

KuppingerCole Report

LEADERSHIP COMPASS

By **Anne Bailey**
January 11, 2022

Privacy and Consent Management 2022

This report provides an overview of the market for Privacy and Consent Management solutions and provides you with a compass to help you find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing solutions that enable you to collect and manage consent in a compliant and privacy-centric manner.



By **Anne Bailey**
aba@kuppingercole.com

Content

1 Introduction / Executive Summary	4
1.1 Highlights	4
1.2 Market Segment	5
1.3 Delivery Models	6
1.4 Required Capabilities	6
2 Leadership	9
2.1 Overall Leadership	9
2.2 Product Leadership	10
2.3 Innovation Leadership	12
2.4 Market Leadership	14
3 Correlated View	17
3.1 The Market/Product Matrix	17
3.2 The Product/Innovation Matrix	18
3.3 The Innovation/Market Matrix	21
4 Products and Vendors at a Glance	22
5 Product/Vendor evaluation	25
5.1 DataGrail	27
5.2 DataGuard	31
5.3 OneTrust	35
5.4 OneWelcome	39
5.5 Piwik PRO	43
5.6 Securiti	46
5.7 Sourcepoint	49
5.8 Syrenis	53
5.9 TrustArc	57
6 Vendors and Market Segments to Watch	61
6.1 BigID	61
6.2 Consenteye	61

6.3 Crownpeak	61
6.4 Cybot	62
6.5 Iubenda	62
6.6 Quantcast	62
6.7 Usercentrics	62
7 Related Research	64
Methodology	65
Content of Figures	71
Copyright	72

1 Introduction / Executive Summary

This Leadership Compass analyzes vendors in the Privacy and Consent Management market segment. The term "Privacy and Consent Management" stands for the administrative and governance capabilities over data privacy within the organization. Privacy and Consent Management impacts every level of the data value chain, from advertisers, AdTech, and publishers, to enterprises and their communication strategies, to end users and the relationships that they build with service providers and third parties that handle their data. Solutions that provide Privacy and Consent Management have the challenge of working for the best interest of all: to enable compliant data collection, build compliant consumer profiles, and monetization while enabling the privacy choices of end users and the intersection of global regulations.

This reports provides an in depth insight into the Privacy and Consent Management market. The key capabilities that make a comprehensive solution are explained, and the different approaches that vendors take to providing a solution are evaluated. The leading vendors are identified according to Product Leadership, Innovation Leadership, and Market Leadership, each with detailed profiles and assessments.

1.1 Highlights

- The term "Privacy and Consent Management" stands for the administrative and governance capabilities over data privacy within the organization.
- The market is very dynamic with new global privacy regulations, eventual reducing in use of third-party cookies, and changing methods to operationalizing privacy.
- Privacy and Consent Management Solutions are primarily delivered as Software as a Service.
- Data governance and automation are key trends in Privacy and Consent Management
- The Overall Leaders (in alphabetical order) are OneTrust, OneWelcome, Securiti, Syrenis, and TrustArc
- The Product Leaders (in alphabetical order) are OneTrust, Securiti, Sourcepoint, Syrenis, and TrustArc
- The Innovation Leaders (in alphabetical order) are DataGrail, OneTrust, OneWelcome, Securiti, and TrustArc
- Leading vendors in innovation and market presence (also called the "Big Ones") in the Privacy and

Consent Management space (in alphabetical order) are OneTrust, OneWelcome, Securiti, and TrustArc

1.2 Market Segment

The Privacy and Consent Management market segment has its roots in collection processes and responsible handling of customer data and entered the public consciousness with the rollout of GDPR regulations and mass data breach scandals. Data privacy regulation and strong public demand have attracted new entrants to this segment, where consent management was a key enabler of compliant data collection. Recent announcements by Google to remove support for third-party cookies from its browser and the rollout of cohort-based profiling of browser activity indicate that the publishing and advertising industries must adjust quickly to different technologies, that the privacy goals of users may move away from consent or emphasize more on first-party consent and consent from authenticated relationships, and that the Privacy and Consent Management solutions may need to support new capabilities.

This has yielded a dynamic, competitive space where vendors provide data consent processes for vendors and consumers. Thus, this Leadership Compass analyzes solutions that provide means for enterprises to assess their privacy compliance, take meaningful action to increase the data privacy protections afforded to end users, and balance the needs of compliance and marketing departments.

At a high level, these solutions should accomplish:

- Compliance support for global privacy regulations including GDPR and CCPA
- Provide insight into movement and protection of personal data within the organization and in transit to partners
- Support in the design, implementation, and enforcement of privacy policies
- Facilitate the compliant collection of consumer consent and preferences, and enforce those decisions
- Enable self-service privacy choices for users

Privacy and Consent Management is a market segment that continues to evolve to meet changing requirements. New privacy legislation is constantly being passed around the world, and the interconnected flow of data up and down the value chain makes it possible that legislation from one jurisdiction may become relevant to an organization based in another. And as more and more users become aware of their data rights and choose to exercise them, there is an increasing need to be able to respond to Data Subject Rights (DSR) requests in a scalable and secure way. There is a trend to operationalize privacy, or to enable action to be taken when a compliance gap is identified, a DSR is filed, or third-party vendor is not acting in a

privacy-preserving way. Better yet is when these workflows can be automated to manage the scale and volume of privacy actions that may need to be taken.

There is an increase of data governance capabilities seen in this year's vendors, indicating a convergence of data governance and privacy management, along with approaches that favor identity and CIAM as a natural bridge to providing privacy management. This could for example mean more focus on data discovery capabilities of structured and unstructured data sources to identify all sensitive data in the organization. Data discovery capabilities support designing a well-informed privacy initiative, with better insight into what type of information is collected, how it is legitimately used or proliferated through the organization and up/downstream, manage data breaches quickly, and fulfill DSRs efficiently. What remains to be seen is if Privacy and Consent Management can move beyond automation for compliance's sake to more transparent relationships.

1.3 Delivery Models

Privacy and Consent Management Solutions are primarily delivered as Software as a Service (SaaS), with all participating vendors providing this deployment model. On-premise deployment is offered by nearly half the vendors, and two thirds of vendors support multi-cloud deployments. This serves as an indicator that although on-premise remains relevant, organizations are requiring more agile multi-cloud and multi-hybrid deployments, especially when it comes to oversight and management of organizational data.

1.4 Required Capabilities

Privacy and Consent Management Solutions can cover some or all of the functional areas described below. Typically, solutions need to manage incoming signals like user consent, information from cookies and trackers, and information from user self-service portals. The solution may also support developing a privacy strategy for the organization, which would involve running assessments to identify compliance gaps, documenting steps taken to reduce those gaps, data governance capabilities, and provide ways to operationalize privacy in a scalable way.

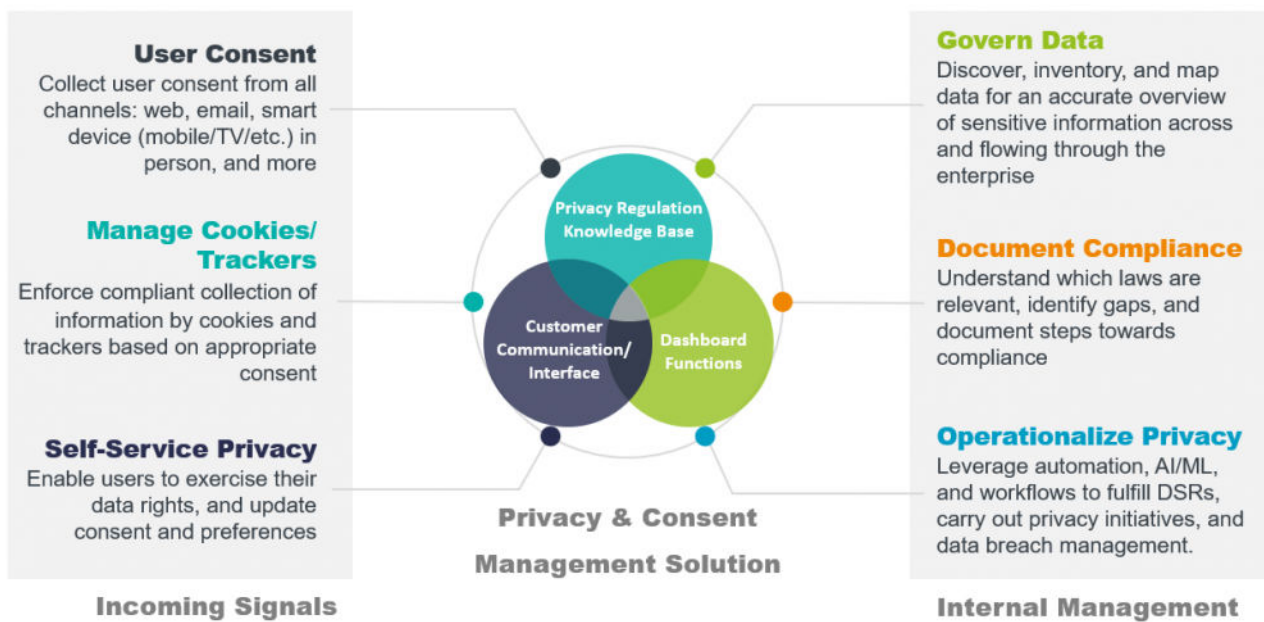


Figure 1: Privacy and Consent Management Solutions, Possible Areas of Functionality

The approach to providing these areas of functionality is still quite varied. Some vendors believe CIAM and identity solutions are best situated to provide management and protection of private information. Others believe data is the foundation of privacy, and take a strong data governance stance. Still others think that the current model for cookies and analytics is too extractive and are designing a privacy-centered alternative to the existing analytics and tag managers. Still others present Privacy and Consent Management as compliance combined with marketing, bringing the best of both worlds.

For vendors to be included in this report, they must have comprehensive solutions that include a majority of these capabilities:

- Compliant collection of user consent
- Enforcement of user consent
- Prevent non-compliant tracking and profiling on customer channels
- Assist in designing and implementing compliant privacy policies, cookie notifications, etc.
- Record progress towards compliance on specific regulations, i.e. GDPR
- Data mapping and inventory of personal data in the enterprise
- Provide data risk management support, for example de-identifying data via anonymization, pseudonymization, aggregation, redaction, or differential privacy
- Enable consumer control over privacy settings and consent choices
- Support workflows for DSR/DSAR/consumer requests and data breach notification

We expect solutions to cover a majority of these capabilities at least at a good baseline level. There is no minimum number of customers or revenue caps that vendors must meet -- both large international companies and small but innovative startups are included in this report. Some vendors did not respond to requests to participate, or chose not to participate. Profiles of these vendors, as well as other interesting vendors, can be found in Chapter 6, "Vendors to Watch".

Vendors with products still in a prototype stage, that provide only a single point solution, or who focus on individual and personal solutions rather than on the enterprise were excluded from this report.

Solutions that do not meet our general inclusion criteria but nevertheless strongly focus on specific types of Privacy and Consent Management may be mentioned separately in our "Vendors to Watch" chapter.

2 Leadership

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

Based on our rating, we created the various ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

2.1 Overall Leadership

We see that several vendors have achieved the rating of Overall Leadership in the Privacy and Consent Management market segment. The distribution of vendors is due to the range of services provided, varying maturity in the market, and numerous other factors.

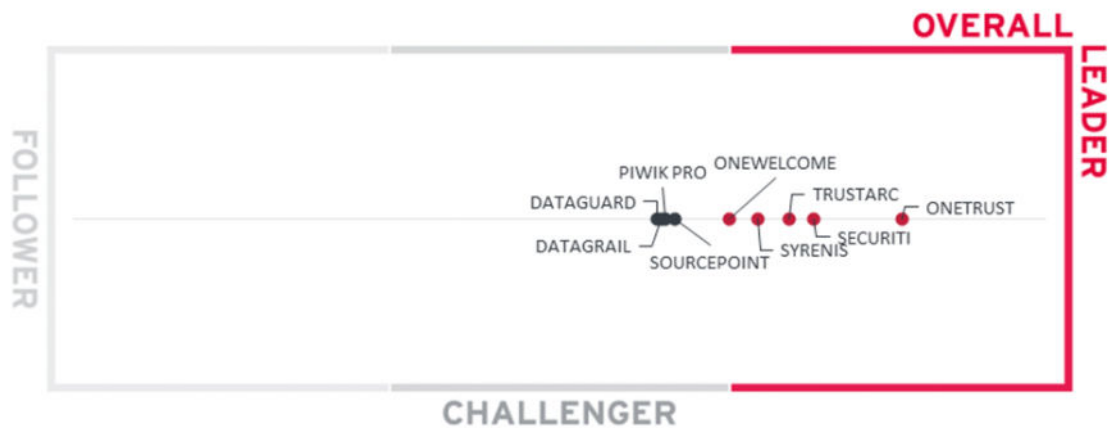


Figure 2: The Overall Leadership rating for the Privacy and Consent Management market segment

In this rating, we see OneTrust ahead of the other vendors because of its comprehensive service offerings, aggressive and rapid growth, and geographical presence, among other factors. Securiti follows as a new entrant to the market, with a compelling data governance approach to privacy. TrustArc also benefits from its overall market position. Syrenis offers a feature-rich solution and stability in a dynamic and constantly changing market. OneWelcome, renamed after a recent merger of iWelcome and Onegini, brings an identity management approach to Privacy and Consent Management.

A group of challengers and other new entrants to the market compete for market space as well. They offer differentiated approaches to the market. Sourcepoint provides a strong consent management platform (CMP) focused on meeting the needs of the publishing industry. Piwik Pro offers analytics and consent management features as a privacy-forward alternative to Google Analytics. DataGuard and DataRail are head to head as new entrants, both bringing promising capabilities to the market.

Overall Leaders are (in alphabetical order):

- OneTrust
- OneWelcome
- Securiti
- Syrenis
- TrustArc

2.2 Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.



Figure 3: Product Leaders in the Privacy and Consent Management market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

The participating vendors are relatively tightly clustered, with those in red having achieved the rating of

product leader. OneTrust provides a leading set of privacy and consent management capabilities. Securiti is a new entrant that offers a competitive breadth of capabilities. Syrenis, TrustArc, and Sourcepoint provide robust and mature privacy and consent management capabilities as well.

Vendors in the challengers section offer more focused capabilities in one area or another, or have room for improvement in their offering. DataGuard and Datagrail are positioned on the boarder of challenger and product leader. OneWelcome has a strong offering that meets CIAM use cases but lacks the breadth of capabilities that would allow it to meet a variety of other use cases. Piwik Pro emphasizes analytics and consent management with fewer capabilities to establish a privacy program for the organization.

Product Leaders (in alphabetical order):

- OneTrust
- Securiti
- Sourcepoint
- Syrenis
- TrustArc

2.3 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.

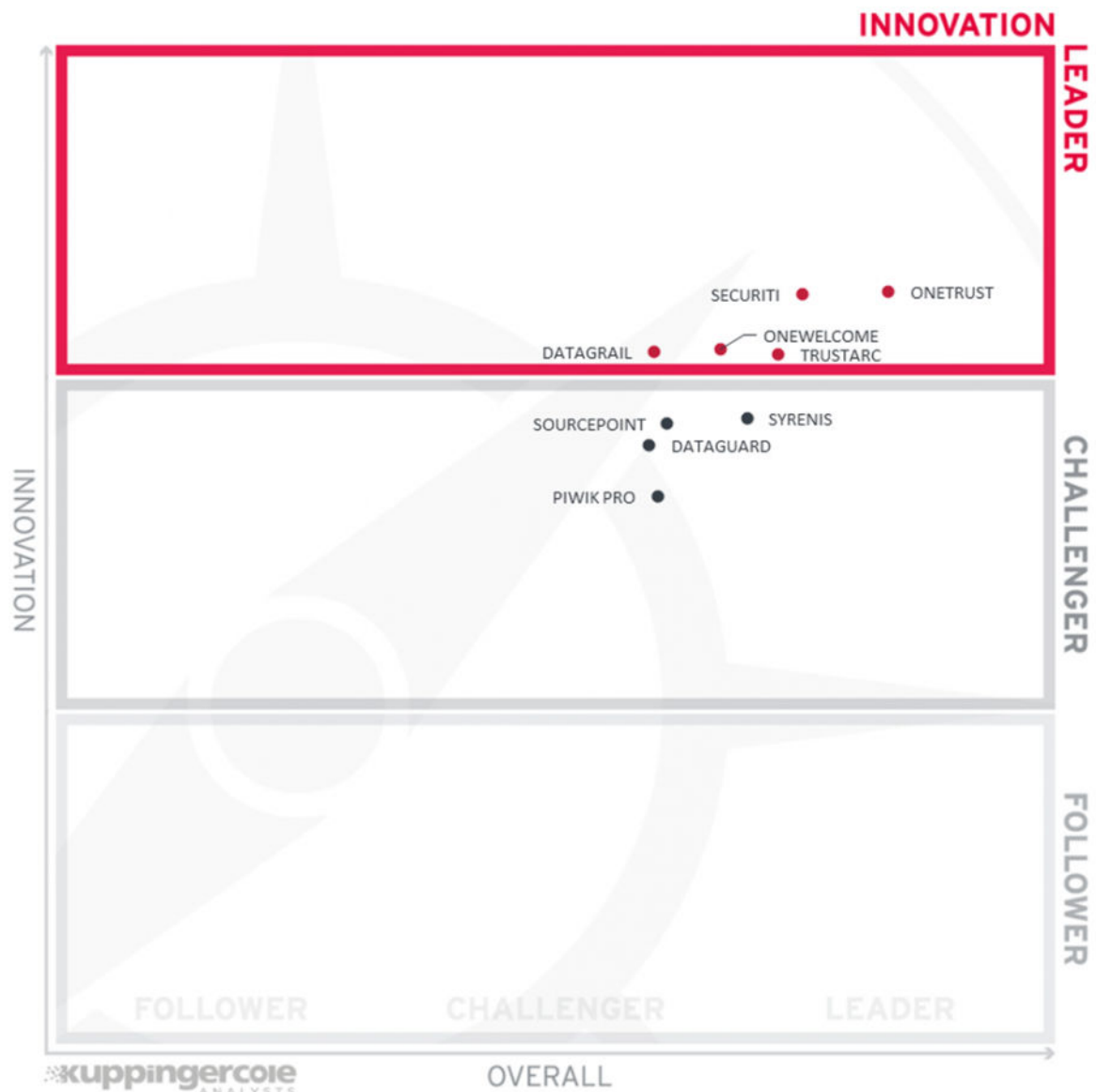


Figure 4: Innovation Leaders in the Privacy and Consent Management market segment

When considering innovation, OneTrust and Securiti are leading the way with a robust feature set on a foundation of data-driven intelligence and automation. OneWelcome's focus on developing attribute-level consent and Just-in-Time consent bring mutual benefit to both enterprises and end users. TrustArc works to enable scalable privacy programs with automation. DataGrail data discovery and mapping capabilities bring innovative approaches to this market segment.

The challenger section includes Syrenis, Sourcepoint, DataGuard, and Piwik Pro. All these vendors have also been able to demonstrate promising innovation in delivering Privacy and Consent Management capabilities, some leveraging automation or intelligent features to do so. Please refer to the vendor pages

below in section 5 of this report for more details

Innovation Leaders (in alphabetical order):

- DataGrail
- OneTrust
- OneWelcome
- Securiti
- TrustArc

2.4 Market Leadership

Lastly, we analyze **Market** Leadership. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.



Figure 5: Market Leaders in the Privacy and Consent Management market segment

The market leadership evaluation shows a group of leading, well-established Privacy and Consent Management players and many new entrants as well as vendors with growing and expanding geographical reach, industry focus, or customer base.

The market leaders in this segment are OneTrust, TrustArc, Piwik Pro, Syrenis, Securiti, and OneWelcome. OneTrust is a global presence but with the majority of customers situated in EMEA and North America. Syrenis's presence is also well distributed in North America and EMEA. Securiti is rapidly growing and gaining market presence. TrustArc tends to serve customers in North America, while Piwik Pro and Onewelcome are European-based.

The challengers include Sourcepoint, DataGuard, and DataGrail.

Market Leaders (in alphabetical order):

- OneTrust
- OneWelcome
- Piwik Pro
- Securiti
- Syrenis
- TrustArc

3 Correlated View

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

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.



Figure 6: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are "overperformers" when comparing Market Leadership and Product Leadership.

OneTrust, TrustArc, Piwik Pro, Syrenis, Securiti, and OneWelcome are ahead of the others, with strong ratings in both product and market leadership.

All the vendors below the line are underperforming in terms of market share. However, given the relative strength of their products, we believe that each has a chance for significant growth. Sourcepoint, DataGuard, and DataGrail have room for growth and expanded market presences.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

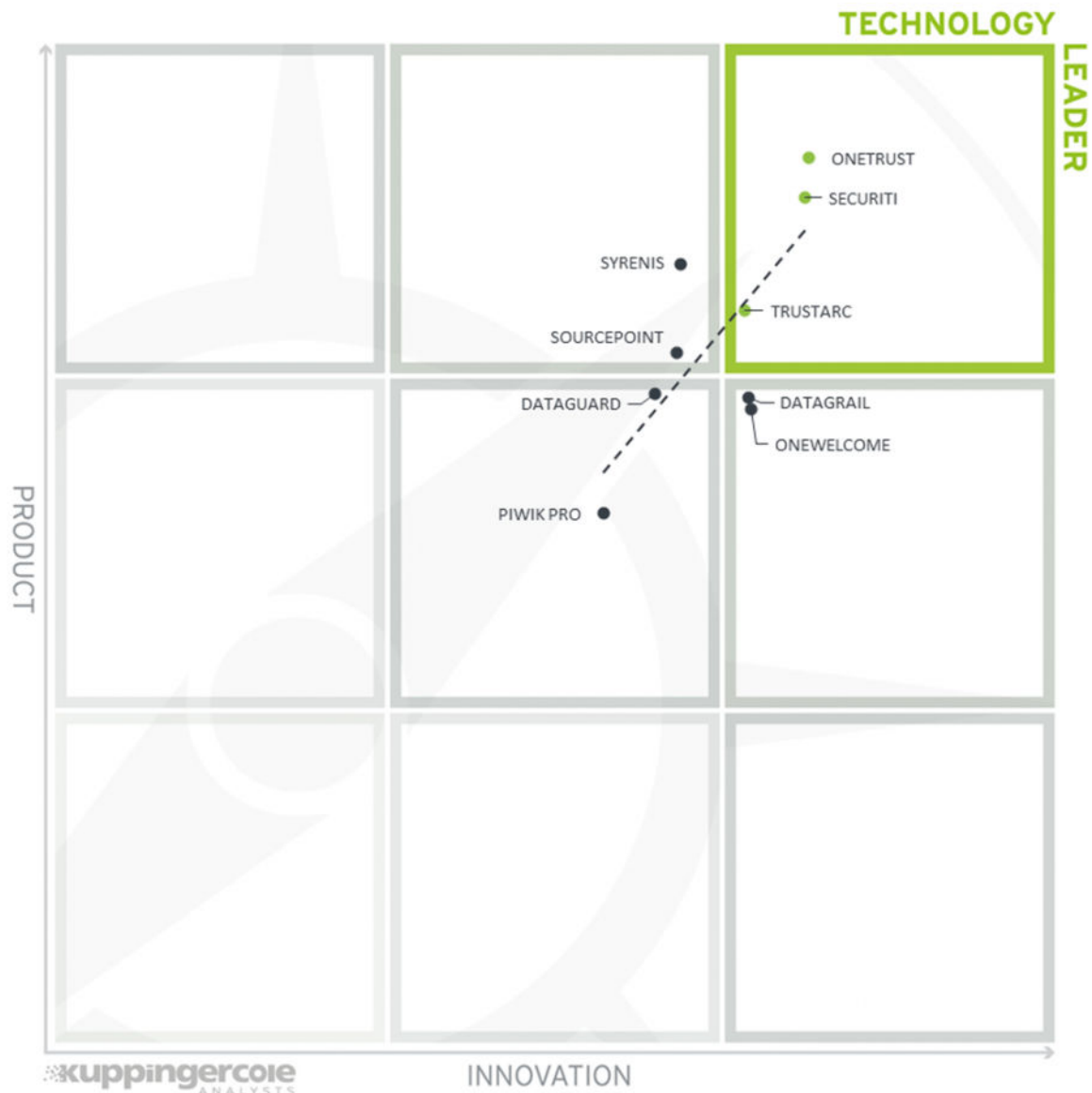


Figure 7: The Product/Innovation Matrix

Vendors below the line are more innovative relative to their product leadership positioning. Vendors above the line are, compared to the current product leadership positioning, less innovative.

OneTrust continues to perform well as we find it in the upper right corner of the matrix. Securiti and Syrenis demonstrate well-rounded capabilities relative to its innovativeness. TrustArc balances on the line, with a strong balance of innovation to product functionality. Sourcepoint and DataGuard also can be found positioned above the trend line.

DataGrail, OneWelcome, and Piwik Pro have relatively stronger innovativeness compared to their product

leadership.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

Vendors above the line are performing well in the market as well as showing Innovation Leadership. Vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

OneTrust, TrustArc, Piwik Pro, Syrenis, and OneWelcome are categorized as vendors with a strong market presence with innovativeness. Sourcepoint, DataGuard, Securiti, and DataGrail involve more innovative practices, and are still working towards market growth.

4 Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Privacy and Consent Management solutions. 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.

Product	Security	Functionality	Interoperability	Usability	Deployment
DataGrail Privacy Platform	●	●	●	●	●
DataGuard Privacy-as-a-Service and Consent Management	●	●	●	●	●
OneTrust Privacy Management Suite	●	●	●	●	●
OneWelcome Consent & Preference Management	●	●	●	●	●
Piwik PRO Analytics Suite with Consent Manager	●	●	●	●	●
Securiti PrivacyOps	●	●	●	●	●
Sourcepoint CMP	●	●	●	●	●
Syrenis Cassie	●	●	●	●	●
TrustArc Privacy Management Platform	●	●	●	●	●
Legend	● critical ● weak ● neutral ● 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
DataGrail	●	●	●	●
DataGuard	●	●	●	●
OneTrust	●	●	●	●
OneWelcome	●	●	●	●
Piwik PRO	●	●	●	●
Securiti	●	●	●	●
Sourcepoint	●	●	●	●
Syrenis	●	●	●	●
TrustArc	●	●	●	●
Legend	● critical	● weak	● neutral	● positive
				● strong positive

Table 2: Comparative overview of the ratings for vendors

While these tables help provide an overview of all the vendors on some comparable features, we recommend reading the Product/Vendor Evaluations in section 5 for an individualized assessment of each vendor.

5 Product/Vendor evaluation

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

Spider graphs

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

- **Data Risk Management:** The ability of the solution to support in establishing good data risk management practices in the customer organization, including preventing against incidents that would jeopardize end user data. Certifications, integrations with SIEM, and data breach response measures are among the capabilities assessed. Use of Privacy Enhancing Technologies (PETs) such as de-identifying data via anonymization, pseudonymization, obfuscation, aggregation, and redaction are also considered.
- **Data Mapping/Inventory:** The ability of the solution to discover, categorize, display, and manage private data within the customer's systems. This could include providing a single source of truth, connecting data sources, classification and data discovery, and mapping of internal and external processes.
- **Compliance Progress:** The methods a solution uses to enable a customer to understand what gaps or failures to meet a privacy regulation exist in their systems or processes, and to provide meaningful ways to identify, communicate, and visualize progress over time to achieve privacy compliance for specific regulations. This should enable compliance of multiple privacy laws/regulations, data transfers, data minimization, and audits to document steps towards compliance.
- **Consent Collection:** The approach the solution takes to manage cookies and trackers, and collect end user consent (and preferences) from multiple channels. This can include measures for the authenticated and unauthenticated web.
- **Consent Enforcement:** The degree to which consent choices are carried out, end user consent decisions are communicated, collected, stored, and enforced all along the data value chain. This

should include localized storage of data, coordination with third-party cookie and tracker vendors, and integrations with internal systems.

- **Consumer Control:** The methods that a solution uses to enable end users to have self-service control over their profiles, consent choices, preferences, and to exercise their data rights.
- **Automation:** The methods that a solution has to leverage automation to operationalize privacy across the organization. This could include responding to consumer requests in a scalable manner, addressing data breaches, receiving automated insights on potential gaps in their privacy program, and more.
- **Analytics:** The ability of the solution to provide analytics on the types of consent signals being collected, including A/B testing, insights on numbers of opt-ins or outs by category, or dashboarding capabilities.

5.1 DataGrail

DataGrail, based in San Francisco, USA and founded in 2018 provides enterprise privacy management by implementing privacy initiatives at the data level. DataGrail aims to enable a one-person team to manage a privacy program with its Privacy Platform, with particular focus on system and private information detection, automatic fulfillment of requests, and consent management through a partnership with UserCentrics.

DataGrail aims to be the privacy system of record for customers by automating workflows for continuous system detection and for managing data subject requests (DSRs) and consent management. Continuous systems detection enables DataGrail customers to locate PII in shadow IT for a more informed data risk assessment. Data sources in the customer's ecosystem are automatically detected, also scanning through apps such as Okta SSO and Expensify to find evidence of forgotten systems and shadow IT. DataGrail connects with over 900 data sources, apps, and infrastructure providers via API, upload, or automated workflows for systems that are not API compatible.

The Live Data Map -- one of three modules offered in the Privacy Platform -- operates from the inputs of the connected data sources by discovering, cataloging, and mapping data. Detected systems are promoted into the systems inventory where additional descriptive fields like business processes that source is used in, types of data it contains, or countries the data resides in can be filled in by administrators. The Live Data Map logs which systems contain personal or sensitive data. A dashboard function is provided for the Live Data Map which contains the number of systems integrations and status (connected to DataGrail or not), the number of newly-detected systems that may contain PII, categorized by business process purpose, and the most recent time that system was connected to DataGrail.

The second module, Request Manager, provides automated workflows for data subject requests (DSRs). DataGrail customers are provided with a branded webpage where end users can access a DSR form, customizable to accept access, deletion, rectification, pause, and do not sell request types. The end user should verify their identity when submitting a DSR, and various options for identity verification are available according to information already stored in the individual's profile: email confirmation, text message, or security questions based on information about when the account was opened, and more. CAPTURA capabilities are available to reduce spam requests. Data on the subject is detected in the connected systems and assembled as a checklist for an administrator to review before fulfilling the data request. The end user is provided with a link to a downloadable results page.

The third module, preference management, is provided in a module called Preference Card. This offering focuses on collecting and updating preferences as well as providing appropriate consent and opt-out options. Consents can be collected via web browsers, Android and iOS mobiles, tablets with a popup window, and via email. Cookies and trackers are blocked until a user gives their consent. End users manage their preferences from a branded web interface, which is then synchronized across the relevant systems including sales, marketing, and product departments.

DataGrail is a Software as a Service offering with subscription-based packages serving primarily North America and EMEA. Overall, DataGrail is a strong choice for organizations that prefer to rely on a data-

centric approach to privacy. The robust systems detection capabilities enables detailed mapping of PII across the organization and delivers intel on the data risk exposure. Automated DSR management detects the location of personal data across the enterprise and pulls it into a dashboard for a quick response to the end user.



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

Strengths

- Support for global privacy regulations including CCPA, GDPR, CPRA, LGPD, CDPA, PIPEDA, PDPA, and more
- Strong system detection capabilities
- Automatic detection of overlooked systems and apps through downstream integrators
- System changes regularly refreshed in Live Data Map
- Inclusion of identity verification in DSR fulfillment
- Automated data extraction of personal data for DSR management
- Robust security posture
- Pre-built connectors for 900+ data sources
- Automatic audit reports produced
- Supports multicloud deployments

Challenges

- Integrations with ticketing systems would strengthen the Request Manager module
- Could include support for reporting and reacting to a data breach
- Support for privacy policies could be added
- A relatively small vendor with a growing geographical reach
- Cookie consent offering could be expanded, including support for AMP pages and in-person interactions
- Adding API availability for consent collection would strengthen this product

Leader in



DATA RAIL



5.2 DataGuard

Founded in 2017 and based in Munich, Germany, DataGuard is addressing privacy from an intersection of information security, consent management, and compliance. Their web-based privacy solution is informed by -- and customers are supported by -- a team of privacy and information security experts. With the acquisition of MyLife Digital in 2021, DataGuard brings extended capabilities for data subject requests (DSRs), preference, and cookie management.

DataGuard offers Privacy as a Service and Consent Management modules which can be used together or in isolation. The Privacy-as-a-Service platform offers ongoing GDPR compliance via a privacy audit, a portal for Data Subject Requests (DSRs), a website cookie manager, privacy training, plus several other features. The Privacy Audit is a series of questionnaires that cover business processes that relate to data protection to gain an overview of the existing compliance status. From this collection of 800-1500 data points, an automated and prioritized list of recommendation actions to better implement privacy in the customer's organization is generated and documentation including Technical and Organization Measures (TOMs) and Record of Processing Activities (RPAs) is generated. To document the customer's ongoing efforts, the customer receives documentation on their actions to implement and improve privacy compliance annually, which is a compilation of the customer's projects with DataGuard's privacy experts, DSRs, Data Processing Agreements (DPAs), and other contracts, and any additional interactions. This audit trail thus documents every action the organization has done to remain compliant, and can be exported and shared with a requesting authority.

Other features included in Privacy-as-a-Service include a Privacy Policy Generator, where a privacy policy for a website is generated based on a questionnaire filled out by the customer. The DSRs portal in the Privacy-as-a-Service platform consists of a web form that can be filled out by current and former employees, end users, and business partners. The request is logged in the platform on a dashboard with manual or automated workflows outlined. Identity verification of the data subject is included to ensure that privacy actions are done on behalf of the correct individual. Legal exceptions can be added in order to close the request early, with full documentation still produced in the platform. Approximately 20 templates of often-used policies and documents are available, written and implemented with the support from the in-house experts. DataGuard Academy consists of online training courses for privacy and information security, a Portal for DPAs and Joint Controller Agreements (JCAs) as a single source of truth and a resource to check new privacy contracts with DataGuard experts. A News dashboard displays relevant articles, customer content, commentary, and advice on new laws and breaches.

Consent Management is available as an independent module. The Consent Management module can collect granular consent and marketing preferences via mobile apps, SMS, web portals, email, keyboardless devices, AMP pages, OTT devices, direct mail, and in-person interactions. On websites, cookies are detected on websites with a technology integration with Usercentrics, and detected cookies are prevented from firing and data being transferred to third-parties until the appropriate consent has been collected. Multiple consent frameworks are supported, including GDPR, CCPA, and ePrivacy Directive. Consent and preference templates are available in over 35 languages. A privacy policy generator creates policies

dynamically. All consent records are linked to a unique individual, creating an auditable consent record. An open API is provided to connect to CRM systems, MarTech solutions, and analytics products, and is synchronized in real-time across all connected systems, consolidating data at the latest state.

The Preference Management module A/B testing is available for consent and preference notifications to optimize performance of consent banners and notices. Opt-ins are incentivized by giving users a preview of content that they are missing. Dynamic or JIT consent is available, as well as adding a consent widget to partner websites for use across an expanded ecosystem. To view, update, or exercise data rights, the user authenticates on the service provider's website. In their privacy portal, they can view individual cookies that have been consented to or denied, and marketing preferences.

DataGuard is a SaaS solution with data hosted in Germany and the UK. Enterprise scalability in number of data subjects and consents is demonstrated. A free option is available with limited capabilities, and fixed monthly costs on a tiered basis allow for predictable expenses that include fixed consulting hours a flexible range of topics and services and liability coverage of up to 650.000 €. It provides a strong approach to documenting GDPR compliance and enabling consent management according to several privacy regulations.

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

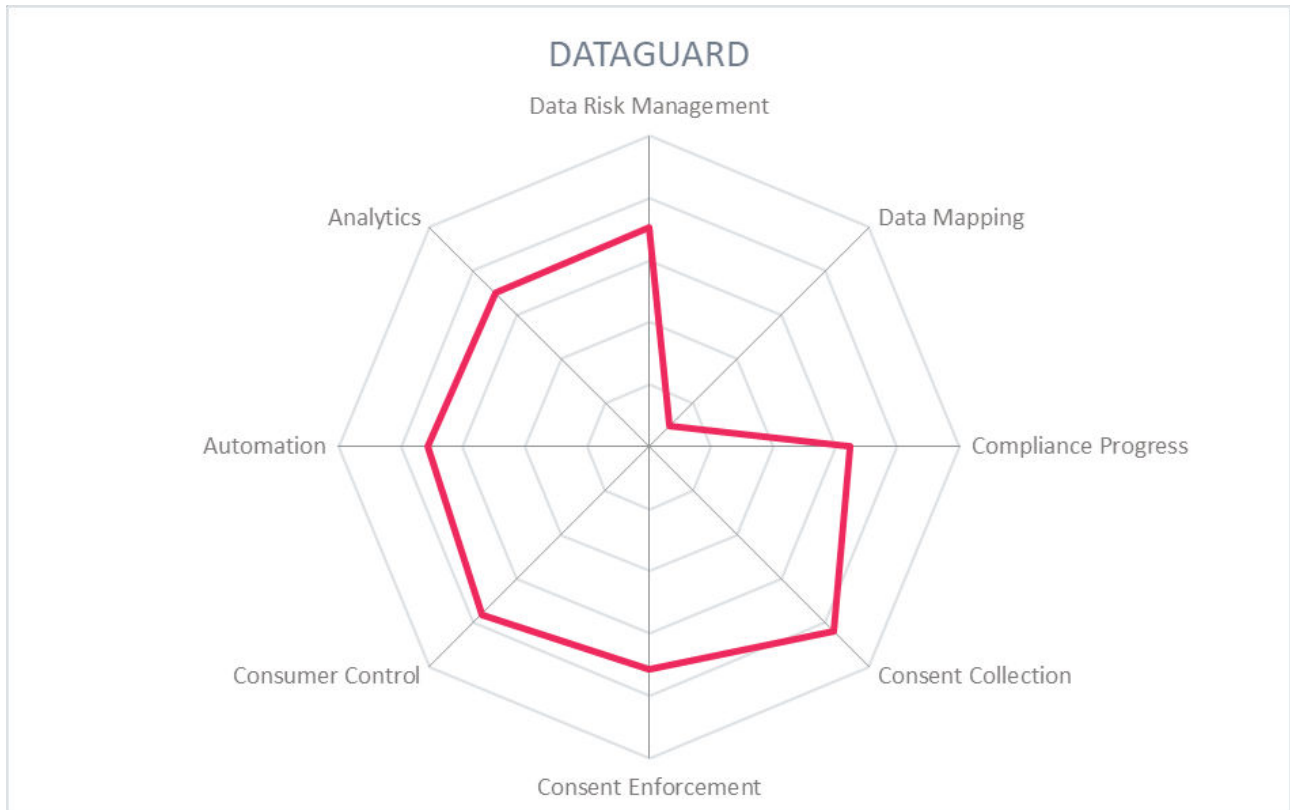


Strengths

- Consent Management module supports GDPR, CCPA, PIPEDA, PDPA, and Australian Privacy Act
- Auditable consent record and privacy audit maintained for consumers
- A prioritized list of recommendations is provided on how to improve the privacy status
- Online and offline channels are reflected in consent record
- Technology integration with Usercentrics for strong cookie scanning function
- Dynamic or JIT consent
- Embed consent widget on partner websites
- DSR can be submitted as employees, end users, or business partners
- Enables privacy partner management
- Fixed monthly costs
- Supports multicloud deployments

Challenges

- At this time, Privacy-as-a-Service facilitates UK and EU GDPR only
- No current data mapping or inventory capabilities, though on the roadmap with expected 2022 release
- DSRs portal may not have secure channels for data transfer



5.3 OneTrust

Founded in 2015 and co-headquartered in London and Atlanta, GA, OneTrust is a fast-growing player in this market. Its Privacy Management Software is a full stack offering that first discovers and governs sensitive data, then applies policies and automated workflows to the data. The platform offers privacy and consent management modules as well as security, data governance, third-party risk, ethics and compliance, and ESG modules.

The product suite is powered by OneTrust Athena AI and Robotic Automation to run OneTrust DataDiscovery, and DataGovernance. These tools discover and classify structured and unstructured data through connectors with mobile platforms, SSO providers, developer frameworks, ad frameworks, and with integrations into platforms such as Salesforce. From this data which is pushed into data maps and catalogs, Athena AI helps build the company profile consisting of relevant jurisdictions, industries, then makes suggestions on relevant templates, geolocation rules, and other automated support to set up a privacy program. DataDiscovery with Athena AI can be used by guiding customers through interactive wizards across all systems, connected to systems through plug-ins. Specific data elements can be targeted and discovered, both structured and unstructured, for example to tag all PII data and compile it in a business-readable context. Data mapping capabilities are highly customizable, and can automate regulatory reporting for compliance with article 30, able to map obligations of data processors and controllers in relation to third-party vendors. Athena AI can automatically set up and suggest relationships between datasets, legal regulations, and more. Dynamic maps that show how data moves across borders and assist in conducting risk assessments on compliance gaps. Retention periods on sensitive data are upheld, and can be automated. Actions can be taken, such as flagging data that poses a risk to the organization or redacting sensitive information based on role.

The Consent & Preference module provides consent solutions including OTT and cross-device consent, cookie compliance, preference management, mobile app consent, consent rate optimization, and tools designed specifically for publishers and streaming services. Websites, apps, and other connected devices are scanned continuously to categorize and disclose the cookies that are present, which dynamically update cookie banners. A patent-pending auto-block is employed to prevent trackers from firing until consent is given. Users are presented cookie banners based on their IP address location to match regional requirements, such as certain cookie groups opted out by default or a link to a Do Not Sell page. Publishers and media customers have access to IAB templates for targeted and nontargeted advertisements. For unauthenticated consent experiences, choices are collected and flags set in the user's browser to signal those choices. For authenticated experiences, the user logs into their account and can set preferences as well as consent choices, where the user also has access to their privacy center.

Administrators have a global view via a dashboard, which provides analytics on Data Rights Requests (DSRs), consent rates, etc., or access to DataGuidance, which is a regulatory research resource.

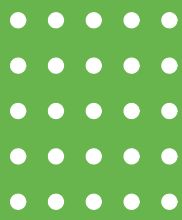
DataGuidance assists the organization in executing its privacy program by assembling a company profile of jurisdictions, regulations, readiness assessment, and current gaps in the privacy program. Processing DSRs are supported by automatically providing recommended responses, and ability to redact structured and

unstructured data. DPIAs and blacklist workflows can be automated, while maintaining a fully auditable record together with the aggregated consent and preference profile of authenticated users. Integrations with major tag managers are included.

OneTrust has multiple deployment options including multi-tenant cloud, private cloud, on-premise, or hybrid. The product modules are available individually, or as a suite. Data compliance risks can be identified with customizable variables, visualizations created, and assign tasks to address risks. The Consumer and Data Subject Rights Management solution provides a secure two-way communication portal to manage this process securely. Vendor risk can be monitored by the intelligent engine by setting up workflows by leading customers through interactive wizards, including proactively monitoring for data breaches anywhere in the vendor supply chain. Customization is a drag-n-drop format. One Trust supports 10 data centers worldwide in the US, EU, UK, and Asia Pacific.

OneTrust and its possibilities for intelligent automation is a good match for customers that have complex or legacy data systems that pose challenges for privacy compliance. The comprehensive data discovery, inventory, and mapping tools enable customers to monitor their ongoing progress towards compliance and visualize gaps. OneTrust is equipped to meet the regulatory needs of all global privacy regulations, and commits itself to same-day support for newly released privacy regulations.

Security
Functionality
Interoperability
Usability
Deployment



OneTrust

PRIVACY, SECURITY & TRUST

Strengths

- Facilitates compliance for GDPR, CCPA, PIPEDA, PDPA, LGPD, India Data Protection Bill, POPIA, CDPA, CPRA and many more
- Support for industry standards such as HIPPA, IAB TCF, NIST privacy framework, and more
- Strong data inventory and mapping capabilities
- Strong analysis capabilities to visualize compliance progress and address gaps
- Risk management capabilities include third-party risk management, data breach monitoring, and detection and visualization of risks
- Support for cross-border transfers to identify potential risks
- Handles up to 10,000 transactions per second thus able to provide privacy management for streaming services
- A registered IAB CMP
- Availability in over 100 languages
- Large in-house legal department covering multiple jurisdictions
- Support for Kantara Consent Receipt standard and for identity verification services
- Growing support for employee DSR
- Integrations with BI platforms such as Power BI and Tableau

Challenges

- Focus on growth and several recent acquisitions indicate a dynamic company, but also bring integration challenges
- Although offering its own privacy certifications, could be certified with external parties like ePrivacy Seal, EuroPriSe and Kantara Initiatives
- Could add support for serverless deployments

Leader in



ONETRUST



5.4 OneWelcome

The result of a 2021 merger between Ongini and iWelcome, OneWelcome is based in the Netherlands. OneWelcome delivers full CIAM and B2B identity capabilities, as well as consent management. OneWelcome CIAM is an integrated set of functionalities, able to be used together or in selected modules such as the Consent and Preference Management. From the recent merger, the Consent Lifecycle Management product gains mobile functionality, and improved data inventory and mapping capabilities. OneWelcome serves the authenticated web for consent and preference management.

OneWelcome facilitates opt-in-based consent flows for authenticated interactions and implements a data model based on the NIST 8112 standard for metadata collection and verification against an authoritative source. An end-user signs up with a customer using OneWelcome's CIAM solution, and their identity profile is built from the individual attributes given, such as name, surname, email, and more. As the end-user interacts, an inbound API manages intake of identity information from external systems such as CRM, HR, AD, and other identity management systems. OneWelcome's Consent-API connects with dialogue boxes or other interfaces with the customer for progressive/just-in-time consent collection. For offline consent, as in phone interactions, the consent manager (often referred to as Data Steward) can send a push notification or email to confirm a consent in an auditable form. In cases of multi-brand or omni-channel environments, the user interacts with the particular brand, but contributes to the same data model and consent information is harmonized between them.

The user's consent interface provides transparency for the user about the attributes retrieved with consent and the associated processing purposes. This is visible to the end-user on their personal dashboard on the customer's website, as well as for the organization. End-users can view their historical login, view which attributes were gathered for which purposes, view benefits from providing further consent, view consent actions as a timeline, as well as make corrections and updates.

The central Consent Ledger, stored with OneWelcome or in an external identity repository, provides a single source of truth for consented user data. The RITM module focusing on B2* relationship management allows for fine grained delegation of authority and flexible capabilities to restrict and audit PI access by other people than the end-user, including customer care, dealers/brokers, and application owners. OneWelcome provides coarse-grained consent at the document level as well as fine-grained consent per attribute, such as email, surname, phone, DOB, etc., and provides easy pathways for customers to gain attribute-level consent for many data processing purposes. These attribute consent management mechanisms enable their tenants to comply with GDPR and to ICO guidelines, and offers full traceability of which attributes are gathered, when they have been gathered, and the reason the tenant asks for consent. OneWelcome supports the right to export data, data deletion upon request, and data age/retention policies. OneWelcome has multiple data centers within Europe and could deploy in the US and Asia for localizing user data in the most compliant way.

OneWelcome is deployed as a SaaS specifically an IDaaS, without managed services or on-premise software. OneWelcome is designed to complement an organization's existing IAM solutions served by a

dedicated API, and able to augment an IdaaS solution with OneWelcome consent. OneWelcome's Consent & Preference Management product can be integrated with existing IAM, CRM, or consumer profile management systems in-house. The consent and identity data inventory is stored and managed from one platform to create a single source of truth, and simplifying reporting responsibilities for data protection officers.

Although OneWelcome lacks third-party cookie and tracker consent tools, OneWelcome is a strong innovator that provides strong CIAM capabilities with transparent attribute-level consent features for end-users. The data model used by OneWelcome to gather progressive and just-in-time consent for individual attributes, as well as to validate the context and reliability of these attributes is a differentiator in this market. OneWelcome has future visions of enabling privacy compliant interactions in the gig-economy, building upon its current capabilities of B2B2X use cases, as well as enabling delegated authorization in privacy-compliant ways.

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

cnewelcome

Strengths

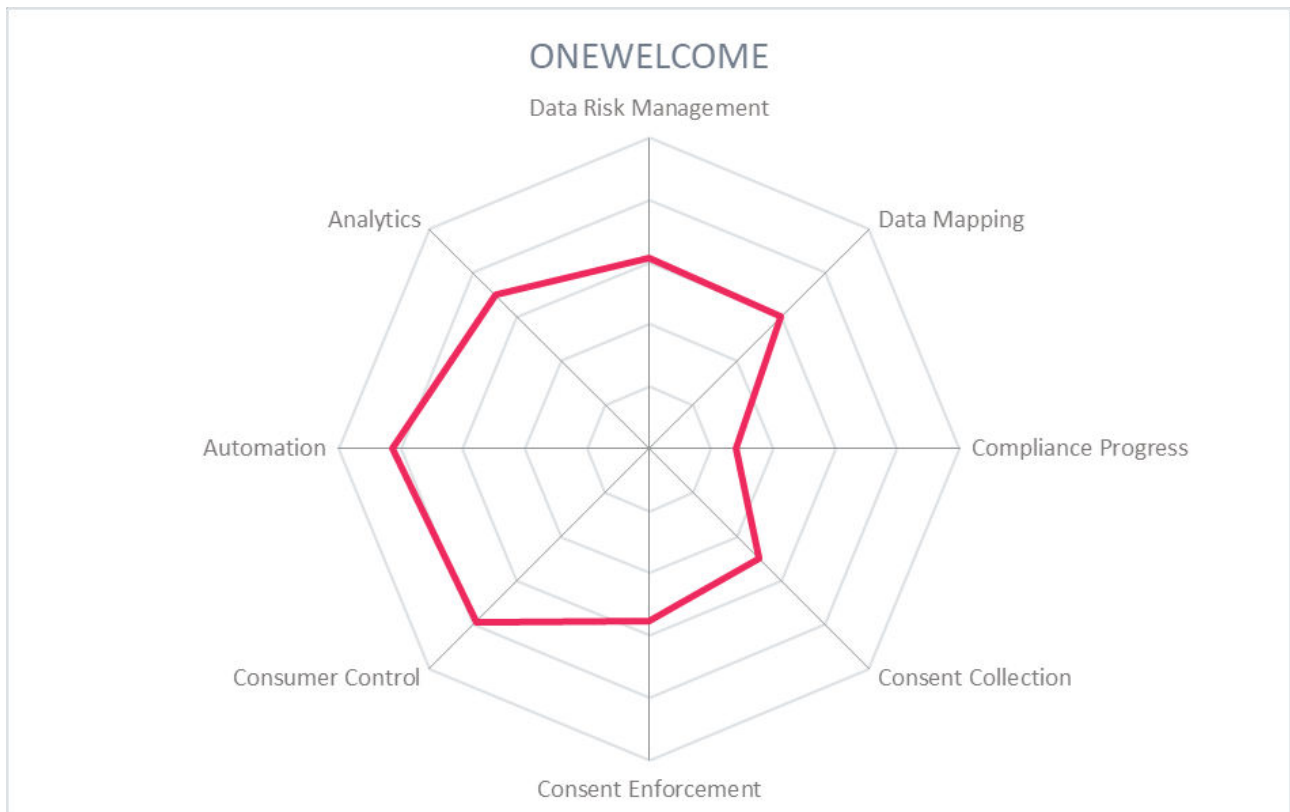
- Supports GDPR, CCPA, PIPEDA, and PDPA, Australian Privacy Act and updates, adheres to the British ICO guidelines, and supports industry standard PSD2
- Able to manage attribute-level consent as well as consent for documents such as updated privacy statements
- Enables parental consent for underaged consumers
- Offers end-user dashboard to manage all devices and methods of granting consent, such as web browser, mobile, IoT, SmartHome products, and entertainment devices
- Strong self-service offering for end-users
- Integrated Tag Manager for analysis and A/B testing

Challenges

- Lacks cookie and tracker consent tools
- Limited global reach, currently only present in the EU
- Support for data locality is limited to European countries
- Could add support to report/respond to a data breach
- Could add deployment options such as multi-cloud, managed services, or on-premise

Leader in





5.5 Piwik PRO

Piwik PRO was founded in 2013 and is based in Poland for a European-based alternative to Google Analytics. It is an analytics suite to analyze the customer journey across websites and apps and provide customer care with a focus on privacy and data security. The Piwik PRO Consent Manager module meets the needs of governments and enterprises primarily in finance, healthcare and other data-centric industries to provide analysis and privacy compliance for the customer journey.

The Consent Manager enables consent collection for privacy statements and cookies and assists organizations to handle data requests. Customers create customizable popups and widgets for end-users to register their consent, which are stored by the Consent Manager. Popups and widgets can collect separate consents for multiple data purposes, and can handle attribute-level consent with customization. When end-users ignore cookie and privacy popups, messages continue to appear on subsequent pages until the end-user gives or refuses consent. Only the accepted tracking technologies are permitted to fire. Piwik PRO also serves the unauthenticated web by collecting event and/or session level data, or by collecting personal data of those who consent.

The platform allows administrators to see the full consent history of end-users with timestamps, and see first-party analytic cookie files that are relevant to that particular end-user. The end-user is identified by anonymized cookie IDs relevant to each individual and -- if a data-request form has been sent -- by the user's email. The dashboard provides insight on overall user consent behavior with charts and visualizations.

Templates for privacy and cookie declarations are available, but Piwik PRO offers an API for customers so that they may completely design their own. Templates are available in English, German, Spanish, Japanese, Dutch, and Polish, with options to self-translate into other languages. Data Subject Request forms are available to end-users on the privacy policy page of an implementing customer's website, and can be fully customized via APIs. Data subject requests are collected and handled in the Consent Manager platform. The privacy policy page also allows the end-user to modify their consent and choose the desired language. Customers can dictate the required geo-location for their data storage, either in the US or EU.

The Consent Manager is implemented as a Javascript script and is delivered as a basic container. It can be deployed on-premise, in the cloud, or hybrid. For customers that have multiple domains or large geographical spread, deployment and management can be centrally coordinated. Rollout of service can be instant if deployed in the cloud, or in one to four weeks if deployed on-premise. The solution can be used to provide compliance for the major regulations, as well as for CCPA, LGPD, HIPPA, Chinese Internet Law, and Russian 526-FZ.

Piwik PRO is an option for organizations that require privacy-focused analytics. The application of analytics to Piwik PRO's own solution delivers value to users, assisting them to methodically design a customer experience that generates high levels of consent.

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

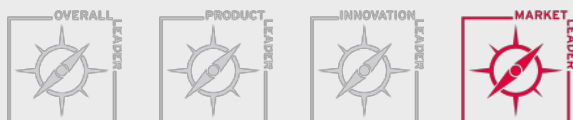
Strengths

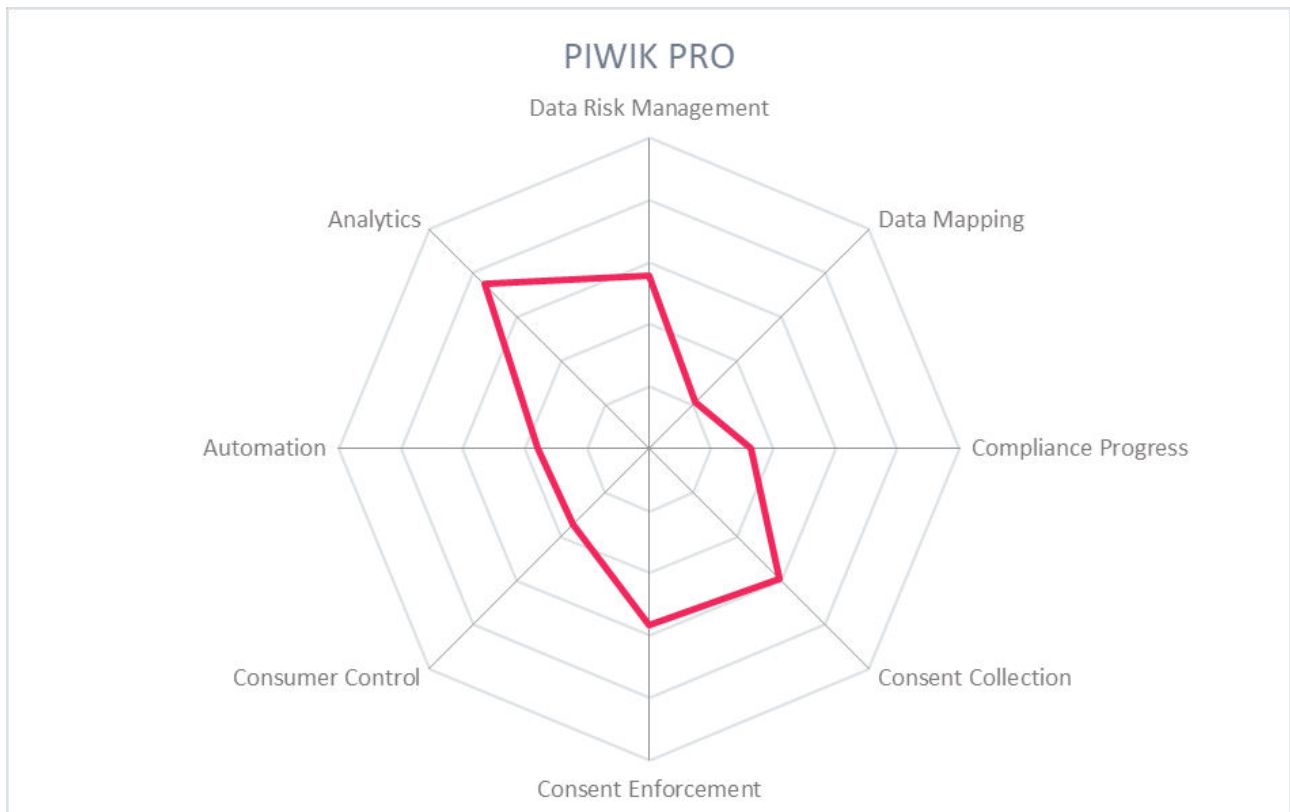
- Consent Manager is part of the free Piwik PRO Core offering
- Supports GDPR, LGPD and CCPA, with capacity for other regulations
- Tools for analytics, conversion tracking, and A/B testing
- Good visualizations on user consent behavior
- Zero cookie load function and comes with integrated tag manager
- Uses a privacy-by-design approach
- ISO 27001 and SOC2 Type 2 certified
- Relatively strong geographic reach and financial stability

Challenges

- No data inventory service, and limited data mapping features
- Does not yet connect to other CRM systems
- Could add support for multi-cloud environments

Leader in





5.6 Securiti

Securiti, founded in 2018 and based in California, USA, aims to operationalize privacy and fulfill data protection obligations. It emphasizes a real time data-driven approach supported by automation for data discovery, data mapping, assessments, data subject rights fulfillment, breach management, privacy notices, and consent management.

The PrivacyOps product is centered on data, and begins with extensive data mapping it calls a People Data Graph. It automatically builds a graph linking an individual to their personal data in the organization, including data residency. Integrations with approximately 200 structured and unstructured data systems allow the system to scan the information they contain for sensitive data. The intelligent system classifies data into types, and structured and unstructured data catalogs are automatically built. Analytics on who has access to what types of data is provided, as well as means to write or update policies to govern access and mask sensitive data when specified. Natural language query allows exploration of data types across the organization. Data mapping is visualized and is interactive with slice and dice capabilities, as well as analytics capabilities for data risk measurement. The customer defines their risk tolerance, and a decision engine calculates the risk of data in each system.

Data Subject Requests (DSRs) are automated, where once a user submits a request, a bot can automatically search connected systems for that user's personal information and show a reviewer the relevant data, and extract to create a report. The bot can then take action, such as redact personal data within the system. In the event of a data breach or incident, the incident response process is automated to summarize details, identify the scope of the data breach, and to optimize who should be notified to comply with relevant regulation. Data privacy assessments can also be automated.

Consent and privacy actions are also primarily automated. For cookie consent, these are scanned on the websites, where they are classified and auto-populate a cookie banner. The cookie banner is customized for look and feel, language, and regulation. These banners and dynamic privacy notices display appropriate text and options depending on the geographical location that traffic originates from. Cookie scanning is triggered at any change of the website or code update, and new cookies automatically updated in banner. Consent analytics are available with A/B testing, and consent audit reports are created that contain one year's worth of information.

This solution is a SaaS product with multicloud options. Onboarding this solution involves connecting to APIs and/or giving IAM privileges. PrivacyOps is powered by machine learning, which requires minimal training to learn how an employee or customer ID looks like for the particular customer.

Security	• • • • •
Functionality	• • • • •
Interoperability	• • • • •
Usability	• • • • •
Deployment	• • • • •



Strengths

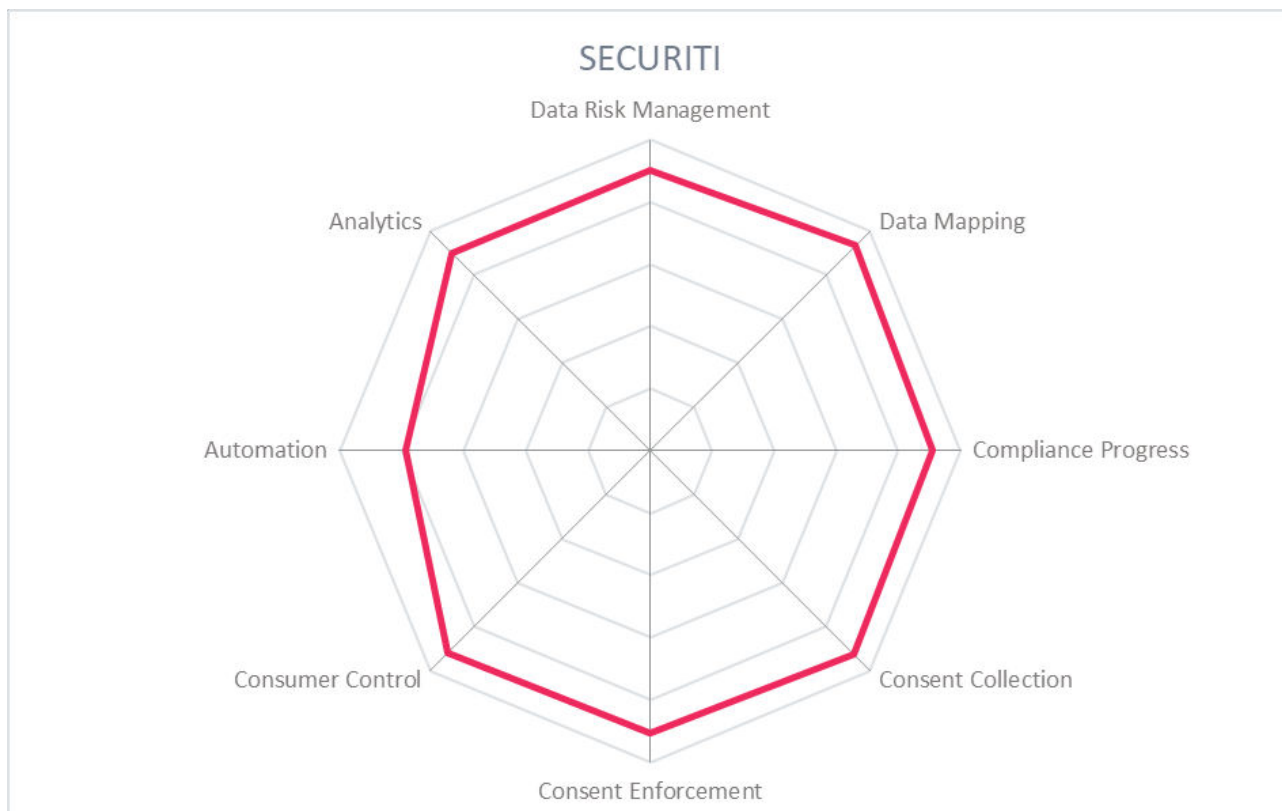
- Supports GDPR, CCPA, PIPEDA, and PDPA, Australian Privacy Act and updates, LGPD, POPIA, and more
- In DSR flows, user identity is verified with flexible methods
- Access management of data enabled
- Delivers risk assessment based on customer's personalized definition
- Has third-party vendor compliance ratings and risk assessment
- SOC Type II certified
- Strong offering for automating privacy tasks
- Capable of detecting sensitive data in both structured and unstructured data stores
- Over 200 connectors to cloud and on-premise data stores
- Supports multicloud deployments

Challenges

- May need higher AI/ML governance integration for ongoing maintenance of models
- Documentation is available in English only
- Offering could be expanded with managed services
- Could add certifications and support for Kantara Initiatives, HIPAA, EuroPriSe, and ePrivacy Seal

Leader in





5.7 Sourcepoint

Sourcepoint was founded in 2015 and is headquartered in New York with offices in London and Berlin. The Consent Management Platform (CMP) is deployed as a SaaS, and focuses on enabling better communication between publishers and end-users, including compliance. An additional layer of functionality -- DIAGNOSE -- provides customers with the ability to evaluate the privacy compliance of different third parties present on their website. The CMP remains focused on serving the digital marketing use cases. The CMP offers specific coverage of the CCPA, GDPR, and ePrivacy Directive, but can be customized to meet upcoming regulation from different jurisdictions.

Sourcepoint's CMP allows for publishers to determine their own user engagement strategy, while still maintaining privacy and cookie compliance. A messaging system collects and transfers consent notifications and end-user preferences. Consent can be specified by the geolocation or IP address of the end-user. These are stored in a secure database so that the preferences and consents may be modified by an end-user at a later time. Signals to third-party cookie vendors are communicated via consent strings developed by the IAB. For third parties that do not participate in the IAB framework, signals are communicated with JavaScript, cookie actions, or via integration with tag management systems that support custom, client-side triggers, such as Google Tag Manager, Adobe, Tealium, and others. End-users can view their Privacy Manager to handle their consent per collection purpose or per cookie/tracker vendor. Sourcepoint's data inventory service is able to identify and classify sensitive data such as PII and PCI supported by their partnership with Segment, allowing customers to better fulfill DSAR and DNS requests.

Sourcepoint uses a scanning technology to identify, evaluate, and categorize the tracking technology that is present on a publisher's website, and the acquisition of Redbud expands this scanning functionality. The results of the scan automatically populate the vendor list for which an end-user provides consent. Expanded scanning functionality includes detailed information about cookie vendors so that customers can make more informed decisions on which vendors to whitelist. GDPR consent data is stored in Sourcepoint's Frankfurt database. Marketing and messaging capabilities include targeting by geography, platform, key value pair data, social referrers, etc. Sourcepoint offers strong analytics capabilities to optimize and gain insight on consent rates, bounce rates, and makes A/B testing available.

The DIAGNOSE module serves as a complement to the CMP by identifying vendors that process data on owned and operated digital properties and assesses the risk level of those vendors. A repository of all data processing instances and the results are benchmarked against other properties selected by the customer to quickly understand the risk level of other vendors. The scan captures content executed via pixels, cookies, JavaScript, API calls, and other methods, as well as simulating consumer interactions.

The compliance dashboard displays analytics information about cookie vendors, consents, and information of non-compliant vendors. Communication with non-compliant vendors is handled manually. Benchmarking against similar companies and websites is available. The Privacy Lens platform scans websites and provides advertisers with the ability to measure whether their advertisements are appearing in privacy-safe environments.

Deployment is in private, multi-cloud, or containerized environments, but Sourcepoint is able to host applications in a client's own data centers and infrastructure. The primary market for Sourcepoint's product is in North America and Europe, and have established a strong reputation among large publishing customers in these regions.

Sourcepoint has overall high performance, with high customization specialized for the needs of large publishers. Its Engage module for DNS/DSARs with options for automation is an advantage for customers with large user bases and many channels for customer interactions. It has more of a focus on providing additional revenue options for publishers through compliant consent and preference collection and providing comprehensive analytics on the end-user's consent journey.

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



Strengths

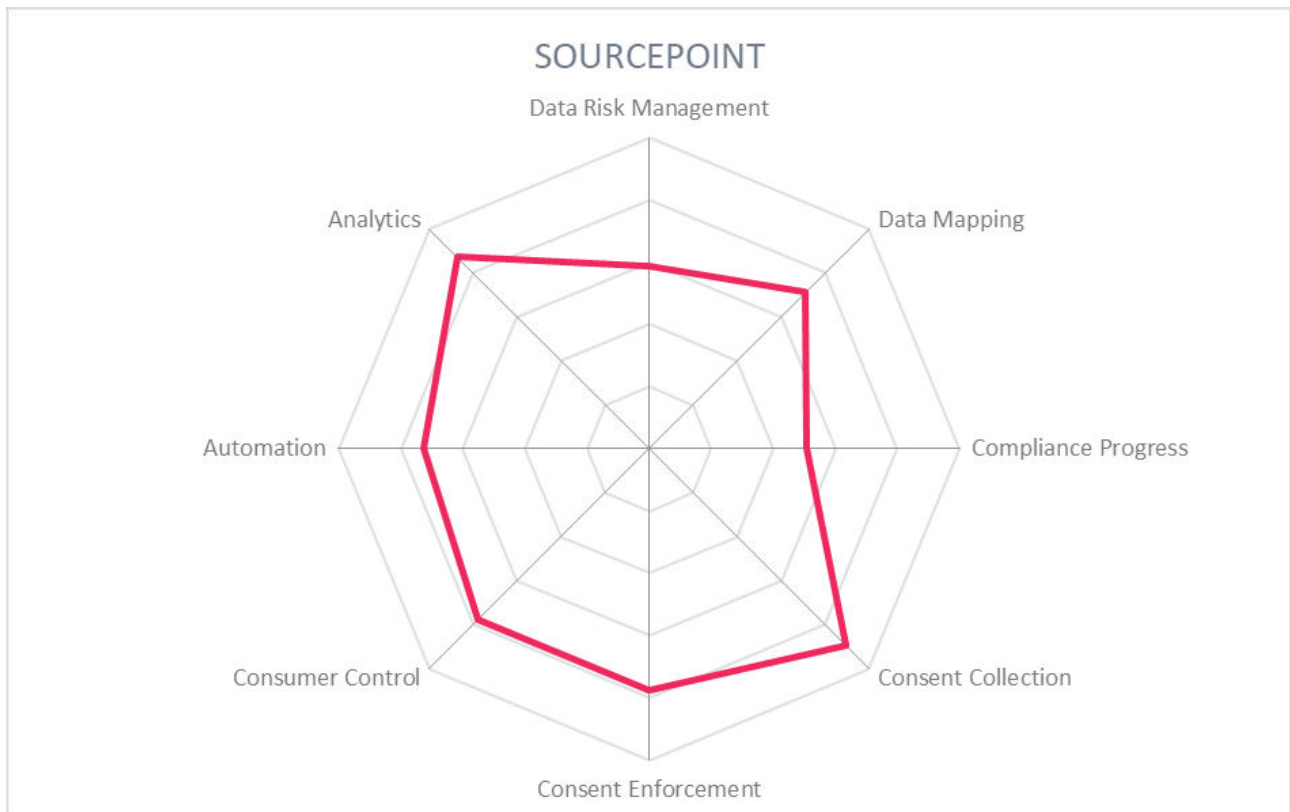
- Supports GDPR, CCPA, PIPEDA, and PDPA, Australian Privacy Act and updates, and LGPD
- Solution is ISO 27001 and ISO 27701 certified
- Allows for customers to do A/B testing with different privacy messages, formats, etc.
- Allows customers to introduce alternative compensation choices (such as whitelisting, micropayments, ad-free access, and more) to provide users access to content in case they don't want to share their personal information
- Supports app, browser, AMP pages, and over the top streaming (OTT)/connected TV
- Provides a module with customization and automation for the end-user's DNS/DSAR process
- Validated for IAB TCF 2.0 for web, mobile, and OTT, and can support custom frameworks and interactions
- Authenticated Consent based on end-user identity
- Privacy Lens is a unique offering for brand safety
- Supports multi-cloud deployments

Challenges

- No SIEM integration available, but maintains logs for all critical systems
- SOC 2 Type 2 certification is in progress
- Communication with non-compliant vendors is handled manually
- Functionality could be expanded by extending scan to include unstructured data

Leader in





5.8 Syrenis

Syrenis was founded in 2000 and is based in the UK. It is a data management company, with its flagship product Cassie being a personal information management system with intelligent features. It has a strong history of working with governments on privacy compliance. Syrenis aims to change the relationship that marketers have with end-user data to one that is proactive and non-exploitative, and is able to handle all major privacy regulations.

Cassie creates a single source of truth for all consent and preference data, including metadata to facilitate consent management across multiple domains. All PII and consents from connected systems, apps, websites, and devices are collected and harmonized this data. This includes data discovery for Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA) and data mapping for Record of Processing Activity (RoPA), determining lawful basis for collection, and security of processing activities. These data flows can be automated and generate visual data maps with cross-border transfers. Structured and unstructured data, surrounded by an API layer, is injected into the platform with a bulk data loader. Ongoing privacy and marketing data management handles cookie consent, privacy policies, preferences, and subject access requests. Customer is able to define the type of consent desired and insert the relevant code into the customer's website for consent collection in the form of a widget.

Data mapping shows how and where the data is being processed, tracks processes, and flags processes that should be formally documented. The dashboard contains key metrics about cookie consent collection, with options to embed in Zoho Analytics or export to other BI platforms.

For online cookie management, a proprietary scanner is used and can be run on demand or scheduled to run at regular intervals. Targeted consent collection allows cookie notifications to be geolocation specific. Cookies are blocked from loading until an end-user provides consent. Consent collection is also possible via email links and smart phone apps. OOTB or customizable cookie banners are auto-populated with the results of the scan. Cookie scripts can be added directly in Cassie to be dropped on a webpage or facilitated with a tag manager that receives signals from Cassie on when to fire scripts. Cassie serves the authenticated web particularly well in regards to streaming services with robust APIs.

End-users have access to a self-service Preference Center with 2Factor or ADFS authentication to limit unauthorized access to their information. The Preference Center has integrations with Salesforce or general API layer. Administrators have a portal where data processing are defined and mapped. Cassie detects data that has not been defined in a process as well as active processes that haven't been defined, and flags them on the portal to be addressed. The portal provides access to real-time data geared towards marketing departments, business users, and legal teams. A Cookie Module, a cookie widget inserted into the customer's website to block cookies from firing until consent is provided. A cookie banner is automated to match the jurisdiction of the end-user. Consent policies are enforced within Cassie by preventing data from being available to downstream systems until consent is collected.

Cassie is a cloud-based, SaaS application, hosted in AWS with instances in the UK, Europe, North America, and Australia. Hybrid and multi-cloud deployments with options for serverless and containerized

environments are possible. A secure API layer surrounds the user interface, and integrations with tag managers are available. Full auditing records are kept with every interaction and update made by the end-user. Cassie has integrations with major marketing automation and Email Service Providers (ESP). To Syrenis, fine-grained means collecting specific preferences to drive end-user consent.

Syrenis is a very strong privacy and consent solution for all verticals. It performs well in all areas, and offers exceptional control for end-users over their data.



Strengths

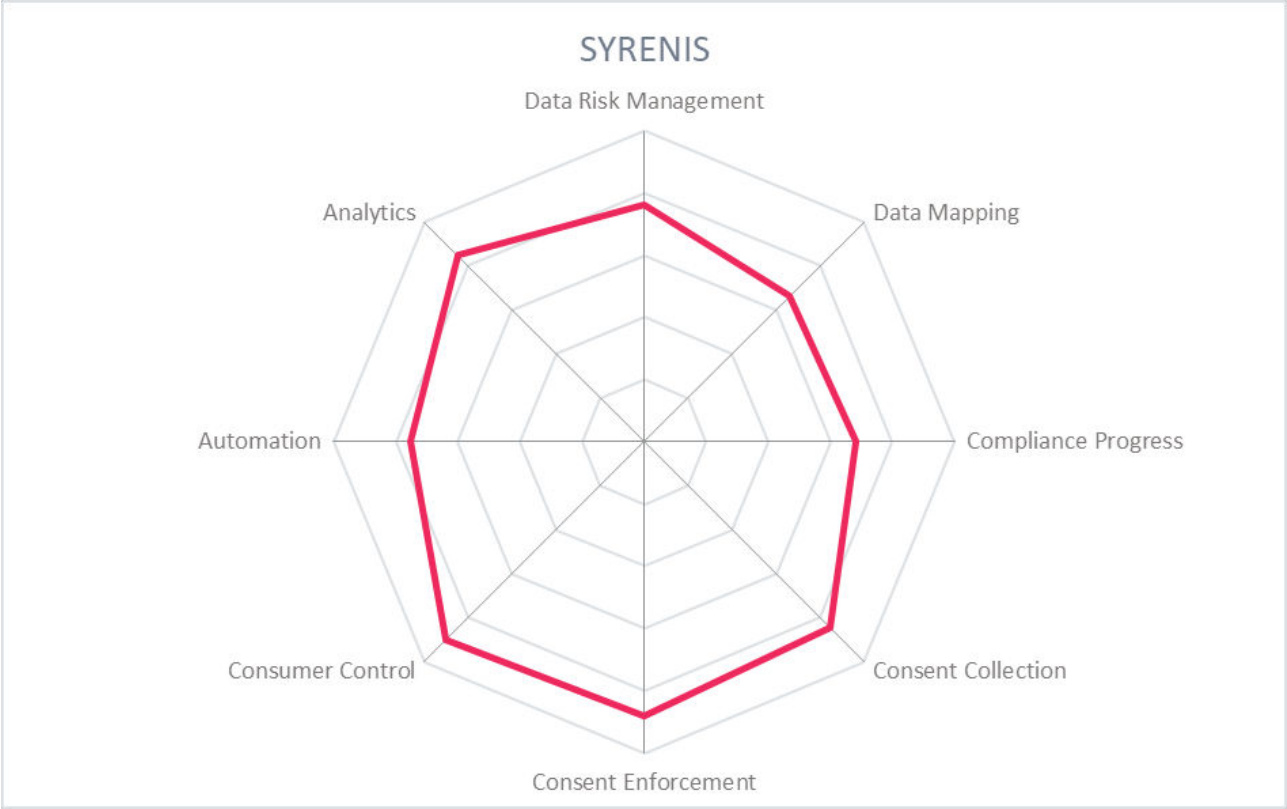
- Supports GDPR, CCPA, PIPEDA, and PDPA, Australian Privacy Act and updates, and HIPAA
- Platform creates a single source of truth at meta-data level
- Strong automation capabilities
- Is IAB compliant
- Data visualizations assist in tracking compliance progress
- Solution serves as a single source of truth for consent and end-user data
- End-user access to self-service portal has authentication services for increased privacy
- Integrations with major authentication standards like Kantara, SAML, OpenID Connect, and OAuth
- Supports multi-cloud deployments

Challenges

- Simple deployments are ready in a matter of days, but clients with more complex integrations may see a relatively long service roll-out of 1-6 months
- May need identity verification for DSR processes
- Automated data mapping could add non-web-connected systems and data

Leader in





5.9 TrustArc

TrustArc was founded in 1997 and is based in San Francisco, California. The TrustArc platform supports the major privacy regulations, as well as being flexibly able to meet future regulatory needs. TrustArc provides a comprehensive and automated privacy solution that helps customers first understand their data and responsibilities, then build and implement a privacy program complete with reporting. TrustArc's PrivacyCentral solution is the command center that that helps organizations identify and manage their privacy regulations and privacy requirements.

TrustArc's approach is to provide simplified visibility into the compliance needs of an organization, and designing a privacy program supported by automated workflows. TrustArc and its 2019 acquisition Nymity have developed proprietary frameworks to meet the privacy requirements of the major global regulations. Supported by the Nymity Research, Operational Templates, Law Comparisons, and Legal Summaries products, TrustArc gives customers the tools to stay informed about privacy regulation with curated news stories available on the platform. TrustArc supports the planning and prioritizing stage of a compliance program with Assessment Manager, Planner & Benchmarks, and Risk Profile products. Risk profiles and DPIA/PIA assessments are available for customers to help business users identify non-compliant data activities, data inventory and mapping provides the business user with audit trails. A risk algorithm dynamically generates risk profiles by detecting if factors of the global privacy regulations from 130 countries are present in the data inventory records.

Implementation is supported by the Data Inventory Hub, Individual Rights Manager, Cookie Consent Manager, and Website Monitoring Manager. The Cookie Consent Manager initiates with a website scan to detect first and third-party trackers. The results are automatically categorized into standard categories. Customers can customize the cookie consent notifications to meet privacy regulations and their own marketing goals, which is implemented on all customer websites with a single JavaScript tag. DSARs can be managed, processed automatically with integrations into major systems, and reports generated on the platform, and the solution offers integrations with the major tag management systems. Many of these capabilities are supported by the intelligence engine.

TrustArc provides features to enable customers to track their own compliance, and customers may be certified through TrustArc's certification subsidiary, TRUSTe. Demonstrating compliance is supported by Attestor, Risk Profile, Awareness Tracker, and Dashboard products. Records of assigned compliance tasks are produced as well as other material for audit reports. TrustArc provides workflows to assist customers to intake and respond to DSARs with full audit trails.

The TrustArc platform is available as single products, or as the suite. The platform is a SaaS, cloud-based solution. TrustArc is building tools to support automatic detection of cross-border transfer obligations. TrustArc's Assessment Manager tool can be used for incident management checklists.

TrustArc is one of the more mature players in this market, with years of experience. Their robust data inventory and mapping capabilities enable customers to gain analytical insights on their data, as well as see the gaps in their journey towards compliance. TrustArc gives a strong focus on audits, assessments, and

providing a simplified overview of complex privacy initiatives.

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



Strengths

- Supports GDPR, CCPA, PIPEDA, and PDPA, Australian Privacy Act and updates, LGPD, and many others
- Supports the IAB Framework
- Parent organization of independent certification organization TRUSTe
- Has options for automation and intelligent recommendation for compliance plan
- Data inventory is able to include text as well as video, image, and audio.
- Integrations with OAuth and SAML, as well as data analytics such as BigID and Sherpa
- Has support for Schrems II data transfers
- Robust assessment and audit capabilities

Challenges

- Can add PAM for solution access management
- Support for the Kantara Initiatives would make this solution even stronger
- No integrations with SIEM environments
- Could add ISO 27001 and SOC Type II certifications and hardening methods
- More consumer control over consent decisions could be offered in customer portal
- Product does not yet include preference management, but is on the roadmap
- Product could have whitelabel option
- Could add support for multi-cloud deployments

Leader in



TRUSTARC



6 Vendors and Market Segments to Watch

6.1 BigID

BigID, based in New York, is a data intelligence platform that harnesses AI and ML to understand what identities and related attributes are within a particular data landscape of an organization. While it does not include consent and preference management, the BigID Data Intelligence Platform manages many of the other key capabilities of this Leadership Compass: data mapping with PI/PII discovery, workflows for CCPA Data Rights Automation, GDPR Records of Processing Activity and DSR fulfillment, and many integrations with third-party systems such as AWS, Microsoft, OneTrust, Salesforce, SAP, and ServiceNow.

Why worth watching: Watch this vendor if you need a privacy-focused data intelligence solution to complement your Privacy and Consent Management solution, or if it expands into the Consent Management space.

6.2 Consenteye

Founded in 2017, Consenteye is a privacy and MarTech solution. It enables organizations to create privacy agreements, collect consents and preferences, generate insights on opt-in data, and generate audit trails. It offers webhooks for real-time data updates, data encryption, and integrations with CRM systems.

Why worth watching: Watch this vendor increase its global reach for Privacy and Consent Management solutions.

6.3 Crownpeak

Founded in 2001 and headquartered in Denver, Colorado, Crownpeak works to transform the user experience into one that operates on a foundation of privacy. The product suite delivers a unified consent solution and additional products: AppNotice for enabling native mobile app compliance, Tag Auditor with Trackermap to give marketers full visibility on all tracking technology on their website, and TagControl to monitor and proactively manage which tags are requesting customer data.

Why worth watching: Crownpeak is a strong contender to deliver high functionality for discovering tracking technology, giving options to customers to restrict certain cookies and tags from firing on a site, managing

numerous domains with ease.

6.4 Cybot

Cybot is based in Copenhagen, Denmark, and was founded in 2012. Its product, Cookiebot, is a focused solution for compliant cookie and tracker management. Their patent-pending scanning technology simulates customer behavior for all possible actions on a website, for example opening all subpages, following links, and putting items into a shopping cart. The scan contributes to Cookiebot's ongoing global cookie repository with descriptions of each cookie's purpose.

Why worth watching: Watch this vendor for a robust cookie management solution with cutting-edge technology.

6.5 iubenda

iubenda was founded in 2011, and is based in Italy. The suite of products includes the Privacy and Cookie Policy Generator, Cookie Solution, and Consent Solution. Its existence pre-GDPR gives it a compliance philosophy that is independent of the recent data privacy legislations, but rather works for 360-degree compliance for a website. It serves a range of customers, from small blogs to large corporate publishers.

Why worth watching: Watch this vendor for a solution ready for any industry, offering a high degree of confidence to deliver legal texts in multiple languages, and providing means to track consent for services beyond just cookies.

6.6 Quantcast

Quantcast was founded in 2006 and is based in San Francisco. It is an analytics and marketing-forward solution with a privacy module, geared towards publishers. Quantcast aims to achieve several privacy objectives: to provide notice to end users in compliant ways, to gather end users' preferences, communicate these preferences downstream in a standardized way, and generate an audit log of all interactions.

Why worth watching: Quantcast is a strong option for marketing-focused publishers of all sizes, and its CMP capabilities are strong with a mature and focused solution to complement other privacy products.

6.7 Usercentrics

Usercentrics was founded in 2018, and is based in Germany. Its Consent Management Platform (CMP) takes a marketing analytics approach to managing end user consent with constant improvements to provide customers with effective online-marketing performance within compliance frameworks.

Why worth watching: Usercentrics is a relatively new player but with a strong presence with enterprise clients in a wide variety of industries.

7 Related Research

[Leadership Compass: Privacy and Consent Management -- 80199](#)
[Leadership Compass: Identity Governance & Administration 2021 -- 80516](#)
[Leadership Compass: Privileged Access Management -- 80636](#)
[Buyer's Guide: Core Features of Privacy and Consent Management Solutions -- 80198](#)
[Whitepaper: California Consumer Privacy Act: The Need for Data-Centric Security -- 80136](#)
[Advisory Note: Maturity Level Matrix for GDPR Readiness -- 72557](#)
[Leadership Brief: Six Key Actions to Prepare for CCPA -- 80353](#)

Methodology

About KuppingerCole's Leadership Compass

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

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

Types of Leadership

We look at four types of leaders:

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

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

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- ****Security**
- **Functionality**
- **Deployment**
- **Interoperability**
- **Usability****

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

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

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

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

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

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

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

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

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

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

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

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

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

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

Rating scale for products and vendors

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

Strong positive

Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability.

Positive

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

Neutral

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

Weak

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

Critical

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

Inclusion and exclusion of vendors

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

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

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

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will

provide regular updates on their Leadership Compass documents.

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

Content of Figures

Figure 1: Privacy and Consent Management Solutions, Possible Areas of Functionality

Figure 2: The Overall Leadership rating for the Privacy and Consent Management market segment

Figure 3: Product Leaders in the Privacy and Consent Management market segment

Figure 4: Innovation Leaders in the Privacy and Consent Management market segment

Figure 5: Market Leaders in the Privacy and Consent Management market segment

Figure 6: The Market/Product Matrix

Figure 7: The Product/Innovation Matrix

Copyright

©2022 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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

KuppingerCole, founded 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.