

## Kuppingercollection Report

# MARKET COMPASS

By **Paul Fisher**  
June 11, 2021

## Data Governance Platforms

The Kuppingercollection Market Compass Data Governance covers platforms that assist organizations in managing data so that it meets stringent compliance regulations in different markets and catalogues data for greater business value. Data Governance Tools are a relatively new addition to the existing catalogue of IT based governance solutions and their growth can in part be attributed to the rise in compliance legislation around the world, but perhaps more pertinently by the explosive growth of data held across all organizations.



By **Paul Fisher**  
[pf@kuppingercollection.com](mailto:pf@kuppingercollection.com)

# Content

<b>1 Management Summary</b>	4
<b>2 Market Segment</b>	6
2.1 Market Description	6
2.2 Major Use Cases	7
2.3 Market Direction	9
<b>3 Capabilities</b>	12
3.1 All capabilities	12
3.2 Capabilities recommended per use case	13
3.2.1 Discovery and search	14
3.2.2 Compliance	15
3.2.3 Auditing & Classification	15
3.2.4 Value creation	16
3.2.5 Cyber security	17
<b>4 Ratings at a Glance</b>	18
4.1 General Product Ratings	18
4.2 Noteworthy Vendors for Specific Capabilities	20
4.2.1 Outstanding in AI Capability: 1touch.io	20
4.2.2 Outstanding in Innovation: BigID	20
4.2.3 Outstanding in Compliance Support: SAP	21
4.2.4 Outstanding in Dashboard support: Varonis	22
4.2.5 Outstanding in Report Generation: Micro Focus	23
<b>5 Product/Service Details</b>	25
5.1 1touch.io	27
5.2 BigID	30
5.3 Concentric	33
5.4 Egnyte	36
5.5 Lepide	39
5.6 Micro Focus	42

5.7 Netwrix	45
5.8 SAP	48
5.9 STEALTHbits Technologies	51
5.10 Varonis	54
<b>6 Vendors to Watch</b>	<b>57</b>
6.1 BlueTab Solutions - Truedat.io	57
6.2 Collibra Governance	57
6.3 CommVault Activate	57
6.4 EverTeam Discover	58
6.5 Global Data Excellence - DEMS-Nexus	58
6.6 IBM Watson Knowledge Catalog Instascan	58
6.7 OneTrust	59
6.8 OvalEdge Data Catalog & Governance Tool	59
6.9 SailPoint - File Access Manager	59
6.10 TopQuadrant - TopBraid EDG	59
<b>7 Related Research</b>	<b>61</b>
<b>Methodology</b>	<b>62</b>
<b>Content of Figures</b>	<b>65</b>
<b>Copyright</b>	<b>66</b>

# 1 Management Summary

The KuppingerCole Market Compass provides an overview of a market segment and the vendors in that segment. It covers the trends that are influencing that market segment, how it is further divided, and the essential capabilities required of solutions. It also provides ratings of how well these solutions meet our expectations.

This Market Compass:

---

*Provides an assessment of the capabilities provided by 10 vendors that compete in the market for Data Governance solutions. It focuses on capabilities to find and make sense of unstructured data and, in some cases, structured data. It further analyses tools to extract business value from data.*

---

Companies and organizations are awash with structured and unstructured data and industry estimates put it as growing by 40-80% per year. The reason: dynamic growth of digital devices, cloud platforms, services, and storage options in organizations. Data is flung far and wide across organizations from email accounts, laptops, smartphones, social media, cloud and web servers right up to the largest data lakes.

The challenge for organizations is to make sense of unstructured data, sort the wheat from the chaff and identify sensitive and business critical data. Organizations require a Data Governance Architecture Blueprint as a working structure within the organization to maintain data integrity, provide security and create value from data. Integral to that are Data Governance platforms such as those presented in this Market Compass. Ideally a Data Governance Architecture Blueprint would already be in place or created before investment in Data Governance solution.

Creating a robust data lifecycle management program is also part of the process. If configured correctly at the outset, a Data Governance architecture and platform should be robust enough to withstand new data flows, corporate changes such as M&A, other business pressures or new compliance rules.

This Market Compass report covers those Data Governance solutions, should provide an overview and analysis of unstructured data typically held on file servers, documents, endpoints, clouds within organizations and provide the tools to organize that data.

## Highlights:

- Ten Data Governance platforms are rated by Senior Analyst Paul Fisher for unstructured data performance and compliance.
- The capabilities and use cases to consider when considering Data Governance platforms.

- Why digital transformation, cloud and collaboration has made the governance of unstructured data essential.
- How Data Governance can assist organizations in meeting compliance regulations and to reduce the number of data breaches.
- Why creating business value from unstructured data has taken on a new importance for organizations of all sizes in the new competitive landscape.
- How Data Governance architectures are now being assisted by AI and machine learning tools in new platforms.

## 2 Market Segment

Data Governance platforms for unstructured data are a relatively new addition to the existing catalogue of IT based governance solutions and their growth can be attributed to the rise in compliance legislation around the world, and the explosive growth of data held across even the smallest of organizations. Data Governance solutions should provide an overview and analysis of unstructured typically held on file servers, endpoints, cloud and databases within organizations. This market now has some small cloud-based providers as well as add-on modules from existing data analytics companies.

### 2.1 Market Description

Readers should note that Data Governance is not the same as Governance Risk and Compliance (GRC) although the two are related. If an organization fails to identify and organize data, it could fail to conduct accurate risk assessments on data and subsequently fall foul of compliance. Finding the right Data Governance platform involves policies, processes, and technology. A growing number of vendors are delivering solutions that can assist with Data Governance for organizations in response to demand.

Many businesses get Data Governance wrong and fail to plan to create a framework before implementing Data Governance policies and related technologies. Sometimes a Chief Data Officer is appointed and tasked with the job of managing unstructured data in the organization, which can have the effect of galvanizing efforts to manage data, but it is not a necessity and there is risk that the role becomes mixed up with market analytics, driven by assertive lines of business such as marketing, or with compliance duties as companies seek to avoid prosecution.

Fundamentally, Data Governance is about taming layers of unstructured data, and aligning data to the business strategy or the organization. Unstructured data has little value if it cannot be organized and shared across the organization and aligned with the business.

#### **The impact of privacy laws**

Privacy laws, regulations, and initiatives are proliferating to address the growing concerns over personal data use and control by corporations. The EU's General Data Protection Regulation (GDPR), seen frequently in the headlines in recent times, gives Europeans the right to control their personal information collected by organizations. In other parts of the world, the Asia-Pacific Economic Cooperation (APEC) initiated Cross-Border Privacy Rules (CBPR), which focus on building trust between consumers and organizations as individuals' data flows between APEC economies.

This is accomplished by requiring participating APEC organizations to implement data privacy policies that

conform to the APEC Privacy Framework. In the U.S., personal data breaches such as at Experian and the Facebook - Cambridge Analytica scandal are compelling legislators in individual states to implement data privacy laws. The state of Vermont enacted the nation's first data broker legislation that requires data brokers to register with the government, inform people on how to opt-out, what is collected and when their data has been breached, and give individuals legal recourse when their data has been abused. Also, in the U.S., California has gone further by introducing new rights for consumers regarding the privacy and use of their data. The California Consumer Privacy Act was enacted and took effect in 2020. It is anticipated that growing momentum for individual data privacy will eventually lead to a more uniform law at the federal level to provide consistency across all states sometime in the distant future.

Another US regulation designed to protect consumers is the NY DFS Cybersecurity Regulation (23 NYCRR 500) that requires New York banks, insurance companies, and other financial services institutions regulated to assess their cybersecurity risk profile. This regulation includes providing audit trails showing that data retention is held for only three years rather than the previous standard five-year data retention period.

Organizations that must comply with these laws and regulations face new challenges and compliance risks. Organizations today must know where their user data resides, categorize the data's level of vulnerability, impact, and risk to the organization, and ensure that they remain in compliance to meet many different regulations.

Some solutions came into being to help address aspects of these issues, such as Identity Governance and Administration (IGA), which was initially driven by SOX regulations that required organizations to ensure separation of duties (SOD) to prevent accounting fraud. But IGA only covers a subset of the data compliance requirements. A comprehensive solution is needed that uses data intelligence to provide governance, privacy, and protection of customers' data.

### **Adding value**

Compliance and security are key drivers for Data Governance platforms, but there is also an added benefit in deriving business value from organized data. Organizations are increasingly looking to Data Governance platform providers to offer capabilities that allow analysis of data to provide unique business insights. This is where governance meets business innovation and competitive instincts.

## **2.2 Major Use Cases**

The primary goal for Data Governance platforms is to classify and protect files and other data sources in line with organizations policies and goals.

These tools can manage access requests, approvals, certification, and analysis of the entitlements at a more granular level. The picture is complicated today by the profusion of data repositories, in the cloud, on end points and on-premises - and the growth of applications available to access and share it across different users.

Data Governance allows building standard access request and approval processes for the fine-grained entitlement management below the level that is covered by typical Access Governance solutions.

The protection of sensitive customer data has become a critical issue of our time, especially for organizations that collect, process, and store PII (Personally Identifiable Information). Privacy laws, regulations, and initiatives are proliferating to address the growing concerns over the use and control of personal data. The European Union's General Data Protection Regulation (GDPR) and the new California Consumer Privacy Act (CCPA) are good examples that will punish organizations for poor Data Governance that results in data loss or privacy incursions.

Major use cases for Data Governance include:

### **Discovery and search of data**

Unstructured data that lies undocumented across an organization represents a security risk and a missed opportunity to create value from that data. Digital transformation creates data on endpoints, within cloud services, in email, messaging and collaboration platforms that can slip under the radar. Often this data can provide valuable insights into what is happening to organizations, especially in terms of customer relations or marketing. It is vital that Data Governance platforms can discover unstructured data, order it, and give the organization the option of what action to take. This can include deleting duplicates, reassigning data to different stewardship or protecting data that contains sensitive information.

### **Compliance**

While personal data held in structured databases is relatively easy to find and protect, the real danger arises with personal information (PII) that lies hidden within unstructured data stacks. For example, a customer may have provided email, home address or even credit card details in an email. Such information may also reside in unprotected documents and spreadsheets created by employees. Health data may be contained in letters and other documents. All modern compliance laws put the responsibility for data protection on the Data Controller defined as the organization that stores such information on behalf of individuals or other organizations. Organizations have been fined large penalties for failing to protect personal data. Without Data Governance in place such data may go unnoticed and unprotected.

### **Auditing and classification**

Data that has been discovered from unstructured sources must be audited and classified if it is to be protected and add value to the organization - data that is not identified and classified is valueless. Tools within Data Governance platforms perform this function with varying levels of automation. Some platforms offer further insight into file access patterns from Active Directory, SharePoint or Teams. Further, data can be divided into functional or business categories from a Business Glossary. For example: customers, suppliers, inventory, personally identifiable information (PII), confidential, protected and so on. A good Data Governance platform should enable the customer to define more categories in line with business policy and sector and define data for future classifications.

### **Value creation**

Unstructured data is like crude oil; value is only extracted once it is refined. Data Governance platforms



assist in creating value from data after discovery, auditing, and classification. While some organizations may initiate processes and applications to generate and analyze specific data - a simple example would be a market research exercise - there is much untapped value to be found from the unstructured data created through normal business processes every day. To find value, Data Governance applications will offer a range of capabilities such as dashboards that display inefficient data flows and data usage, data duplication and data usage that violates business policies. Interactions between customers and employees can also be mapped, some platforms also monitor data shared on social media platforms.

### **Cyber security**

Data that is not governed remains at constant risk of being lost or stolen, which is a big problem if it contains information that is confidential, such as PII or is critical to the security of the organization. A Data Governance framework that includes a Data Governance platform is an important part of cyber security, so that high value and confidential data can be found, classified, and protected on an ongoing basis. The platform must be intelligent enough to recognize PII data or other critical data or use business policies to identify and treat it accordingly. The Data Governance platform cannot apply protection, and therefore, the organization must use other tools in its cyber security portfolio to protect it: encryption software, privileged access management (PAM) and identity governance & administration (IGA) tools. Data Governance is a welcome tool to have in the frontline against data breaches. Organizations cannot protect what they do not know exists.

## **2.3 Market Direction**

Data Governance platforms for unstructured data are of increasing importance to modern organizations as data levels exponentially increase. Privacy laws, regulations, and initiatives are proliferating to address the growing concerns over the use and control of personal data. The European Union's General Data Protection Regulation (GDPR) and the new California Consumer Privacy Act (CCPA) are good examples that will punish organizations for poor Data Governance that results in data loss or privacy incursions.

While most platforms currently offer the basic level of capabilities, more advanced capabilities are undoubtedly on the horizon. There is great potential for further integration with other security, access and governance platforms. Data Governance allows building standard access request and approval processes for fine-grained entitlement management below the level that is covered by typical Access Governance solutions.

Many of these tools also offer data classification and access management options to prevent more sensitive data being viewed by unauthorized parties. In this way, there is potential for integration with IAM and PAM applications and support for the stages and controls of the new Information Protection Life Cycle Framework that KuppingerCole is now developing. This documents three stages in the life of information and six categories of controls to secure information.

Some vendors offering Data Governance tools come from the business analytics space and add extra

insight to managed data, but this is not a prerequisite, as the primary goal for Data Governance is to classify and protect files and other data sources in line with organizations policies and goals. Much insight and business value can be gained from data simply by classifying it, and this a lesson that increasing numbers of organizations are learning, from SMBs up to Enterprise level.

The security lesson of Data Governance is one that is being taken on board also. Data Governance tools provide an extra layer of defence against data by helping to find and classify personal data. Such classifications can then be used by access control systems to make more accurate authorisation decisions.

Data Governance platforms that can tame unstructured data are far from full maturity and for all the reasons mentioned above we not only anticipate more interest from the market but also other new players entering the market, particularly those that can offer some form of automation and AI to assist in the discovery and classification process. We should see the development of Data Governance tools that can assist with IAM, PAM by adding more granular control on access rights to data.

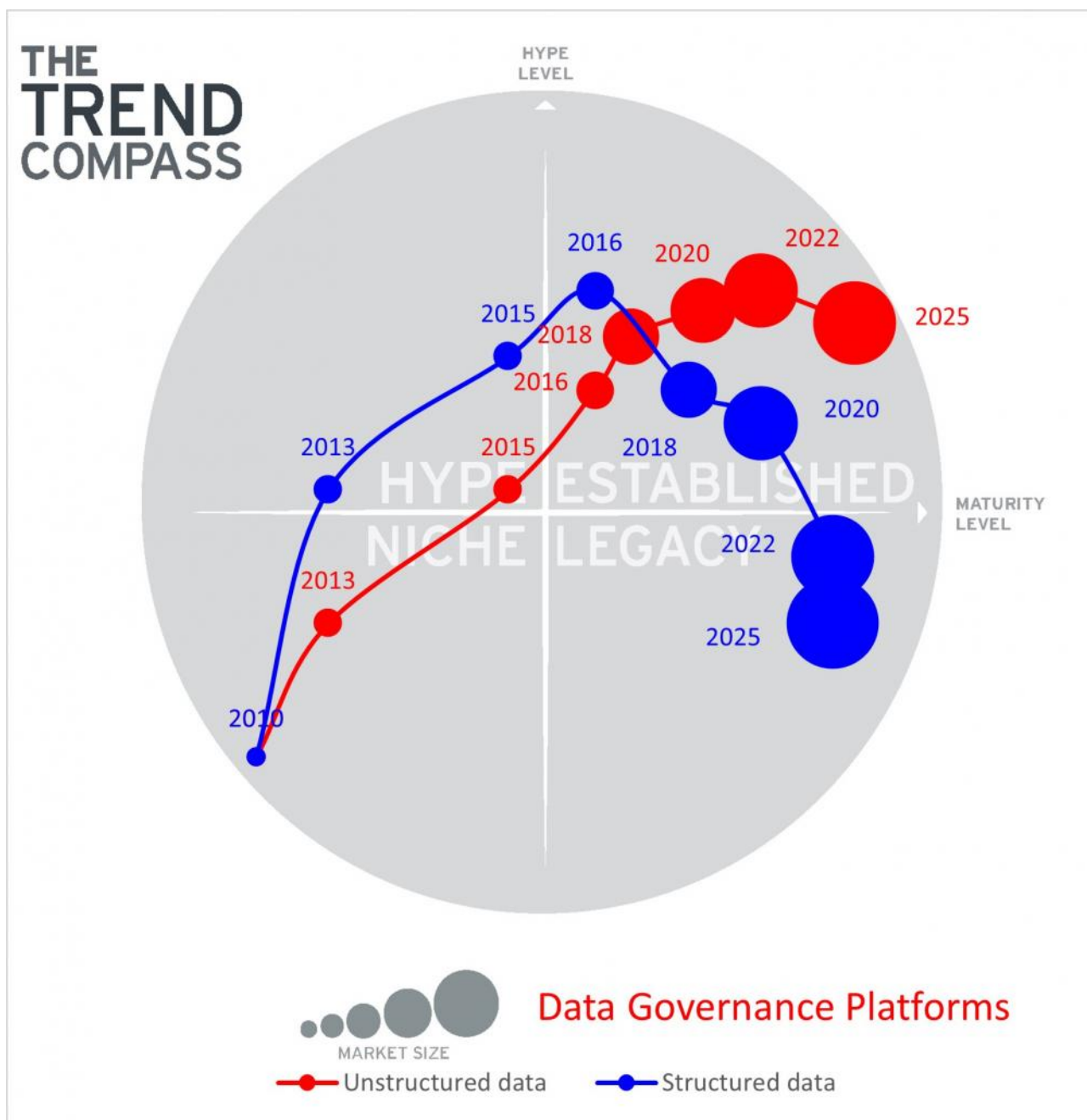


Figure 1: Trend Compass for Data Governance platforms.

Figure 1 shows how the impact of rapidly increasing growth in data volumes, rising regulatory and compliance mandates, has driven demand for Data Governance platforms. However, while organizations have been aware for a longer time of the need to manage structured data, the growth of unstructured data through digital transformation took place later in the hype/maturity cycle. It is possible the market for Data Governance platforms that control unstructured data will be larger.

## 3 Capabilities

The Market Compass is designed to profile and compare vendors across numerous capabilities. This section details the capabilities that one should expect to see in this market segment and breaks them down according to relevance per use case.

### 3.1 All capabilities

The important capabilities provided by Data Governance platforms to ensure data is discovered, mapped and coordinated are listed in the table below.

Capability	Description
Social media	In modern organizations social media platforms such as Facebook, Twitter and Instagram are used by employees within the enterprise infrastructure as well as formally by LOBs such as marketing. Content created on these platforms should be included in any Data Governance architecture and covered by Data Governance platforms.
Office applications	The majority of unstructured data is created in mainstream office applications such as Office 365, SharePoint, Google Docs, Adobe Acrobat and many other applications that are popularly used. Data Governance platforms will offer different levels of support for these types of applications, the more the better.
Chat and messaging	Text messages, collaboration software, Chat and Instant Messaging are all integral parts of the modern enterprise and data generated here must be discovered and audited according to business and security policies.
PII discovery	Personal Identifiable Information (PII) is often hidden in seemingly innocuous documents or even in messaging logs. For this reason, it is important that Data Governance tools can search and identify PII wherever it sits in unstructured data.
Automation, Machine Learning/AI tools	Machine Learning and AI capabilities are being added to some Data Governance platforms and provide a boost to data discovery and to assisting with data classification but also increasingly to assist with alerts to misuse of data and instances of oversharing. Data Governance automation will become increasingly important as unstructured continues to multiply.
Report generation	Without timely reports, making decisions on data is hard. Report generation allows all stakeholder to have a clear idea on the creation and usage throughout the organization.

Capability	Description
Compliance support	Supports compliance with PII, GDPR, HIPPA, PCI, and other regulatory standards.
Dashboard	A dashboard giving an overview of Data Governance positions is almost essential. This can give admins and governance specialists real time reporting and alerts to potential abuse of data that puts data at risk. It can also be used to track users and suspicious activity.
Business glossary	Support for a business glossary is important. This document is part of a Data Governance program that proves the organization has an agreed-upon understanding of key business concepts, business terms and the relationships between them and how data relates to those.
Cloud integration	Unstructured data will be hard to manage on-premises but harder still when it sits in cloud and multi-cloud infrastructures. Data Governance platforms should therefore be capable of linking to all major cloud platforms if search and discovery is to be fulfilled.

Table 1: Ten major capabilities for Data Governance platforms.

## 3.2 Capabilities recommended per use case

The Data Governance segment is evolving to meet several distinct use cases, as described in section 2.2. Below, the capabilities are displayed according to their relevance for each use case.

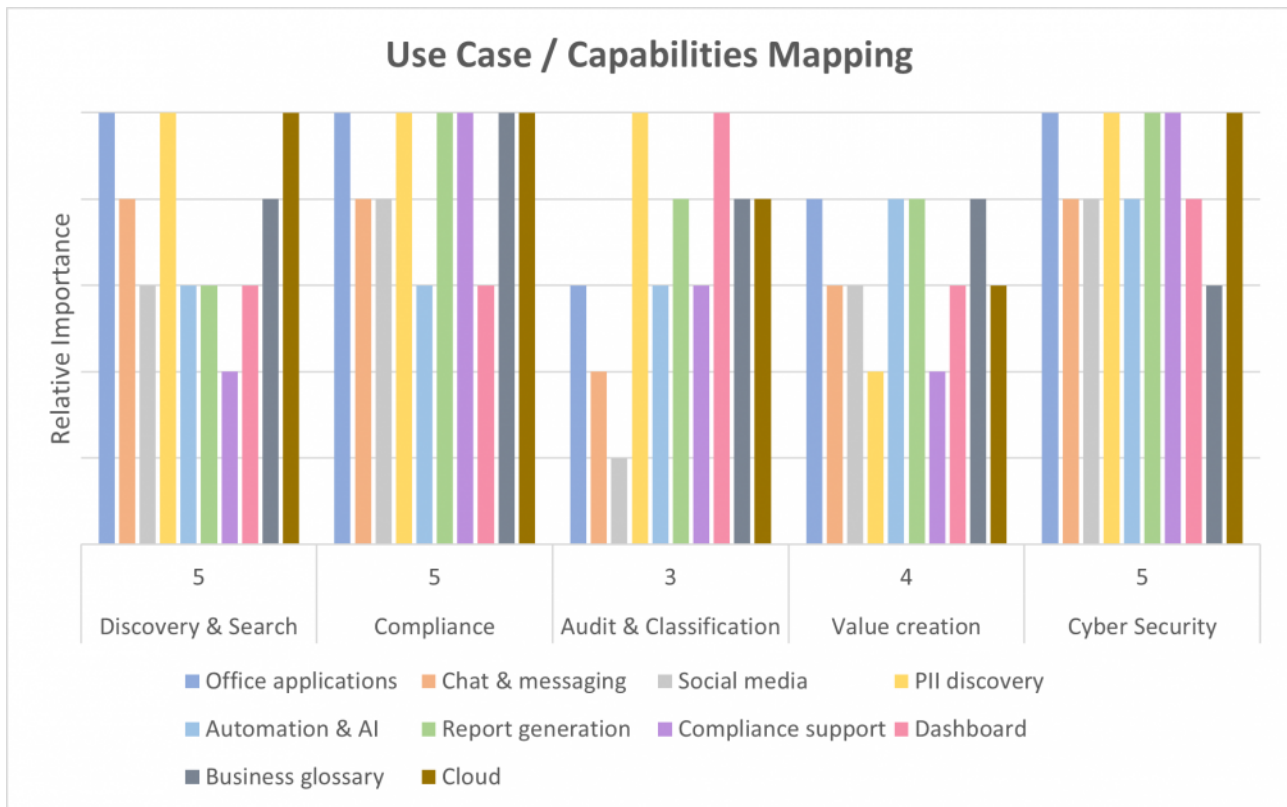


Figure 2: Use cases and capabilities mapping.

### 3.2.1 Discovery and search

Unstructured data that lies undocumented across an organization represents a security risk and a missed opportunity to create value from that data

Essential capabilities for this are:

- Office applications
- Chat and messaging
- PII discovery
- Business glossary
- Cloud

Recommended capabilities for this are:

- Social media

- Automation and AI
- Report generation

### 3.2.2 Compliance

Data compliance regulations are increasing around the world as legislative bodies respond to public concerns about privacy, and the risk that personal data held by organizations is not properly protected.

Essential capabilities for this are:

- Office applications
- Chat & messaging
- Social media
- PII discovery
- Compliance support
- Report generation
- Business glossary
- Cloud

Recommended Capabilities for this are:

- Automation and AI
- Dashboard

### 3.2.3 Auditing & Classification

Data that has been discovered from unstructured sources must be audited and classified if it is to be protected and add value to the organization - data that is not identified and classified is valueless.

Essential capabilities for this are:

- Auditing & classification
- Report generation
- Dashboard
- Business glossary
- Cloud

Recommended capabilities for this are:

- Office applications
- Automation and AI
- Compliance support

### **3.2.4 Value creation**

Unstructured data is like crude oil; value is only extracted once it is refined. Data Governance platforms assist in creating value from data after discovery, auditing, and classification.

Essential capabilities for this are:

- Office Applications
- Automation and AI
- Report generation
- Dashboard
- Business glossary
- Cloud

Recommended capabilities for this are:



- Social media
- PII discovery

### 3.2.5 Cyber security

Data that is not governed remains at constant risk of being lost or stolen, which is a big problem if it contains information that is confidential, such as PII or critical to the security of the organization.

Essential capabilities for this are:

- Office applications
- PII discovery
- Report generation
- Compliance support
- Cloud

Recommended capabilities for this are:

- Chat & messaging
- Social media
- Automation and AI
- Dashboard

## 4 Ratings at a Glance

This chapter provides a comparative overview of the participating vendors for five categories: security, deployment, interoperability, usability, and market standing. It also highlights the outstanding performers in each of the nine capabilities that were assessed.

### 4.1 General Product Ratings

Based on our evaluation, a comparative overview of the ratings of the general standing of all the products covered in this document is shown in table 2.

Product	Security	Interoperability	Usability	Deployment	Market Standing
1touch.io Inventa	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
BigID Data Intelligence Platform	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Concentric Semantic Intelligence	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Egnyte Platform	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Lepide Data Security Platform	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Micro Focus File Governance Suite	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Netwrix Data Security Platform	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
SAP Information Steward	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Stealthbits StealthAUDIT	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Varonis Data Security Platform	<div></div>	<div></div>	<div></div>	<div></div>	<div></div>
Legend	<div></div> critical	<div></div> weak	<div></div> neutral	<div></div> positive	<div></div> strong positive

## 4.2 Noteworthy Vendors for Specific Capabilities

Some vendors are better positioned to meet narrow use cases, while others have stronger offerings across the range of this market segment. We have identified a few vendors that are notable for their strengths for specific capabilities. A vendor has been selected as outstanding based on information collected during our neutral research and rating process.

### 4.2.1 Outstanding in AI Capability: 1touch.io

Many companies boast of using AI capability to boost the efficacy of their platforms, but not all execute well on that promise. Using AI to assist in the management of data would seem an obvious step, and 1TouchIO have done a good job of harnessing AI to drive data classification. Currently the platform's lead in AI does not yet impact on other areas of Data Governance, such as access management and value creation, but we expect the AI capability to further capability options soon.



Figure 3: Outstanding in AI Capability: 1touch.io

### 4.2.2 Outstanding in Innovation: BigID

Data Governance is assuming new importance in modern organizations thanks to data overload caused by

digital transformation. Therefore, it needs more than legacy applications or manual data governance processes to keep on track. In short, Data Governance needs to innovate. By being only five years old, BigID has had the opportunity to start with a clean slate. This has resulted in a cloud friendly, AI powered platform that is particularly strong on discovering sensitive data of all types from across the enterprise.



Figure 4: Outstanding in Innovation: BigID

#### 4.2.3 Outstanding in Compliance Support: SAP

Organizations that run SAP tend to be big, sprawling and data intensive. SAP's Data Governance tools, which include Data Mapping and Protection by BigID are comprehensive enough to meet the data compliance needs of such organizations. Compliance managers will find a lot to like here - if they work in an SAP environment.



Figure 5: Outstanding in Compliance Support: SAP

#### 4.2.4 Outstanding in Dashboard support: Varonis

Like trends in other areas of governance, identity and access management, ease of use and UX are assuming new importance. Reliance on admins is giving way to empowering regular employees to undertake certain administrative tasks. A dashboard interface is central to this and in this regard, Varonis has taken the lead with an interface that has much in common with consumer-focused applications



Figure 6: Outstanding in Dashboard support: Varonis

#### 4.2.5 Outstanding in Report Generation: Micro Focus

While discovering and classifying data are vital functions of Data Governance, larger organizations will also expect detailed reports that Data Privacy and Compliance officers can use in their own audits and assessments. Micro Focus has one of the strongest propositions in the market for allowing organizations to generate fully detailed reports.



Figure 7: Outstanding in Report Generation: Micro Focus



## 5 Product/Service Details

In the following section, each participating vendor is profiled with particular attention paid to the functionality of its product. Several important capabilities for providing Data Governance have been selected and rated, displayed as a spider chart. For this Market Compass, we look at the following 10 areas:

- **Social media**  
Considers how well the platform is able to scan social media applications for sensitive data and policy violations.
- **Office applications**  
Considers how well the platform integrates with popular office applications and suites such as O365.
- **Chat and messaging**  
Considers how well the platform can interrogate chat and messaging applications for sensitive data and policy violations.
- **PII discovery**  
Considers how well the platform can discover and classify PII across applications, servers, and data centres.
- **Automation, Machine Learning/AI tools**  
Considers how well the platform has used AI and Machine Learning tools, especially in the process of discovery and analysis of data.
- **Report generation**  
Considers how well the platform can produce in-depth governance reports that professionals can use for decision-making.
- **Compliance support**  
Considers how well the platform supports and flags potential violations with contemporary compliance regulations.
- **Dashboard support**  
Considers how well the platform deploys dashboards to support usage and deployment of Data Governance functions.
- **Business glossary**  
Considers how well the platform integrates with and assist in the compilation of a business glossary.
- **Cloud integration**  
Considers how well the platform integrates with cloud-based data and cloud applications for complete governance.

These spider graphs provide comparative information by showing the areas where the products are stronger or weaker. Some products may have gaps in some areas, while being strong in others. These might be a good fit if only the specific features are required. Other services deliver strong capabilities across all areas, thus being a better fit for strategic choice of product.

## 5.1 1touch.io

Country: United States/Israel

HQ: New York

Type: Private

Founded as recently as 2017, 1touch.io takes a full-blooded AI approach to Data Governance. The US-Israeli company sells Inventa as a solution to discover and track sensitive data across all IT stacks within the organization.

The AI engine within Inventa is said to constantly monitor data movements and update the inventory of data as it is used. Risk scoring is achieved through integrations with third party platforms. . The platform can be run fully in the cloud but is often deployed in a hybrid architecture with components on-prem and in the cloud.

To discover data across the enterprise, Inventa uses a well presented and easy to use Wizard tool, Supervised AI. This in effect is a training tool for the neural network powering the platform. An advantage of this approach is that takes a huge amount of work away from human users - as long as you can trust the Wizard to correctly identify data found on-premises, cloud and hybrid cloud stacks. The SupervisedAI tool allows the Wizard to be adjusted to specific business needs, however. In demo this worked, but real use case should be tested before purchase. The engine and ease of use is impressive, however, as is the clean interface and presentation of data.

Once the model is trained, it continually scans the environment and updates when a new data source or sensitive information is identified. The engine can relearn data positions in relation to new compliance laws such as CCPA etc. accommodate those changes.

Overall, this is a powerful data discovery and risk management tool that makes good use of the potential of neural networks. Its ease of use and Wizard based operation will appeal to organizations looking for a tool that does not need fully trained Data Governance professionals to interrogate it.

That said, it is not yet a full enterprise level Data Governance solution on its own; it lacks connectors and integrations with other related applications - but as a tool for improving data understanding across the organization it is worth considering. One to watch in this market.

Security	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Market Standing	● ● ● ○ ○

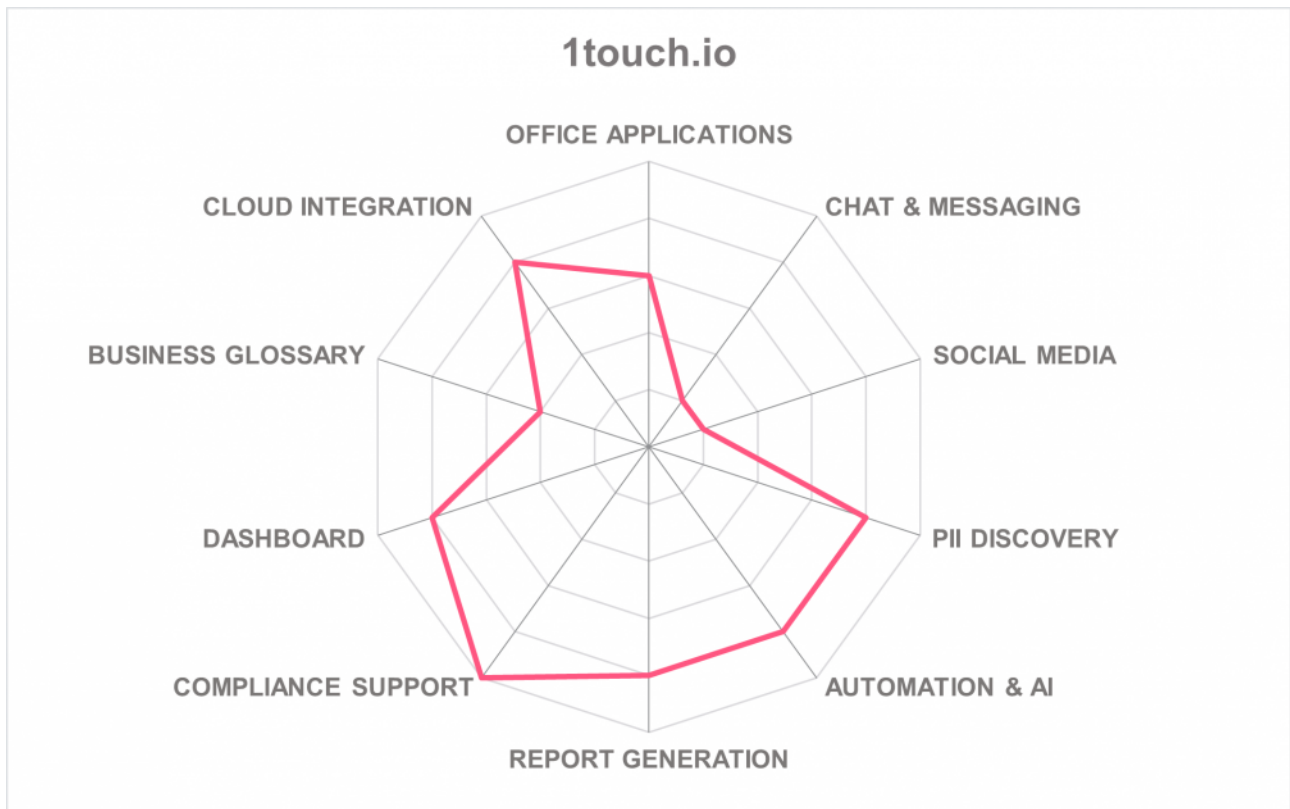
**1touch.io**  
Discover. Map. Comply.

## Strengths

- Puts AI tools to good use once the platform is trained to the needs of the organization.
- Can relearn data positions to compliance rules as they are updated, or new ones appear.
- Continuously updated risk score for data.
- SaaS model will appeal to SMB and smaller enterprises.
- Wizard tool is eye catching feature and takes much of the work out of data discovery and classification.
- Ease of use and interface are impressive.

## Challenges

- A full SaaS version may appeal to cloud native organizations.
- Some customers may prefer more granular control to data classifications than the Wizard tool provides.
- Cannot be viewed as a fully featured Data Governance solution as it lacks connectors and integrations.



## 5.2 BigID

Country: US

HQ: New York

Type: Private

BigID's Data Intelligence Platform can discover and classify data files in Office365, SharePoint, Azure, Box, AWS S3, Adobe PDF, Google Apps, Zip files as well as image and OCR files. It can also support Structured Databases - making it a versatile package. The platform consists of a data discovery foundation to find, inventory, and classify data of all types by sensitivity, regulation, and more - with an app framework and apps to act on that data for privacy, security, and governance: including apps for data remediation, access intelligence, data retention, and more.

Of interest is the more specialist support of messaging tools such as Outlook, Gmail, Slack and Teams - important in modern digital organizations. Its support for cloud applications is also good with Salesforce, Workday, ServiceNow and Box among the primary platforms supported. To round out its compatibility it boasts a rich collection of Apps and APIs to take action and build further integrations.

BigID's Data Discovery Foundation is, as its name suggests primarily a data discovery tool. It uses a clean looking, web-based interface that gives a single pane of glass view of data across the organization. Within the dashboard PII, PI, and sensitive data - along with other ungoverned data -can be highlighted to reduce risk of exposure and compliance failure. BigID also uses a graphical approach to map data relationships and other data correlations. This could be clearer in its presentation however.

Further, data can be classified after discovery and the platform is assisted by AI and Natural Language Processing (NLP) - classification is based on correlations, enrichment, and proximity. Data can be useful classified under the following buckets: person & identity, sensitive data, regulation, document type and policy and security attributes. This last is quite unique and useful to security by discovering security attributes such as tokens, passwords, unencrypted and encrypted private keys and other credentials. Cluster analysis finds duplicate and redundant data across the IT infrastructure.

To ease the classification process, BigID offers hundreds of classifiers out of the box including data types to specific data privacy and protection regulations, while new ones can be added by admins as they progress in line with business policies. For unstructured data specifically, BigID has multiple ML-based scanning approaches to reduce the time it takes to discover and identify data in unstructured.

Security  
Interoperability  
Usability  
Deployment  
Market Standing



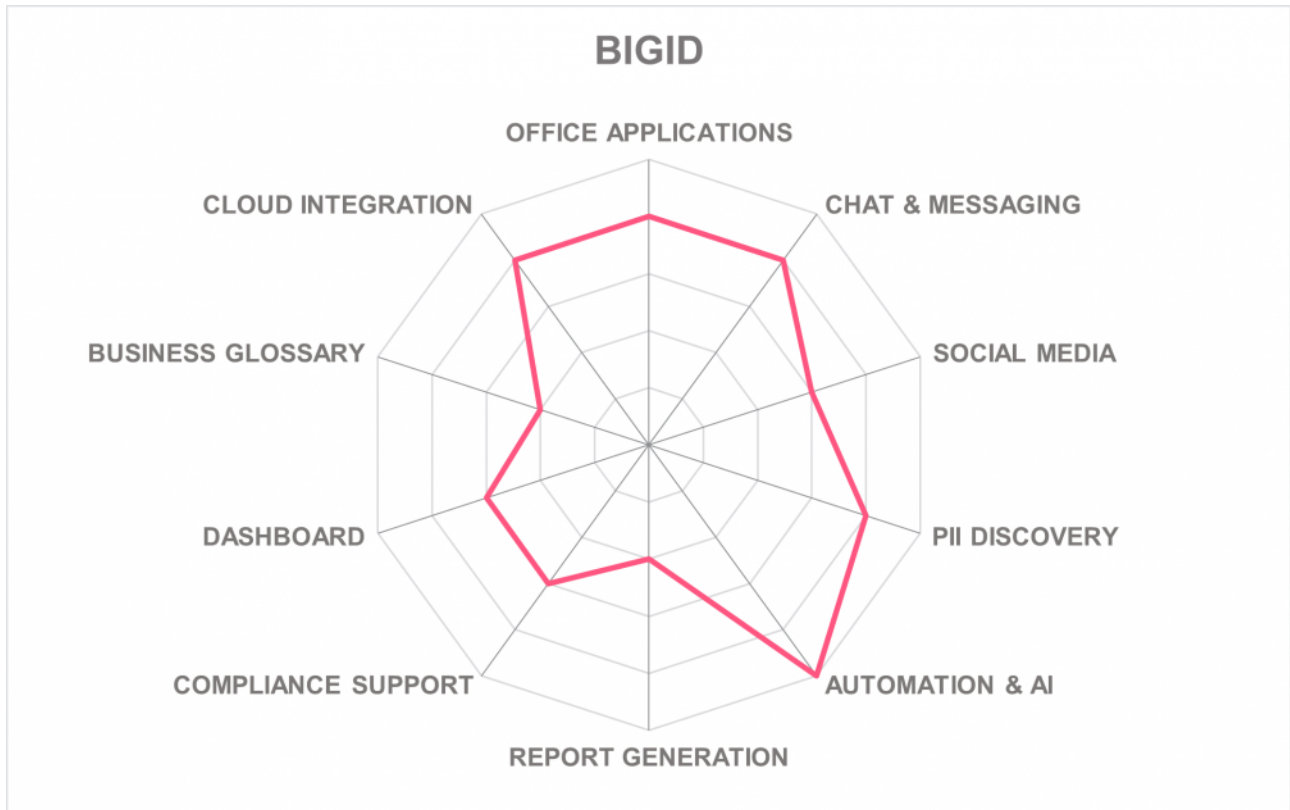
**BigID**

## Strengths

- Huge range of integration available which is further boosted by API connectivity
- Automation tools above average with NLP boosting data discovery and correlation
- Strong security tools that can discover hidden passwords and tokens significantly assist with compliance too
- Hundreds of classifiers available out of the box.
- Automatic discovery of PII data also assists with compliance
- Works well with O365 and other office applications

## Challenges

- UX and parts of the dashboard lags the sophistication found elsewhere
- Would benefit from more business focused analytics
- Would benefit from more comprehensive report generation





## 5.3 Concentric

Country: US

HQ: San Jose, California

Type: Private

This is a young company with some innovative approaches to Data Governance based around AI and deep learning. Believing that data oversharing is a prime reason for Data Governance failures, the company has focused on this to assert Zero Trust for data that might be shared outside of the organization, or beyond policy rules. The tool can automatically remediate permissions and sharing issues on its own or leverage other security solutions through APIs to make essential changes.

The Semantic Intelligence platform uses an AI-based technique called Risk Distance analysis to discover at-risk files by comparing each file to its peers. The technique finds documents that have been shared outside the company, shared with email accounts, are missing file information, have inappropriate access permissions, or are stored in incorrect locations. The tool then allows common action to be taken. Analysis is based on file meaning (as derived by the AI system) rather than file location or keyword count. The product also includes deep learning tool MIND which runs as a service, ensuring that the latest AI models, including models developed by other customers, are always available. It will search data held on premises, within cloud applications, cloud storage and structured data repositories. Sharing can be searched down to link sharing, sharing with internal and third parties and sharing with personal email addresses.

Central to Concentric Semantic Intelligence is its Natural Language Processing (NLP) which is claimed to be able to define the meaning of the same word used in different contexts, which is beyond most keyword-based searches. A demo proved that this could work in a controlled environment but much longer experience would be needed to judge the full efficacy of NLP, and whether it achieves better governance of data.

The platform integrates with third party platforms including DLP, CASB and Microsoft Information Protection (MIP). There is a risk dashboard which in line with modern practice makes the platform pleasingly easy to navigate.

There are some ambitious technology claims for this product but its success depends much on proper integration with existing governance policies and tagging frameworks, it cannot perform magic on its own. It does have some innovative features that potential buyers may find attractive such as the above mentioned RiskDistance tool, auto search of unstructured data for Data Subject Access Requests and Document Business Criticality assessment - all three hugely valuable to the governance of any modern organization.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ○

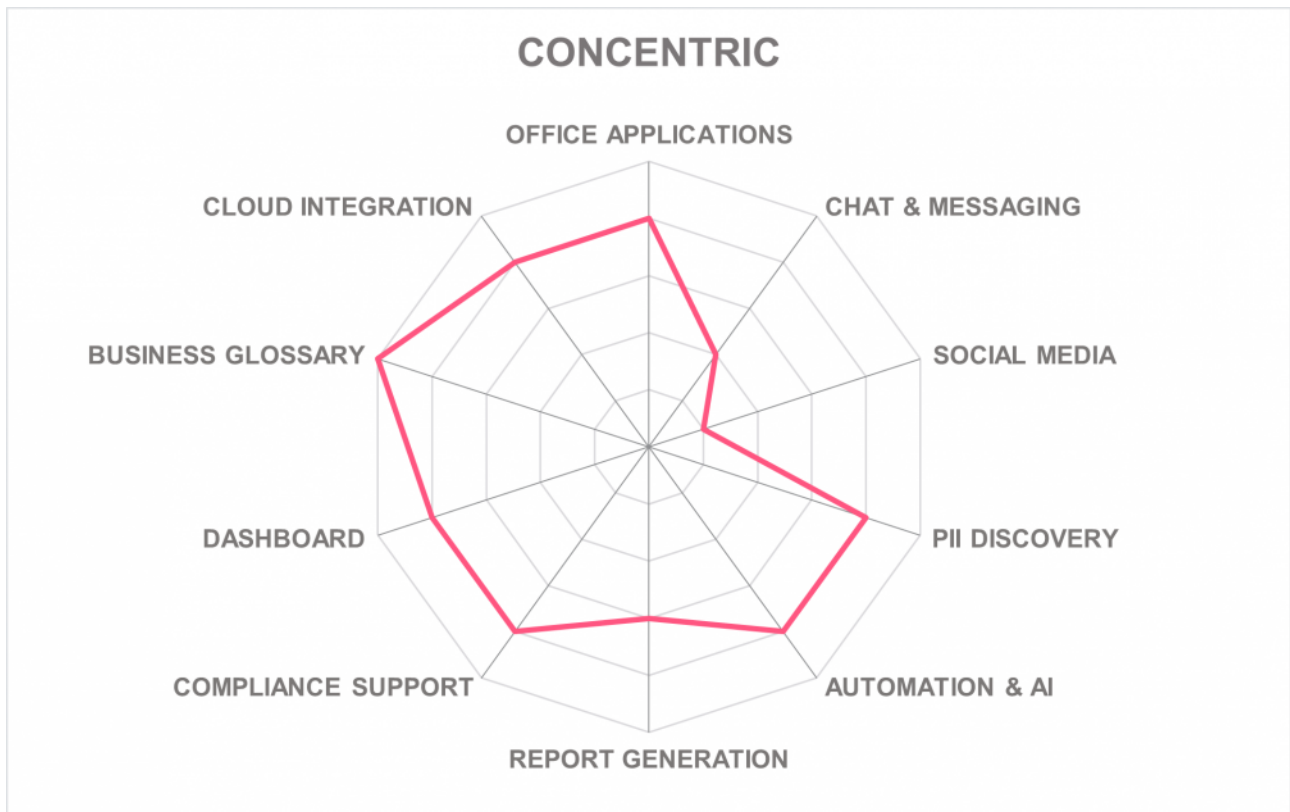


## Strengths

- SaaS approach delivers always on updates and scanning
- No need for APIs or agents to install applications
- Risk scoring of files and data is well presented
- Zero Trust approach is a positive way to reduce data risk from poor governance of access permissions
- AI engine can take a granular view of data across IT stacks
- Includes integration with DLP and CASB platforms boosting its cybersecurity credentials

## Challenges

- NLP capability needs to be tested in real world environment, preferably in a trial run for customer
- Lacks the integration support of some its rivals
- We hope to see support for data contained in Social and Chat/Messaging tools in the future



## 5.4 Egnyte

Country: US  
HQ: Mountain View  
Type: Private

Egnyte presents a data access platform that also encompasses several compliance and Data Governance applications. The platform itself is designed for remote access to files from web, desktop, tablets and mobile apps and from cloud services such as Slack, Salesforce, Gmail and Teams, and across multiple clouds and geographies.

Then platform is particularly focused on Data Governance across the Microsoft stable of Windows FileServer, OneDrive, Teams and SharePoint - cloud tools that can become overshared and unwieldy very quickly. Folders can be permissioned to individuals, which is designed to remove the need of file sharing or granting permissions to groups, IP addresses or network locations. This makes sense for compliance purposes and to track anomalous behaviour immediately at the level of an individual, rather than searching through groups or multiple users of network addresses.

A unique feature of Egnyte is its own SOC2 certified cloud repository, that provides access to the latest version of any file but for the end users it is accessed through the Teams or SharePoint interface - but the data is fully classified and protected by the platform behind the scenes.

Egnyte uses a combination of machine learning and AI to makes sense of unstructured data and its usage by all those connected to an organization (which can be third party individuals also). It classifies unstructured data across all repositories and looks for compliance sensitive data such as credit card numbers, PII and health related data. The platform has several OOB configuration options that allow admins to select areas of operation and map the relevant compliance regulations that apply.

Data is then classified according to those rules. Data can also be organized and ranked according to internal policies and privilege based on keywords, metadata, file types etc. A neat tool is the more than 30 out of the box patterns deigned to classify data against new and emerging data privacy regulations - a drop down menu performs a scan against these new rules.

API support extends support beyond the 150 third party apps already built in. Beyond classification Egnyte offers a good level of tools, to decide where data can and cannot reside. It can also permission and alert sharing of data.

Egnyte provides can customize alerts based on recipient, issue type, sensitive content type, and level of severity. All this achieved through an easy-to-use browser-based interface the platforms uses. The platform supports MFA, full AD integration, encryption if required and secure storage in SOC2 certified data centres.

Auditing includes key actions taken in the system, like logins, allowing or disallowing sensitive content in specific locations, moving, or deleting files, viewing sensitive content and identifying and removing old and unused data before it can be compromised.

Security	● ● ● ● ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Market Standing	● ● ● ○ ○

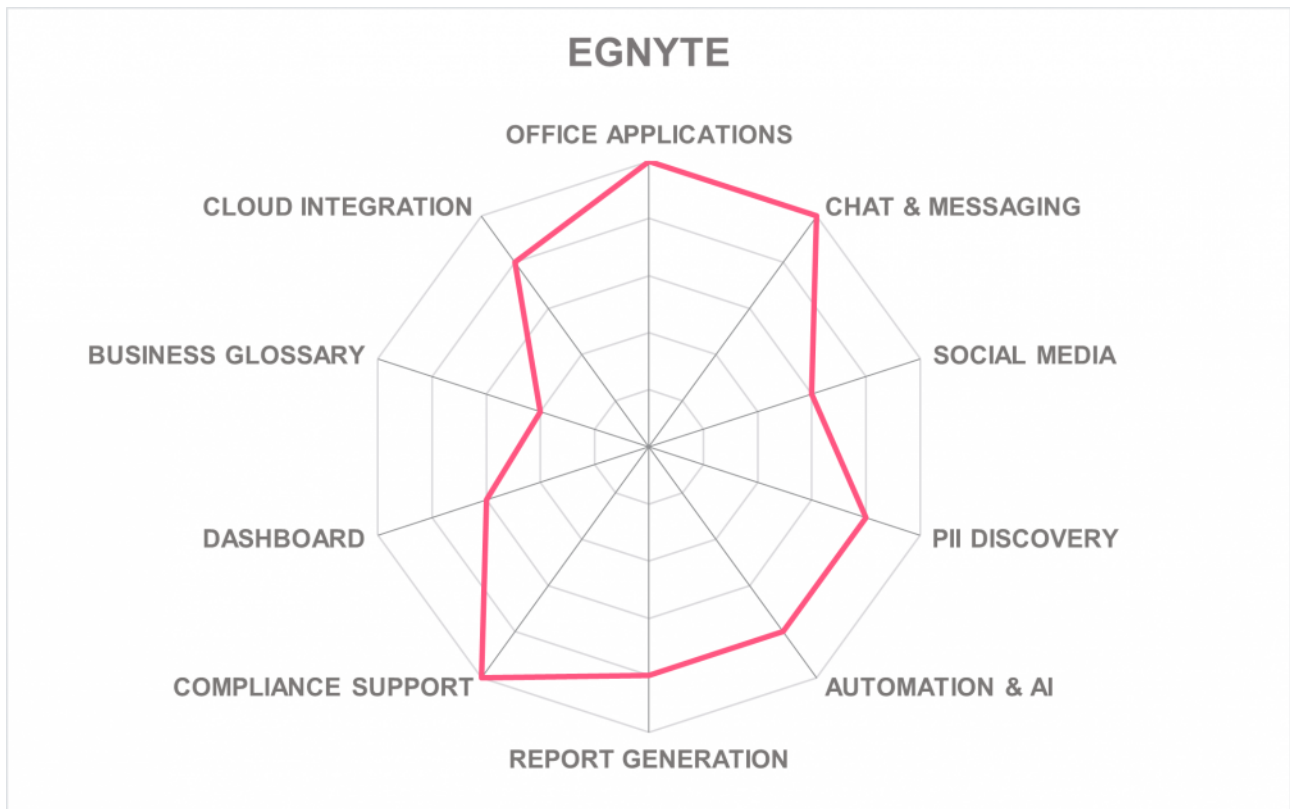


## Strengths

- Strong support for popular office cloud services such as Slack, Salesforce and Google Mail
- Well suited to Office 365 applications and reduces oversharing of files and data in Microsoft applications
- SOC2 certified cloud repository reduces file duplicates
- Machine-learning based threat and anomaly detection
- Out of the box data classifications for primary compliance regulations

## Challenges

- Would benefit from more capabilities to define and add value to data on top of security and compliance features.
- Full Data Governance tools and security tools only available as part of most expensive enterprise options, separate availability may assist smaller businesses.
- Rivals offer similar Data Governance features to wider customer base
- No business library capability to assist in classification



## 5.5 Lepide

Country: US  
HQ: Austin, Texas  
Type: Private

Founded in 2015, Lepide has around 1400 customers and offers its Data Security Platform to the market. The platform covers governance of unstructured data with four modules: Lepide Identity discovers and identifies sensitive data, Lepide Trust identifies which entities have accessed data and tracks permissions, Lepide Insight audits systems and IT stacks for data and Lepide Detect alerts admins to anomalous user behaviour. Lepide bases much of its capabilities and logic on measuring the value of data as well as monitoring access.

This approach works in terms of making it easy to see who has accessed data, which like others in this group, allows oversight of privileged users activity - although cannot be considered a substitute for a dedicated PAM platform. Lepide is easy to use. It consists of a single dashboard that provides an overview of all main module as well as a live feed of data changes, a compatible mobile app can send live reports to smart devices.

Lepide Data Security Platform on premises support includes AD, Windows File Server, NetApp, SharePoint and Exchange and in the cloud for Office 365, Azure AD, Teams, Amazon S3 and G-Suite, Dropbox for Business and others. A feature of note is Active Directory Cleanup, which runs in the background to scan for inactive and obsolete AD accounts and enables admins to reset passwords or delete altogether. An important security and compliance function which would save much effort for organizations of all sizes.

Lepide automatically scans and classifies data in accordance with regulations that impact on PII, PHI, PCI, IP and others. Admins can reverse user permissions and receive alerts to unusual data requests or changes made to data. Reports can be generated directly from the platform to provide an oversight of the data posture of the organization, and example is to instantly highlight all open shares at any given time.

Lepide offers a single platform for the mid-market (2,500 to 10,000 users) that would enrich an existing PAM and security portfolio. It does not possess the richest data classification or access management platform and for now most customers use the platform for on-premises data, although enhanced cloud capabilities are promised in the product pipeline.

Security	●	●	●	●	●
Interoperability	●	●	●	●	○
Usability	●	●	●	○	○
Deployment	●	●	●	○	○
Market Standing	●	●	●	○	○



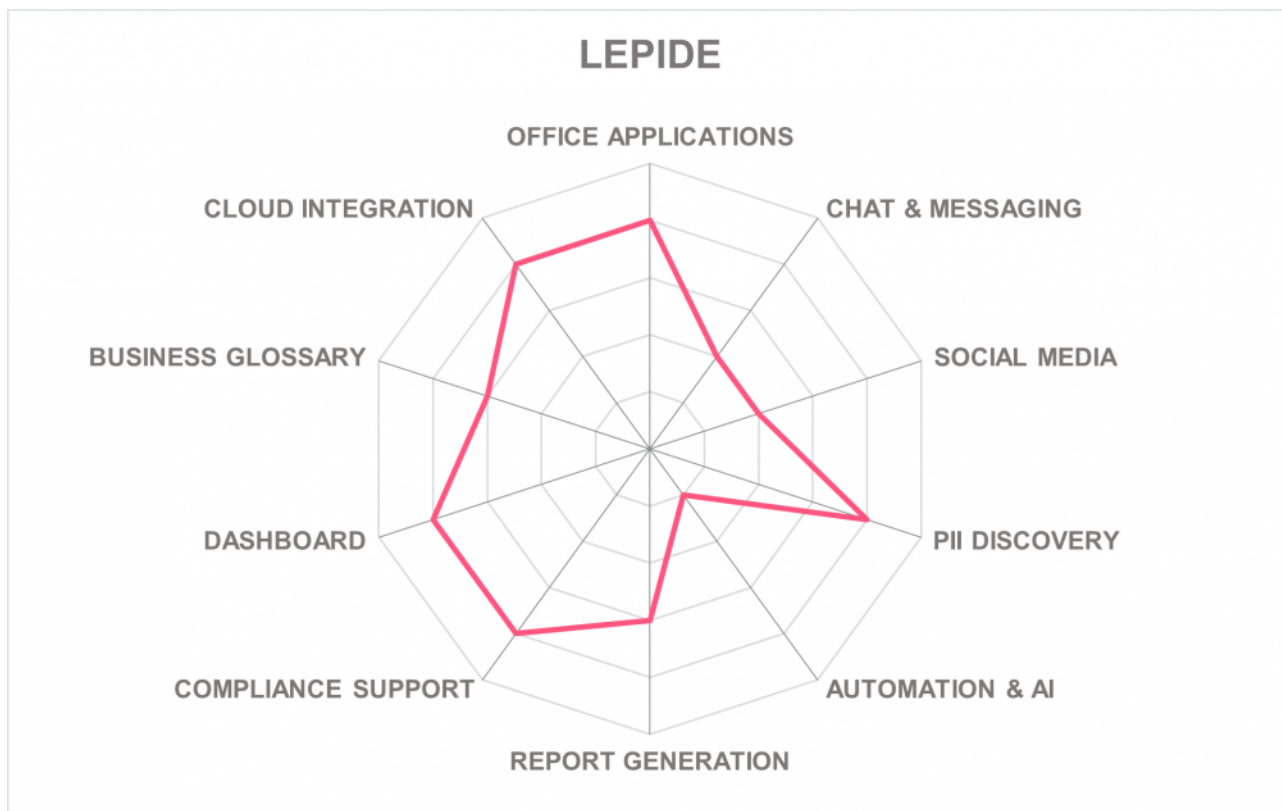
## Strengths

- Well featured platform that focuses strongly on access and identity for smaller businesses.
- Active Directory CleanUp feature automatically deletes obsolete AD accounts
- Automatic scanning of data for exposure to compliance regulations such as GDPR etc.
- Basic PAM tools add an extra dimension to the package

## Challenges

- Badly needs promised improved cloud compatibility to compete in this market
- Data classification tools need improvement to complete the picture
- Needs more to attract large enterprise customers in this space.





## 5.6 Micro Focus

Country: UK  
HQ: Newbury, UK  
Type: Public

Micro Focus is a software company noted for its wide range of identity management, governance, and data products. So wide in fact that it is hard to find the right solution from a catalogue of over 300 products, swollen by a string of acquisitions. For Data Governance it offers File Governance Suite which comprises several tools to help organise unstructured data and access.

This consists of two major components: File Reporter and File Dynamics. Both are aimed at Microsoft 365 applications and networks - cloud, and on-premises. File Reporter is a scanning tool that integrates with Active Directory and Azure Directory to determine access permissions. A web dashboard tool is used to highlight Windows Share access, direct and inherited permissions through a single path and a list of a user's or group's access permissions.

It can also highlight which NTFS permissions have changed between two points in time. Scans also include information on the file types users are storing, who can access sensitive files, if users have duplicated the files, where duplicate files reside, when users created the files, modified the files.

Built-in to the tool are the means to highlight PII, personal folders and to measure unstructured data against compliance regulations. From all this, reports can be generated to classify, data at risk and access rights allowing action to be taken by admins and Data Privacy professionals. Reports are templated or can be custom made using graphical analytics.

While File Reporter provides a breakdown of file usage in the organization, File Dynamics provides a way of doing something about it and organizing access. It automates tasks such as provisioning user and collaborative storage, setting rights, setting quota limits, migrating storage, redistributing storage, archiving storage, and cleaning up storage. Policies can be stabilised to provide role-based access to files.

Security of data is enhanced through back up of data in case of ransomware attack, and automatic notification of changers to data-to-data owners. Data can also be automatically relocated in response to changes in Active Directory of policy changes. Take together as a suite these products form a robust way to organize unstructured data from an identity point of view.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ●

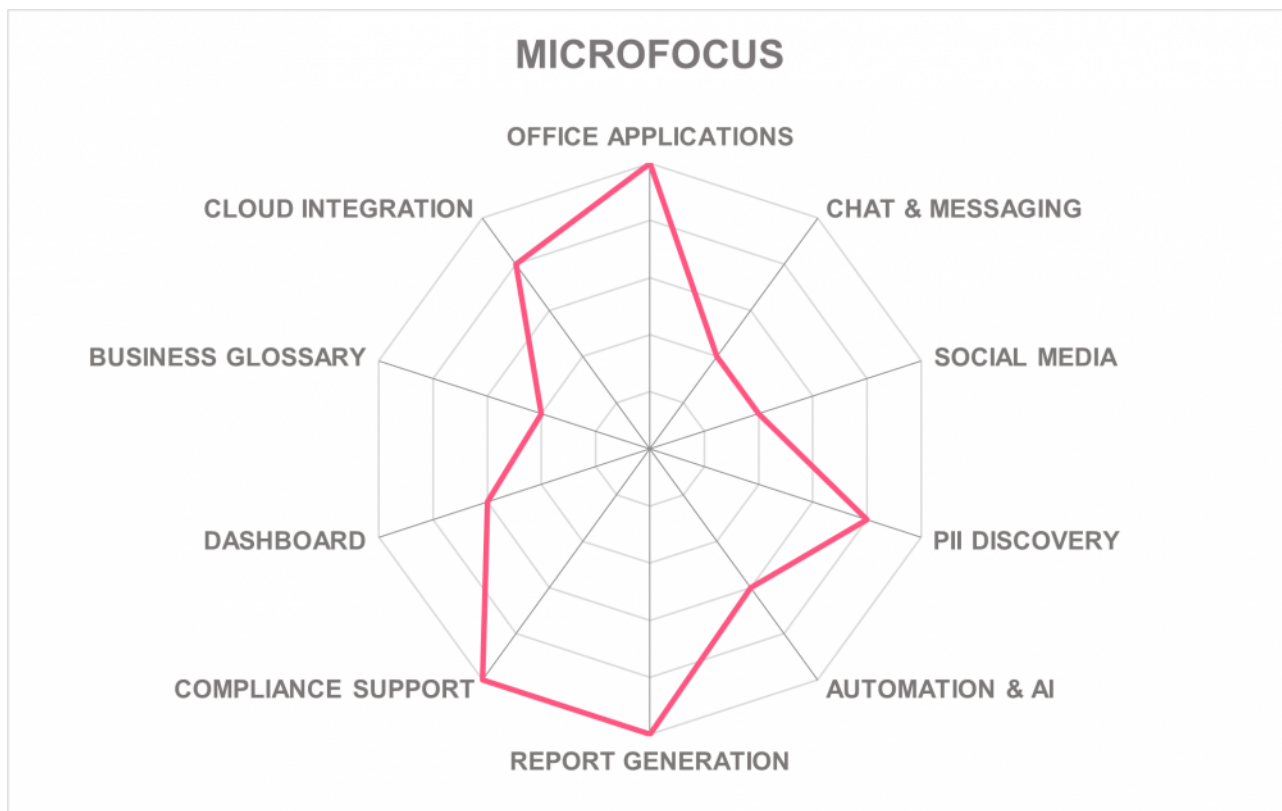


## Strengths

- Builds on Micro Focus strengths in identity management and maps well to Data Governance
- Well suited to Office365, Active Directory and Microsoft architectures
- Comprehensive reporting capability including reports templates out of the box
- Delivers a very granular level of information on file usage by individual users
- Useful to break down usage of files and to assists in Data Lifecycle Management
- Security of data managed well by parts of the platform

## Challenges

- Micro Focus website is almost impossible to navigate to find a specific solution, information duplication and overlap
- Not much in the way of creating extra value from data within the platform
- Less "business" focused than other platforms, does not support a business glossary for example
- Lacks specific social media and messaging discovery



## 5.7 Netwrix

Country: US  
HQ: Irvine, CA  
Type: Private

The Netwrix platform comprises several modules for data classification, security and auditing across both unstructured and structured data silos, online and on premises.. Like others, it has an easy-to-use dashboard in which admins can add their own taxonomies such as GDPR and other metadata and boasts strong search and discovery tools. Central to its security and classification functions is the management of Data Access Requests (DAR)

Central to the platform is the Risk Assessment Overview that assigns numeric value and risk level scores to users and computers as well as an overview of data which highlights number of shared folders or file names that contain sensitive data. In addition, there is a more granular count of sensitive files by source, for example in LOBs such as Finance or HR.

These can also be pivoted against compliance regulations that may be impacted such as GDPR, HIPAA or PCI-DSS for example. Admins or Risk Managers can further investigate those file or folders that may be overexposed again checked against the compliance regulations that may be breached. Altogether, a decent amount of Data Governance can be managed in a short time in a crowd-pleasing interface.

The same can be said of the tools to assess permissions and to control access to data on a least privilege basis across directory groups and users. SharePoint is increasingly used in organizations and has added to some complications for Data Governance; wisely Netwrix has added separate control for data and files in SharePoint Server, SharePoint Online, and Microsoft Teams. Support for all of these platforms is included in the same application license, so customers in hybrid environment or in process of migration to the cloud have full flexibility. The Data Remediation Workflow wizard can update access permissions.

Finally, there is support for detect privilege escalation attempts, which alerts to users and file/folder granularity making it simple for admins to stop access. The functionality extends to the cloud in addition. Such activity can also be recorded by video to identify how users gain access.

It supports PDF, TXT and Office documents. It integrates with encryption software Secure Circle and standard APIs. Netwrix auditor reports on who is looking at documents and an intelligence report can investigate incidents and instigate actions. Other features include Raise Tickets through ServiceNow and a Risk Assessment report based on permissions.

Easy to deploy and use, build in policies and rules. Reporting is very deep and easy to understand and customize. The reports are clean and eye catching which means they may be used for business value. In addition, the ability to record desktop sessions when needed can prove useful in disciplinary cases, and the User Behavioural Analytics can identify rogue behaviour before it gets out of hand. AD auditing and real time alerting are the icing on the cake.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ●

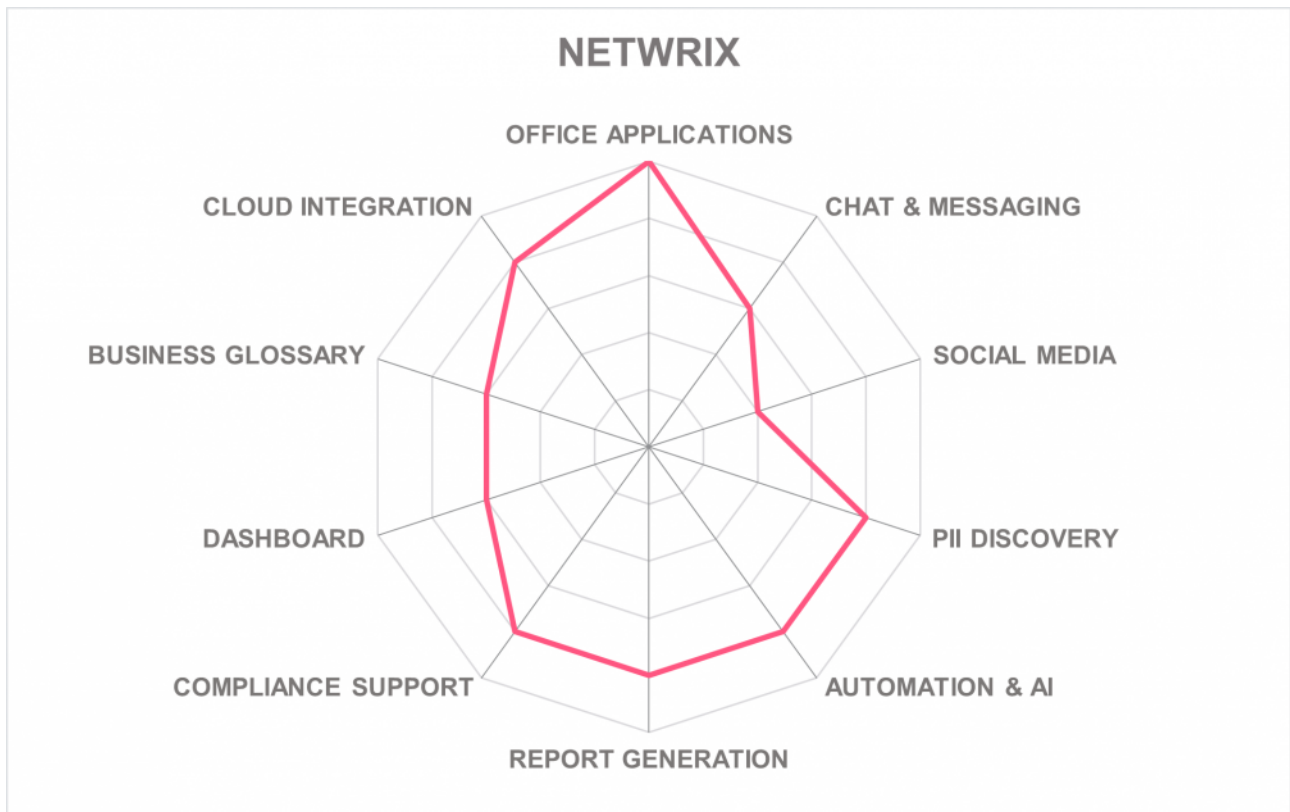


## Strengths

- Simple interface is one of the best, making it quick and easy to see risk to data and user activity
- Good reporting and policy integration tools and strong integration with business apps such as ServiceNow and SharePoint
- Good linkage of risks to file structures and users by LOB
- Data Access Governance focus would complement other security and larger Data Governance platforms

## Challenges

- Focus on data access governance means that it misses out on better classification and value creation tools
- Netwrix Data Classification supports taxonomy integration but we would like to see richer business glossary integration
- Merger with Stealthbits may cause some product and integration teething troubles



## 5.8 SAP

Country: Germany  
HQ: Walldorf, Baden-Württemberg  
Type: Public

SAP's Data Governance platform is a mixture of its own technologies and third party integrations for data mapping, protection, and governance. SAP Information Steward covers a broad scope of the end-to-end data governance process - from data understanding, analysis to improvement and monitoring. It has a broad range of integrated and interconnected capabilities, including metadata management (with metadata cataloging, impact analysis and data lineage), information policy management, a business glossary, data profiling, data validation and quality rules, cleansing rules, match (group) review, data quality scorecards, business value analysis and email notifications when quality falls below acceptable thresholds.

Integration with SAP Data Services allows organizations to share cleansing, validation and quality rules they have built using SAP Information Steward and put them into action to be used to process existing and new data sources on a larger scale.

Users can also review the results of the SAP Data Services matching and de-duplication process within SAP Information Steward's match review, in an easy-to-understand UI. Integration with SAP Master Data Governance allows for access to SAP Information Steward's rules and scorecards. The integration with SAP PowerDesigner allows terms to be shared with SAP Information Steward. And finally, SAP Information Steward can share approved data quality rules and business glossary terms with the integration to SAP Data Intelligence Cloud.

Dashboard analytics and depth of granular information are exhaustive and highly impressive although will take some learning for admins and users to discover all the features and to make the best of the tools available. While this is almost a no-brainer for SAP applications, there are also plenty of integrations with third party applications too which extends functionality considerably. Multiple users can access data simultaneously. Overall, this tool is designed to clear not just compliance but to divine, real useful business value from data.

Machine learning can propose new data quality rules based on scans of data usage and dat type being stored by employees. Data can be delivered to specific domains such as specific and defined LOB processes, third party applications on premises as well as cloud applications. The platform also enables mass loading of data for trend reports on request, and requests for data can be drilled right down to single errors. There are two versions of SAP Master Data Governance on SAP S/4 HANA and for SAP ERP.. Overall, a big, serious, and fully featured Data Governance tool clearly aimed at large, complex SAP enterprises.



Security	● ● ● ● ●
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ●

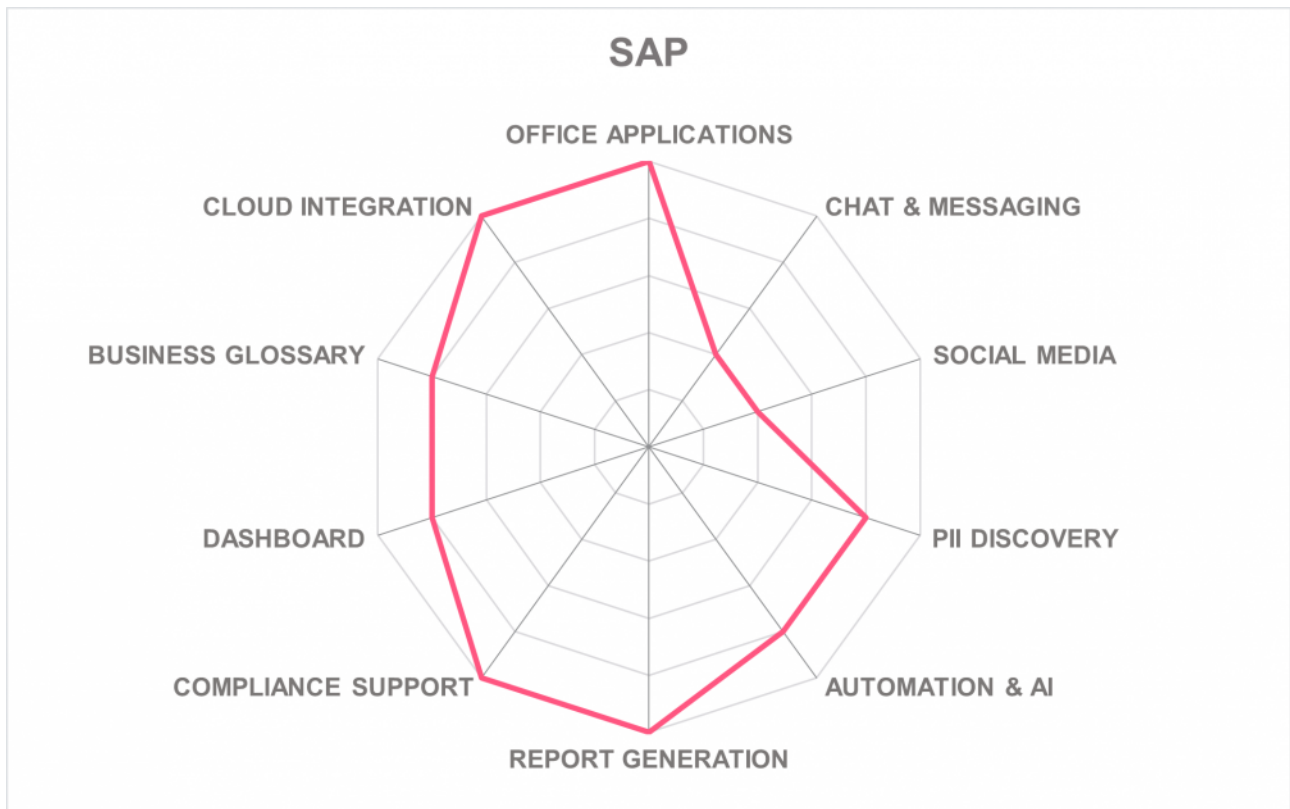


## Strengths

- Strong data intelligence functionality
- Wide range of data connectors out-of-the-box with a connector SDK on their roadmap
- Wide integration with SAP and third-party tools makes this highly configurable and powerful
- Flexible data inventory
- Strong data visualization tools
- Covers a wide range of data compliance use cases
- Ideal for large SAP running enterprises

## Challenges

- Data access policies can be considered somewhat coarse grained
- Blockchains are currently not supported as a data source category
- Not appropriate for small businesses or non-SAP houses



## 5.9 STEALTHbits Technologies

Country: US  
HQ: New Jersey  
Type: Private

Although Stealthbits recently merged with Netwrix, the combined company will continue to offer separate Data Governance solutions to the market for the foreseeable future. Stealthbits' StealthAUDIT is focused on the business benefits of Data Governance and its primary use case is controlling access and usage of data across numerous data points.

StealthAUDIT can discover data across directories, in unstructured and structured receptacles and in the cloud. Unstructured data can be discovered across SharePoint, Office365, Box, AWS, NetApp and others. There is yet no support for social media data buckets.

The platform deploys over 40 built-in data collection modules covering both on-premises and cloud-based data. A well-designed and easy to use Wizard based interface allows admins to find and access the data that need managing. The data reports are equally well presented in the dashboard modules.

Data can be further assessed for Identity, Permissions, Activity and Content and then further controls can be set for real-time alerts, user behaviour analytics, privacy and reporting. Those organizations needing further architecture enhancements will appreciate integrations with Splunk, IBM Security, MS Azure, Saviynt, Micro Focus, Symantec and ServiceNow.

StealthAUDIT Analysis Modules allow correlation of other data sources, report views, historical trending, injection of business rules and logic, notification, and more. Users can also extend analysis with powerful SQL and Power-Shell modules, as well as alternative script inputs and outputs. In addition, the StealthAUDIT Action Modules Framework provides a wide range of remediation and orchestration options.

Stealthbits' Data Privacy Engine can be added to StealthAUDIT as a package to effectively connect identities with the location of PII. This is of benefit to privacy officers wanting to action critical data privacy workflows like Data Subject Access Requests (DSAR).

For structured data, StealthAUDIT supports Microsoft SQL Server, Azure SQL and Oracle. The platform runs on Windows and supports collection of data from Unix and Linux platforms. A tidy and neatly designed package, with clever integrations that covers data access governance well although full enterprise Data Governance is slightly out of reach.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Market Standing	● ● ● ● ○

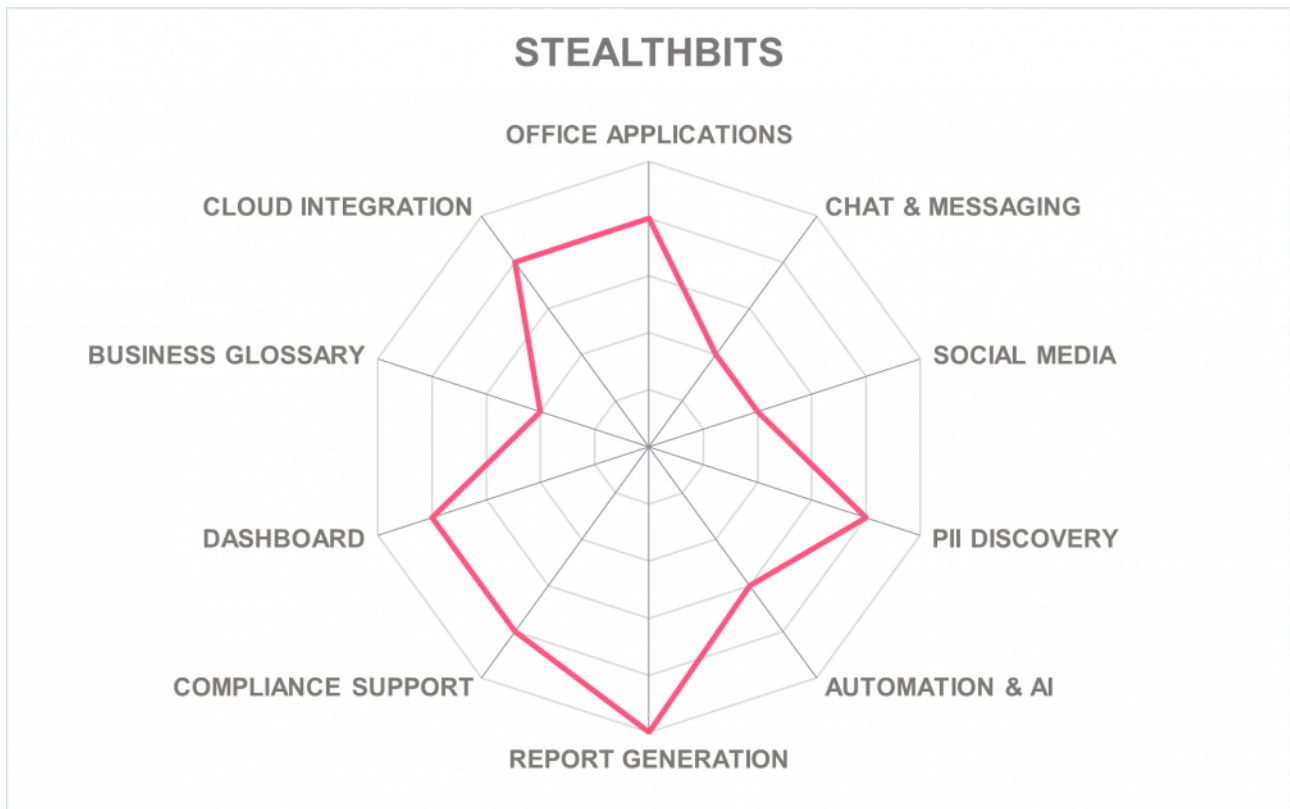


## Strengths

- Integrates well with Stealthbits' PAM, Data Privacy and Threat Detection engines
- Integrations and features make this a security first solution with an emphasis on Access Governance
- Strong analysis modules that can correlate other data sources
- Easy to use wizards and well- designed dashboards make data governance easier to process for LOB managers and non-specialists
- Can also discover data in structured silos with support for major DB platforms

## Challenges

- Acquisition may have impact of product development in the short term
- No input from data from social media data buckets such as Twitter
- Lacks some GRC features but Data Privacy integration addresses some of this



## 5.10 Varonis

Country: US

HQ: New York

Type: Public

Varonis has one of the most complete offerings in Data Governance and continues to build market share in this space at a steady rate. The platform presents a Risk Dashboard which delivers a bird's eye view of Data Governance for an organization. Varonis Data Security Platform is very much geared towards making sense of the unstructured data created by adoption of Microsoft 365, SharePoint, Teams, Exchange and OneDrive.

Varonis Data Security Platform benefits from a single platform and a single code basis and an up-to-date UX in most areas although the deeper lying DatAdvantage interface is less easy on the eye. The power of the search makes up for this, however. Search is by Tags and the DatAdvantage replicates the organizations file and directory structure in its entirety. This delivers granular access to files. The search engine is fine and works by looking for Tags made in document classification; the tags can be created by Varonis natively or created in association with Microsoft Information Protection.

Data Governance is also about managing data access and Varonis does a good job of determining who needs access and who might miss it. In modern organizations, it is easy for too many users to have access to files or directories they do not need. The platform is ably assisted here by the presence of the Varonis DatAlert UBA tool. By auditing access, Varonis Data Platform provides an instant overview of the number of times users accessed files and those they did not, although they had permissions. It is easy then to restrict these, or to reassign folders so that only those that need access are given permission in the future. There is also a small element of PAM built in; Varonis Data Privilege that offers access to files on a JIT basis. All good.

Varonis recently acquired Polytrize which will extend visibility into data held on cloud applications such as Salesforce, Slack, Zoom and Google Drive among others. Overall, this is a powerful tool that hides its power behind an easy to configure and use interface that makes the process of mastering Data Governance and controlling access attainable from one box.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●
Market Standing	● ● ● ● ●

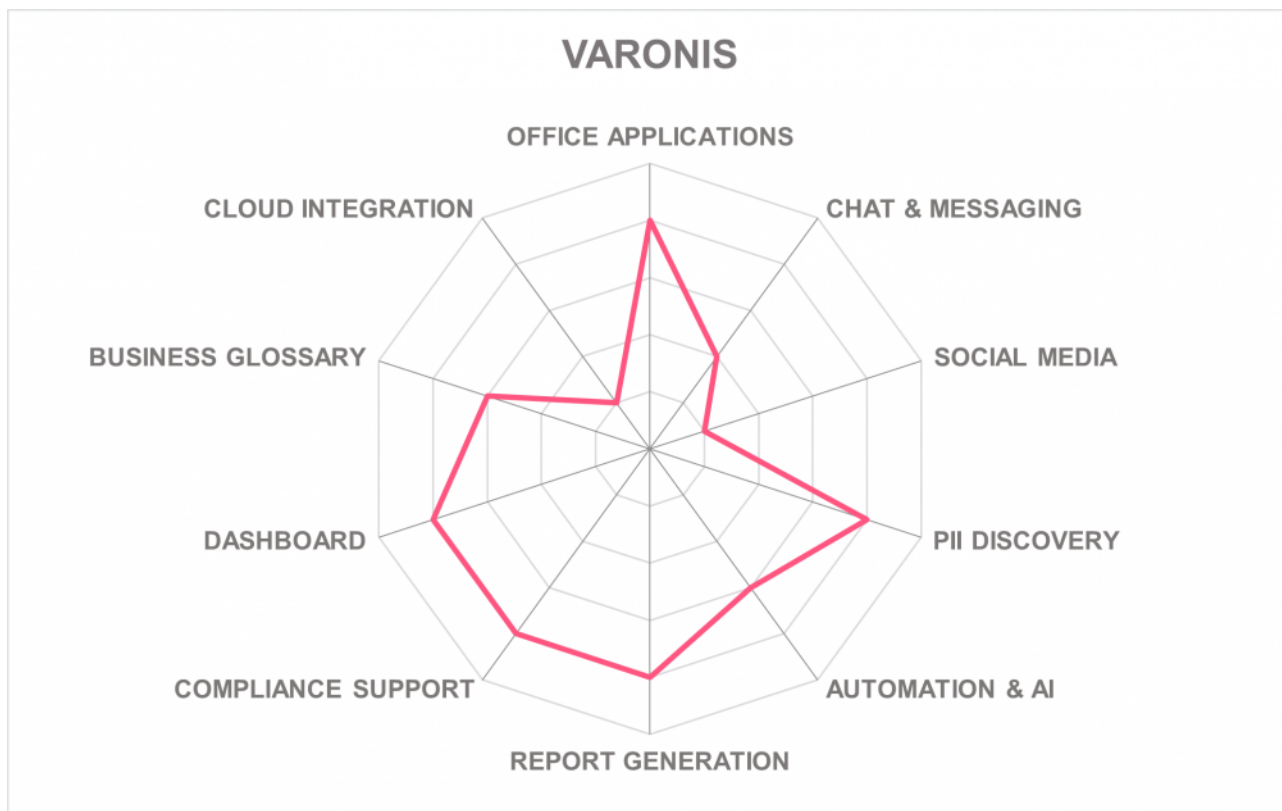


## Strengths

- Excellent dashboard gives overall risk posture for data across the organization
- Highly compatible with O365 and other key Microsoft applications and platforms
- Data access and sharing controls invaluable for controlling data usage in collaboration tools
- Single platform and clear UX ease deployment and learning curve
- Mini-PAM capability offers JIT access to data and files

## Challenges

- Search tool not as intuitive as rest of the platform.
- Firmly focused on the data access governance capabilities, more general Data Governance tools would broaden its appeal
- Will also benefit from cloud services compatibility when it arrives





## 6 Vendors to Watch

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

### 6.1 BlueTab Solutions - Truedat.io

Truedat.io is unusual in that it is an open source based platform marketed by a private company. It offers a basic level of Data Governance but with excellent ease of use and deployment. The software is completely developed by the company's own development team. It does not sell any licenses; the business is based on offering professional services and expertise towards the implementation of the tool.

*Watch this vendor for continuous development by the company's own developers and a clean, customisable, and modern interface.*

### 6.2 Collibra Governance

Founded in 2008, Collibra focuses on deriving business value from data and to help end users collaborate on data driven projects. It comes with best practice reporting templates out of the box. Among seven data products in its platform, its Data Governance product is designed to be easy to set up and use with a business glossary at its heart and APIs to connect with existing applications.

*Watch this vendor for a platform that puts data science in the background and allows business users to make decisions based on their own data analysis.*

### 6.3 CommVault Activate

Based in the US, CommVault can trace its lineage back to Bell Labs and became an independent business in 1996. Its Data Governance platform is aimed at data held in the cloud and is part of a portfolio of modules

for data management that can operate stand alone, or as an integrated package to add compliance tools. The company also offers BaaS solutions for Office 365 and VM environments after it acquired Metallic.

*Watch this vendor for a well packaged and easy to deploy set of data management solutions that can monitor live production data - backed by many years data management experience.*

## 6.4 EverTeam Discover

Now part of Kyocera, France based EverTeam provides a platform that discovers and archives valuable data and separates it from so-called dark data, also known as Redundant, obsolete, and trivial (ROT). It separates its platform into three modules for discovery, archive and policy - to ensure data conforms with business policy. All modules use Natural Language Processing (NLP) and AI to perform Data Governance tasks

*Watch this vendor for greater market presence now that it has been acquired by the \$14bn Japanese industrial group Kyocera.*

## 6.5 Global Data Excellence - DEMS-Nexus

Global Data Excellence was founded in 2007 and has developed a Data Governance platform that uses AI techniques to make sense of unstructured data. Accessed through HTML5, the platform attempts to make sense of data by converting natural language searches into machine language, and thus classify it based on business value.

*Watch this vendor for a traditional data governance approach well assisted by natural language search tools and compatibility with machine language and a graphical mapping approach to data relationships.*

## 6.6 IBM Watson Knowledge Catalog Instascan

IBM uses its AI engine Watson to discover risk that lies hidden in unstructured data. It uses automation and statistical sampling models to quickly identify areas that could cause compliance failure. Firmly focused on risk reduction and compliance it can perform risk assessments, automatically apply classification, and make data ready for audit

*Watch this vendor for adding a proven AI layer to the Data Governance architecture of large enterprises, and as a simple plug into other IBM data modules.*

## 6.7 OneTrust

OneTrust is a company of around 2000 employees co-headquartered in Atlanta, US and London.

This five-year-old company built a GRC management platform from the ground up in the enterprise and is valued at around \$5.1bn. As well as Data Governance, the platform assists with Privacy, Third Party Risk and Ethics.

*Watch this vendor for its innovative use of AI and Machine Learning to monitor changes to compliance laws, and to automatically discover and classify next-generation content.*

## 6.8 OvalEdge Data Catalog & Governance Tool

OvalEdge was founded in 2013 with a goal to provide easy access to Data Governance and catalog information to all stakeholders and employees across an organization, through a central repository. It is firmly focused on analytics and deriving business value from organised data. It allows employees with Excel skills to look at trends, see opportunities, and gain deeper perspectives. Users can also build recommendation or predictive engines from the data presented by OvalEdge.

*Watch this vendor for a unique approach to Data Governance that provides insight to users right across the enterprise.*

## 6.9 SailPoint - File Access Manager

SailPoint is an Identity Access Management (IAM) vendor founded in 2005. Its File Access Manager complements its line of IAM tools by providing insight into unstructured data accessed by users. The tool can detect sensitive information in data stacks, define who has access and if that access is appropriate. Trusted data users can also manage their own access via File Access Manager.

*Watch this vendor for an innovative solution to combining fundamental Data Governance functionalities with an established IAM platform.*

## 6.10 TopQuadrant - TopBraid EDG

TopQuadrant focuses heavily on a semantic approach to define and map data patterns across an organization with what it calls "Knowledge Graphs" which display connections between data, and by extension, its metadata. Knowledge graphs are designed to display more information than conventional Property and RDF graphs. As for the platform, Knowledge Graphs are effectively an extension of the RDF graphs designed by TopQuadrant

*Watch this vendor for Out of the Box pre-built asset definitions that help speed time to value and a modular approach that allows customers to add and adapt to platform as need arises.*

## 7 Related Research

[Advisory Note: GRC Reference Architecture - an72582](#)

[Advisory Note: Maturity Level Matrix for GDPR Readiness - 72557](#)

[Buyer's Compass: Identity Governance & Administration - bc80512](#)

[Leadership Brief: Six Key Actions to Prepare for GDPR - 70340](#)

[Leadership Brief: Working for the Business, not the Auditors - lb72583](#)

[Leadership Compass: IT Service Management - lc80259](#)

[Market Compass: Digital Workplace Delivery Platforms - mc80475](#)

[Market Compass: IT-GRC Tools - mc71165](#)

[Survey: KuppingerCole and BARC Joint Study: Big Data and Information Security - 74001](#)

## Methodology

### About KuppingerCole's Market Compass

KuppingerCole Market Compass is a tool which provides an overview of a particular IT market segment and identifies the strengths of products within that market segment. It assists you in identifying the vendors and products/services in that market which you should consider when making product decisions.

While the information provided by this report can help to make decisions it is important to note that it is not sufficient to make choices based **only** on the information provided within this report.

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

### Product Rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Deployment
- Interoperability
- Usability
- Market Standing

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

the way the vendor deals with them.

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

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

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

**Market Standing** is a measure of financial strength and market position. This is based on publicly available information, and takes the amount of funding received, the profitability, and the private or public status of the vendor into consideration.

We focus on security, deployment, interoperability, usability, and market standing for the following key reasons:

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

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

## Rating scale for products

For vendors and product feature areas, we use a separate rating with five different levels. These levels are:

- **Strong positive**

Outstanding support for the subject area, e.g. product functionality, or security etc.)

- **Positive**

Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

- **Neutral**

Acceptable support for feature areas but with several of our requirements for these areas not being met. Using functionality as an example, this could indicate that some of the major feature areas we are looking for aren't met, while others are well served.

- **Weak**

Below-average capabilities in the area considered.

- **Critical**

Major weaknesses in various areas.



## Content of Figures

Figure 1: Trend Compass for Data Governance platforms.

Figure 2: Use cases and capabilities mapping.

Figure 3: Outstanding in AI Capability: 1touch.io

Figure 4: Outstanding in Innovation: BigID

Figure 5: Outstanding in Compliance Support: SAP

Figure 6: Outstanding in Dashboard support: Varonis

Figure 7: Outstanding in Report Generation: Micro Focus

## Copyright

© 2021 Kuppinger Analysts AG. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice.

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

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

For further information, please contact [clients@kuppingercole.com](mailto:clients@kuppingercole.com).