-owned keys.

Customers can choose between several modules. Titaniam Vault is a self-contained standalone solution that provides full-featured search and analytics capabilities for relational and NoSQL data, supports encryption-in-use, searchable encryption as well as traditional controls such as vaulted and vaultless tokenization, regular and format-preserving encryption, static and dynamic data masking, and is guaranteed never to release any data unencrypted.

Titaniam Plugin is intended for extensible data platforms like Elastic, Titaniam Proxy for external databases and object stores, and Titaniam API for direct application integrations. The Titaniam Studio provides this centralized configuration and management UI across the entire deployment. Titaniam also provides granular key derivation as well as BYOK/HYOK functionality for data owners to own and control the security of their own data.

It’s worth highlighting, however, that the company’s technology can only work to its full potential on data sources where schemas and required computational operations on them are known in advance and then appropriately configured within the Titaniam Studio. For traditional controls like tokenization or masking, Titaniam offers additional new capabilities such as search and analytics without detokenization as well as granular policies that can include multiple private data formats in the same policy.

Still, the product is also suitable for many general-purpose deployment scenarios, such as creating a secure data lake on top of encrypted S3 object stores. For unstructured data, Titaniam can encrypt at the file level as well as create a search index that allows files to be searched without decryption.

Data protection is also the only focus of the entire platform. There are no vulnerability assessment or attack prevention capabilities, and the approach toward data classification is also completely different from other vendors. However, one can argue that by keeping the data encrypted 100% of the time, customers dramatically minimize their attack surface and are automatically protected from most infrastructure-related risks. It is also worth noting that the company is already working on integrations with external data discovery solutions.

Security	Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

Table 15: Titaniam's rating

Strengths

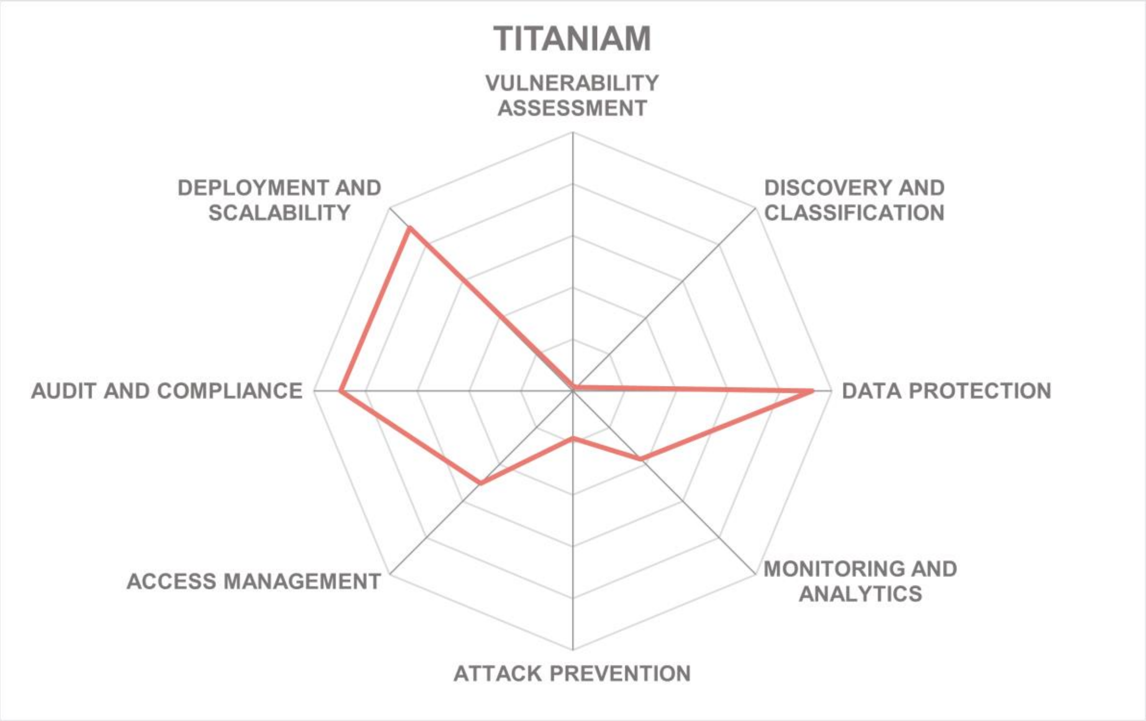
- Unique encryption-in-use technology offered as a lean, high-performance alternative to homomorphic encryption and similar concepts.
- A comprehensive set of additional data security controls including tokenization, encryption, static and dynamic data masking, redaction, and hashing.
- Native support for Bring/Hold Your Own Key scenarios.
- Centralized configuration, management, monitoring, and reporting of the entire platform in a single Studio console.
- Quick and easy deployment at the customer's own pace, minimal performance overhead.

Challenges

- A highly specialized solution that only focuses on data protection.
- Applications are limited to use cases where the data schema is known in advance.
- Early-stage startup, yet to reach a substantial market presence.

Leader in

OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


TITANIAM
VULNERABILITY ASSESSMENT
DISCOVERY AND CLASSIFICATION
DATA PROTECTION
MONITORING AND ANALYTICS
ATTACK PREVENTION
ACCESS MANAGEMENT
AUDIT AND COMPLIANCE
DEPLOYMENT AND SCALABILITY

TrustLogix – Data Access Governance Platform

TrustLogix is an American cybersecurity startup based in Mountain View, California. Established in 2019 by a team of veteran IAM and security specialists, the company's vision is to develop a unified approach to Data Security Governance. In a world where businesses are struggling to find a balance between accessing and securing numerous isolated data platforms, TrustLogix offers a unified platform that centralizes observability and simplifies the implementation and enforcement of fine-grained access control across all environments.

The company has introduced its own universal security governance framework to observe and discover data access patterns across heterogeneous data platforms, provide unified visibility and recommendations for data owners, provision and enforce local access controls, and re-certify users accessing the data according to corporate policies.

TrustLogix's platform is the reference implementation of this framework. With its containerized and/or serverless architecture, the data plane components (Trustlets) of the platform can run in multiple clouds close to supported data platforms (such as Snowflake, Microsoft SQL Server, or Amazon RedShift) and scale natively with demand. The decoupled control plane is deployed only once (customer-managed or SaaS), delivering full visibility into activities across all connected environments.

Customers can easily identify how much data is not yet covered by protection, identify ineffective access controls, observe anomalous activities, and receive actionable recommendations for improving the current posture. The actual access controls are configured directly in the target platforms using their native capabilities – thus the platform itself operates completely out-of-band and transparently for applications and users.

The platform ships with a library of predefined monitoring policies, so there is no need for a lengthy initial setup. Instead of risk scores or timelines, TrustLogix focuses on delivering timely recommendations for turning observed activities into access policies. With time, it learns to understand customer baselines better without additional training.

Access policies operate on native principals and other artifacts from target platforms and are directly translated into their native access controls but are maintained in an agnostic form to ensure that monitoring, access management, and privacy controls function uniformly across heterogeneous environments.

Currently, TrustLogix partners with major data platform vendors, such as Ataccama, AWS, Collibra, Databricks, or Snowflake. Additional partnerships (for example, with Google Cloud) are planned for the future.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

TRUSTLOGIX

Table 16: TrustLogix's rating

Strengths

- A unique universal security governance framework with a reference implementation in the company's platform.
- Cloud-native containerized architecture that seamlessly supports multi-cloud deployments and unlimited scalability along with centralized management.
- Out-of-band transparent operations – no need to change applications, no performance overhead.
- Partnerships with numerous leading cloud data platform vendors.
- Ease of deployment directly from the target platforms' respective marketplaces.

Challenges

- By design, only manages target platforms' native capabilities; does not provide its own controls.
- Requires native-level integrations with specific data platforms, expanding the list of supported ones is still on the roadmap.
- Early-stage startup, yet to reach a substantial market presence.

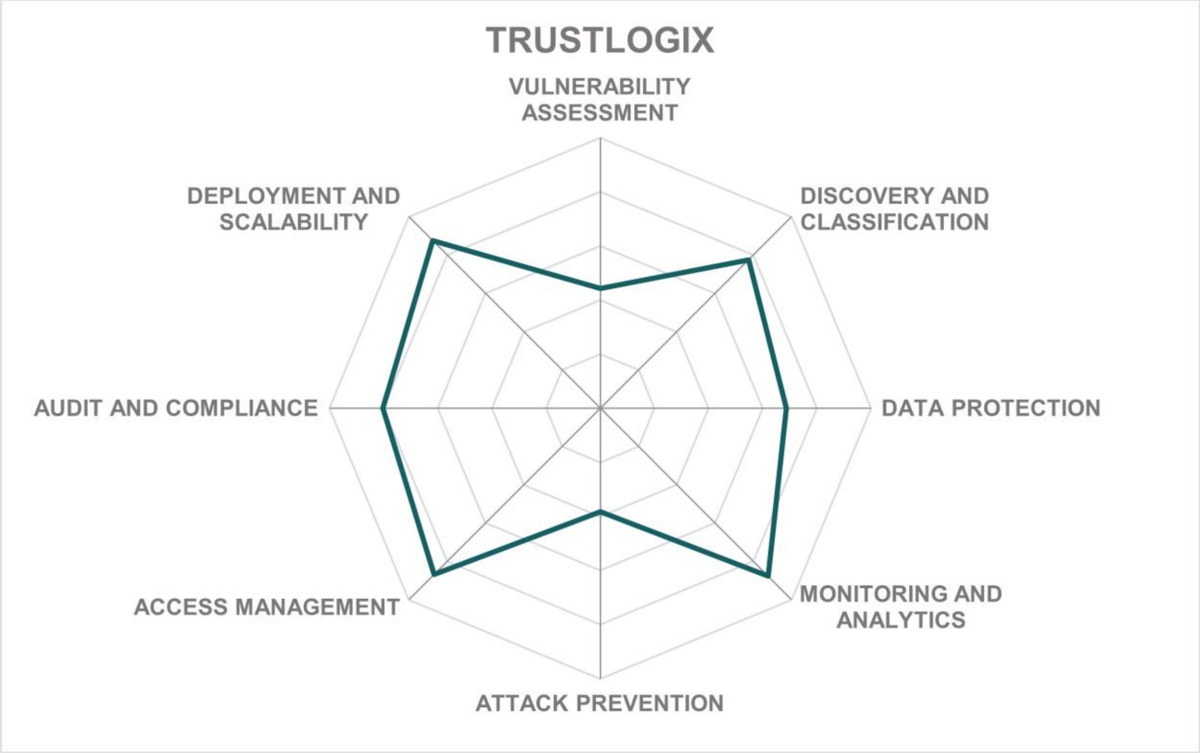
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment, or they may be a fast-growing startup that may be a strong competitor in the future.

Special cases for this particular market segment are the major public cloud providers. Although Oracle is perhaps the only CSP that, due to its historical roots as a database vendor, places such a strong emphasis on data security capabilities of its cloud infrastructure, other major companies, including AWS, Google Cloud, and Microsoft Azure, offer their own database and other data management services, naturally complemented with various security and compliance controls.

Although such services are usually limited to the CSP’s own cloud-native technology stacks and management APIs, they can be perfectly sufficient for a broad range of use cases and should be taken into consideration before making any 3rd party investment decisions.

1touch.io

1touch.io is a private, US-headquartered, Israeli-based technology company providing automated real-time discovery, mapping, and tracking of sensitive data. Founded in 2017 with the main seat in New York, the company offers its Inventa platform as a universal solution to track sensitive data across all IT systems within an organization, including both structured and unstructured data of various formats.

Why worth watching: 1touch.io has OEM technology partnerships with several major data security vendors, including some of the leaders covered in this rating. You might be already using it, even if you don’t know the name.

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. Axiomatics is a major contributor to the OASIS XACML standard, and all their solutions are designed to be 100% XACML-compliant. The company offers a wide range of authorization solutions for applications, databases, and cloud data stores.

Why worth watching: 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.

BigID

BigID is an American vendor of data governance, security, and privacy solutions based in New York. Founded in 2016, the company started as a primarily privacy-centric solution but has expanded to include other industry use cases ranging from security to data integration and quality management. The company’s integrated platform covers a broad range of data sources and offers innovative capabilities like strong ML support.

Why worth watching: The BigID Data Intelligence Platform offers strong support for DevOps and automation to help even the largest businesses understand and protect their data with minimal effort.

CyberRes

CyberRes is a line of business originally within Micro Focus, a large multinational software vendor and IT consultancy established in 1976 in the UK. In early 2023, OpenText, a leading Canadian Information Management vendor, completed the acquisition of Micro Focus, gaining control over the entire CyberRes security portfolio. Voltage SecureData Enterprise is the company’s data security platform for protecting sensitive enterprise data.

Why worth watching: The platform provides comprehensive data protection through transparent encryption and pseudonymization across multiple database types and Big Data platforms, on-premises, in the cloud, and on the edge.

IDERA

IDERA is a division of Idera, Inc, a global supplier of B2B software productivity solutions that manages a large number of development and database brands. Founded in 2000 and based in Austin, Texas, IDERA offers a broad portfolio of data modelling, monitoring, and protection products spanning on-premises, cloud, and hybrid platforms. The family of IDERA PROTECT products focuses on protecting data integrity and compliance.

Why worth watching: the company’s comprehensive portfolio can provide solutions for the entire lifecycle of data protection and compliance, starting from the early design stage.

Immuta

Immuta is a provider of cloud data access solutions headquartered in Boston, Massachusetts. Founded in 2015, the company strives to help its customers speed up access to their sensitive data in the cloud by removing the complexity associated with data protection and compliance. The company’s Data Access Platform integrates with all major cloud-native data platforms.

Why worth watching: with Immuta, customers can create data policies once and ensure that they are enforced consistently and transparently across multiple clouds and data platforms.

Informatica

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

Why worth watching: Data Privacy Management provides sensitive data risk management and mitigation tools in a single product with integrations with Informatica's flagship data masking products as well as some third-party data protection products and security information systems.

MinerEye

MinerEye is an Israeli data governance and protection vendor based in Hod Hasharon, Israel. Established in 2014, the company focuses on solving the greatest challenge of unstructured data – understanding its content and criticality. Analyzing data, classifying it, and monitoring its use is the core goal of the MinerEye DataTracker product – both on-premises and in the cloud.

Why worth watching: thanks to the high degree of automation and scalability and out-of-the-box integrations with all major cloud data stores, MinerEye helps to not just achieve consistent data governance quickly, but to substantially reduce overall cloud costs.

Okera

Okera is a US provider of data access management solutions headquartered in San Francisco, California. Founded in 2016 and privately funded, the company is developing its flagship Dynamic Access Platform as a solution for centralized managing, enforcing, and auditing of platform-agnostic data access policies that speak the language of business. On this foundation, Okera offers a range of vertical solutions for highly regulated industries.

Why worth watching: migrating from traditional role-based permissions to dynamic, business-focused policies assisted by automated discovery, classification, and usage intelligence can dramatically reduce complexity and reduce data friction.

Privitar

Headquartered in London, UK and founded in 2014, Privitar has its roots in academic research on data privacy. Nowadays, it provides a range of data provisioning, privacy, and compliance solutions suitable for regulated industries like finance and healthcare. These tools ensure that customers can safely access and analyze highly sensitive data, while maintaining worldwide compliance with privacy and data protection laws.

Why worth watching: Privitar’s services are trusted by major financial and healthcare institutions for their strict adherence to privacy principles and compliance with all notable regulatory frameworks.

Protegrity

Protegrity is a privately held software vendor headquartered in Salt Lake City, Utah. Since 1996, the company has been in the enterprise data protection business. The Protegrity Data Protection Platform helps organizations discover, classify, and maintain full visibility into their sensitive data and then implements a variety of technologies, including data encryption, masking, tokenization, and monitoring across multiple environments – from mainframes to clouds.

Why worth watching: the platform focuses on providing full transparency regarding the state of data, so that customers can always choose the most appropriate protection technology suitable for their business processes.

Raito

Raito is a cloud data access management startup based in Brussels, Belgium. Established in 2021, the company develops a cloud-based solution for observability, collaboration, and automation for data teams to ensure frictionless yet secure access to cloud data at scale. With productivity and automation as a primary focus, Raito strives to provide developers, data scientists and businesspeople with quick, painless access to their data, while hiding the complexity of security and compliance from them.

Why worth watching: Raito’s solution is designed for modern, innovative, cloud-native organizations, and the tools they are offering reflect this focus.

Satori

Satori is a security startup vendor based in Rehovot, Israel. Founded in 2019, the company offers its Secure Data Access Cloud as a platform for decoupling access, security, and privacy from the data layer and replacing platform-specific permissions and policies with a single unified authorization engine. Deployed as a transparent proxy, Satori supports fault-tolerant, highly scalable configurations.

Why worth watching: with out-of-the-box support for major cloud-native databases and data platforms, Satori can be deployed within days, does not require changes in existing infrastructure or applications, and does not impact users.

Methodology

The KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

Types of Leadership

We look at four types of leaders:

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well, there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logical and intuitive, as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are, in general, more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a “good citizen” in heterogeneous IT environments.

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

Rating scale for products and vendors

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

Strong positive
Outstanding support for the subject area, such as product functionality, or outstanding position of the company for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren’t met, while others are well served. For Market Position, it could indicate a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

- Limited market visibility: There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This is usually a clear indicator of a lack in Market Leadership.
- Declined to participate: Vendors might decide not to participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- Lack of information supply: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

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

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

Related Research

Leadership Compass: Database and Big Data Security

Leadership Compass: Enterprise Databases in the Cloud

Leadership Compass: Data Quality and Integration Solutions

Market Compass: Data Governance Platforms

Buyer’s Compass: Database and Big Data Security

Whitepaper: Why Your Organization Needs Data-centric Security

Leadership Brief: Introduction to the Information Protection Life Cycle and Framework

Executive View: comforte AG SecurDPS Enterprise

Executive View: Delphix Dynamic Data Platform

Executive View: Oracle Database Security Assessment

Executive View: Oracle Data Safe

Executive View: Thales Vormetric Application Crypto Suite

Executive View: Informatica Data Privacy Management

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.

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

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

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