kuppingercole ANALYSTS

Data Security Platforms

Alexei Balaganski

March 12, 2025

The KuppingerCole Leadership Compass on Data Security Platforms provides a comprehensive analysis of the current market landscape, highlighting the evolving nature of data security solutions. As the digital landscape continues to change, the need for adaptable and comprehensive data security platforms becomes increasingly critical for organizations aiming to protect sensitive information across diverse environments. This report identifies key players in the market, categorizing them based on product capabilities, innovation, and market presence.

Contents

Executive Summary

Over the past decade, the data security landscape has undergone significant transformation, transforming from traditional database protection mechanisms to comprehensive platforms addressing diverse data environments. KuppingerCole Analysts has been at the forefront of this evolution, providing in-depth coverage and guidance to organizations navigating these changes. Our initial focus on database security has expanded to encompass broader data security platforms, reflecting the industry's shift towards more integrated and versatile solutions.

Data security is, of course, much older than a decade and in a sense, even predates computers and the IT in general. Nowadays, however, it usually refers to the practice of protecting digital information from unauthorized access, corruption, or theft. It involves implementing measures to safeguard data from cyber threats, accidental loss, and malicious attacks. This functional area covers various security controls for the information itself stored and processed in systems, underlying computing and network infrastructures, as well as the applications accessing the data.

Figure 1: Data challenges the businesses are facing nowadays.

As computing and storage technologies continue to improve, and modern applications embrace distributed, heterogeneous, cloud-native architectures, the very notion of a data store is changing as well. Just a decade ago, specialized and expensive “big data” solutions affordable only to large enterprises were necessary to deal with business analytics or scientific research. They coexisted with more traditional relational databases, as well as various methods of storing unstructured information. Later, various kinds of NoSQL alternatives have emerged, such as document, graph, or vector database engines.

However, a modern distributed, loosely coupled, and heterogeneous application can easily deal with multiple data models and thus work with multiple databases in parallel. Since all these engines can be deployed in public clouds using commodity infrastructure, the technical differences between them are gradually becoming less and less important. In a sense, from

a business perspective, data is data, regardless of the underlying storage technology. Organizations are much more concerned with the business challenges and risks of data.

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 in 2024 exceeding $4.88M globally (and up to $9.36M 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.

Data only generates value when it is moving or transforming, creating insights, analytics, statistics, etc. – that is, it serves a tangible purpose for a certain business process. A data security solution 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, even in use.

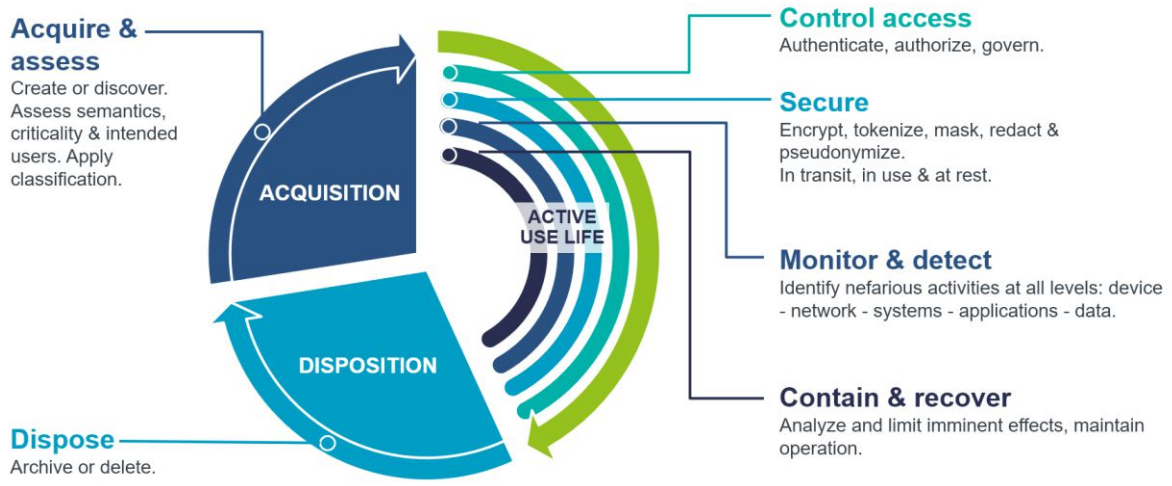


Figure 2: Information protection lifecycle.

Digital data can be exposed to the following types of security risks:

- Denial-of-service attacks that lead 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 unprotected 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.

Several more recent pivotal trends and challenges have heightened the importance of data security for businesses.

The proliferation of multi-cloud and hybrid environments: multi-cloud strategies offer organizations flexibility and scalability. However, they create additional complexities in data management and security. As data flows between various platforms, each with distinct security protocols, ensuring consistent security policies and maintaining visibility across these environments are critical challenges.

Increasingly harsh and complex privacy regulations: as the result of growing political tensions, countries introduce their own stringent requirements for sensitive data handling and protection. Organizations must implement and sustain comprehensive data governance frameworks to ensure compliance, avoid penalties, and maintain customer trust.

The rise of Generative AI (GenAI): AI has revolutionized data processing and utilization. However, it also raises various concerns regarding data privacy and security, as multiple new threat vectors and potential data leaks are introduced in GenAI systems.

Therefore, customers are encouraged to look at 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.

This Leadership Compass is designed as a tool to help organizations to identify their requirements and map them to the capabilities offered by specific vendors, considering the size, growth, skills, and budget of the customer organization. To better understand the fundamental principles this report is based on, please refer to the KuppingerCole Leadership Compass Methodology.

Key Findings

- Data security is a key discipline that is critical for safeguarding the business continuity and the very livelihood of modern businesses by protecting their valuable and sensitive data from cyber threats, accidental loss, and malicious attacks.
- Key aspects of data security are maintaining confidentiality, integrity, and availability of digital information; ensuring regulatory compliance with multiple international, industry-wide, and local laws and regulations; as well as building and maintaining trust with customers and stakeholders.
- The emergence of new trends like Generative AI and multi-cloud architectures has even further increased the complexity of modern data processing and consequently made the scope of data security even broader and more complex.
- Data Security Platform is a recently emerged term that represents the customer demands for a universal data protection solution that provides comprehensive security and compliance capabilities, regardless of the data format, platform, or location.
- However, alternative approaches like Data Security Posture Management (DSPM) solutions are also rapidly gaining popularity due to their relative simplicity and fast deployment possibilities.
- The rapid transformation of the market continues. Some 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.
- The Overall Leaders in Data Security Platforms are (in alphabetical order): IBM, Netwrix, OpenText, Oracle, SecuPi, Thales, TrustLogix.

Market Analysis

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 to develop a solution that covers all or at least several functional areas. As a consequence, some 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-the-art tools that require additional effort to make them work together. Individual

evaluation criteria and the spider charts demonstrating our assessment of each of those areas for each solution will provide you with further guidance in this process.

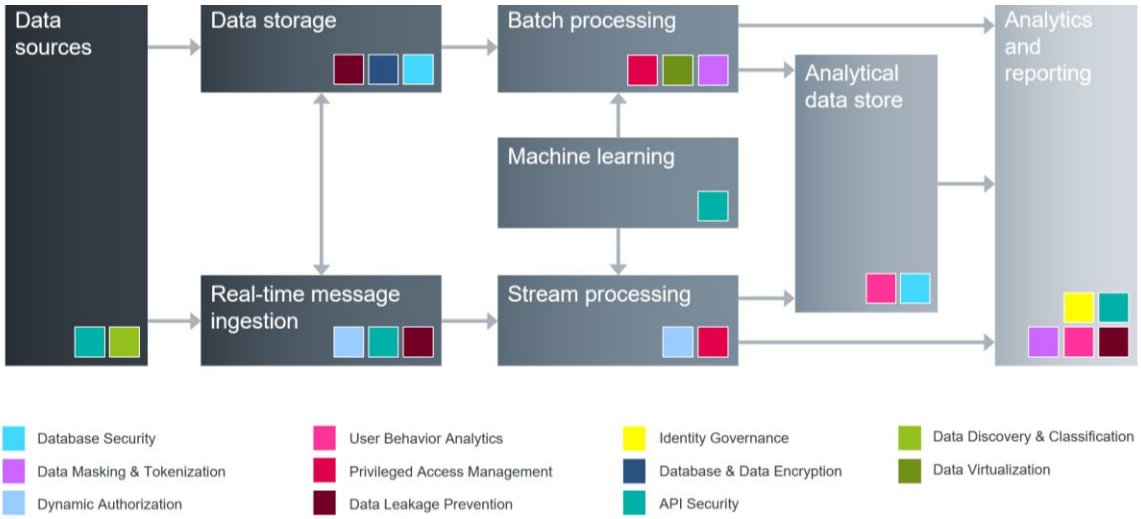


Figure 3: Data movement and transformations, which must be covered by data security controls.

Another complicating factor that must be considered is the turbulent nature of the entire market – after years of constant mergers and acquisitions, it is still far from stabilizing. Just since the publication of our previous Leadership Compass, the data security sector has witnessed significant changes.

In December 2023, Thales completed its acquisition of Imperva, a leader in application and data security. This strategic move positioned Thales as a global cybersecurity leader, enhancing its capabilities in protecting data across various environments, and also promotes the company to the overall leadership in this report. Earlier that year, OpenText acquired Micro Focus, gaining control over their entire security portfolio. The company has also been recognized among the overall leaders in our current rating.

Concurrently, several smaller firms have left the data security market, either through acquisitions or due to their inability to keep pace with rapidly changing security demands. For example, Titaniam, an encryption-in-use startup we praised as an innovation leader last time, has completely disappeared from our radars after a rebranding and switching focus to the generative AI market. This trend underscores the increasing necessity for comprehensive platform-oriented solutions and the challenges smaller providers face in delivering them.

Delivery Models

As opposed to many other segments of the entire cybersecurity market, data protection solutions do not necessarily follow the universal trend of transitioning from on-premises deployments to the fully SaaS-based delivery model. On the one hand, this can be explained by the complex, hybrid nature of the systems they are supposed to secure.

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.

On the other hand, multiple compliance regulations and corporate policies strictly prohibit sending sensitive business data to the public cloud, especially outside the region where the customer organization is operating. Thus, even entirely cloud-native organizations might opt for deploying and managing security tools on their own cloud infrastructure instead of trusting a third party to manage it for them. Still, even among the vendors covered in this report, some specifically offer solutions that only collect desensitized metadata from customers and not the data itself, thus working around potential compliance violations.

DSP vs. DSPM

A **Data Security Platform (DSP)** is an integrated suite of tools designed to safeguard sensitive information across an organization's entire data landscape. Their key capabilities include:

- **Data Discovery and Classification**: Identifying and categorizing sensitive data to apply appropriate protection measures.
- **Data Access Control**: Managing user permissions to ensure that only authorized personnel can access critical data.
- **Data Protection:** Protecting data at rest and in transit to prevent unauthorized access during storage or transmission.
- **Monitoring and Analytics:** Continuously overseeing data activities to detect and respond to potential security incidents promptly.

In fact, the major required capabilities for such solutions are outlined later in this chapter, and they were utilized as the basis for our assessment of the products covered in this Leadership Compass. These platforms aim to provide a holistic approach to data security, ensuring comprehensive protection across diverse environments. 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.

While at KuppingerCole, we remain the proponents of comprehensive, full-featured data security platforms, we cannot ignore the rising popularity of **Data Security Posture Management (DSPM)** solutions. Unlike conventional data security solutions that primarily focus on access control and encryption, DSPM tools specialize in identifying misconfigurations, access anomalies, and compliance gaps in real time. Just like their spiritual predecessors Cloud Security Posture Management (CSPM) tools, DSPM solutions are primarily aimed at customers with large cloud and multi-cloud presence and rely largely

on cloud-native APIs to perform their assessment, thus claiming to offer an agentless alternative to more traditional tools.

While DSPM tools are lacking several substantial capabilities of more comprehensive data security platforms, they find plenty of customers with their promise of a comparatively simple and quick solution for numerous challenges of migrating sensitive data to the cloud. They have emerged as a critical component of modern data security strategies, particularly for cloud-first organizations. They provide **essential visibility, risk assessment, and security posture management**, helping enterprises mitigate misconfigurations, access risks, and compliance challenges.

It is however important to stress that DSPM solutions only represent a subset of capabilities that are required to provide comprehensive protection of sensitive data from leaks and breaches, as well as to establish quick and automated response to security incidents. A DSPM solution can be a sensible first step towards building a comprehensive data security architecture for your organization, but it should not be the last one. Look for solutions that can grow with your organization's demands and evolve from a security posture assessment tool to a full-featured data security platform by adding data encryption, leak prevention, and threat protection capabilities. KuppingerCole's research can be your guide on this journey.

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

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

Access Management – this includes not only 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 detecting 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, as well as tools supporting forensic analysis and compliance audits.

Performance and Scalability – although not a security feature per se, it is an important 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. Key criteria we're looking for include:

- Unified support for multiple relational and NoSQL database engines.
- Support for cloud-native data analytics and intelligence platforms.
- Expanding coverage to semi-structured and unstructured data stores like object stores, file servers, etc.
- Support for hybrid deployments across on-premises and cloud infrastructures or managed database services.
- Centralized management, analytics, and audit across multiple data stores.
- Out-of-the-box support for most important compliance frameworks.
- Internal security capabilities such as strong authentication, segregation of duties, privacy-enhancing technologies, etc.

If you are interested in DSPM-related capabilities, you can focus your analysis on just the following selection from the list above:

- Vulnerability assessment
- Data discovery and classification
- Audit and Compliance

Leadership

When selecting a vendor for a product or service, the decision should not be based solely on the information provided in a Leadership Compass. While the Leadership Compass offers a valuable comparison based on standardized criteria and helps identify vendors for further consideration, a thorough selection process requires a detailed analysis and a Proof of Concept (PoC), or pilot phase tailored to the specific needs of the customer.

Based on our own research and analysis of the vendor responses, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for Product, Innovation, and Market Leadership.

Overall Leadership

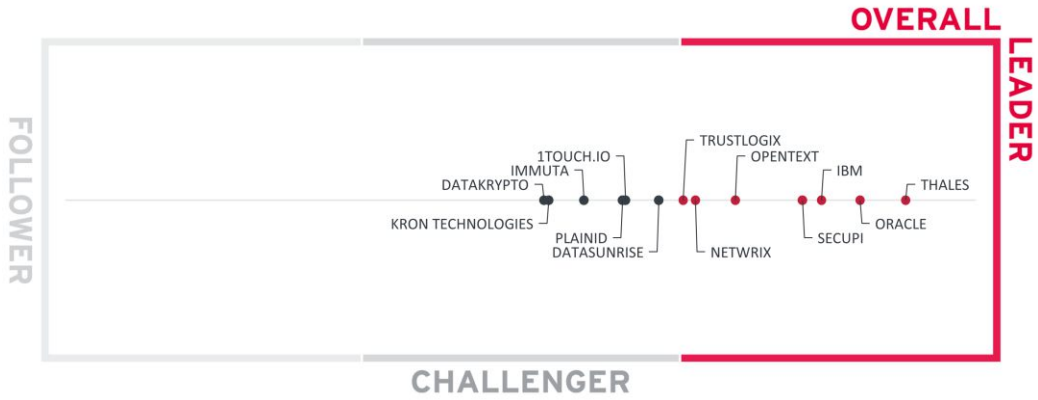


Figure 4: Overall Leadership in the Data Security Platform market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

When looking at the overall leaders, we can see a combination of familiar names that were leading the previous edition's rating, sch as IBM, Oracle, SecuPi, and Thales. All of them demonstrate broad functional capabilities, strong global market presences, as well as a healthy dose of innovation in their solutions. Since Thales has now acquired Imperva and integrated its capabilities into a unified portfolio, their combined strengths helped the company to become the new leader in our overall rating.

OpenText, a newcomer in this Leadership Compass, has also demonstrated all the strengths expected from a veteran global vendor with a massive security portfolio, thus being recognized as one of the Overall Leaders as well. Finally, Netwrix and TrustLogix both have substantially improved their ratings since our previous review, rising to the ranks of Overall Leaders as well.

The rest of the vendors populate the Challengers segment. The only companies that were present in our past rating are DataSunrise with their functionally comprehensive platform that is yet to achieve its deserved recognition by the market and Kron Technologies, which has significantly improved its ratings this year. Unfortunately, the rest of the companies we reviewed back in 2023 have either left the data security market entirely or at least reduced their presence.

However, we do have several interesting newcomers instead. Some of them are already well-established vendors that focus on solving specific aspects of data security. 1touch.io is a leading provider of data discovery and classification tools, whose technology is found in products of many other vendors. PlainID is a veteran provider of policy-based access management tools, not just for data sources. Immuta offers data access governance and data marketplace solutions for cloud-native customers. DataKrypto is a startup that develops a highly innovative fully homomorphic encryption technology for protecting sensitive data in use.

While these companies do not deliver comprehensive data security platforms in the strictest sense, their solutions are nevertheless excellent at solving specific individual disciplines within data security and can be used as building blocks for designing your own custom security architecture.

Just like last time, there are no Followers in our overall leadership rating.

Overall Leaders are (in alphabetical order):

- IBM
- Netwrix
- OpenText
- Oracle
- SecuPi
- Thales
- TrustLogix

Product Leadership

The first of the three specific Leadership ratings is about Product leadership. This view is mainly based on the presence and completeness of the required functional capabilities as defined in an earlier section. 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.

Figure 5: Product Leadership in the Data Security Platform market

In this rating, we look specifically for the functional strength of the solutions, regardless of the vendors' current ability to grab a substantial market share. It is worth noting again that, with the broad spectrum of functionality we expect from a comprehensive data security

solution, it is hard to achieve a Product Leader status for a smaller company. It is therefore unsurprising that the Leaders segment is dominated by large, established vendors.

Thales has been recognized as the product leader due to its strategic integration of Imperva's data security capabilities with its existing CipherTrust platform, resulting in comprehensive data security solutions that protect data across all paths with advanced encryption, data risk intelligence, and a broad partner ecosystem.

Oracle has again maintained the close second place due to its comprehensive approach to database security, particularly with its Autonomous Database that provides self-securing capabilities, integrated Data Safe features for unified security management, and strong focus on mandatory security controls throughout its entire stack.

SecuPi is notable for its innovative capabilities in integrating data security posture management with a focus on protecting sensitive data through dynamic masking, encryption, privilege access brokering, and the application of complex policies for identity and access management across various platforms, enabling compliance with privacy regulations.

IBM’s Guardium Data Security Center’s highlights include its comprehensive data discovery, classification, and protection across both cloud and on-premises environments, and addressing security challenges with innovative capabilities like advanced cryptographic posture management.

Netwrix’s comprehensive approach to data security and governance, enabling organizations to effectively manage risk and ensure compliance across diverse IT environments, gains them a Leader position in our rating as well.

TrustLogix has been recognized as a leader due to its innovative data-centric security solution that provides a non-intrusive architecture with broad data protection capabilities, AI-driven policy recommendations, and comprehensive security and compliance management across multi-cloud environments.

DataSunrise is noted for offering a wide range of proactive and reactive security measures, including dynamic data masking, vulnerability assessment, and support for NoSQL databases across cloud and on-premises environments, as well as its audit and compliance capabilities.

Finally, OpenText offers comprehensive data lifecycle management and security solutions as well as integrations within existing enterprise ecosystems, all supported by a global reach and a wide range of further products within its cybersecurity portfolio.

The rest of the vendors are, as mentioned earlier, focused on solving a specific challenge within data security, such as access management, discovery and classification, or encryption in use. While they excel within their corresponding focus areas, this also means that they were unable to achieve product leadership status and are found among the Challengers.

Still, none of the reviewed solutions belong to the Followers segment, which indicates that all solutions covered in this report offer strong functional capabilities and are definitely worth your consideration and closer attention.

Product Leaders (in alphabetical order):

- DataSunrise
- IBM
- Netwrix
- OpenText
- Oracle
- SecuPi
- Thales
- TrustLogix

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree 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.

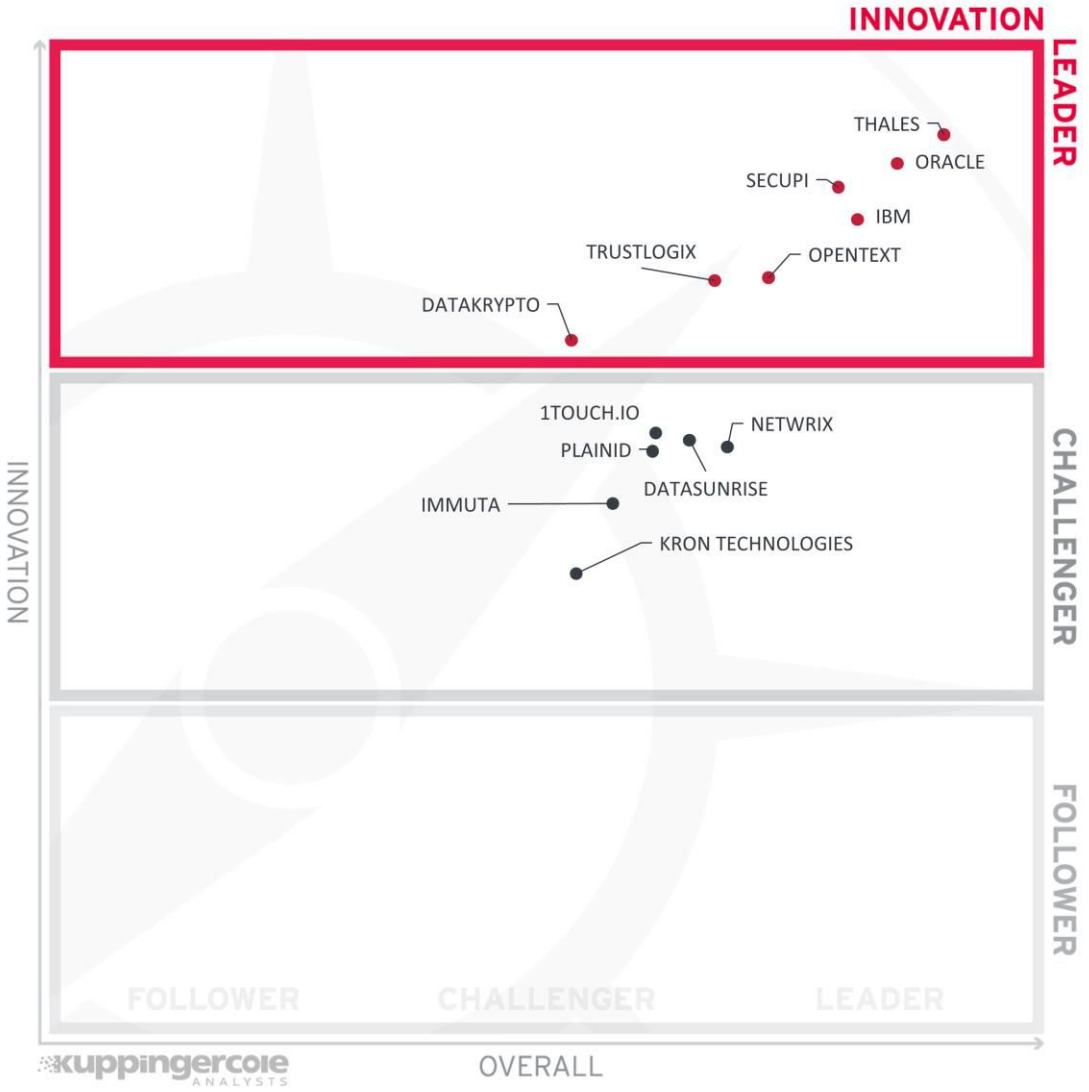


Figure 6: Innovation Leadership in the Data Security Platform market

Innovation Leaders are those vendors that deliver cutting-edge products, not only in response to customers' requests, but also because they are driving technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

For the data security market, we were looking for capabilities that were aimed at disrupting the existing conventions and shaping the future of the entire market for the years to come. Such groundbreaking features might be related to intelligent automation using machine learning and generative AI, quantum-safe cryptography and data encryption in use, substantial improvements in deployment and operations at massive cloud scale, etc.

As expected, the majority of the Innovation Leaders in our rating are large vendors with impressive functional capabilities (rightfully recognized as Product Leaders above) and a strong financial posture to be able to invest substantially into R&D. The only newcomer in this segment is DataKrypto, which is a relatively small startup company with a proprietary homomorphic cryptography solution to secure text and image data in use.

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

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

Innovation Leaders (in alphabetical order):

- DataKrypto
- IBM
- OpenText
- Oracle
- SecuPi
- Thales
- TrustLogix

Market Leadership

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

In this chart, 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 7: Market Leaders in the Data Security Platforms Market

Again, completely unsurprisingly, most market leaders in our rating are large, veteran vendors with broad product portfolios going beyond just data security, as well as large partner networks and strong customer bases. These include vendors like Thales, IBM, Oracle, OpenText, and Netwrix.

SecuPi, although a more narrowly specialized vendor, is still known for its close business relationships with major cloud service providers to reach its customers through their online marketplaces and is thus able to reach a position among the leaders as well.

All the other vendors can be found in the Challengers segment, indicating that they have not yet been able to achieve a substantial global market presence to compete with their larger counterparts. However, the fact that none of the participating vendors can be found among the Followers is a sure sign that all of them have already been able to carve their own market shares and are working hard to expand them in the future.

Market Leaders (in alphabetical order):

- IBM
- Netwrix
- OpenText
- Oracle
- SecuPi
- Thales

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. 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

Vendor	Security	Functionality	Deployment	Interoperability	Usability
1TOUCH.IO	positive	positive	positive	strong positive	positive
DATAKRYPTO	positive	neutral	positive	neutral	neutral
DATASUNRISE	strong positive	positive	strong positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive	strong positive
IMMUTA	positive	positive	strong positive	neutral	strong positive
KRON TECHNOLOGIES	positive	neutral	strong positive	neutral	positive
NETWRIX	strong positive	positive	strong positive	strong positive	strong positive
OPENTEXT	strong positive	strong positive	positive	positive	strong positive
ORACLE	strong positive	strong positive	strong positive	strong positive	strong positive
PLAINID	strong positive	positive	strong positive	positive	positive
SECUPI	strong positive	strong positive	strong positive	strong positive	strong positive
THALES	strong positive	strong positive	strong positive	strong positive	strong positive
TRUSTLOGIX	strong positive	positive	strong 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
1TOUCH.IO	positive	neutral	neutral	positive
DATAKRYPTO	strong positive	weak	weak	neutral
DATASUNRISE	positive	positive	neutral	positive
IBM	strong positive	strong positive	strong positive	strong positive
IMMUTA	positive	neutral	neutral	neutral
KRON TECHNOLOGIES	neutral	neutral	neutral	positive
NETWRIX	positive	positive	positive	positive
OPENTEXT	strong positive	positive	strong positive	positive
ORACLE	strong positive	strong positive	strong positive	strong positive
PLAINID	positive	neutral	positive	positive
SECUPI	strong positive	positive	strong positive	positive
THALES	strong positive	strong positive	strong positive	strong positive
TRUSTLOGIX	strong positive	weak	neutral	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 papers 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 this market segment, 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 the 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 cyberattacks 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.

1touch.io – Inventa

1touch.io is a privately held, venture-backed company specializing in data security, with a particular focus on sensitive data intelligence. 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. Operating globally, 1touch.io maintains a strong presence across North America, Europe, the Middle East, and Latin America, catering primarily to large enterprises and mid-market organizations. Strategic partnerships with system integrators in North America further enhance its service delivery and market reach.

At the core of the platform is its automated discovery and classification engine, which enables organizations to identify and catalog structured and unstructured data across their environments including for the mainframe with their recent VSAM release. Unlike conventional data security solutions that rely on predefined rules and limited scanning capabilities, it leverages network-based discovery to map out data flows, including those originating from shadow IT and unknown data sources. Similarly, Inventa specializes in contextualizing data classification to get past just “a credit card number found in a dataset” to “a credit card number of Hans Schmidt, a German resident with GDPR controls, found in a US data center”. This way, it enables action and prioritization based on contextual insights.

Inventa exhibits broad database support, encompassing traditional relational databases, NoSQL architectures, legacy systems like mainframes, and cloud data platforms (like Snowflake or Databricks). This level of extensibility allows organizations to unify security policies across disparate environments. It can address post-quantum cryptography concerns by identifying legacy encryption schemes that may be vulnerable to emerging quantum-based threats. Additionally, proactive monitoring of GenAI interactions help detect and mitigate potential data leakage risks within AI and ML environments.

While primarily a data discovery and management solution, Inventa incorporates substantial security and risk assessment capabilities as well as orchestration based off these assessments. The platform facilitates automated vulnerability discovery for databases and integrates with third-party scanners such as IBM Guardium, enabling enterprises to assess and remediate potential exposures. Additionally, automated risk assessment and ticketing integrations simplify the mitigation of data security posture issues.

Inventa aligns closely with global compliance mandates, offering auditing and reporting functionalities that support regulatory frameworks such as GDPR and PCI DSS. The platform enables centralized compliance monitoring across complex enterprise infrastructures while delivering real-time compliance alerts to address potential violations proactively. It provides detailed auditing of user entitlements, highlighting excessive permissions and potential security risks. However, automatic remediation of privilege misconfigurations remains a gap in its current functionality.

A defining strength of Inventa is its extensive third-party integration ecosystem, enabling enterprises to incorporate its capabilities into broader security frameworks. The company

also has OEM technology partnerships with several major data security vendors, including some of the leaders covered in this rating.

Beyond its core functions, the platform offers specialized capabilities, including mainframe scanning and dormant account monitoring, ensuring security coverage for legacy systems and inactive user accounts that could pose hidden risks

With the Inventa platform, 1touch.io empowers businesses to maintain a comprehensive data inventory, providing unparalleled visibility, risk assessment, and compliance enforcement across hybrid IT environments. Enterprises operating in highly regulated, multi-cloud, and distributed environments will benefit the most from its capabilities.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

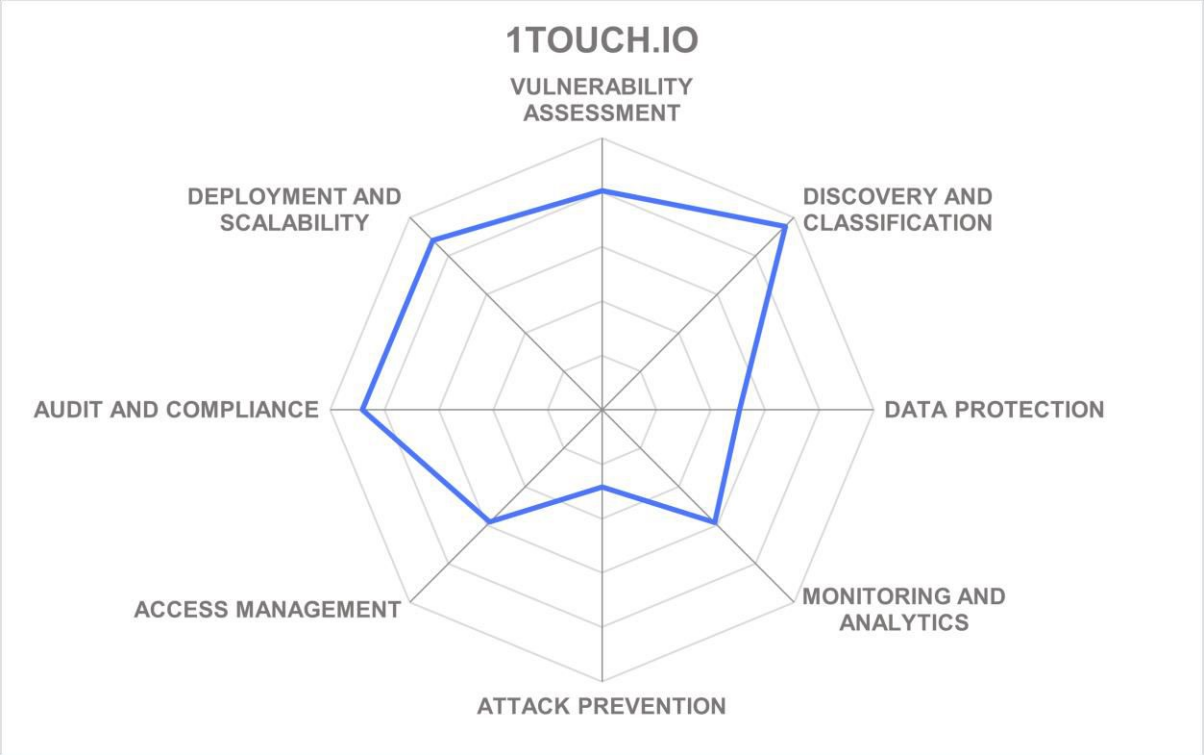
Table 3: 1touch.io's rating

Strengths

- AI-driven automated data discovery and classification
- Flexible deployment options spanning on-premises, cloud, and managed services
- SaaS model with the appeal for smaller businesses
- Broad integration ecosystem with SIEMs, vulnerability management tools, IAMs
- Comprehensive compliance support for major regulatory frameworks

Challenges

- Limited threat detection, no anomaly detection or real-time analytics
- Does not provide any substantial proactive attack mitigation features
- Limited automated remediation capabilities, mostly through third-party tools
- Relatively unknown brand due to reliance on OEM partnerships


1TOUCH.IO
VULNERABILITY ASSESSMENT
DISCOVERY AND CLASSIFICATION
DATA PROTECTION
MONITORING AND ANALYTICS
ATTACK PREVENTION
ACCESS MANAGEMENT
AUDIT AND COMPLIANCE
DEPLOYMENT AND SCALABILITY

DataKrypto – FHEnom

Founded in 2021 and based in Burlingame, California, DataKrypto is a privately held cybersecurity firm specializing in advanced encryption and data security solutions. Operating across North America and the EMEA region, DataKrypto serves a diverse customer base spanning small enterprises to large corporations, with a strong presence in sectors such as manufacturing, healthcare, and telecommunications. Despite its relatively small operational footprint, the company is notable for strong technological innovation and a growing partner ecosystem.

DataKrypto's offering comprises its flagship solution, FHEnom, alongside FHEnom for Images. These products leverage proprietary Fully Homomorphic Encryption (FHE), an innovative cryptographic technology that enables operations on encrypted data without requiring decryption. FHEnom supports a wide array of traditional data types and operations (numerical calculations, sorting, search, and filtering) with encrypted data, allowing organizations to maintain privacy and security of business data without losing any application functionality.

FHEnom for Images extends these capabilities specifically to image-based data, addressing security challenges in fields such as healthcare, where the protection of patient data is essential. By protecting sensitive images from exfiltration and unauthorized access, DataKrypto provides a highly specialized solution that enhances data integrity and compliance.

The encryption model is built upon symmetric FHE, ensuring comprehensive data protection at rest, in transit, and in use. This ensures continuous data confidentiality across hybrid and multi-cloud environments. A key differentiator is the flexibility of encryption key management: customers can opt for on-premises, cloud-based, or third-party key custodianship. DataKrypto also claims to deliver quantum-resistant encryption, preparing organizations for the anticipated challenges of post-quantum cryptography.

DataKrypto offers software development kits (SDKs) that enable embedding of its encryption technology directly into existing applications. This approach eliminates the need for major architectural overhauls and ensures compatibility with diverse IT environments, including Kubernetes and leading cloud providers such as AWS, Azure, and Google Cloud. However, the reliance on SDKs necessitates developer expertise, potentially limiting accessibility for smaller organizations.

Although end-to-end data encryption does substantially reduce the overall attack surface of any application, organizations deploying DataKrypto must supplement their security stack with additional solutions for holistic risk management, since the product itself does not provide any other security controls.

FHE approach aligns well with global compliance mandates, including GDPR, CCPA, and PCI DSS. By ensuring data remains encrypted throughout its lifecycle, the platform inherently supports regulatory requirements for data privacy. However, it still requires

integrating with third-party governance tools to provide proper compliance monitoring and reporting.

A unique differentiator of DataKrypto is its industry-first application of FHE to image data, making it particularly relevant for sectors reliant on sensitive imaging, such as healthcare. This specialization, combined with its strong focus on quantum-resistant encryption, positions it as an attractive choice for organizations that prioritize protection of the entire data lifecycle. Still, the company faces challenges in broadening its market adoption due to a very focused approach that requires additional development skills from potential customers.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Neutral
Usability	Neutral

Table 4: DataKrypto's rating

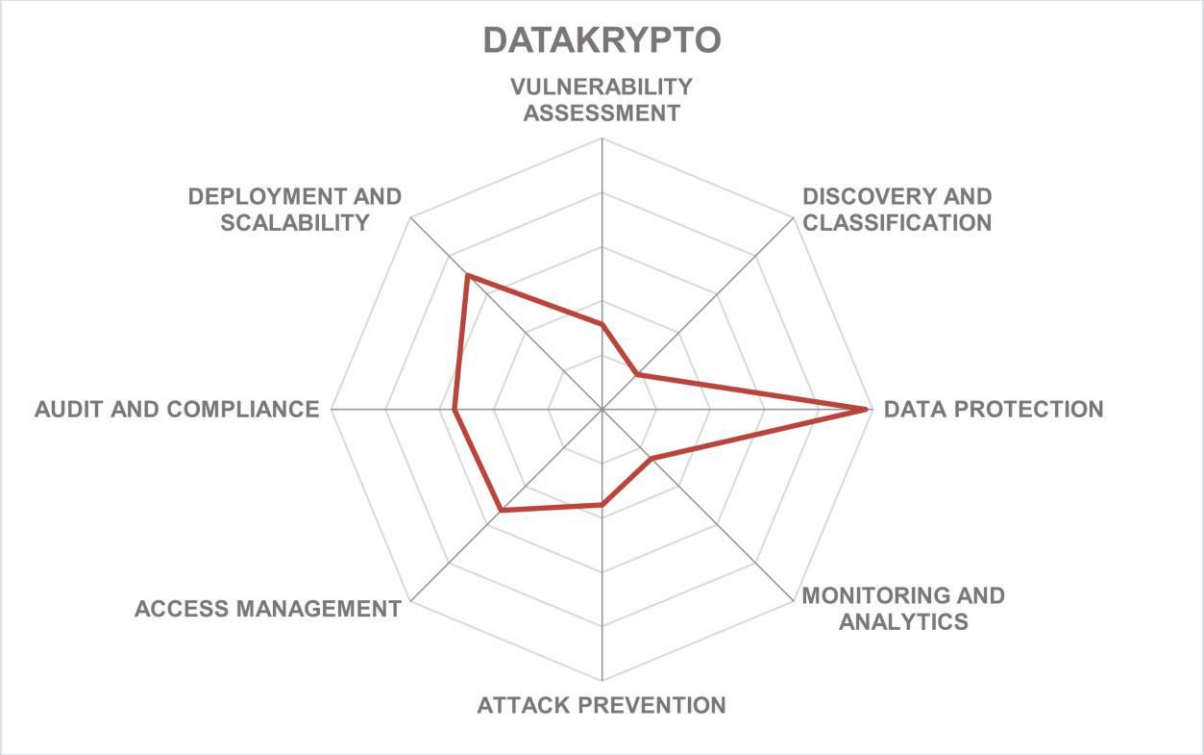
Strengths

- Based on an innovative Fully Homomorphic Encryption (FHE) technology
- Strong compliance alignment through complete data lifecycle encryption
- Developer-friendly SDKs for seamless application integrations
- Implementing quantum-resistant encryption, ready for post-quantum security
- Unique specialization in image encryption for high-security sectors

Challenges

- Limited built-in security features, such as vulnerability management or threat detection
- Limited direct audit and compliance reporting capabilities
- SDK-based deployment model requiring developer expertise
- Modest market presence and financial scale

Leader in


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

DataSunrise – Database and Data Security

Founded in 2015 and headquartered in Seattle, Washington, DataSunrise, Inc. is a privately held cybersecurity company specializing in data and database security solutions. Operating without venture capital backing, the company has grown through organic revenue generation and founder investment. DataSunrise serves a diverse global clientele, focusing on mid-market and enterprise customers across North America, EMEA, APAC, and Latin America. Its international presence is reinforced by a strong network of system integrators that extend its reach and deployment capabilities.

DataSunrise Database and Data Security is a multifaceted solution designed to provide comprehensive protection for structured and unstructured data across hybrid IT environments. The platform supports a wide range of relational and NoSQL databases, along with cloud storage services and file systems, ensuring seamless security across on-premises and cloud-based deployments. The platform is built on a combination of proprietary and open-source technologies, ensuring both performance efficiency and security resilience.

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. 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. A key differentiator for DataSunrise is its deployment flexibility, catering to diverse IT architectures. The platform supports on-premises installations for organizations with strict data residency and compliance requirements as well as managed services and cloud-native deployments across AWS, Microsoft Azure, and Google Cloud.

DataSunrise’s approach to threat detection and prevention integrates automated security mechanisms with configurable policy controls. Key capabilities include real-time activity monitoring and SQL injection detection, mitigating risks associated with database exploitation, and denial-of-service prevention and dynamic protocol validation, ensuring uninterrupted service availability. In addition, it provides encryption for data at rest and in transit, alongside row-level access controls that enforce least-privilege access policies.

The company’s Data Security Posture Management (DSPM) platform offers a comprehensive solution for safeguarding cloud-based data assets. It employs advanced scanning techniques to automatically discover and inventory data across various cloud environments, including databases on EC2 instances and cloud-based file systems. The platform provides continuous monitoring and protection. Additionally, it delivers detailed audit trails and real-time insights into data access patterns, enhancing an organization's ability to detect and respond to potential security incidents. A recently added automated regulatory compliance manager greatly simplifies compliance with GDPR, PCI DSS, HIPAA, and other important regulatory frameworks.

While the platform delivers detailed vulnerability analysis and misconfiguration detection, it does not perform automated patching. However, its policy-driven security model compensates by allowing enterprises to predefine risk mitigation strategies. Another new

capability that sets DataSunrise apart is its synthetic data generation and test data management, providing organizations with the ability to create realistic test environments without exposing sensitive production data. It also offers advanced AI security capabilities designed to protect components of Generative AI systems, such as ChatGPT, Amazon Bedrock, and vector database Qdrant.

DataSunrise presents a solid yet adaptable data security solution that caters to enterprises requiring comprehensive database protection, compliance enforcement, and access governance. Its ability to secure multi-cloud, hybrid, and on-premises infrastructures makes it a strong contender in the DSP market. For enterprises prioritizing flexibility, integration, and granular security controls, DataSunrise provides a compelling option for strengthening their data security posture.

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

Table 5: DataSunrise's rating

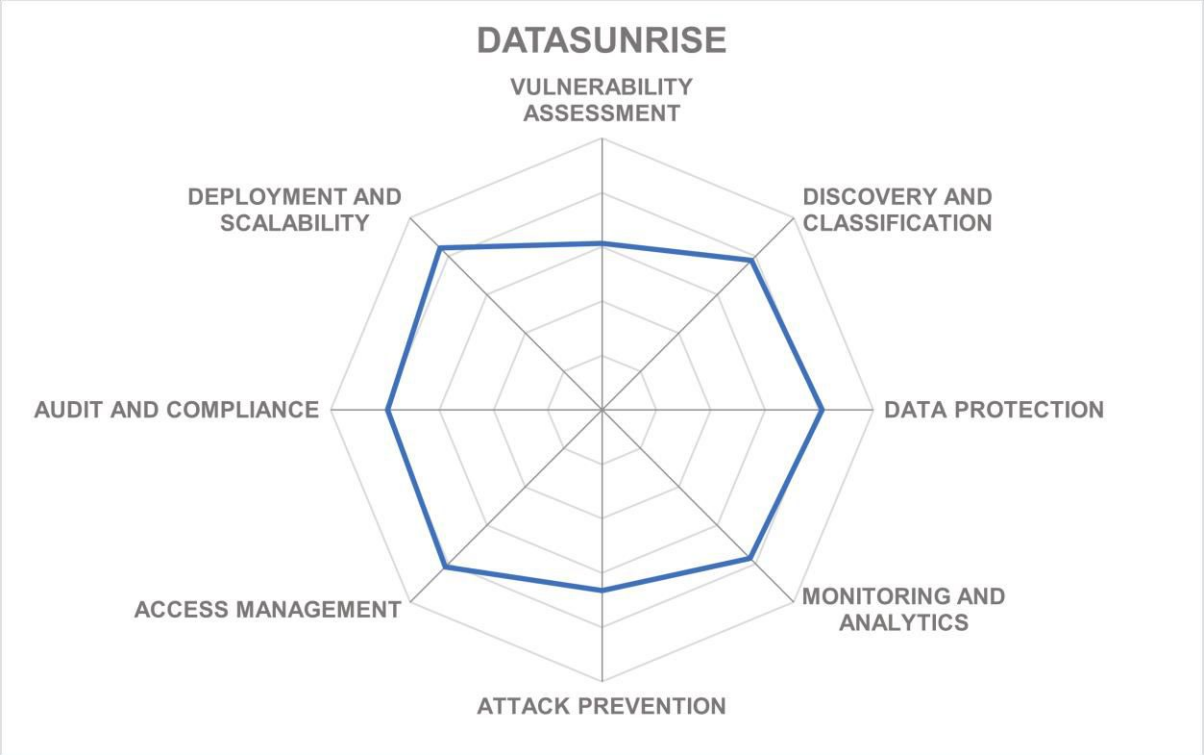
Strengths

- 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.
- Vulnerability assessment is limited to recommendations, does not do remediation.
- Reliance on partners for SaaS-based offerings

Leader in


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

IBM – Guardium Data Security Center

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 to an industry leader in enterprise IT solutions. With a strong focus on data security and cloud-based services, the company continues to expand its extensive portfolio, catering primarily to large enterprises across diverse industries. Its well-established partner ecosystem, comprising over a thousand system integrators across North America, EMEA, APAC, and Latin America, reinforces IBM's global reach and enhances its service delivery capabilities.

At the heart of IBM's data security portfolio is Guardium Data Security Center, a fully integrated suite designed to address the full spectrum of modern data protection challenges. The platform provides comprehensive capabilities, from vulnerability identification and risk mitigation to compliance enforcement and advanced threat detection. It supports a broad range of traditional and modern database technologies, as well as emerging cloud-based platforms, ensuring coverage across complex enterprise environments. It provides a consolidated view of data assets and their protection, removing organizational silos to simplify the data security mission. In addition, Guardium Data Security Center provides clients with opportunities to protect against emerging threats including AI security and quantum-powered attacks.

IBM offers flexible deployment models, allowing organizations to implement Guardium on-premises, in the cloud, or as a managed service through IBM and its network of business partners. This approach helps customers future-proof their capabilities and investments, allowing their data security strategy to grow in tandem with business needs. The SaaS deployment is hosted on AWS, granting clients geographic flexibility. The platform's vulnerability discovery mechanisms provide in-depth visibility into database infrastructures, detecting potential misconfigurations and security gaps. In addition to automated remediation capabilities, IBM Guardium provides detailed risk assessment insights and pre-built code snippets, helping security analysts to automate certain mitigation tasks.

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.

IBM Guardium delivers real-time monitoring and advanced threat prevention, incorporating capabilities such as SQL injection detection and denial-of-service (DoS) protection. Its policy-driven approach to access management enhances security postures. The platform also provides strong compliance auditing functionalities, supporting key regulatory frameworks such as GDPR and CCPA, with real-time alerts to facilitate proactive compliance

management. Guardium's audit capabilities extend beyond native logs, enabling independent data collection to strengthen audit readiness. Compliance Accelerators for specific frameworks like PCI DSS, HIPAA, SOX, GDPR, or FedRAMP ensure that following strict personal data protection guidelines becomes a continuous process.

A key advantage of Guardium is its extensive API-based integration capabilities, allowing connectivity with third-party SIEM solutions, analytics platforms, and ticketing systems. This interoperability ensures that Guardium fits into broader enterprise security architectures.

IBM Guardium Data Security Center is a highly capable enterprise-grade data security solution, well-suited for large organizations requiring scalable, policy-driven security and compliance enforcement. Its comprehensive monitoring, broad integration support, and flexible deployment options make it an impressive option in the even-changing landscape of data security.

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

Table 6: IBM's rating

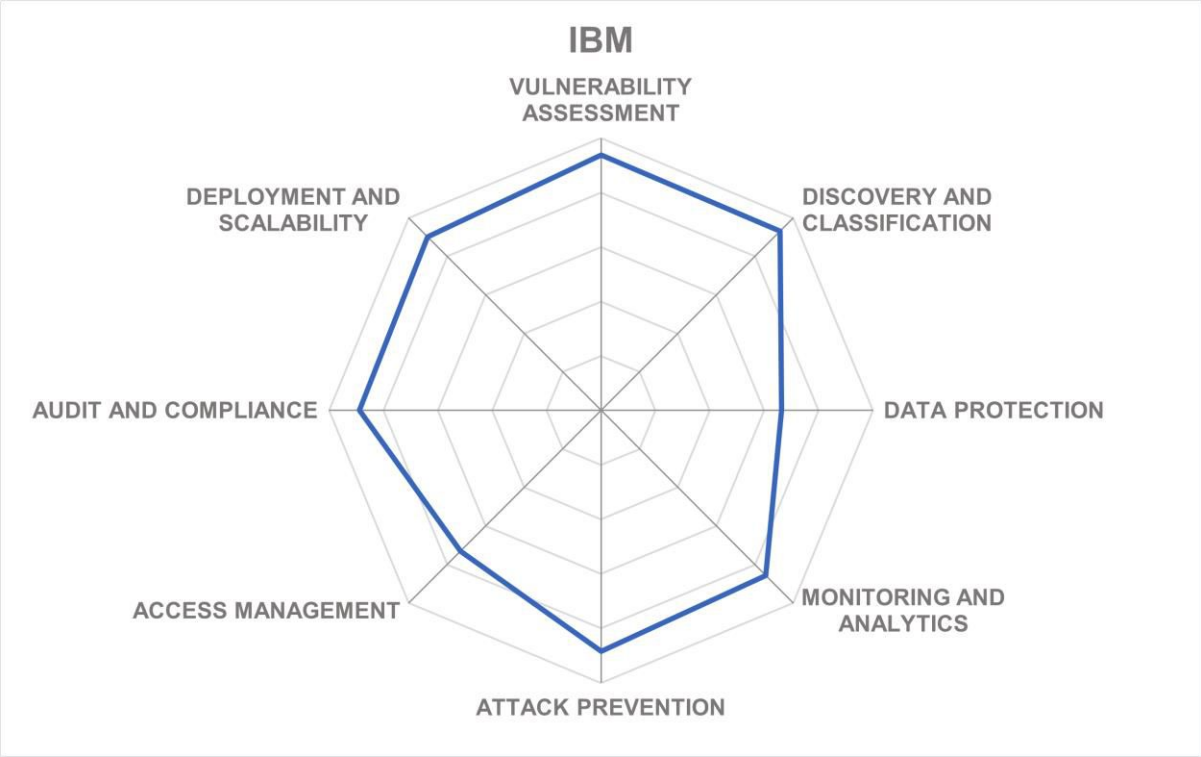
Strengths

- Full range of security capabilities for structured and unstructured data
- Support for hybrid multi-cloud environments
- Broad coverage, including traditional RDBMS and cloud-native platforms
- Comprehensive vulnerability detection and threat monitoring
- Extensive market presence and enterprise adoption

Challenges

- Setup and operations may be complicated for customers, especially smaller ones
- Dependence on third-party tools for certain integration functionalities
- Somewhat limited tokenization and static masking capabilities

Leader in


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

Immuta – Data Security Platform

Immuta is a provider of data security solutions, focusing on dynamic access control and governance for cloud environments. Founded in 2015 and headquartered in Boston, Massachusetts, 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 primarily serves enterprise and mid-market organizations, with a strong presence in North America and growing expansion into EMEA and the Asia-Pacific region. Immuta's extensive partner ecosystem, comprising system integrators and technology consultants, further extends its reach and enhances its service capabilities.

Its flagship product is the Immuta Data Security Platform, designed to address the challenges of data governance, compliance, and security in cloud environments. The platform facilitates automated classification and tagging of sensitive data, including personally identifiable information (PII), payment data, and healthcare records. It enables highly scalable dynamic real-time enforcement of attribute-based access policies (ABAC) without requiring data duplication or movement, distinguishing itself from traditional static access models. Additionally, its activity monitoring capabilities provide administrators with granular overview of data interactions, allowing visibility into both standard and anomalous behaviors.

Immuta’s architecture integrates with cloud-based data ecosystems, offering broad compatibility with AWS, Google Cloud, and Microsoft Azure as well as with Snowflake and Databricks, leading cloud-native data platforms. The platform supports both SaaS-based and self-managed Kubernetes deployments, ensuring flexibility for enterprises operating across multi-cloud and hybrid environments. It is also available directly from all major CSP’s cloud marketplaces. Its dynamic policy enforcement and native integrations with major data platforms ensure minimal performance impact and high operational efficiency.

Although the company does not position itself as a threat detection platform, it provides security controls to mitigate insider risks and unauthorized data access. The platform includes user behavior analytics to identify compromised credentials or policy violations. It offers configurable alerts and reports on administrative and non-administrative activities.

Policy-based access controls allow business users to define and enforce access policies without requiring deep technical expertise, streamlining governance and compliance efforts. Customers can create data policies once and ensure that they are enforced consistently and transparently across multiple clouds and data platforms. AI-powered capabilities, including Immuta Copilot, simplify policy authoring for non-technical stakeholders by turning plain-language text prompts into comprehensive access policies.

The platform secures data transmission through encryption and employs dynamic and conditional data masking techniques to protect sensitive information. Privacy-enhancing technologies reinforce data protection strategies without compromising usability. Additionally, its centralized auditing capabilities facilitate compliance reporting for regulatory frameworks such as GDPR, CCPA, and HIPAA.

The most recent addition to Immuta's portfolio is Data Marketplace, a purpose-built solution designed to streamline and accelerate data sharing within organizations. It enables data owners to publish data as business-relevant products, while allowing data consumers to quickly search, find, and access the data they need. Because the entire access provisioning process is automated, customers can enjoy the benefits of simplified data sharing, improved collaboration between teams, substantially increased productivity, and enhanced data security and governance. The platform's modular approach integrates seamlessly with existing data infrastructure, providing the flexibility to meet diverse organizational needs.

Immuta's strengths lie in its scalable, dynamic policy enforcement, which enables seamless data governance, compliance, and privacy enforcement across multi-cloud and hybrid environments, supporting all leading data platforms. The platform simplifies governance with business-friendly policy management and improves operational agility by avoiding data duplication or movement. With its strong partner network, which includes system integrators and technology vendors, Immuta can deliver broader adoption and flexible deployment options.

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

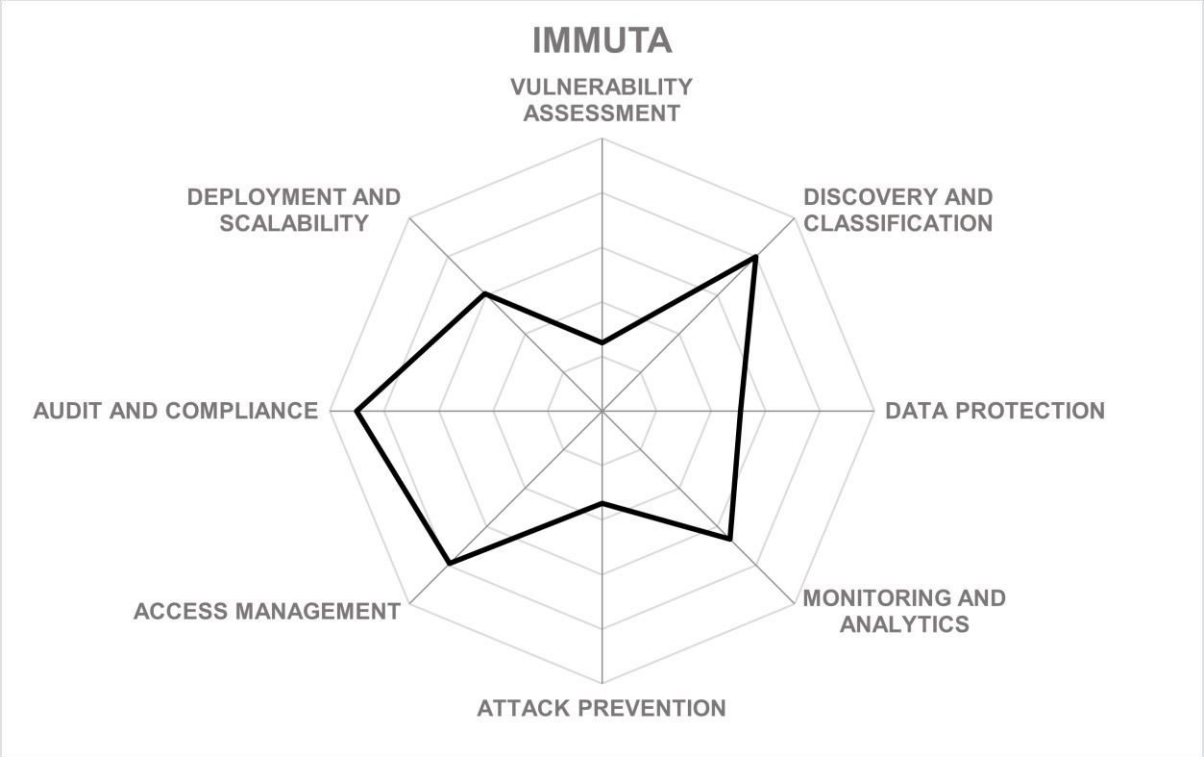
Table 7: Immuta's rating

Strengths

- Dynamic policy enforcement across multi-cloud and hybrid environments
- Native cloud integration with leading data platforms
- Data Marketplace improves secure sharing, data governance, and productivity
- Flexible deployment options – SaaS or self-managed
- Simplified governance with business-friendly access management
- Strong partner network, direct presence in all cloud marketplaces

Challenges

- Supported integrations are mostly limited to cloud-native data platforms
- Limited native threat detection capabilities
- Lack of built-in database vulnerability assessments
- Minimal language support and customization for the user interface


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

Kron Technologies – Database Access Manager and Dynamic Data Masking

Founded in 2007 and headquartered in Istanbul, Turkey, Kron Technologies has established itself as a notable player in the data security and access management space. With a core presence in the EMEA region, Kron has expanded its global reach through a well-established partner network across North America, APAC, and Latin America, ensuring scalability and localized customer support. The company's US office is located in Jersey City, New Jersey.

Perhaps primarily known for its Single Connect and Kron PAM brands of privileged access management tools, Kron also offers a portfolio of data management and security solutions with a strong focus on database access management (DAM) and dynamic data masking (DDM). Kron's flagship solution, Kron DAM/DDM, is designed to address the stringent security and compliance requirements of enterprises across industries such as finance, government, IT, and telecommunications.

Kron DAM/DDM is an access control and data protection platform that enables organizations to monitor and secure database environments in real time. The solution provides granular access management, real-time user activity monitoring, and policy enforcement, ensuring compliance with multiple regulatory frameworks. A key feature of the platform is its dynamic data masking, which helps safeguard sensitive information from unauthorized exposure while maintaining operational efficiency.

The solution is highly adaptable and integrates easily into existing IT ecosystems, supporting a broad range of relational databases, select NoSQL databases such as Cassandra and Couchbase, as well as data platforms like Hadoop and Teradata, making it suitable for hybrid and multi-cloud environments.

Kron supports multiple deployment models, including on-premises, cloud-based, and managed services. The platform is compatible with leading cloud providers such as AWS, Microsoft Azure, and Google Cloud, as well as regional Infrastructure-as-a-Service (IaaS) providers. High-availability configurations ensure minimal downtime and enhanced performance for large-scale deployments.

Kron DAM/DDM integrates essential database audit and sensitive data discovery tools, providing organizations with the visibility needed to detect vulnerabilities and enforce compliance policies. While SQL injection prevention and advanced attack mitigation are on the product roadmap, the current version enables comprehensive misconfiguration detection and sensitive data classification for compliance audits. Data protection measures include encryption for data in transit, data tokenization, and granular data masking techniques to prevent unauthorized access to sensitive records.

It leverages machine learning-driven analytics to identify and mitigate potential threats in real time. Its anomaly detection engine helps uncover suspicious user behavior and enforces predefined security policies to block unauthorized actions. It also provides detailed insights into shared account usage, ensuring tighter governance over privileged access.

The platform delivers centralized and unified auditing capabilities, enabling organizations to streamline compliance reporting for frameworks such as GDPR, PCI DSS, SOX, and HIPAA. It provides independent audit logs and facilitates custom compliance policy development. As part of a broader security ecosystem, DAM/DDM integrates with other Kron security solutions, third-party SIEM platforms, analytics tools, and ticketing systems.

Kron DAM/DDM is a well-rounded data security platform that delivers strong database access control, compliance enforcement, and real-time monitoring for enterprises operating in diverse regulatory environments. Its scalability, machine learning-powered analytics, and flexible deployment options make it an interesting option for hybrid and multi-cloud environments. 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	Strong Positive
Interoperability	Neutral
Usability	Positive

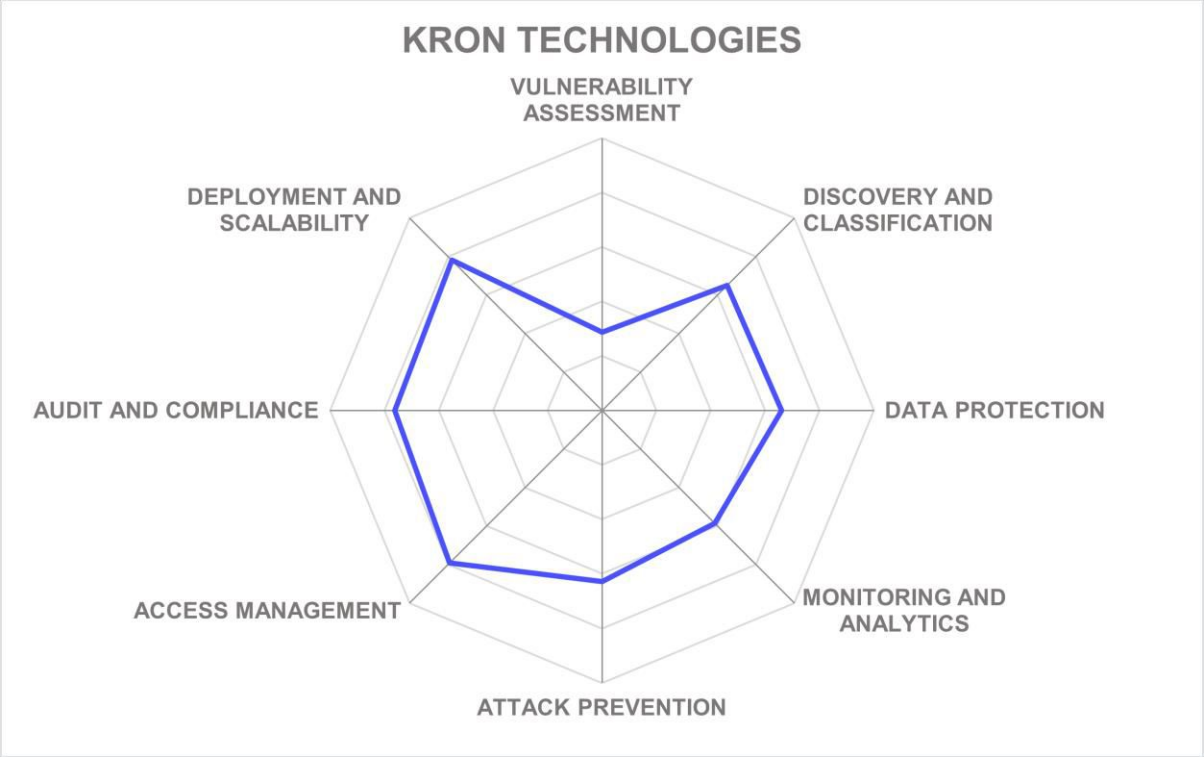
Table 8: Kron's rating

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, cloud data platforms
- Strong IAM capabilities, such as account auto-discovery, real user identification, etc.
- Comprehensive discovery and data masking capabilities
- Comprehensive activity monitoring, audit, and compliance features
- AI-driven threat analytics

Challenges

- Limited coverage of advanced database attack mitigation
- Fairly small visibility outside the company's PAM market focus
- Customization requires specialized technical expertise
- Needing improved support for cloud and big data platforms


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

Netwrix – Enterprise Auditor

Founded in 2006 and headquartered in Frisco, Texas, Netwrix Corporation is an IT security and governance vendor, catering to mid-market and enterprise customers across North America, EMEA, APAC, and Latin America. The company focuses on critical sectors such as finance, healthcare, manufacturing, and government, leveraging a broad ecosystem of system integrators to deliver assessment, consultation, implementation, and managed security services.

Netwrix Enterprise Auditor is a core component of the company's integrated security suite, designed to streamline data collection, analysis, and security management for complex IT infrastructures. The solution automates routine security and compliance tasks while facilitating interoperability across diverse systems.

Its key capabilities include vulnerability discovery across structured and unstructured data repositories and leveraging behavioral analysis and security intelligence to detect anomalous activities and mitigate threats proactively. On this foundation, Netwrix Auditor provides data governance and security posture management with continuous visibility into data risks and compliance violations.

The platform provides flexible deployment models, supporting on-premises installations, cloud-based deployments (AWS and Azure), and a SaaS-based offering called 1Secure. Netwrix Enterprise Auditor supports a wide range of traditional relational databases alongside cloud-native databases such as Azure SQL. The platform extends its capabilities to unstructured data repositories, covering Windows and Linux file servers, SharePoint, Box, and OneDrive.

While native encryption and masking functionalities are not offered, Netwrix mitigates data security risks through behavioral analytics and automated anomaly detection. The solution enables continuous monitoring of data activities, integrating with third-party tools for vulnerability management and automatic remediation. The platform integrates with leading SIEM and analytics platforms via pre-built connectors.

Netwrix Enterprise Auditor integrates with 3rd party identity providers, offering single sign-on (SSO) support via industry-standard authentication protocols. Its coverage extends beyond just databases, as the product can monitor and protect Microsoft directories and other cloud services, like Nutanix or Qumulo.

Netwrix Enterprise Auditor presents a compelling solution for organizations seeking to strengthen their security posture through automated governance, compliance monitoring, and risk management. While it excels in data security intelligence and behavioral analytics, enterprises requiring end-to-end data protection, including encryption and masking, may need to complement it with third-party solutions.

Nonetheless, Netwrix continues to refine its offering, and remains a relevant and adaptable player in the turbulent security and compliance landscape.

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

Table 9: Netwrix's rating

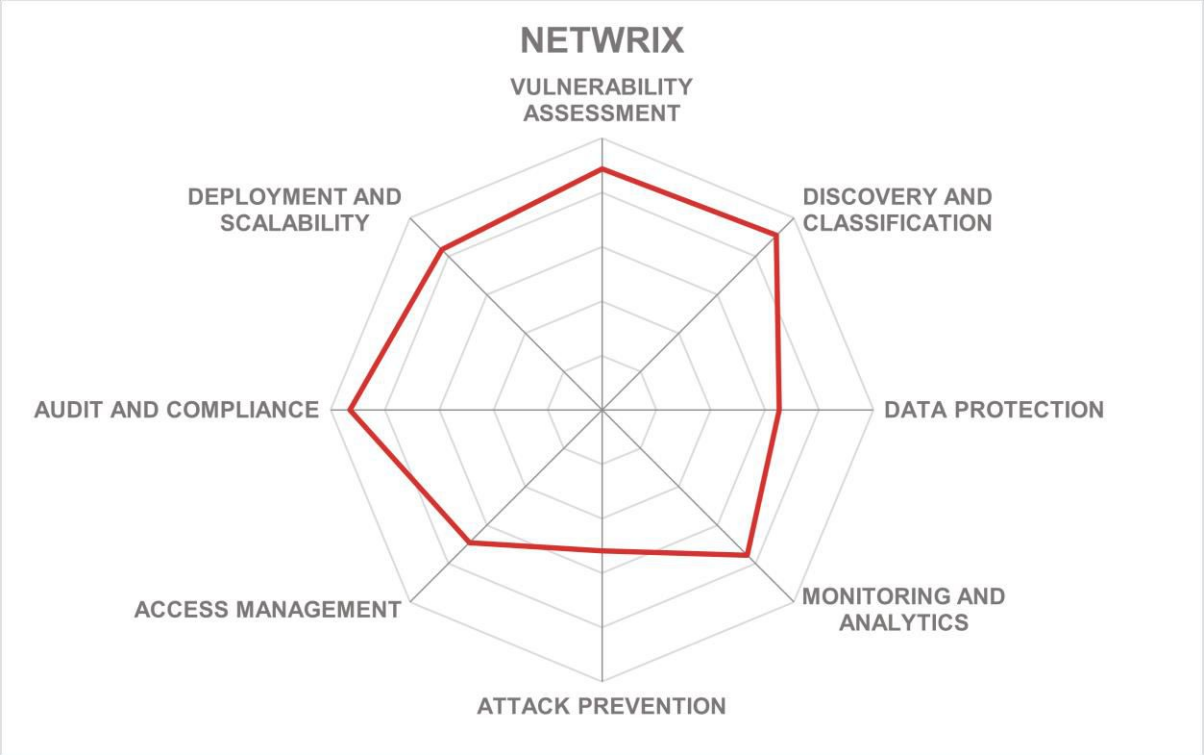
Strengths

- Broad target platform coverage, including structured and unstructured data sources
- Highly accurate data discovery and classification
- Visibility and analytics across heterogeneous environments
- Impressive integrated security ecosystem with a large partner network
- Flexible deployment options spanning on-premises, cloud, and SaaS environments
- Ability to address the entire market from SMBs all the way to large enterprises.

Challenges

- The feature parity between self-managed and SaaS solutions is not reached yet
- No built-in support for emerging cloud data platforms
- Dependency on Microsoft infrastructure for on-prem deployments
- Lacks native encryption and data masking features

Leader in


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

OpenText – Data Security Platform

Founded in 1995 and based in Waterloo, Ontario, Canada, OpenText Corporation has evolved into a leading provider of enterprise information management and data security solutions. As a publicly traded company, it maintains a strong presence across North America, EMEA, and APAC, serving clients ranging from mid-sized businesses to large multinational enterprises. In 2023, it completed the acquisition of Micro Focus, gaining control over its entire range of security solutions. OpenText's broad portfolio is reinforced by an extensive global partner network, enabling deep market penetration and comprehensive customer support.

OpenText's approach to data security is centered around a unified, intelligence-driven platform that integrates cybersecurity functions with enterprise data governance. The company's flagship offerings in this space include OpenText Data Discovery & Risk Insights (Voltage Fusion, OpenText Data Privacy & Protection Foundation (Voltage SecureData) as well as OpenText Structured Data Manager (Voltage Structured Data Manager) along with solutions derived from its Identity & Access Management and Threat Detection and Response portfolio.

These technologies collectively provide an end-to-end framework for data discovery, risk analysis, and proactive security enforcement. Designed to support complex regulatory environments, they prioritize seamless integration across enterprise IT ecosystems while maintaining a balance between usability, governance, and compliance. Solutions are available as cloud-based services, managed offerings, or on-premises appliances, ensuring adaptability across different IT environments. The platform's architecture emphasizes high availability and scalability, with compatibility across AWS, Microsoft Azure, and additional enterprise platforms.

Core capabilities include industry-standard encryption mechanisms, tokenization and masking capabilities for privacy enhancement, and format-preserving encryption to avoid compromising existing applications. The platform's compliance framework aligns with standards like GDPR, CCPA, and PCI DSS. Through centralized auditing and reporting, organizations gain holistic visibility into data interactions, ensuring adherence to governance requirements.

OpenText supports traditional relational databases, alongside modern distributed data frameworks like Databricks and Snowflake. OpenText integrates with NoSQL databases and cloud-based object storage solutions across AWS, Google Cloud, and other leading providers. This broad compatibility enables enterprises to secure and manage data across operational landscapes.

The platform integrates seamlessly with enterprise directory services, supporting advanced authentication protocols, including SAML, and OAuth. Audit functions provide continuous monitoring of administrative actions to uphold compliance with regulatory requirements. Leveraging capabilities from NetIQ, OpenText strengthens its IAM with advanced user behavior analytics and identity governance.

OpenText offers a comprehensive, intelligence-driven approach to data security, seamlessly integrating cybersecurity, identity governance, and data protection. With a strong foundation in regulatory compliance and a focus on adaptability, the company's platform is well-positioned to address the expanding security demands of modern enterprises.

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

Table 10: OpenText's rating

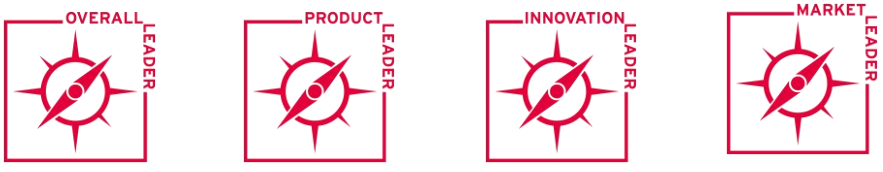
Strengths

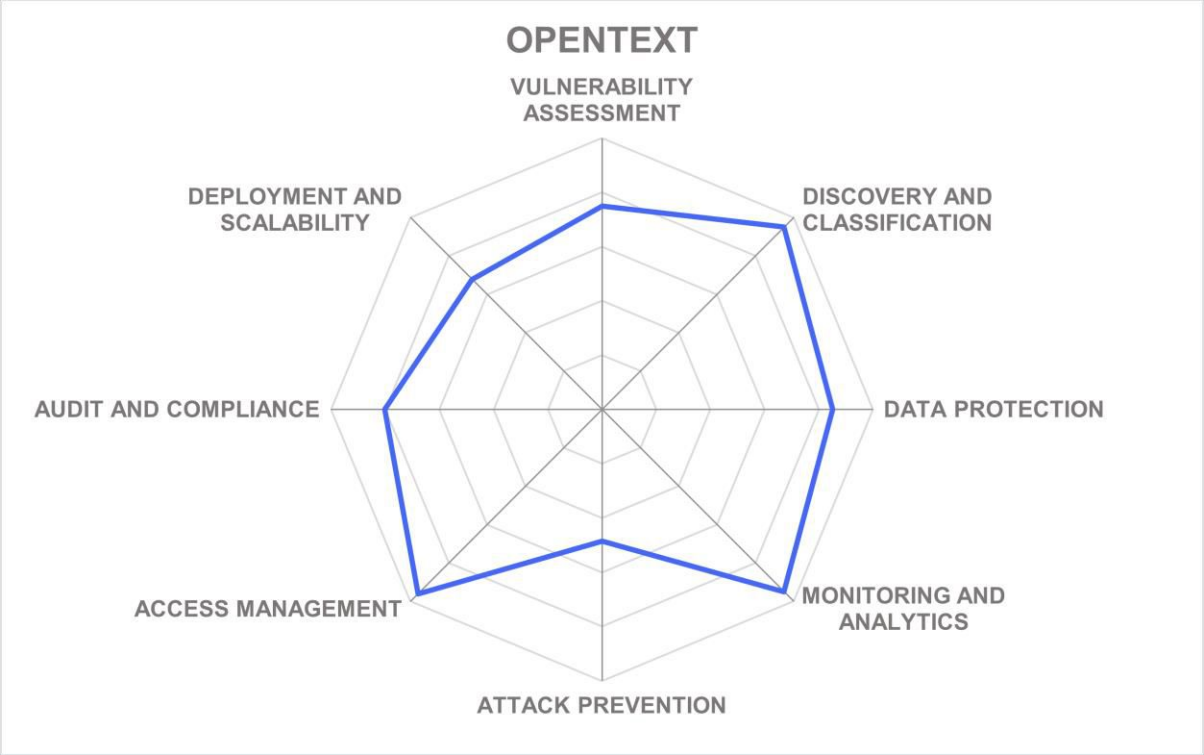
- Extensive technology ecosystem, combining traditional and modern data platforms
- Comprehensive data protection capabilities
- Advanced threat detection features
- Compliance automation with support for major regulatory frameworks
- Global market penetration and large partner network
- Seamless integration with enterprise workflows

Challenges

- Enterprise-grade deployment options might be too complex for smaller customers
- Broad feature set requires substantial configuration and maintenance
- Limited native real-time anomaly detection capabilities
- Lack of a unified security management console

Leader in




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

Oracle – Oracle Database and Cloud Services

Oracle Corporation, established in 1977, has long been a dominant force in the global technology landscape. Headquartered in Austin, Texas, the company is renowned for its extensive portfolio of database software, cloud solutions, and security technologies. With a strong focus on serving large enterprises across diverse industries, Oracle maintains a global reach supported by an expansive partner ecosystem.

Leveraging its longstanding expertise as a database provider, Oracle integrates advanced security features directly into its database core. This architecture minimizes performance impact while enhancing security, offering capabilities such as database encryption, data access control, dynamic data masking, privileged user control, privilege analysis, and an SQL firewall.

Beyond built-in controls, Oracle extends its data security capabilities through a suite of tools including Data Safe Cloud Service, Audit Vault and Database Firewall (AVDF), and Data Masking and Subsetting. These tools deliver a range of Data Security Posture Management (DSPM) capabilities, such as risk assessment, policy-driven monitoring, threat detection, data discovery, and data masking. While these solutions are designed to work together as an integrated suite, they can also be deployed individually to meet specific security needs. With support for multi-cloud and on-premises environments, Data Safe enhances compliance and governance for Oracle deployments.

Oracle’s native security tools primarily focus on its own database, but the Oracle Audit Vault and Database Firewall also provide activity monitoring and threat prevention for other databases, including MySQL, PostgreSQL, Microsoft SQL Server, IBM DB2, MongoDB, and SAP Sybase. Similarly, Oracle Key Vault offers secrets and key management for Oracle, MySQL, MongoDB, and additional systems, along with SSH key governance and management. For applications, Oracle's Virtual Private Database (VPD) and Real Application Security (RAS) apply access controls based on end-user identity, allowing granular restrictions to specific rows and columns. This capability is particularly relevant for mitigating risks associated with automated SQL execution by advanced AI models.

The Oracle Autonomous Database (ADB), the company’s flagship cloud database, integrates advanced security measures like always-on encryption, automated patching, and backups. It also includes Database Vault, Label Security, and Data Safe without additional licensing costs, delivering robust Data Security Platform capabilities. Similarly, Oracle's Exadata Database Services offer these enterprise-class security features, combining DSPM and DSP functionalities within a unified solution.

Oracle's converged database approach enforces consistent security policies across all data types and workloads. By reducing reliance on multiple specialized database engines, Oracle minimizes data movement and simplifies security administration, reducing management overhead and risk. The Oracle security suite emphasizes ease of management through a centralized console, multi-language support, and extensive automation. Additionally, Oracle’s broad API ecosystem facilitates orchestration, automation, and advanced customizations.

The company has also enhanced MySQL capabilities with HeatWave, delivering enterprise-grade scalability and performance for analytical workloads. Recent updates introduce native support for vector data models, allowing seamless integration of traditional database workloads with AI-driven systems. This ensures that sensitive data remains within a single database, reducing the risks associated with ETL processes, particularly in cloud environments.

Oracle remains a leader in enterprise database security, offering an unparalleled blend of automation, scalability, and integration across its ecosystem. Enterprises seeking a future-ready security posture will find Oracle's solutions well-equipped to address their needs.

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

Table 11: Oracle's rating

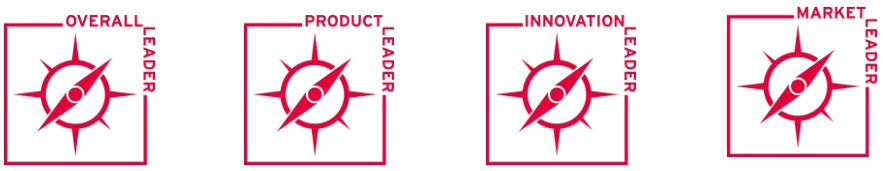
Strengths

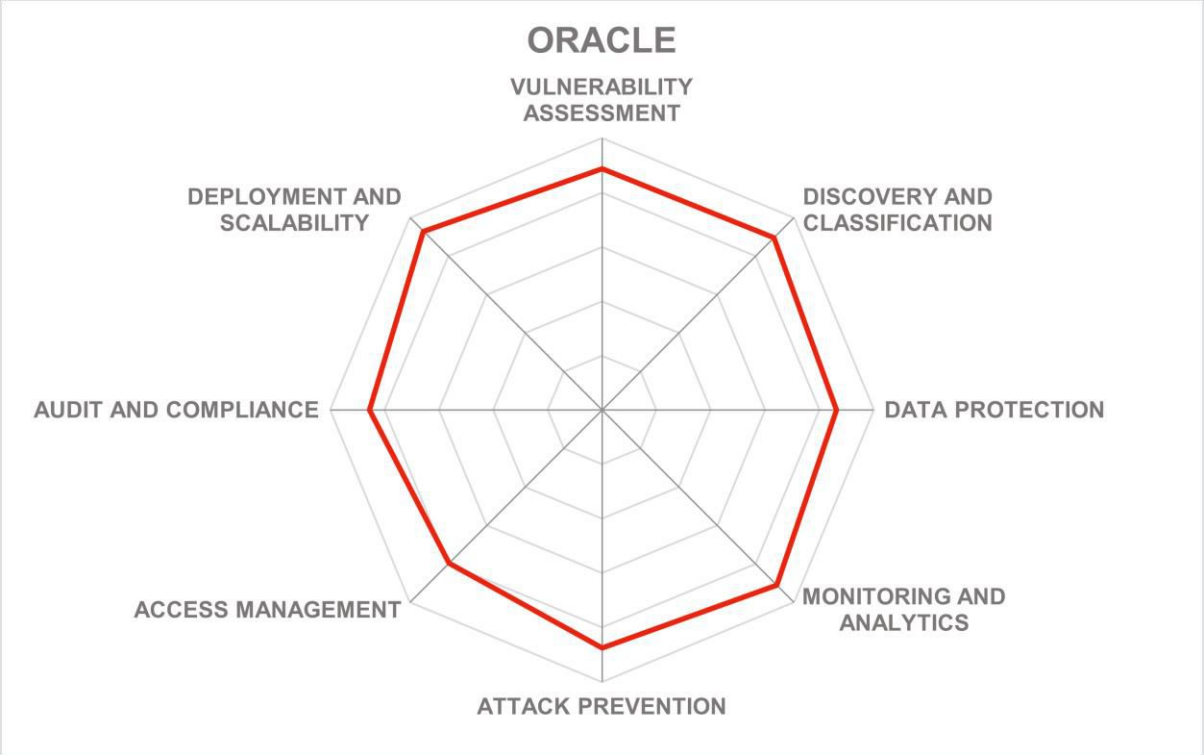
- Security capabilities integrated directly into the Oracle database core
- Broad range of tools and services for the whole information protection lifecycle
- Comprehensive database and data risk assessment, and user monitoring
- Risk mitigation for SQL generated by GenAI and agentic AI systems
- Autonomous database platform, eliminating human administrative access

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, including AWS, Azure, and GCP)
- Go-to-market approach primarily focused on existing Oracle enterprise customers

Leader in




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

PlainID – PlainID Platform

Founded in 2014, PlainID, headquartered in Tel Aviv, Israel, has established itself as a key player in the dynamic authorization management market, delivering a solid and scalable policy-based access control (PBAC) platform. With a global footprint spanning North America, EMEA, and APAC, PlainID primarily serves large enterprises across various industries. Its extensive partner ecosystem, which includes strategic alliances with system integrators, facilitates efficient market penetration and seamless solution deployment.

The company portfolio is centered around the PlainID Platform, a sophisticated access management solution that centralizes policy administration across diverse IT environments. By leveraging PBAC principles, the platform enables organizations to enforce fine-grained access control policies dynamically, ensuring precise and contextual authorization decisions. Its integration capabilities extend across traditional and modern infrastructure, supporting relational databases, while also providing seamless API-based interoperability with cloud platforms, including AWS, Google Cloud, and Microsoft Azure.

One of the platform's key differentiators is its deployment flexibility, catering to a wide spectrum of enterprise requirements. Organizations can choose between on-premises deployment, managed services, or a fully cloud-based SaaS model. The platform is designed for high availability and scalability, addressing the performance demands of large-scale environments.

PlainID seamlessly integrates with existing IAM infrastructures, reinforcing identity federation mechanisms via OAuth 2.0. Its business-friendly policy editor enables non-technical stakeholders to create and manage access rules without deep technical expertise, which may help to bridge the gap between security teams and business units. To address access governance at multiple levels, it supports role-based access control (RBAC), attribute-based access control (ABAC), and PBAC, enabling enterprises to define and enforce context-aware access policies.

Despite its strong authorization capabilities, the platform does not include native vulnerability scanning or real-time threat detection. However, its modular design allows integration with third-party security tools, ensuring that it complements rather than replaces an organization's broader security ecosystem. The PlainID Integration Hub provides a unified list of available out-of-the box integrations; additionally, the company offers a flexible SDK for custom use cases. Administrative monitoring is supported through activity logging, providing insights into access patterns and policy enforcement.

From a data protection standpoint, PlainID provides static and conditional row-level masking, allowing organizations to implement granular access restrictions. This is offered as a more secure alternative to tokenization and dynamic masking, since the data that users have no access to is never exposed at all, thus the additional privacy-preserving steps are not needed. The platform provides logging and audit capabilities, capturing authorization activities for forensic analysis and compliance reporting. Logs can be centrally managed using syslog or database-backed storage. While PlainID does not natively enforce regulatory

mandates such as GDPR or HIPAA, it equips organizations with the necessary policy management tools to support compliance efforts.

The company has recently introduced notable innovative capabilities. First, the PlainID GenAI Authorizer enhances AI security by enforcing granular access controls across the Retrieval-Augmented Generation (RAG) pipeline, securing query inputs, governing AI system access to data, and ensuring AI-generated responses align with user permissions. Second, PlainID has advanced API-driven data access control, introducing a multi-layered approach that combines API gateway and microservices controls with dynamic, identity-aware masking and filtering for JSON and SQL databases. These developments not only improve security automation at cloud scale but also help secure both direct and indirect data access across modern architectures.

PlainID offers a mature and adaptable authorization management platform designed to meet the complex access control needs of modern enterprises. By centralizing policy enforcement across applications, data layers, and cloud environments, it provides a powerful framework for securing sensitive data throughout the entire technology stack of modern applications and services. Organizations seeking a scalable, business-friendly authorization platform will find PlainID to be a strong contender.

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

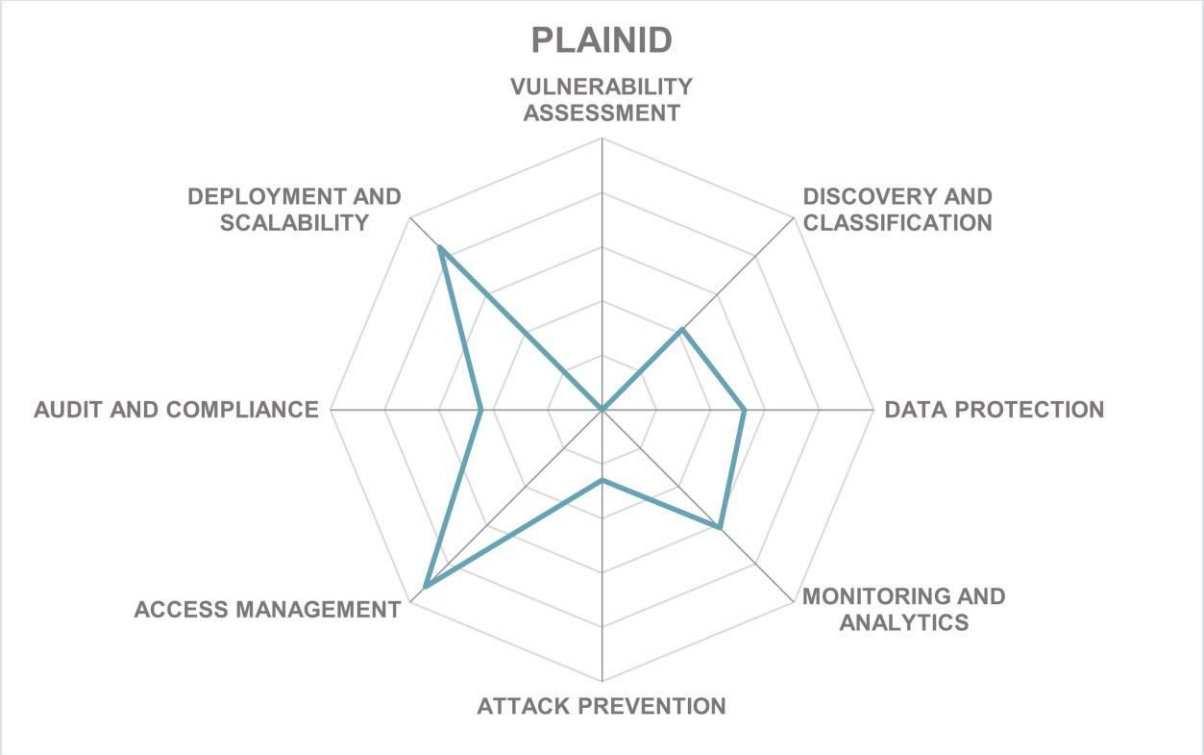
Table 12: PlainID's rating

Strengths

- Comprehensive implementation of policy control with PBAC, RBAC, and ABAC
- Flexible deployment options, including on-prem, cloud, and SaaS
- Extensive integration ecosystem with a convenient Integration Hub
- Business-oriented policy editor to reduce technical complexity
- Authorization-as-a-Service to address modern enterprise demands

Challenges

- Limited threat prevention and vulnerability management
- Discovery and classification are supported by 3rd party tool integrations
- Data protection functionality focuses primarily on policy-based orchestration
- Absence of multilingual support or documentation


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

SecuPi – Data Security Platform

Founded in 2014 and based in Jersey City, New Jersey, SecuPi operates as a privately held company, independent of venture capital funding. The company has built a strong financial foundation through sustained revenue streams from Fortune 100 clients and other large enterprises across North America, EMEA, and APAC. This financial independence has enabled SecuPi to maintain a steady growth trajectory while remaining focused on delivering enterprise-grade data security solutions.

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 and leverage the full user identity context attributes as well as the data request and response. It also includes gateways for controlling direct DB tools and analytics environments with no APIs or business-processes changes, enabling low-risk low-cost deployment.

The company's flagship product is the SecuPi Data Security Platform, an end-to-end integrated solution designed to address a broad spectrum of data security challenges. With a strong presence in highly regulated industries such as finance, insurance, healthcare, government, and retail, SecuPi's platform offers advanced security and compliance capabilities tailored for complex enterprise environments. Designed for deployment across on-premises, private, and public cloud environments, the platform ensures broad compatibility with leading cloud providers such as AWS, Azure, Google Cloud, and Oracle Cloud, as well as NoSQL solutions.

One of the platform's strengths lies in its fine-grained access control mechanisms, utilizing Attribute-Based Access Control (ABAC) to enforce security policies based on user attributes, contextual parameters, and role-based permissions. This approach allows enterprises to implement dynamic and adaptable access controls tailored to their specific operational needs. In addition, the platform provides dynamic data masking and encryption capabilities. By supporting column- and row-level masking and incorporating cryptographic techniques such as Format-Preserving Encryption (FPE) and tokenization, SecuPi enables secure data handling while maintaining business continuity and regulatory compliance. The platform offers unmatched flexibility to apply different security controls and mechanisms at rest and in use, across different classifications and data access scenarios.

The platform integrates with various enterprise identity and authentication solutions, including Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) protocols. To enhance security further, multi-factor authentication (MFA) options, including biometric recognition and passkey-based authentication, provide additional layers of protection against unauthorized access. SecuPi incorporates advanced real-time user behavior analytics (UBA) to monitor and assess data access patterns. This capability enables the platform to detect anomalies and proactively mitigate potential threats.

Moreover, the platform is designed to help organizations meet stringent regulatory compliance requirements, such as GDPR, HIPAA, SOX, PCI DSS 4.0 and others through

automated sensitive data discovery, classification, and policy enforcement, all without the need to adapt existing database structures or deploy agents.

The 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.

SecuPi's ability to deliver a comprehensive, non-intrusive, and scalable data security platform makes it a compelling choice for organizations looking to harmonize data security policies across complex IT environments. The company's focus on enterprise-wide visibility, automated compliance, and real-time analytics positions it as a strong contender in the competitive data security landscape.

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

Table 13: SecuPi's rating

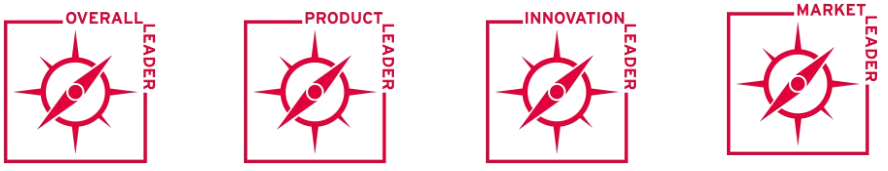
Strengths

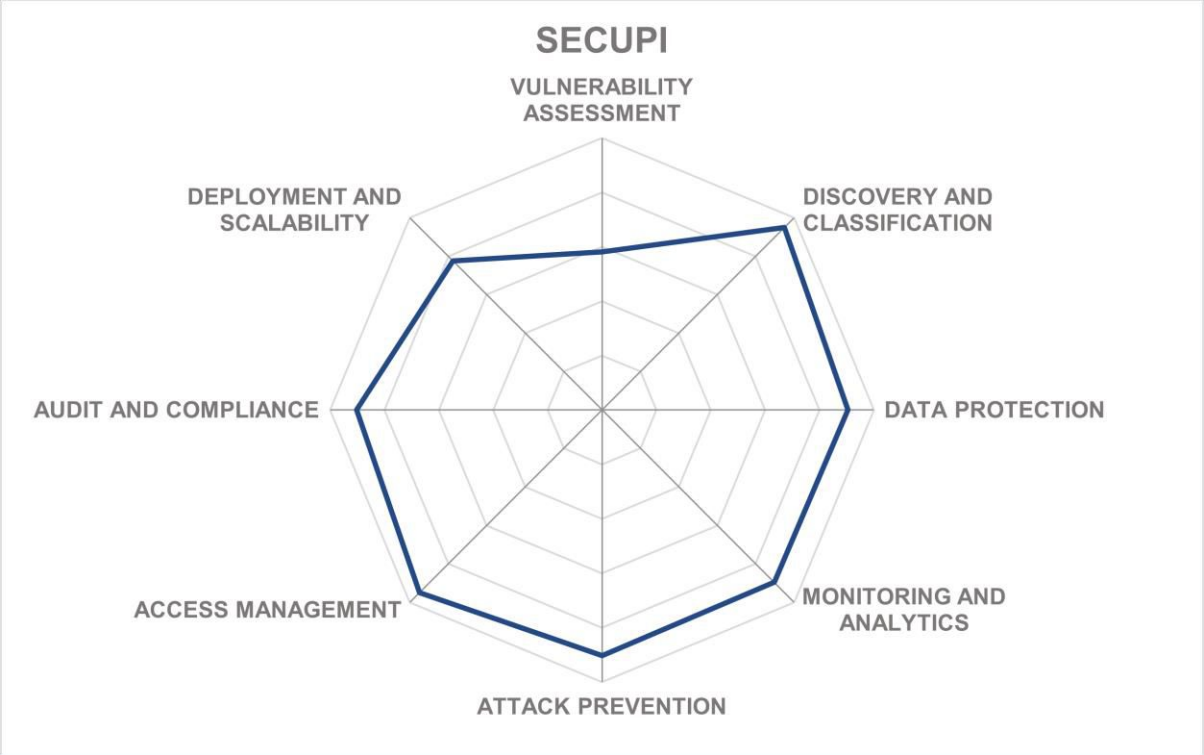
- Integrated data protection and privacy platform with a strong focus on regulatory compliance and de-identification of critical data in the cloud
- Full coverage for the data protection lifecycle
- Application-level protection overlays simplify deployment and management
- Broad support for big data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

Challenges

- Support of legacy platforms requires additional effort
- Might require substantial initial setup and configuration for complex deployments
- Not focusing on database infrastructure assessment

Leader in




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

Thales – CipherTrust Data Security Platform and Imperva Data Security Fabric

Thales Group, a leading cybersecurity vendor, has significantly expanded its presence in the data security market through a strategic series of acquisitions, including SafeNet, Vormetric, Gemalto, and most recently, Imperva. Originally established in 2000 and headquartered in Paris, France, the company now operates under the Thales Cybersecurity Products division, delivering a broad spectrum of security solutions worldwide.

With a presence spanning North America, EMEA, APAC, and Latin America, Thales serves enterprises of all sizes. Its core customer base includes key industries such as finance, retail, manufacturing, and healthcare - sectors with tight regulatory requirements and high-value data assets. Additionally, Thales maintains a vast global network of partners, including system integrators, channel resellers, and distributors.

At the heart of Thales' data security strategy are its two flagship solutions: CipherTrust Data Security Platform and Data Security Fabric. Together, these platforms offer a holistic approach to data protection, governance, and compliance, addressing security concerns across complex, multi-cloud, and hybrid environments. Both platforms are architected to support a wide range of structured and unstructured data repositories, spanning relational databases, NoSQL environments, and cloud-native data services.

CipherTrust Data Security Platform (CDSP) provides a centralized management framework for data discovery, classification, encryption, key management, and tokenization. By integrating third-party technologies, Thales has further expanded its coverage in areas such as advanced unstructured data discovery and secrets management.

Data Security Fabric (DSF), a product of Thales' acquisition of Imperva, enhances data visibility, observability, and analytics. By integrating real-time insights, behavioral analytics, and risk-based threat detection, DSF plays a pivotal role in proactive security and compliance enforcement across modern data ecosystems.

In December 2024, Data Risk Intelligence (DRI) was added to the Data Security Fabric to help organizations prioritize risks and address security gaps like access anomalies, shadow data, AI risks, and cryptographic posture. It fuses together a comprehensive range of data risk indicators, including user permissions, data source vulnerabilities, encryption status, and suspicious activities. As part of the Data Security Fabric, DRI mitigates risks and ensures robust data protection and posture management in hybrid environments.

Thales' comprehensive data security approach covers three critical areas: protection, monitoring, and compliance. CDSP offers extensive encryption capabilities for data at rest, in transit, and in use. Complementary techniques, including tokenization and dynamic data masking, provide additional layers of security for sensitive information.

DSF delivers comprehensive monitoring functionalities, including UBA, anomaly detection, and real-time mitigation for threats such as SQL injection and Denial-of-Service (DoS) attacks. Automated remediation further enhances incident response efficiency, minimizing

exposure to security breaches. For audit and compliance, Thales supports a broad range of regulatory frameworks, including GDPR, HIPAA, PCI-DSS, ISO/IEC 27001, and US FedRAMP. The solutions feature extensive audit logging and centralized reporting.

Thales has positioned itself as a strong leader in data security, leveraging a combination of strategic acquisitions and continuous innovation to address the challenges of enterprise data protection. By offering a unified, scalable, and compliance-ready security framework, Thales enables organizations to secure their sensitive data assets across complex IT environments.

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

Table 14: Thales Group's rating

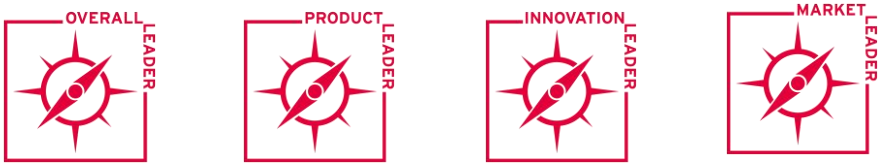
Strengths

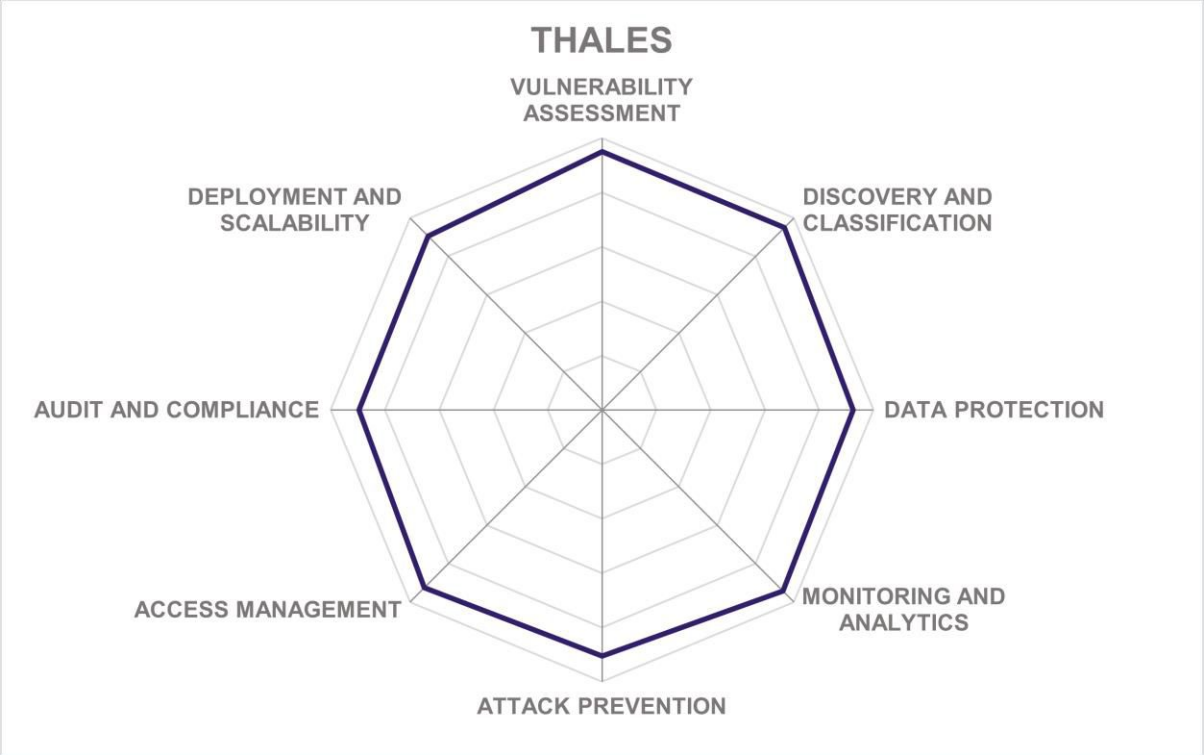
- A comprehensive data security portfolio addressing all aspects of data security
- Broad coverage of databases and cloud data platforms
- Strong multi-cloud and hybrid cloud support, ensuring consistent security policies across distributed environments
- Advanced threat detection and automated remediation capabilities
- Compliance-centric design, facilitating regulatory adherence for enterprises

Challenges

- Integrating all capabilities into a single platform is still work in progress
- Complexity and cost of implementation might be significant for smaller companies
- Some buyers might not initially require all available capabilities

Leader in




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

TrustLogix – Data Security Platform

Founded in 2019 and based in Mountain View, California, TrustLogix is a relatively new yet innovative player in the data security space, aiming to simplify and centralize access control across multi-cloud, on-premises, and hybrid environments. The company primarily serves mid-market and enterprise customers across North America and EMEA. Its key industries include financial services, manufacturing, and healthcare. TrustLogix has established a modest but growing partner ecosystem, including system integrators and resellers, particularly in North America.

TrustLogix positions itself as a data-centric security platform that enforces access control and data governance policies without directly handling or storing sensitive data. This proxy-less architecture ensures minimal performance impact while maintaining strict security postures across cloud and on-premises data platforms. The solution supports an extensive range of relational databases with ongoing expansion into NoSQL environments.

A core focus of the platform is data security posture management (DSPM), helping organizations detect and remediate overprivileged access, unmasked sensitive data, and other security misconfigurations. TrustLogix employs a combination of role-based access control (RBAC) and attribute-based access control (ABAC) to provide granular access governance across multiple cloud databases, warehouses, object storage services, and managed databases like MS SQL Server, PostgreSQL, or Oracle.

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.

TrustLogix follows industry-standard security best practices, including encryption, automated backups, and a non-intrusive deployment model that does not process transactional customer data. Its architecture allows for multiple deployment models, including full SaaS and hybrid configurations, where TrustLogix's TrustLet service can be deployed within a customer's cloud environment. While it does not incorporate traditional intrusion detection capabilities, its security posture management helps identify high-risk configurations and provides guidance for remediation.

TrustLogix enables data protection through native platform capabilities, leveraging cloud provider mechanisms such as dynamic data masking and tokenization. In addition, the platform facilitates continuous assessment of access permissions, policy enforcement, and exposure risks. Access management remains a core strength, with policy-based controls and support for external integrations via open APIs.

The platform ships with a library of predefined monitoring policies. 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.

TrustLogix presents a compelling solution for enterprises seeking a modern, cloud-native approach to access governance and data security posture management. By avoiding the complexities of proxy- or agent-based architectures, it enables organizations to enforce security policies efficiently across multi-cloud environments. For enterprises prioritizing cloud-native security governance, risk management, and compliance automation, TrustLogix represents a forward-thinking solution without the burden of traditional data security tools.

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

Table 15: TrustLogix's rating

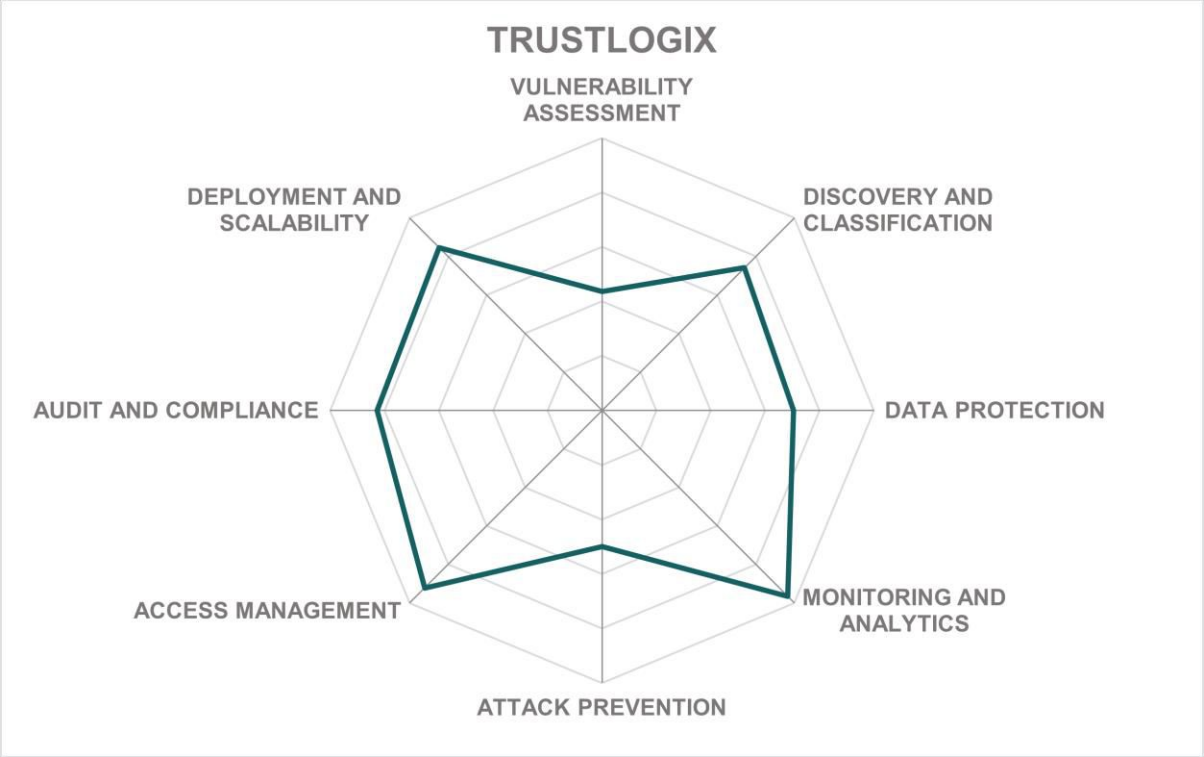
Strengths

- 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
- Full support for unstructured data sources is still being developed
- Limited language support beyond English

Leader in


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

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors could not participate in our rating for various reasons but nevertheless offer a significant contribution to the market space.

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. 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.

Comforte

Comforte AG is a privately held software company specializing in data protection and digital payment solutions based in Wiesbaden, Germany. Having its roots in the development of critical business applications, the company now offers a comprehensive platform for protecting sensitive business data with encryption and tokenization, tailored specifically for scenarios that do not allow even minimal downtime.

Why worth watching: Comforte's Data Security Platform offers a decentralized and fault-tolerant architecture that supports multi-cloud and hybrid deployments. It enables high-performance sensitive data processing and strong regulatory compliance even for the most demanding industries.

Databricks

Databricks is a cloud-based data and AI company that offers a unified analytics platform for processing large-scale data, perform advanced analytics, and deploy AI/ML models efficiently. Founded in 2013 by the creators of Apache Spark, the company is headquartered in San Francisco, California. The Databricks Data Intelligence Platform is built upon an open data lakehouse and powered by a Data Intelligence Engine to offer a single foundation for data science, business intelligence, analytics, machine learning, and AI. In 2023, Databricks acquired Okera, a provider of AI-centric data governance solutions.

Why worth watching: Databricks' built-in security, regulatory compliance, and natural language capabilities make it a versatile solution for enterprises handling large-scale data and AI applications. The company's partner ecosystem offers a broad range of cybersecurity solutions built on top of the platform.

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. The recent acquisition of Privitar has further strengthened Informatica's privacy portfolio.

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.

Mage Data

Mage Data is a company that has provided sensitive information management solutions since 2004. It is based 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.

Why worth watching: the company provides a unified platform for test data management and database security, delivering an integrated solution for secure digital transformation for businesses migrating their data to the cloud. Its capabilities are also available through multiple third-party vendors.

MinerEye

MinerEye is a 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.

PKWARE

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.

Why worth watching: the company's PK Protect Suite enables comprehensive sensitive data protection by securing both data stores and endpoints, ensuring consistent discovery, classification, masking, and encryption across environments. Its broad compatibility with diverse data stores, automation of privacy compliance processes, and endpoint security integration make it a flexible solution for organizations handling regulated or sensitive information.

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 various 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 offers a centralized platform to monitor, manage, and automate data access controls across various cloud data providers, enhancing data security and compliance. Its integration capabilities with tools like CI/CD pipelines and identity providers streamline workflows, enabling efficient and scalable data access management.

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.

Sentra

Sentra, established in 2021, is a cloud-native data security company co-headquartered in Tel Aviv, Israel, and New York City, USA. The company specializes in providing comprehensive data security solutions for cloud-driven organizations. Sentra's platform offers automatic data discovery, classification, monitoring, and protection services, enabling businesses to regain control over their sensitive data across various cloud environments.

Why worth watching: Sentra's Cloud-Native Data Security Platform enables security teams to automatically classify sensitive data, assess risks, and remediate threats across various environments, including cloud, SaaS, and on-premises systems. By leveraging AI capabilities, Sentra provides continuous, accurate classification of data to assess and maintain its security posture.

Varonis

Varonis is a data security and analytics company based in New York City, NY, USA. Founded in 2005, the company focuses on protecting the entirety of enterprise data, from sensitive files and emails to databases containing patient data or financial records. The unified Data Security Platform provides real-time visibility into heterogeneous data stores, proactive detection of abnormal and malicious activities, and automated prevention of issues that can lead to data breaches.

Why worth watching: Varonis offers a strongly unified approach to data security by addressing various challenges of structured and unstructured, cloud-native and on-premises data in a single platform powered by strong AI-powered detection and remediation capabilities. It secures enterprise data where it lives, including all systems that provide access to it (from proxies and firewalls to identity providers and generative AI models).

Velotix

Velotix, founded in 2020 and based in Ramat Gan, Israel, is a data security company specializing in AI-driven data protection and access governance. The company's portfolio includes self-service data access, automated policy management, and AI-powered policy databases, enabling organizations to discover, visualize, and securely utilize their data while ensuring compliance with internal and external regulations.

Why worth watching: the company’s data security platform integrates automated policy management, data visibility, and policy-based access control to provide compliant data access at scale, helping customers to grant secure access efficiently while adapting to changing regulations.

Related Research

Leadership Compass: Data Security Platforms (2023)Leadership Compass: Data Leakage PreventionLeadership Compass: Data GovernanceLeadership Compass: Synthetic Data for Security and PrivacyLeadership Compass: Data Quality and Integration SolutionsWhitepaper: Understanding and Managing Privileged Access to Databases and Other Data ResourcesWhitepaper: Why Your Organization Needs Data-centric SecurityAdvisory Note: Cybersecurity Resilience with Generative AIAnalyst Chat: The Future of Data Security

Copyright