KuppingerCole Report

LEADERSHIP COMPASS

By Anne Bailey
August 25, 2020

# Privacy and Consent Management

This report provides an overview of the market for Privacy and Consent Management platforms and provides you with a compass to help you to 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

Nearly all enterprises have an online presence and seek to better serve their customers and end-users by understanding who they are and what they want. Compiling customer profiles from personal interactions has long been standard practice to deliver personalized services, but data collection in the era of tags, cookies, and numerous other technologies that reside on web browsers to gather information are now considered essential for marketing and functional purposes. Many are first-party technologies set by the site owner, and many are set by third parties that elongate the data value chain beyond the organization's boundaries. The implicit consent from end-users that such cookies and trackers are active on any site that they visit has been the modus operandi since the mid-1990s, with their derived insights gaining sophistication over time.

Cookies and trackers are highly desirable from a marketing perspective but generate concerns for privacy and use of data without the consent of end-users. There is a wave of privacy regulations across the globe that have been or will be released: EU GDPR, US CCPA, Canadian PIPEDA, Singaporean PDPA, Australian Privacy Act, Brazilian LGPD, Japanese APPI, Indian PDPB, Russian 152-FZ, and many more. Most countries require privacy policies on websites as part of their privacy laws. Vendors did offer enterprise tools to safeguard the privacy of their customer data before the 2018 GDPR, but its and the subsequent release of other privacy regulations have stimulated the growth of Privacy and Consent Management solutions, and increased the demand for solutions that offer a path to compliance.

This Leadership Compass analyzes vendors in the Privacy and Consent Management segment that provide tools to manage cookie consent, preference management, privacy statements, data usage, and compliance for global data protection and privacy regulations. These solutions are often called Consent Management Platforms (CMPs), a user interface for end-users to register or revoke their consent and adjust their preferences. There is a clear trend that prioritizes cookie consent management for ePrivacy compliance for companies in the publishing industry, but we consider this market segment to have a broader definition to include privacy tools for all verticals and for data collected via channels other than browser cookies, attempt to integrate principles of privacy-by-design, and innovative efforts to align the – at times – conflicting needs of marketing and legal departments.

You gain a full insight into the Privacy and Consent Management market with this report. 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 Market Segment

The enterprise Privacy and Consent Management market segment has its roots in processes for the

responsible collection and handling of customer data, but has recently entered the public consciousness with the rollout of GDPR regulations and mass data breach scandals. Strict, binding regulation and strong public demand have attracted new entrants to this segment. This has yielded a dynamic and competitive space where vendors provide the means to collect consent for processing of end-user data.

This Leadership Compass analyzes vendors in the Privacy and Consent Management segment that provide tools to manage cookie consent, preference management, privacy statements, data usage, and compliance for global data protection and privacy regulations. These solutions are often called Consent Management Platforms (CMPs), a user interface for end-users to register or revoke their consent and adjust their preferences with an administrative dashboard for a customer to customize privacy policies, cookie notifications, and integrate with marketing systems, CRM systems, and analytics platforms. There is a clear trend that prioritizes cookie consent management for ePrivacy compliance for companies in the publishing industry, but we consider this market segment to have a broader definition to include privacy tools for all verticals and for data collected via channels other than browser cookies. Solutions should attempt to integrate privacy-by-design principles, and make innovative efforts to align the – at times – conflicting needs of marketing and legal departments.

The current rapid growth of the Privacy and Consent Management segment for enterprises is dependent on the opposing pressures of marketing technology and the increasing number of privacy regulations. In an ideal world the goals of these departments should be aligned, and with the help of innovative products in the privacy space, they can be. Marketing technology (MarTech) has a strong influence on a company's revenue, nearly irrespective of industry vertical. In the publishing and content-production industry, revenues can be solely dependent on advertisements and successfully understanding the end-user's behaviors and interests to deliver personalized ad experiences. This strategy is heavily dependent on collecting personal data from end-users, often through cookies and tracking technology. Collection of this data has come under heavy scrutiny in recent years, with regulation eventually following. The EU was the first region to take meaningful action with the GDPR, ePrivacy Directive, and PCER in the UK. Other regulations from the US and globally are in development, among these being the California Consumer Privacy Act (CCPA). The concern over end-user privacy and data usage predates the 2018 GDPR, and many of the vendors assessed in this Leadership Compass have been offering privacy solutions before the GDPR was enforced.

Although Privacy and Consent Management solutions are necessary in all verticals, the business models of publishers and content creators are especially intertwined with the collection of end-users' data. This causes publishers to have very complex and multi-layered tag and tracker ecosystems. Many CMPs are primarily concerned with creating transparent and standard data exchanges between publishers, advertisers, and the vendors that fire third-party http/JavaScript cookies, HTML5 Local Storage, Flash Local Shared Object, Isolated Storage, IndexedDB, ultrasound beacons, and pixel tags. Gathering consent and implementing end-user choices can be relatively straight-forward for first-party owned cookies and trackers – those that are set by the organization owning the website they are fired on – as the process can be managed internally, although this is challenging for companies that own numerous domains and high volumes of site visitors. First-party control of third-party tech and wholly third-party cookies are cookies that belong to a domain that is different than the hosting website, and implementing end-user choices means interacting with external vendors. Piggyback tags are usually from third-party vendors that are invoked by another tag, making it possible for third parties to set cookies on a website without the site owner's permission or knowledge. These cookies and trackers have many purposes, including personalization and collection of preferences, session management and login activities, and tracking end-user browsing behavior.

Data usage is a key aspect of protecting the privacy and enforcing the consent choices of end-users. Effectively communicating an end-user's consent choices to relevant departments within an organization as well as to downstream partners in the digital advertising chain is critical to a Privacy and Consent Management solution. This is typically achieved in one of two ways, and sometimes in combination: either by scanning websites for cookies and trackers then blocking these from firing until adequate consent has been collected, or by following the IAB Europe Transparency and Consent Framework (TCF) that whitelists compliant cookie and tracker vendors and proactively communicates via standardized signals. A non-exhaustive list of other data usage aspects that should be considered are: data protection (including data minimization, storage limitation, etc.), breach notification, consent per purpose, extension of data subject rights (such as the right to be forgotten), data portability, Data Protection Impact Assessments (DPIA). Privacy-by-design that considers these aspects should be a goal for all Privacy and Consent Management solutions.

At this point, there are no universally recognized interoperability standards for Privacy and Consent Management. There is a voluntary framework called the IAB Europe Transparency and Consent Framework (TCF) to assist participants in the digital advertising chain – including publishers, advertisers, vendors, and Consent Management Platforms (CMPs) – to meet the requirements of the ePrivacy Directive and GDPR. This is heavily focused on cookie and tracker management by establishing standard signals that indicate an end-user's consent choice to easily and instantaneously communicate with participants downstream. There are four aspects to the TCF: a Global Vendor List, a Transparency and Consent (TC) String for data storage, an API for Consent Management Providers or Platforms (CMPs) to create and process the Transparency and Consent String, and the governing policies of the TCF. Many solutions covered in this Leadership Compass that specifically serve the publishing industry are certified IAB CMPs, meaning that they offer an option to their customers to configure the CMP according to IAB specifications. The benefits of such a framework include the ability to identify cookie vendors who are also part of the framework, which increases the transparency and auditability of data and consent collection throughout the digital advertising chain.

An IAB compliant cookie notice shows different categories for cookies than the typical four of strictly necessary, functional, marketing, analytics. These different categories are personalization, linking devices, experience enhancement, precise geographic location data, and provides information on individual vendors. In an IAB-compliant CMP, consents and preferences are packaged in a standardized payload called the TC String, which carries additional information such as the metadata, legitimate interest, publisher restrictions, and specific jurisdiction disclosures. The API provided by the TCF is a standardized means for parties in the digital advertising chain – being a hosting publisher, CMP, or an advertising vendor – to access the consents and preferences in the TC String.

The uncertainty that impending regulation brings for companies creates the conditions for this market segment to develop rapidly. But until the regulatory environment is stable, the Privacy and Consent Management segment will continue to grow with a variety of service offerings to help businesses achieve privacy compliance.

## 1.2 Delivery models

This Leadership Compass accepted vendors regardless of delivery model, although most are SaaS with an

option to deploy on-premise if requested. Vendors that have a strong IAM background deploy on-premise as well.

Privacy and Consent Management solutions have several different approaches that differentiate the suitability of solutions to different contexts.

**Analytics/marketing approach vs. compliance approach:** solutions tend to have either an analytics and marketing background, or a compliance background. This orients the solution to a slightly different audience within the customer's organization: either the marketing department by prioritizing the collection of preference data and maximizing the number of consent opt-ins, or the legal department by emphasizing privacy and compliance training for organizations, tools to measure an organizations progress towards compliance, and in-house legal teams. This distinction is not always black or white. We consider the best approach to be a mixture of the two, where vendors strive to create a symbiotic relationship between legal privacy obligations and generating actionable marketing insights.

**Publishers approach vs. general approach:** Because the revenue stream of online publishers is often dependent on advertisements, data collected from cookies and trackers is the primary interaction between company and end-user. Solutions for publishers often have robust cookie consent management capabilities, but lack other systematic tools like data inventories, mapping, and tools for compliance progress. Companies in other verticals have a need for Privacy and Consent Management solutions that cover a much wider variety of interactions with end-users, and vendors that have a general approach typically have well-designed data inventory and mapping tools and integrate with CRM and email tools. Determining the better approach here is dependent on the customer's own vertical and the breadth of their compliance needs.

## 1.3 Required capabilities

When evaluating Privacy and Consent Management solutions, we begin by assessing standard criteria such as:

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

Each of the features and criteria listed above are considered in the product evaluations below. We also consider unique selling propositions (USPs) and innovative features of products that distinguish them from other offerings available in the market.

**Baseline criteria that we look for in a Privacy and Consent Management solution are:**

- Generation of privacy policy notifications
- Generation of cookie notifications
- Collection of end-user consent for cookies and trackers
- Prevention of cookie firing until appropriate consent is captured
- Reporting and auditing functions
- Means for end-user to view and update privacy and consent choices
- DSARs workflows

**Advanced capabilities we are interested in seeing as part of these products:**

- Data mapping and inventory
- Preference customization
- Detection and visualization of progress towards compliance
- Access Management
- Data Risk Management

**Inclusion Criteria**

- Support for several of the criteria above

**Exclusion Criteria**

- Solutions that only addressed end-user use cases without offering solutions for enterprise Privacy and Consent Management
- Any solution still in a prototype stage
- Solutions with a low maturity that restricts the overall functionality

We invited numerous vendors to participate in this report to provide a comprehensive overview of the current state of the market. This information should help inform you to choose a vendor that fits your specific requirements, and your current and future landscape to be managed.

# 2 Leadership

*Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help 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.*

## 2.1 Overall Leadership

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

- Product Leadership
- Innovation Leadership
- Market Leadership


Figure 1: The Overall Leadership rating for the Privacy and Consent Management market segment

The consolidated view of the Overall Leaders provides a universal impression of our rating of the vendors'

offerings in this market segment. Notably, some vendors that benefit from a strong market presence may slightly drop in other areas such as innovation, while others show their strength in the other categories while having a relatively low market share or lacking a global presence. Therefore, we strongly recommend looking at all leadership categories, the individual analysis of the vendors, and their products to get a comprehensive understanding of the players in this market.

The vendors who are Overall Leaders in this segment combine very strong all-around functionality with a solid market presence and financial security. OneTrust is a relative newcomer to the market, established in 2015, but has shown traction and significant growth in that time bringing an extremely comprehensive product to market. TrustArc was an early pioneer in the Privacy and Consent Management space and focuses on the full organization including robust data inventory and mapping capabilities, analytical insights on their data, and helping customers measure their progress towards compliance. Akamai is a well-known player in the CIAM market, which has provided a strong platform to expand its offering to include preference management. Akamai's emphasis is on delivering a preference solution that integrates well with CIAM and marketing systems and enables progressive consent to be collected only when it is needed. Syrenis brings strong cookie consent management with an intelligent engine that supports the rest of its well-rounded functionalities. iWelcome is another established CIAM vendor with very strong preference management, self-service consent management for end-users, and of course access management capabilities. Quantcast is an analytics and marketing-forward solution with a privacy module that has made significant contributions to the IAB TCF framework.

In the Challengers section we find many vendors with strong solutions in Privacy and Consent Management, but may have a smaller market share or global presence. Sourcepoint has overall high performance, with high customization specialized for the needs of large publishers, and Piwik PRO has positioned itself to be a compliance-focused alternative to Google analytics. Sovy, Usercentrics, MyLife Digital, Crownpeak, and iubenda are specialized vendors. Sovy is focused on providing an end-to-end SaaS privacy compliance solution for SMEs and multi-national enterprises with complex or decentralized legal and departmental structures. Usercentrics works to harmonize the marketing and compliance aspects to achieve the highest marketing performance for customers within the framework of respective legal requirements. MyLife Digital provides a modern consent and preference management solution that works with the dynamic customer consent journey. Crownpeak's real-time scanning and auto-blocking brings very strong cookie compliance to its consent solution. iubenda is a relative newcomer with very specific offerings for cookie consent management and preference management.

Overall Leaders are (in alphabetical order):

- Akamai
- iWelcome
- OneTrust
- Quantcast
- 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 products.


Figure 2: Product Leaders in the Privacy and Consent Management market segment

Product Leadership is where we examine the functional strength and completeness of the vendors' solutions.

OneTrust, Akamai, Syrenis, TrustArc, and Sourcepoint are all Product Leaders. Solutions that are Product Leaders strive to protect end-user privacy in a holistic way, often incorporate intelligent aspects to flag compliance issues, have safeguards in place to protect against unauthorized access and cyber incidents, and make significant efforts to extend privacy protection beyond the organization for a more privacy-centered marketing environment. OneTrust has very strong overall capabilities. Akamai also demonstrates high product functionality, bringing particular expertise in Access Management. Syrenis and TrustArc both deliver the core Privacy and Consent Management capabilities with slightly different approaches; Syrenis focuses particularly on the needs of the marketing segment which is reflected in the capabilities it builds up, while TrustArc takes a wider lens and puts more emphasis on demonstrating the customer's progress towards compliance. Sourcepoint joins the ranks of Product Leaders with its detailed control for end-users, preference customization, and approach to managing cookies and trackers.

The Challengers offer competitive solutions that have been designed to meet the varying needs of different industries. Each of these vendors presents their Privacy and Consent Management solution in combination with compliance, CIAM, analytics, or marketing tools. The Challengers section includes Sovy, Piwik PRO, Crownpeak, MyLife Digital, Usercentrics, iWelcome, Quantcast, and iubenda. These vendors generally deliver excellence for select capabilities.

Product Leaders (in alphabetical order):

- Akamai
- OneTrust
- 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.

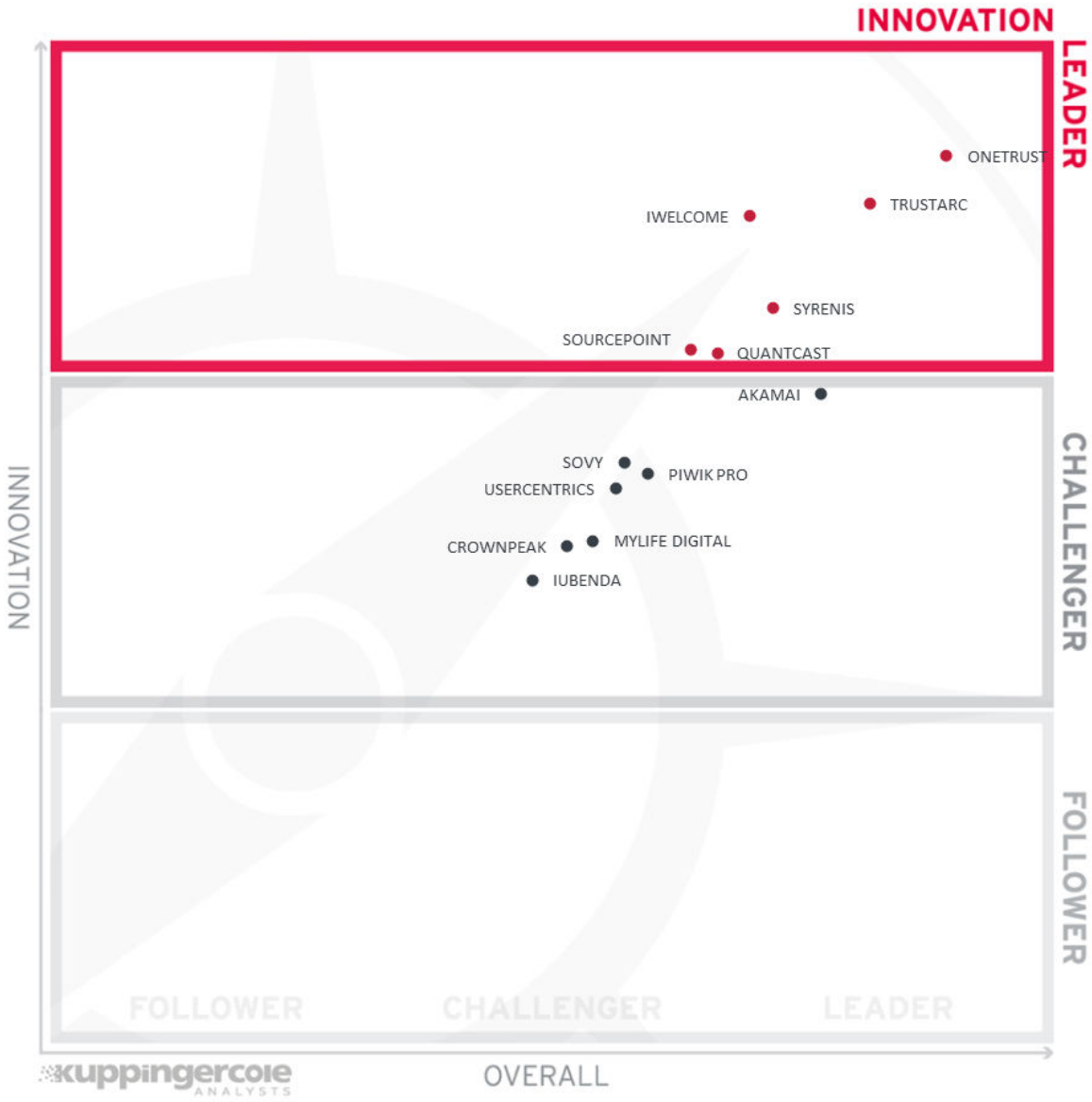



Figure 3: Innovation Leaders in the Privacy and Consent Management market segment

Innovation is spread across this market segment. In the Leaders section we see OneTrust, TrustArc, iWelcome, Syrenis, Sourcepoint, and Quantcast. OneTrust has experienced rapid growth through product success and numerous acquisitions, and their comprehensive product is supported with an intelligence engine. TrustArc has employed intelligent features to support end-to-end privacy and enabling automation. iWelcome's focus on developing attribute-level consent and Just-in-Time consent bring more mutual benefit to enterprises and end-users. Syrenis has incorporated automation supported by an intelligent engine for across-the-board functionality. Sourcepoint's approach towards Privacy and Consent Management is multifaceted, working to provide authenticated consent, improving an end-user's profile specificity and

experience. Its and Quantcast's effort to standardize consent signals is a valuable contribution to the industry.

The Challenger section includes Akamai, Sovy, Piwik PRO, Usercentrics, MyLife Digital, Crownpeak, and iubenda. All these vendors have also been able to demonstrate promising innovation in delivering specific Privacy and Consent Management capabilities. Please refer to the vendor pages below in section 5 of this report for more details.

Innovation Leaders (in alphabetical order):

- iWelcome
- OneTrust
- Quantcast
- Sourcepoint
- Syrenis
- 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 4: 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 or vendors with limited geographical reach, limited industry focus, or relatively smaller customer base.

The Market Leaders in this segment are OneTrust, Quantcast, TrustArc, Akamai, and iWelcome. Aside from OneTrust, these are established vendors with pre-GDPR experience in privacy and with foundations in either analytics or IAM. OneTrust is a more recent entrant, still with pre-GDPR privacy experience, but has quickly gained a large usership in both the US and European region. TrustArc is primarily present in the North American Market, Quantcast and iWelcome in the European market, and OneTrust and Akamai active

in both markets.

The Challengers include the relatively smaller vendors that do have a presence in their local markets but do not yet have a significant global presence. Near the Leader section we find Syrenis and Piwik PRO. Clustered together are MyLife Digital, Usercentrics, iubenda, Sourcepoint, Crownpeak, and Sovy whose placement is affected by several factors, geographical reach being one of them.

Market Leaders (in alphabetical order):

- Akamai
- iWelcome
- OneTrust
- Quantcast
- 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. 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.

## 3.1 The Market/Product Matrix

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

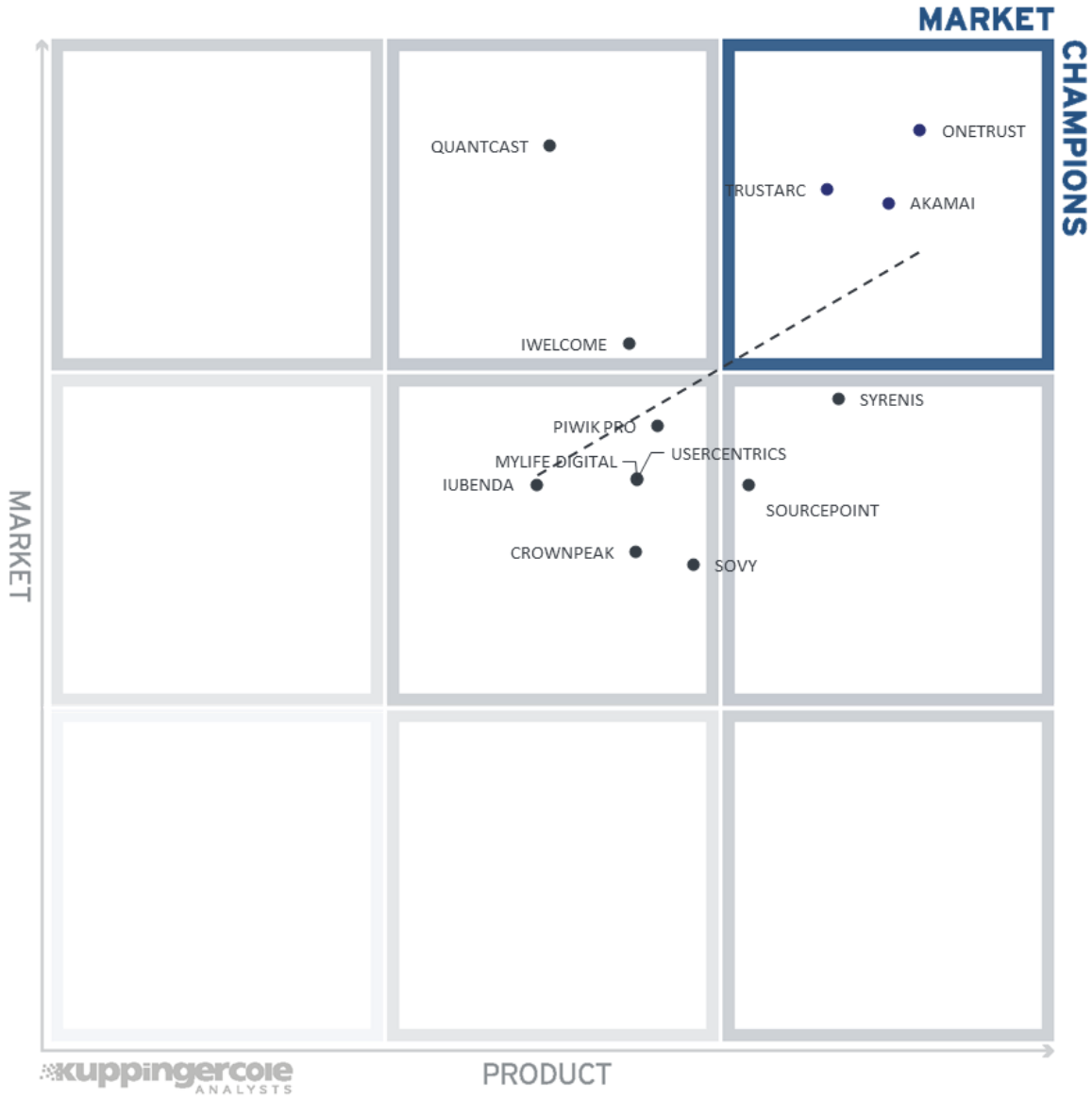



Figure 5: The Market/Product Matrix

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

Akamai, OneTrust, and TrustArc are ahead of the others, with strong ratings in both Product and Market Leadership.

In the upper middle section we have Quantcast, which has a very strong market position compared to its more focused solution. iWelcome’s market position is also strong. iubenda is financially performing well

given its size and product comprehensiveness. MyLife Digital, Piwik PRO, and Usercentrics are relatively balanced in terms of their market and product leadership. Syrenis, Crownpeak, Sovy, and Sourcepoint all provide strong products but have room for growth and expanding their 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.

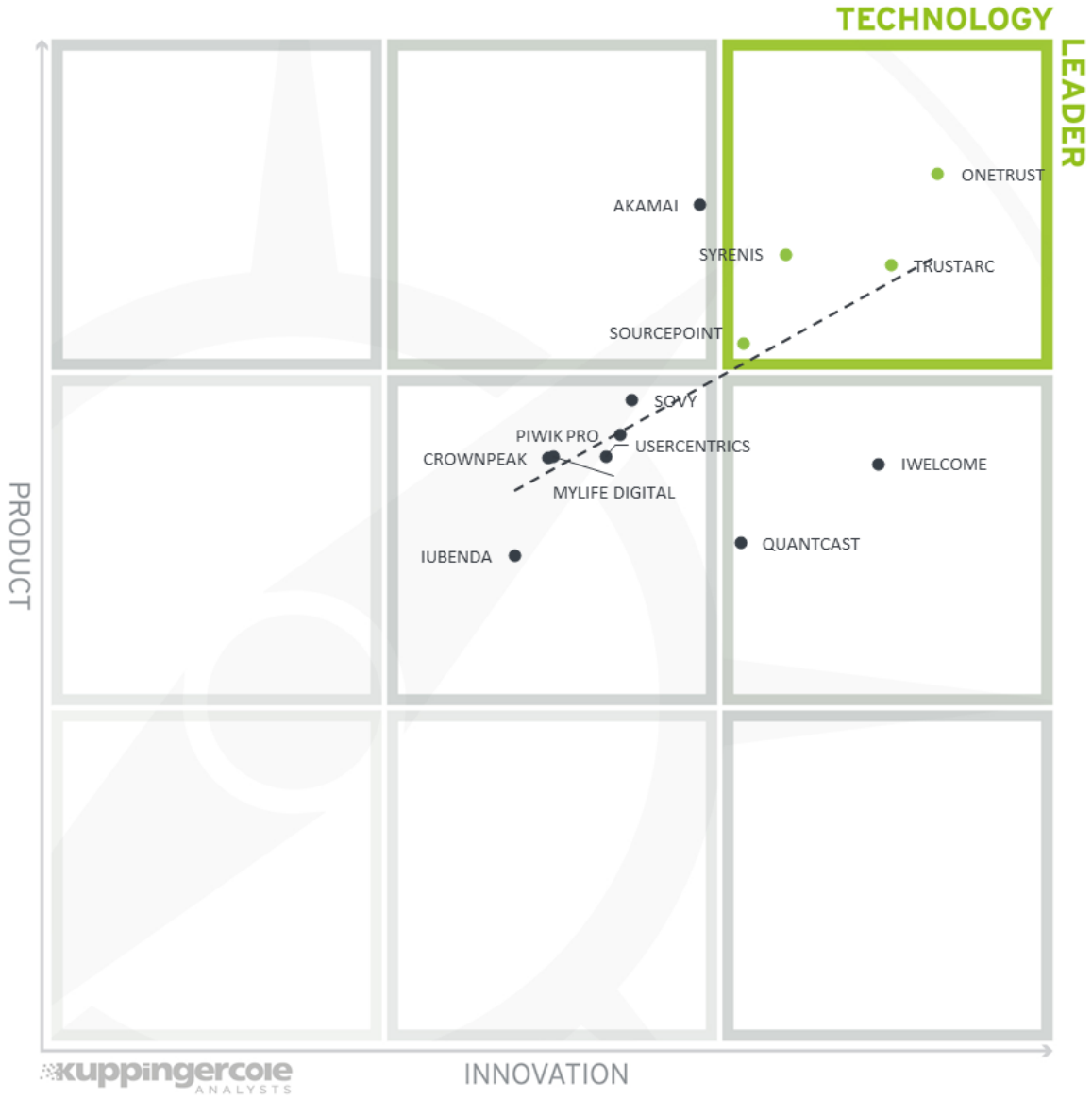



Figure 6: The Product/Innovation Matrix.

Vendors below the line are more innovative, and 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. Syrenis, TrustArc, and Sourcepoint also demonstrate high innovation paired with well-rounded product capabilities. Akamai shows higher product functionality relative to its innovativeness.

We find the majority of our vendors in the center of the matrix. Sovy, Piwik PRO, Usercentrics, Crownpeak, MyLife Digital, and iubenda demonstrate a relative balance between product capabilities and

innovativeness. iWelcome and Quantcast are overperforming in terms of their innovativeness, with iWelcome's work on integrating privacy control with identity, and Quantcast's efforts to standardize consent signals.

## 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.


Figure 7: The Innovation/Market Matrix

Vendors below the line are more innovative, vendors above the line are – compared to the current Market Leadership positioning – less innovative. The matrix for Privacy and Consent Management solutions shows a wide spread of market position and innovativeness. Although a few are clustered around the line, most show a dominance in market position or innovativeness.

OneTrust, TrustArc, Quantcast, and iWelcome are categorized as vendors with a strong market presence with innovativeness. Akamai is seen in the top center of the matrix with relatively larger market presence than innovative strategies. Conversely, Syrenis and Sourcepoint involve more innovative practices, and are still working towards market growth.

Piwik PRO, UserCentrics, MyLife Digital, iubenda, Crownpeak, and Sovy demonstrate balance between market strength and innovation.

# 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. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

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 |
|---|---|---|---|---|---|
| Akamai Identity Cloud Preference Center | ● | ● | ● | ● | ● |
| Crownpeak Universal Consent Platform | ● | ● | ● | ● | ● |
| iubenda Privacy and Cookie Policy Generator, Cookie Solution, Consent Solution | ● | ● | ● | ● | ● |
| iWelcome CIAM | ● | ● | ● | ● | ● |
| MyLife Digital Consentric | ● | ● | ● | ● | ● |
| OneTrust OneTrust Privacy Management Suite | ● | ● | ● | ● | ● |
| Piwik PRO Analytics Suite with Consent Manager | ● | ● | ● | ● | ● |
| Quantcast Choice | ● | ● | ● | ● | ● |
| Sourcepoint CMP | ● | ● | ● | ● | ● |
| Sovy GDPR Privacy Essentials | ● | ● | ● | ● | ● |
| Syrenis Cassie | ● | ● | ● | ● | ● |
| TrustArc Privacy Management Platform | ● | ● | ● | ● | ● |
| Usercentrics Consent Management Platform (CMP) | ● | ● | ● | ● | ● |
| Legend | | ● critical | ● weak | ● neutral | ● positive ● strong positive |

In addition, we provide 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 |
|---|---|---|---|---|
| Akamai | positive | strong positive | strong positive | strong positive |
| Crownpeak | positive | positive | neutral | positive |
| iubenda | positive | positive | strong positive | positive |
| iWelcome | strong positive | positive | positive | strong positive |
| MyLife Digital | positive | positive | positive | neutral |
| OneTrust | strong positive | strong positive | strong positive | strong positive |
| Piwik PRO | positive | positive | strong positive | positive |
| Quantcast | positive | strong positive | strong positive | strong positive |
| Sourcepoint | positive | positive | neutral | positive |
| Sovy | positive | positive | neutral | positive |
| Syrenis | positive | positive | strong positive | positive |
| TrustArc | strong positive | strong positive | strong positive | positive |
| Usercentrics | positive | positive | positive | positive |
| Legend | critical | weak | neutral | positive | strong positive |

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

# 5 Product/service evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass. 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 Leadership Compass on Privacy and Consent Management solutions, we look at the following six categories:

- Cookie & Tracker Approach
  The approach the solution takes to detect cookies and trackers, to categorize and populate a cookie notification with options for automation, and to prevent cookies from firing before consent is collected.
- Preference Customization
  The ability and level of detail with which the solution can collect end-user preferences with consent. It should include preference collection from multiple channels such as browser widget, email, access from a consumer portal, and manual functions to facilitate updates from personal interactions.
- Compliance Progress
  The methods a solution uses to enable a customer to understand what gaps or failures to meet privacy regulation exist in their system, and provide meaningful ways to identify, communicate, and visualize progress over time to achieve privacy compliance for specific regulations.
- Consumer Control
  The methods a solutions uses to enable end-users to retrospectively update their privacy profile, including the degree of control they have, what preferences and privacy information they can view and update, and the channels by which they can make these changes.
- Policy Enforcement
  The means by which end-user consent decisions are communicated, collected, stored, and enforced. This should include localized storage of data, coordination with third-party cookie and tracker vendors, and integrations with internal systems.
- Access Management
  The ability of the solution to support multiple identity types, standards, protocols, and tokens. This includes the ability of users to requesting access, of managers approving that access, and of solutions that help in managing and optimizing roles in target systems.

- Data Mapping/Inventory
  The ability of the solution to categorize, display, and manage private data within the customer's system. This could include automated or semi-automated data discovery, classification, mapping of internal and cross-border processes.
- Data Risk Management
  The ability of the solution to prevent against incidents that would jeopardize end-user data. Certifications, integrations with SIEM and other preventative actions are included.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while are strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of Privacy and Consent Management technologies.

## 5.1 Akamai

Akamai Identity Cloud is a CIAM solution with a customer trust and consent module. Its main features are control of consent settings by end users, progressive permissioning, and compliance with multiple jurisdictions' privacy regulations. This solution is suited for all industry types that require a Customer Identity and Access Management (CIAM) solution.

Being a CIAM solution with consent and privacy management built in, it offers identity management as a platform or software as a service. At the point of sign-up or login, an end-user is presented with a detailed legal consent to gather initial consent on trackers, privacy policy, and terms of service. Consent is collected through many different methods: popups and modal windows, emails, and payment interactions. When a customer changes their consent, for example opting out of a service they had previously agreed to (an email newsletter), an automated webhook is sent in real-time to all relevant systems, or implemented as a patch, to enforce the end-user's new preference immediately.

Progressive profiling allows the customer to build a continuously more detailed understanding of each end user, but with detailed versioning and audit trails for end-user consent. Administrators can add a product to a "wish-list" for a particular end-user, and the preference center sends a one-off consent to the end-user to provide more personalized content. The preference center can gather billing information that when consent is given, can deliver data downstream to CRM systems, or integrate with payment systems. Audit logs include a high degree of detail on how consent was collected for each item, including from what device, date and time, and the change of consent from one status to another. Administrators may track the level of consent collection by searching for end-users by attributes, such as birthdate, client ID, having been presented with the newest consent form, email, etc. Audit trails are downloadable as CSV, or may be viewed onsite. Administrators may update the consent and preference texts with a GUI, but may also be automated with APIs. Akamai's definition of fine-grained means the storage of complex data of end-users at an attribute level, and consent is inclusive of preference information. Detailed attention to preferences helps to keep the business reason intact as the reason to collect data.

Identity Cloud creates a Unique User ID (UUID) for every data record, and all external applications – such as websites, mobile apps, data integrations, etc. – that access the user profile data are assigned a unique set of credentials for the specific reading, writing, or tracking of specific fields in the included database for both structured and unstructured data. Security measures have been taken to prevent an outage of Akamai's CIAM services regionally and globally. Identity Cloud enables download of SIEM events directly, and in the future point-to-point integration via APIs to a variety of SIEM platforms will be possible. APIs support the development of custom consent management workflows. Compliance can be facilitated for all major regional regulations, and numerous data centers globally.

One of the strongest benefits of using Akamai for a Privacy and Consent Management solution is that these capabilities are part of a complete CIAM offering. Identity Cloud can integrate multiple data sources with an organization's enterprise data infrastructure. Over 30 social logins are possible for users. Privacy-centric approaches are built into other Akamai products such as Hosted Login to create user experiences that enable consent and privacy control as an inherent aspect to CIAM. Identity Cloud supports the SSO, OAuth, and OIDC interoperability standards.

| | |
|---|---|
| Security | ● ● ● ● ● |
| Functionality | ● ● ● ● ● |
| Interoperability | ● ● ● ● ● |
| Usability | ● ● ● ● ● |
| Deployment | ● ● ● ● ● |

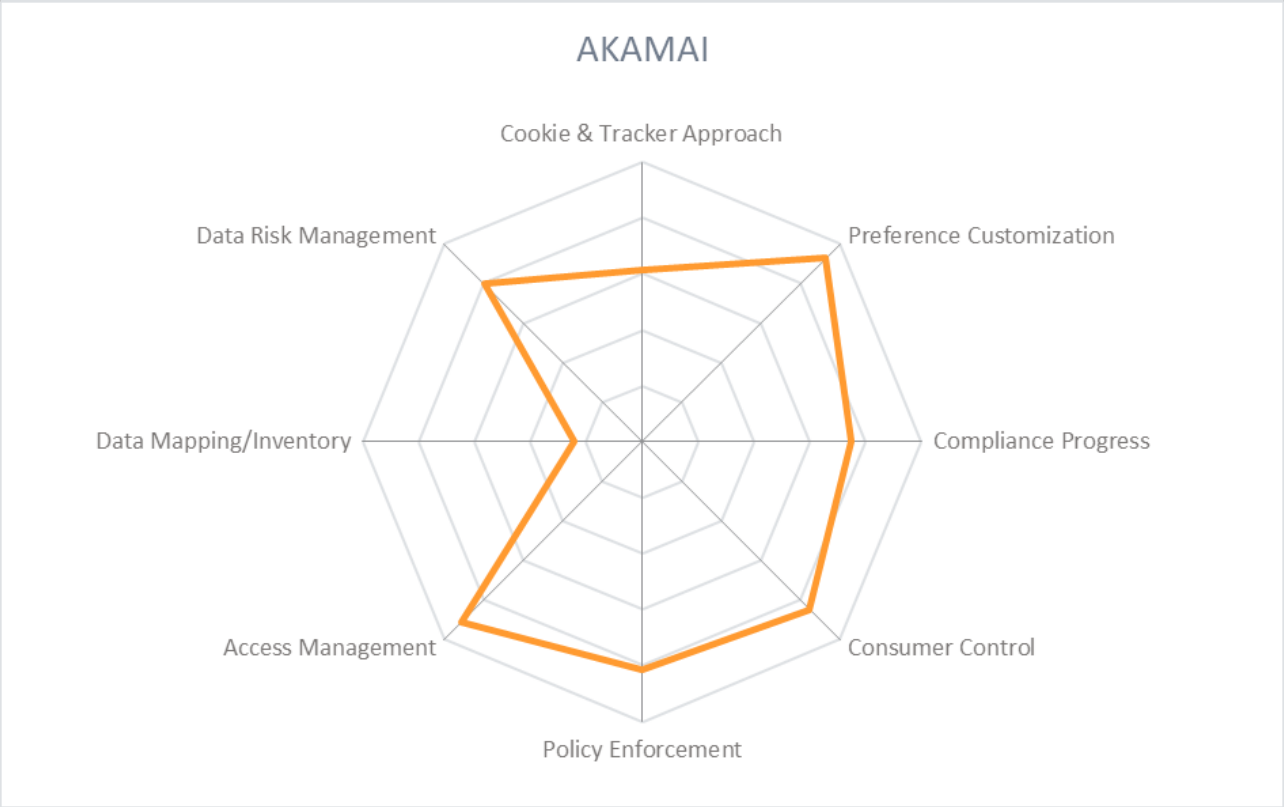

## Strengths

- Privacy and Consent Management is part of a comprehensive CIAM offering
- Progressive consent to achieve marketing needs with attention to compliance
- Paired with scoped access control, which only allows entitled admin to manage consumer consent data
- Able to manage attribute-level consent
- BI and marketing analytics functionality allow end-user data to be automatically displayed in reports

## Challenges

- Although good for delivering information in real-time, webhooks may be difficult to implement and manage; Akamai addresses this with an upcoming offering to enable more integrations with enterprise systems
- No scanning technology for cookie and tracker detection

## Leader in


AKAMAI
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.2 Crownpeak

Founded in 2001 and headquartered in Denver, Colorado, Crownpeak has a foundation in web content management. Through the acquisition of Evidon it has worked 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. Crownpeak's customers span a wide variety of verticals, including highly regulated industries and global brands.

Crownpeak's philosophy is to deliver value to the content-consumer before blocking their experience with a privacy notice or cookie banner. Cookies and tags are prevented from firing until consumer consent is given, enabling end-users to consume content before being required to interact with a pop-up or banner. When an end-user views a site, they are presented with a privacy and cookie notification banner that allows the user to see what type of tracking technology is being used on the site and for what purpose – including third-party and piggy-back tags – and to provide or withhold consent for the collection of their data. If the user chooses, they may view more detailed information on each tag vendor, supplied by Crownpeak's vendor database of over 6,000 vendors. When an end-user gives or withholds consent, a hashed IP address of the consent records is captured and stored.

Crownpeak's solution uses a scanning technology and database of cookie and tracker vendors to automatically generate reports to inform end-users of which vendors are active on a website and what data is being collected. Crownpeak first scans the website and generates a list of tags and cookies that are present. The customer then chooses the vendors that they consent to. Once this refined list is created, a policy is generated to only allow the selected cookies and tags to fire after consent is collected. A key differentiator is Crownpeak's approach to identifying cookies and trackers on a website; Crownpeak identifies the vendors who are dropping cookies and tags rather than identifying the cookies and tags themselves. This provides more context to the end-user to make an informed decision on whether to allow a vendor to collect their data. For administrative control, the Tracker Map on the consent management platform (CMP) dashboard represents the cookies and tags a map, showing the location of the vendor to allow better visibility for piggyback tags at the 3$^{rd}$, 4$^{th}$, and 5$^{th}$ level.

Deployment is as a SaaS with the launch of a single JavaScript tag to collect data on all vendors in real-time. Deployment may only require a few hours, or as long as the customization process takes. Access request forms are available for GDPR compliance so that end-users may request erasure and other rights to their data. User experience can be customized through APIs to deliver the appropriate languages, look and feel, and options to be compliant with the relevant data privacy regulations. Short-term goals include expanding the CIAM functionality to better manage cross-device and granular consent. Consent can be facilitated for all major regional regulations, and is flexible to adapt to future regulations.

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, and managing numerous domains with ease. In addition to easy "no-code" customizations, companies can make CSS changes on their sites if they want additional options.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●○ |
| Interoperability | ●●●○○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |

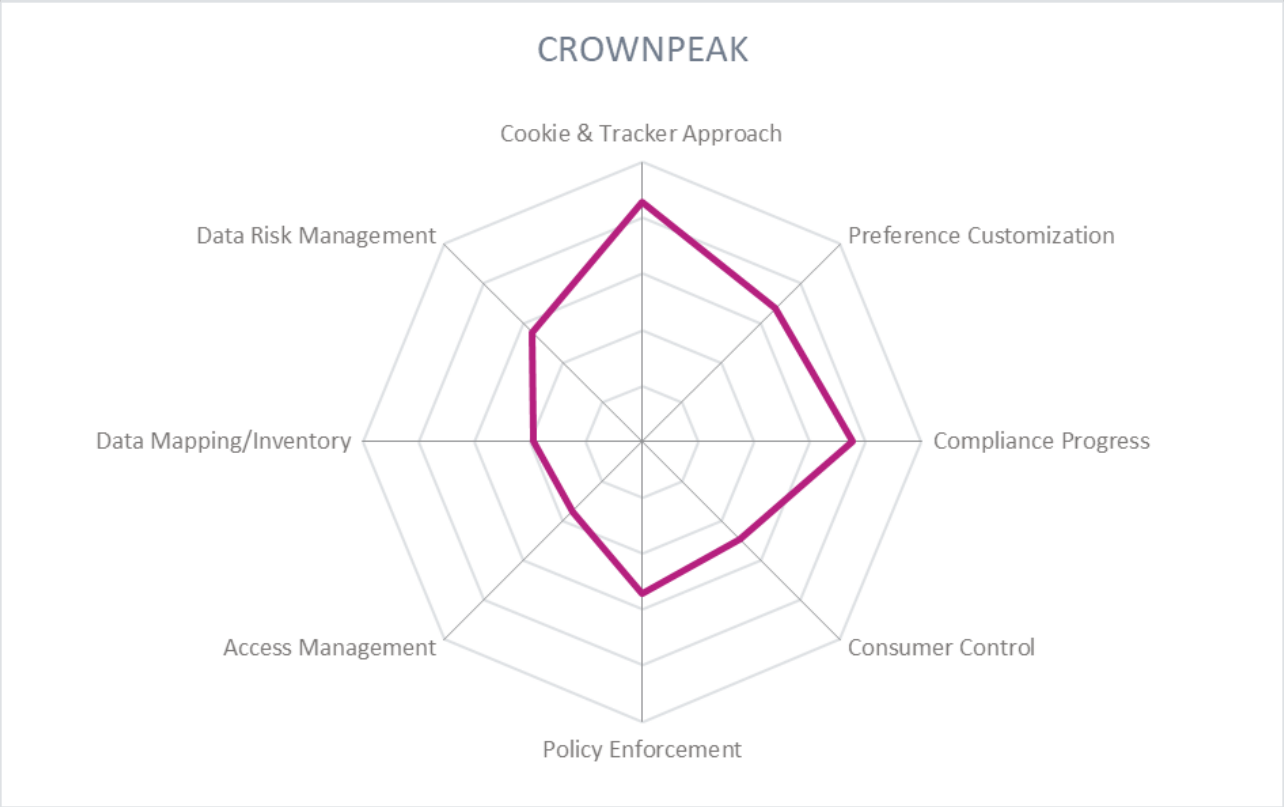
crownpeak

## Strengths

- Is a CMP registered with IAB
- Timeseries testing is available
- Integrates with tag managers
- Has features for automation in data inventory and mapping
- Includes Tracker Map to display parentage of 3rd party data being shared
- Offers ability to track consent in web, mobile, email forms, IOT devices, chatbots, etc.

## Challenges

- Does not have SIEM connectors
- Customers are unable to choose the geographical region for data storage
- OAuth is supported, but more integrations with access management standards such as SAML or OpenID Connect would make this product even stronger


CROWNPEAK
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.3 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.

A unique factor that iubenda offers is the modular design of privacy policies, constructed by the customer in a dashboard. The Privacy and Cookie Policy Generator has 1,300 clauses drafted by iubenda's in-house legal team. These clauses are available in eight different languages, reflecting the legal phrases and legislations that are relevant to different regions. Customers can select the clauses that are relevant to the regions they operate in and the activities that require disclosure, for example Google Analytics, Google AdSense, Facebook conversion tracking, and newsletters. Privacy and cookie policies are integrated in a customer's website via widget, JavaScript, or API. Policies are hosted by iubenda to undergo automatic updates when relevant legislation changes, overseen by the legal team and with advance warning provided to the customer. A site scanner auto-detects the tracking technology and services in use on a customer's website to auto-generate the cookie policy.

The Cookie Solution enables customers to create a customizable cookie banner, collect consent for those cookies, and block any cookies from firing before consent is collected. One unified dashboard is available for customers to manage one or all of the product suite for one or all website domains and apps. The cookie banner can reflect the look and feel that the customer chooses, and is able to be white-labeled. Customers set up their cookie solution by selecting the appropriate regional legislation – GDPR, CCPA, or both – to collect consent accordingly, and add IAB format to cookie categorization and disclosure in the dashboard. Once consent is given, cookies are asynchronously re-activated for higher speed and performance. The Consent Solution, via API, helps the customer to keep track of all consent activities from webforms, email, newsletters, etc. This is also a method to track marketing preferences. The information recorded in the solution database is a timestamped identifier on the data subject's unique ID, email, name, and their preferences. Data inventory services are provided by an additional product, the Internal Privacy Management solution, where records of processing activities are recorded.

The product suite can be run on-premise, as a cloud service, or as a managed service. Deployment takes between hours to two days, There are many plugin options including WordPress, Google Tag Manager, PHP class for parsing and replacing scripts, webserver module to automatically block all tracking technology that are subject to prior consent. The iubenda team works actively with vendors through the IAB Transparency and Consent Framework to achieve balance between privacy and marketing needs.

iubenda is a solution for any industry, offers a high degree of confidence to deliver legal texts in multiple languages, and provides means to track consent for services other beyond cookies. It has strong market position and easy deployment.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●○○ |
| Usability | ●●●●○ |
| Deployment | ●●●●● |

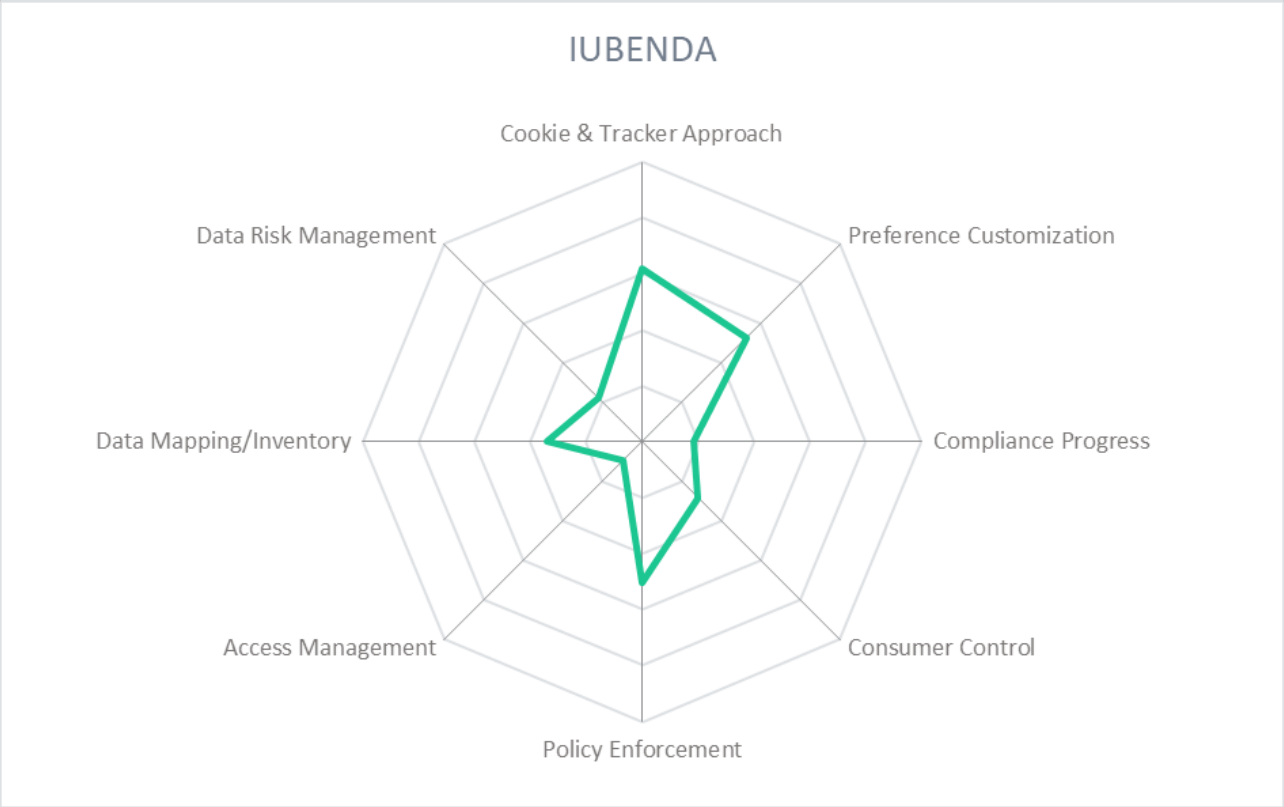
iubenda

## Strengths

- Uses scanning technology to detect cookies and trackers on customer sites
- Includes support for email compliance
- Has in-house international legal team to help develop compliant privacy notifications
- Plugins for common web platforms like WordPress
- Integrated with IAB Framework, and an active participant in shaping the IAB Framework and US Privacy Framework

## Challenges

- Does not provide an audit trail for customer's administrative activities
- Automation is being developed for automatic notifications for end users to update consent when policy expires.
- Does not have configurable connectors to SIEM
- Does not support individual rights requests
- Customers are unable to choose the geographical region for data storage


IUBENDA
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.4 iWelcome

Founded in 2011 and based in the Netherlands, iWelcome delivers SaaS for consent lifecycle management. iWelcome CIAM is an integrated set of functionalities, able to be used together or selected modules such as the Consent and Preference Management or Mobile SDK may be purchased separately. iWelcome takes a holistic approach to consent management and privacy protection for B2C, B2B, and B2B2C use cases. The industries iWelcome serves include insurance, utilities and other regulated industries, organizations built on an AWS environment, and organizations that have an obligation to implement the GDPR. To iWelcome, fine-grained consent means the ability of end-users to give consent for individual attributes for multiple purposes.

iWelcome facilitates opt-in-based consent flows and implements a data model based on the NIST 8112 standard for meta-data. An end-user signs up with a customer using iWelcome's CIAM solution, and their identity profile is built from the individual attributes given, such as name, surname, email, etc. As the end-user interacts, iWelcome's Consent-API connects with dialogue boxes or other interface with the customer for progressive/just-in-time consent collection. The interface provides transparency for the user about the attributes retrieved with consent and the associated processing purposes, visible to the end-user on their personal dashboard, as well as for the organization. End-users can view their historical login, back-tracing attribute gathering, and consent actions as a timeline, as well as make corrections and updates.

The central Consent Ledger 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 restric and audit PI access by other people than the end-user, including customer care, dealers/brokers, and application owners. iWelcome 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 to 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. iWelcome supports the right to export data, data deletion upon request, and data age/retention policies. iWelcome has multiple data centers within Europe and could deploy in the US and Asia for localizing user data in the most compliant way.

iWelcome is deployed as a SaaS, specifically an IDaaS. Welcome is designed to complement an organization's existing IAM solutions served by a dedicated API, and able to augment an IDaaS solution with iWelcome consent. iWelcome'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 iWelcome lacks cookie and tracker consent tools, iWelcome is a strong innovator that providing very strong CIAM capabilities with transparent attribute-level consent features for end-users. The data model used by iWelcome to gather progressive and just-in-time consent for individual attributes is a differentiator in this market.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●○ |
| Interoperability | ●●●●● |
| Usability | ●●●●○ |
| Deployment | ●●●●○ |

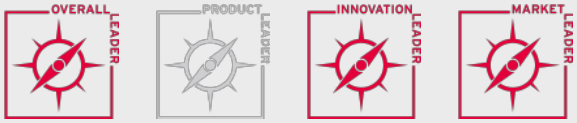

## Strengths

- 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, and thus does not prevent tags from firing until consent is received
- Limited global reach, currently only present in the EU
- Support for data locality is limited to European countries

## Leader in




IWELCOME
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.5 MyLife Digital

MyLife Digital was founded in 2014 and is based in the UK. Its flagship product, Consentric, takes a pre-GDPR, marketing-led approach to generate mutual benefit for both end-users and organizations. MyLife Digital believes that a modern consent and preference management solution needs to cater for a dynamic customer consent journey that benefits our customers and their end-users. Consentric is for use in all industry verticals, including transportation, charities, publishers, and utilities services. Consentric is able to address GDPR and CCPA requirements, and can be adjusted to meet the needs of other regulations.

Using Consentric web components, consent capture can be tailored to specific user journeys. Highly configurable templates are used to create the widgets and other views that contain the consents, preferences, and Privacy Statements that can be deployed at various touchpoints in a user's journey. This flexibility allows the capture of an initial set of consents that can then be augmented with end-user preference selections on the types of marketing material they prefer to receive. Once deployed, these templates can be adjusted centrally through intuitive interfaces and updates deployed without the need for additional IT resource. Audit trails for each end-user including the lawful basis for data collection, how, when, and where data was captured, and the organization's Permission Statements and Privacy Policy. Consentric is able to collect consent and update preferences to its central store via email forms, through third-party integrations, on websites via popups, and SMS and App notifications. If the end-user is reached via a marketing call, consents and preferences can also be updated manually. Consentric integrates with tag mangers to enable progressive consent capture, for example when a customer clicks on a specific product category a popup offering the end-user to subscribe to material relevant to that product category appears.

Authentication is managed through Auth0, which facilitates connections to AD and LDAP. Recent developments include incorporating consent management into the authentication journey of the end-user. Consentric provides a basic cookie consent module that displays cookie disclosures, requests consent, and prevents cookies from being dropped prior to consent. Where customers require detailed tracking or scanning capabilities for multiple domains, then MyLife Digital will deploy TrustArc's cookie consent module.

Consentric is a microservices-based SaaS solution, built on top of APIs for fast and easy integration, and rapid deployment. It is fully integrated into the SalesForce platform, with additional plug-ins to other systems. A full audit trail of all consents captured per end-user is available. Data mapping tools in SCV and CRM systems can be easily integrated using Consentric's open API. Linking functionality exists to enable organizations to inform Consentric of customer relationships and create a single consent and preference view across data silos. MyLife Digital's data centers are located in the EU, but deployments can be delivered into other jurisdictions, with expansion soon to the US. To Consentric, fine-grain means capturing consent and preferences in detail, like providing the end-user with the ability to unsubscribe from the specific type of email that they don't want, but remain subscribed to the emails they do want to receive. It is capable of serving multiple domains, and provides a user-friendly cross-domain view on the Consentric platform.

MyLife Digital's strength is in relationship management and assisting organizations to understand the preferences of their end-users while ensuring the data is compliantly captured and used for the right

purpose. The flagship product Consentric, a strategic partnership with TrustArc and the recent Guestbook app that uses Consentric back end features (currently being showcased a track and trace app), MyLife Digital demonstrate awareness of the complexity of the modern customer consent journey. A privacy-by-design architecture means that Consentric only needs to hold anonymized end-user data.

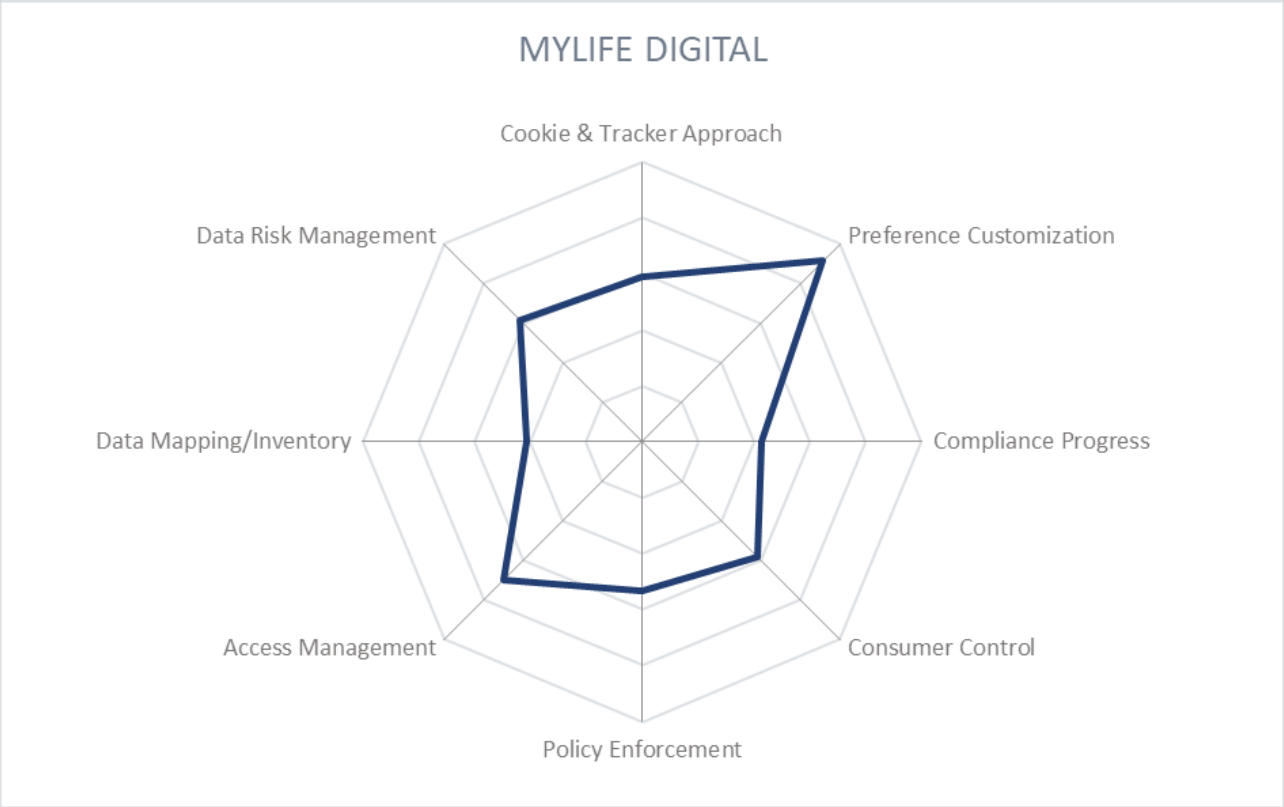
| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●○ |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |


## Strengths

- Salesforce App & connectors to other systems
- API layer for easy integration, supported with comprehensive user and developer documentation
- Ability to tailor consent framework to business processes
- Central control of consent messages across multiple sites and domains
- Enables progressive consent
- Integrates with SIEM environments
- ISO 27001 certified
- Supports Kantara Initiative's Consent Receipt Specification

## Challenges

- Inventory and mapping functionalities are delivered through TrustArc partnership
- Basic own cookie manager available that prevents cookies from being dropped, but can deliver a full solution through strategic partnership with TrustArc


MYLIFE DIGITAL
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.6 OneTrust

Founded in 2015 and co-headquartered in London and Atlanta, GA, OneTrust is a fast-growing player in this market. Its Privacy Management Suite is a complete offering of data inventories, cookie management, preference setting, and compliance progress. OneTrust takes a multi-stakeholder approach to meet the needs of legal departments, marketing departments, and end-users.

The product suite is powered by OneTrust Athena AI and Robotic Automation to run OneTrust DataDiscovery – an intelligent classification tool – and OneTrust DataGuidance – a regulatory research software. These two tools enable the customer to know the data they hold and the laws that apply to them to be aware of their journey towards compliance, and support the product modules that make up the Privacy Management Suite: OneTrust Privacy, PreferenceChoice, Ethics, Vendorpedia, and GRC. The PreferenceChoice module provides consent solutions, cookie compliance, preference management, mobile app consent, and tools designed specifically for publishers and streaming services. The Privacy module is built for legal teams, handling data mapping DSARs, targeted data discovers, maturity planning, program benchmarking, among other capabilities.

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. Data Rights Requests, DPIAs, and blacklist workflows can be automated, while maintaining a fully auditable record. OneTrust manages cookies and trackers by deploying a website scan to detect tracking technologies, automatically categorizes the results and generates a customizable banner and cookie declaration, and employs a patent-pending auto-block to prevent trackers from firing until consent is given. The cookie policy is automatically updated with each scan and auditable reports are generated and maintained. Scanning and consent functions are applied to mobile apps with the Mobile App Consent Solution. Includes integrations with major tag managers. Consent collection can be customized by user geolocation. OneTrust takes a wide approach to consent and preference collection to centralize multiple channels of end-user interaction into a single dashboard.

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 straightforward 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

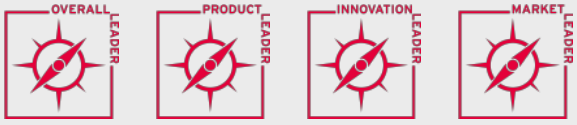
## Strengths

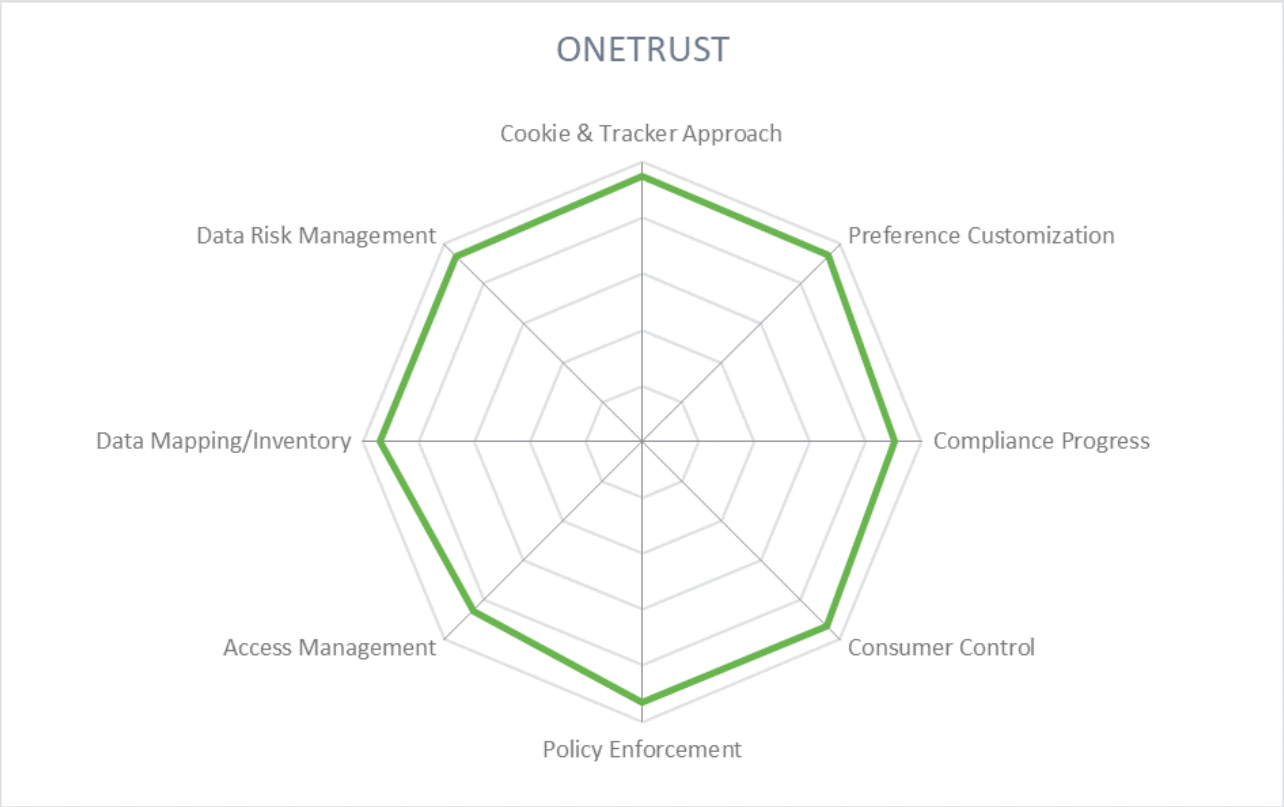
- Strong data inventory and mapping capabilities
- Strong analysis capabilities to visualize compliance progress and address gaps
- Risk management capabilities include third-party risk management, data breach monitoring, and detection and visualization of risks
- Support for cross-border transfers to 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

## Challenges

- Attribute level consent and preference would make this an even stronger solution

## Leader in




ONETRUST
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.7 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 with a focus on privacy. 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. Data subject requests are collected and handled in the Consent Manager platform. 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. 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. This 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.

GDPR Consent Manager can be deployed on-premise, in the cloud, or hybrid. 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.

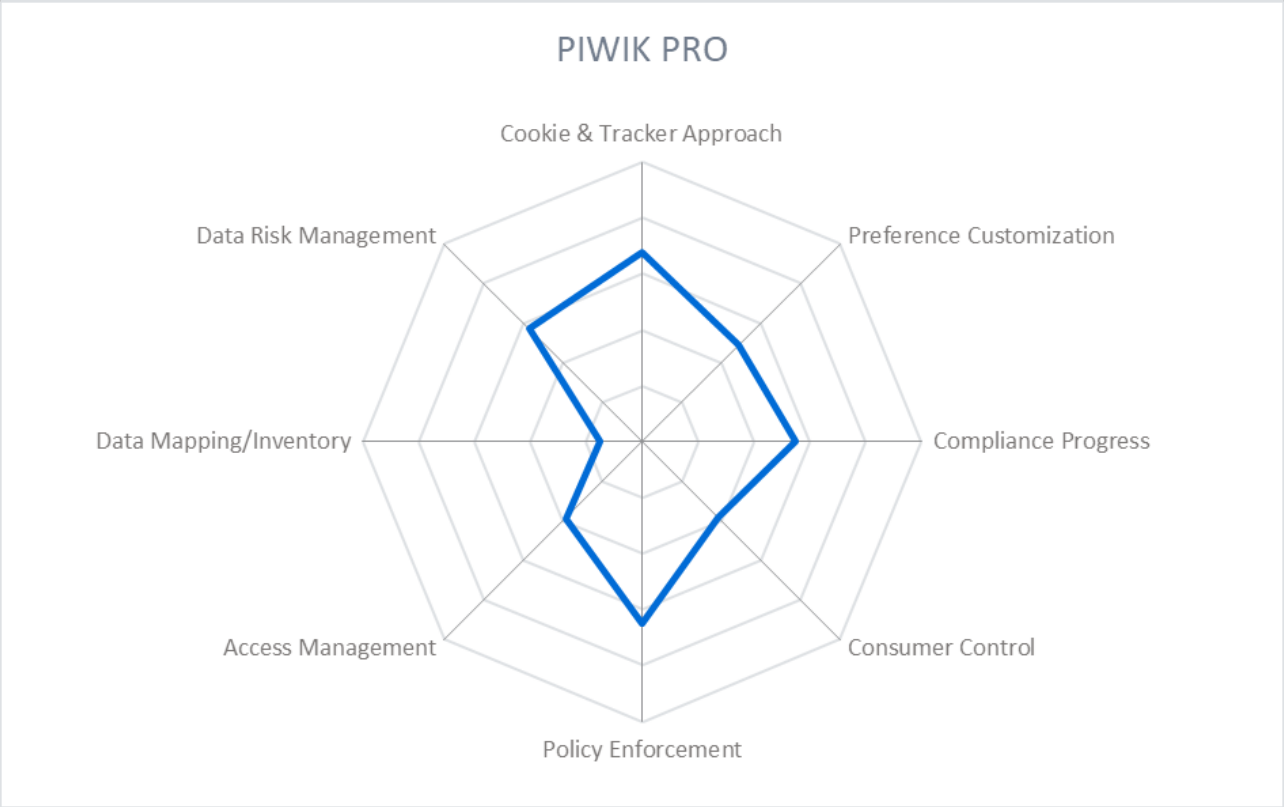
Piwik PRO is an option for organizations that require privacy-focused analytics. The application of analytics to Piwik PRO's own solution delivers value to users, assisting them to methodically design a customer experience that generates high levels of consent.


## Strengths

- 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

## Challenges

- No scanning for trackers and cookies
- Four language offerings, more languages could be offered
- No data inventory service, and limited data mapping features


PIWIK PRO
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.8 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 covers the GDPR, ePrivacy Directive, CCPA, and plans to expand coverage to other jurisdictions.

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. Customers are able to customize popups and banners to collect consent for privacy statements and tracking technology using an easy to use drop-down menu to identify aspects such as reason for data processing. Quantcast employs a "blocking experience" where an end-user may not continue using the site until a consent decision has been made, which prompts a clear consent decision from the end-user. Default settings trigger reconsent whenever new vendors are added, and is able to be customized based on customer needs.

Quantcast enables customers to control tracking technology on their site by proactively choosing which vendors may drop cookies and tags, creating a "whitelist". Those cookies and trackers that are selected are blocked until the end-user provides consent. Quantcast's active participation in the development of the IAB Transparency and Consent Framework has yielded a top performing solution in generating TCF consent signals for downstream members of the advertising ecosystem. Quantcast's consent management platform is also able to flag any customizations that are in breach of the IAB TCF or of GDPR and CCPA regulation policies. DSAR forms are an optional customization, and can be easily addressed in the customer portal.

Quantcast is a SaaS, with rollout of service taking approximately two hours. A universal JavaScript tag is embedded on each of the customer's website to coordinate the consent collection across all domains, managed centrally in the customer portal, which is key for scaling across multiple domains or across groups of sites.

Quantcast is strong option for marketing-focused publishers of all sizes. Its CMP capabilities are very strong and it offers a mature and focused solution to complement other privacy products. Quantcast's proactive role in developing the IAB TCF is a desirable quality and is indicative of its innovation. General usability is high.

| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●○○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |

# Quantcast

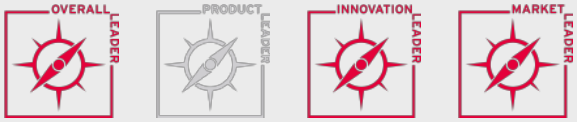
## Strengths

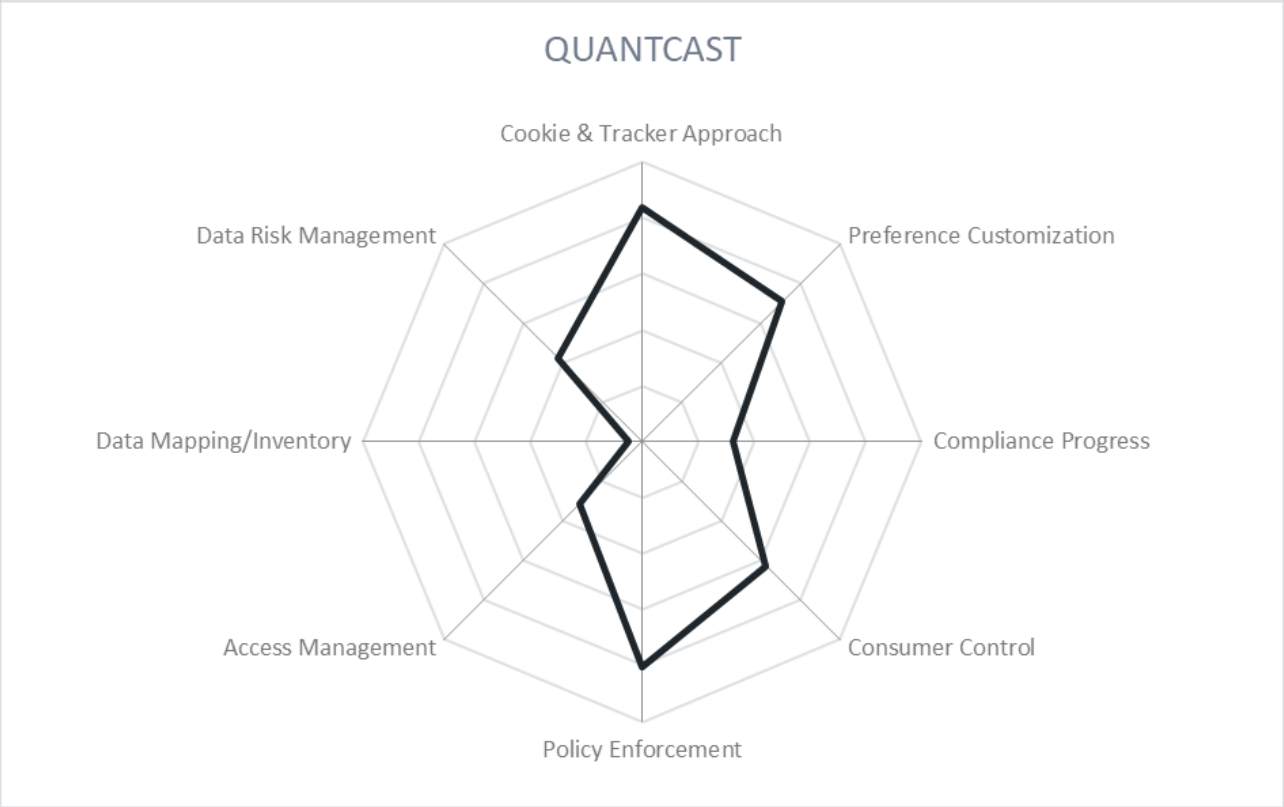
- A persistent thumbnail on each website subpage allows end-users to access and update consent choices
- IAB compliant and helped to design and standardize the Transparency and Consent Framework
- Integrates with tag management systems
- Enables customers to proactively choose which vendors may drop cookies and tags with a “whitelist”

## Challenges

- Customers cannot choose the region their data is hosted in
- Focused approach on consent as pertains to analytics
- No inventory or mapping service to support privacy tasks
- No SIEM integration

## Leader in




QUANTCAST
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.9 Sourcepoint

Sourcepoint was founded in 2015 and is based in New York. The Consent Management Platform (CMP) is deployed as a SaaS, and focuses on enabling better communication between publishers and end-users, including compliance. 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, or with JavaScript, cookie actions, or using Google Tag Manager integration for third-parties that do not participate in the IAB framework. 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 the tracking technology that is present on a publisher's website. The results of the scan automatically populate the vendor list for which an end-user provides consent. 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.

Deployment is in private, multicloud, 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 | ●●●●● |

Sourcepoint

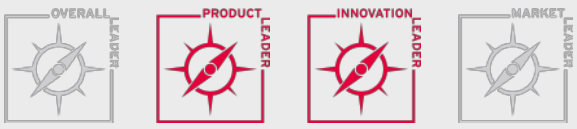
## Strengths

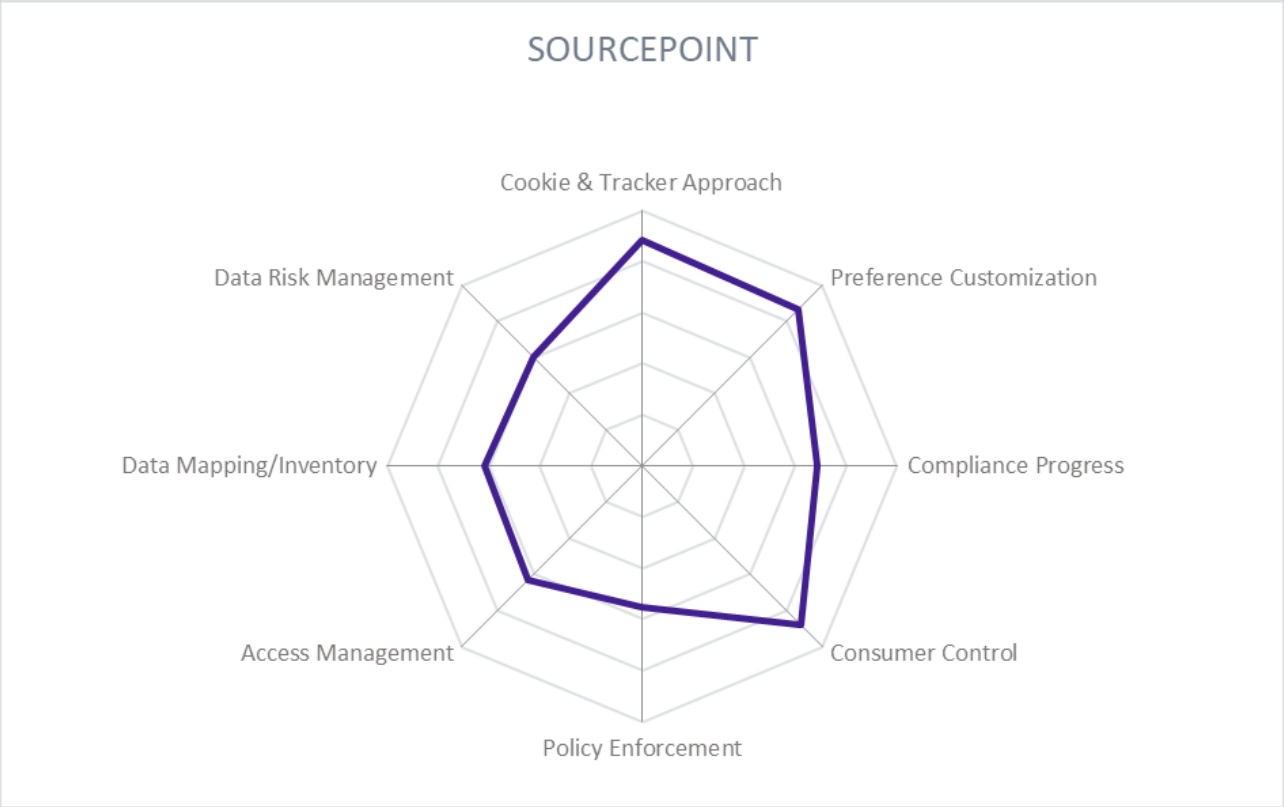
- Allows for customers to do A/B testing with different privacy messages, formats, etc.
- Allows customers to introduce alternative compensation choices (such as whitelisting, micropayments, ad-free access, and more) to provide users access to content in case they don't want to share their personal information
- Supports app, browser, AMP pages, and over the top streaming (OTT)
- Provides a module with customization and automation for the end-user's DNS/DSAR process
- Validated for IAB TCF 2.0 for web and mobile, and can support custom frameworks and interactions
- CMP platform earned and maintained the ePrivacy seal since 2018
- Authenticated Consent based on end-user identity

## Challenges

- No SIEM integration available, but maintains logs for all critical systems
- Solution is ISO 27001 and SOC 2 Type 2 is in progress

## Leader in




SOURCEPOINT
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.10 Sovy

Sovy was founded in 2017 in response to the global reach of GDPR as a SaaS compliance solution for SMEs and decentralized enterprises. The team behind Sovy has a background in regulatory technology and enterprise risk management. Sovy's founders previously served as enterprise risk and security executives and brought this expertise to Sovy. Sovy focuses on delivering an end-to-end privacy and consent solution for small and mid-sized companies, with special attention to those that must provide evidence of continuous compliance in an enterprise supply chain. Sovy offers a well-rounded option for SMEs and scales for its enterprise clients that have decentralized organizations, with multi-language requirements. Although the name indicates a priority for meeting GDPR needs, the solution is able to address CCPA, PIPEDA, and LGPD regulations.

Sovy provides an automated and easy-to-use portal to create and manage end-to-end privacy programs, maintain data inventories and records of processing, tailor privacy policies, manage cookie consent, train staff on GDPR compliance, manage data processing activities, and evaluate a customer's ongoing journey to compliance. New customers begin with a guided approach to assessing personal data handled and the data inventory, providing competency-based training for Data Protection Officer, Data Processor, and Data Controller roles, as well as for IT and for general employees. Sovy uses wizards to walk customers through the process of building a PI inventory, generating guidance documents and tailored policies, determining the lawful basis for data collection, performing data privacy impact assessments, cookie consent banner creation, and more. Privacy and compliance categories cover general processing, security, international data transfers, automated processing, consent, and awareness. Sovy periodically scans the customer's website for cookies and trackers and generates a cookie declaration banner and privacy policy. Sovy has a machine learning component to examine the policies against existing rules and parameters. This ML component is in beta. The scan results reveal what areas still need improvement, and results are saved in chronological order to show improvement over time. A second scan is done for cookies and tracking technology, the results of which are automatically categorized by the ML engine. Sovy enforces a no-cookie-drop policy until consent is granted, and clears cookies when consent is withdrawn. Sovy's tag management and integration are in development, along with connector APIs.

Sovy considers education of companies on privacy and data protection an essential aspect to providing a compliance hub. Sovy offers eLearning modules for GDPR for general information and to specifically educate people for the different Data Protection Officer, Data Processor, and Data Controller roles. Guidance on regulations is available on the Sovy compliance hub. Sovy provides modular privacy policy templates that can be customized according to the company's specific requirements. Templates are updated to match global regulation. When regulation changes, all customers are informed that their privacy policies should be updated.

The GDPR Privacy Essentials solution is a multi-tenant SaaS solution with a cloud-first approach to deliver compliance as a service. The solution is also available as a managed service with private-tenant hosting for enterprises with decentralized or multi-legal entity structures, and for multinational corporations with local language requirements. The solution is designed to complement a small or mid-sized company's privacy and security system, with integrations for DLP systems, email security, anti-malware, etc. Sovy provides modules for conducting data privacy impact assessments and handling compliance operations such as

rights-request management. Sovy provides kits and advisory to achieve ISO compliance or pass supplier-risk assessments for a variety of verticals to enable organizations to gain the knowledge to implement it themselves. To Sovy, fine-grained consent means going beyond collecting implied or active consent towards explicit consent that includes multi-media consent for images, voice recordings, ect.

Sovy's offering is very promising for enterprises of all sizes. It has a global customer base, but its size is currently a limiting factor. The value it offers as a compliance-as-a-service in maintaining a compliance program, performing required compliance operations activities, tracking compliance progress and enabling organizations to become operationally proficient in privacy and data compliance is a differentiator in the market.

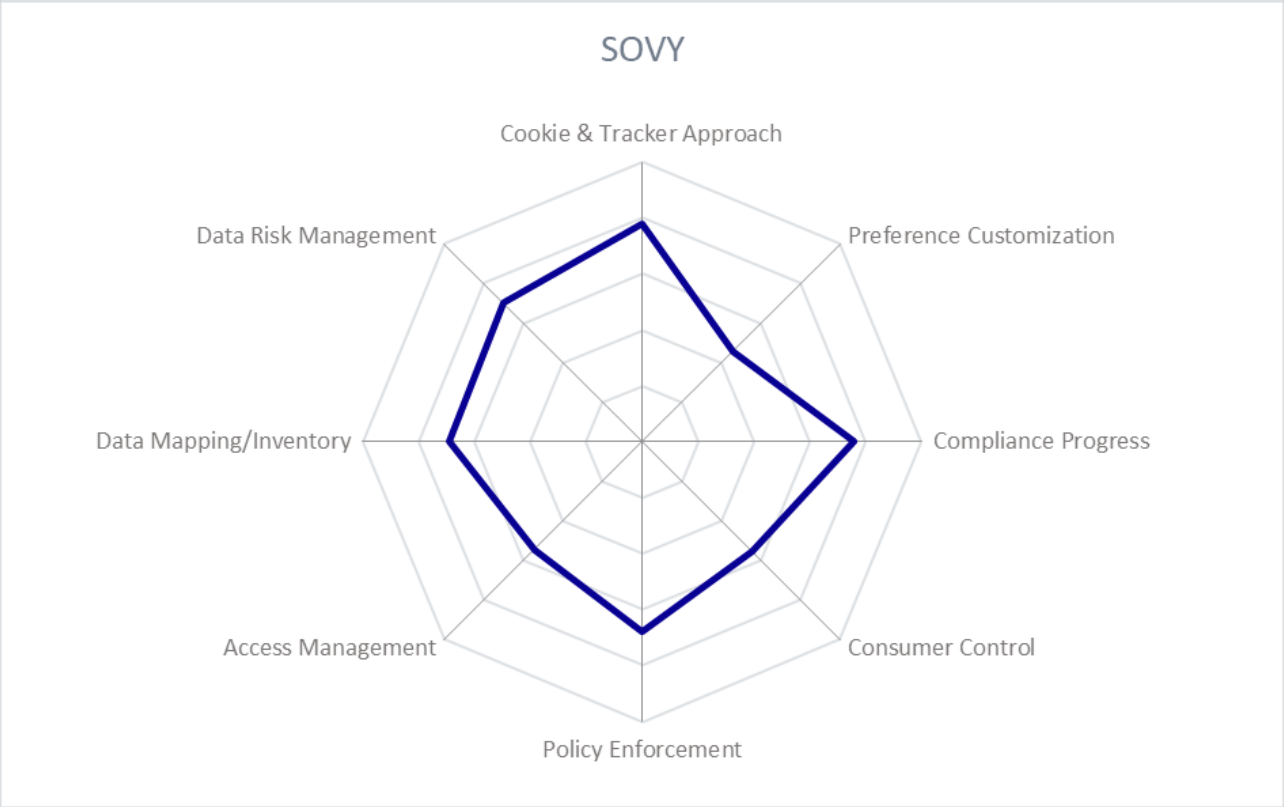
| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●○ |


## Strengths

- Scalable SaaS privacy tools to maintain a compliance program
- Strong emphasis on competency-based eLearning and simplified compliance operations
- Provides DIY approach and outsourced compliance operations as a service
- Displays compliance progress over time
- Affordable solution with free options for small organizations, including a knowledge portal
- Documentation and compliance courses are offered in most major languages
- Operates with privacy-by-design principles

## Challenges

- No integration with Tag Managers yet, but in development
- Does not prevent tags from firing until consent is received
- ISO 27001 and SOC 2 Type 2 certification is set for 2020
- Data locality features are still in development
- APIs for cookie consent collection are still in development
- Integrations with authentication standards are lacking


SOVY
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.11 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.

Creates a single source of truth for private data, including meta-data to facilitate privacy and consent management across multiple domains. 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. Scans for cookies and trackers 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.

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.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |

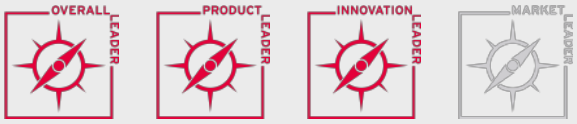

## Strengths

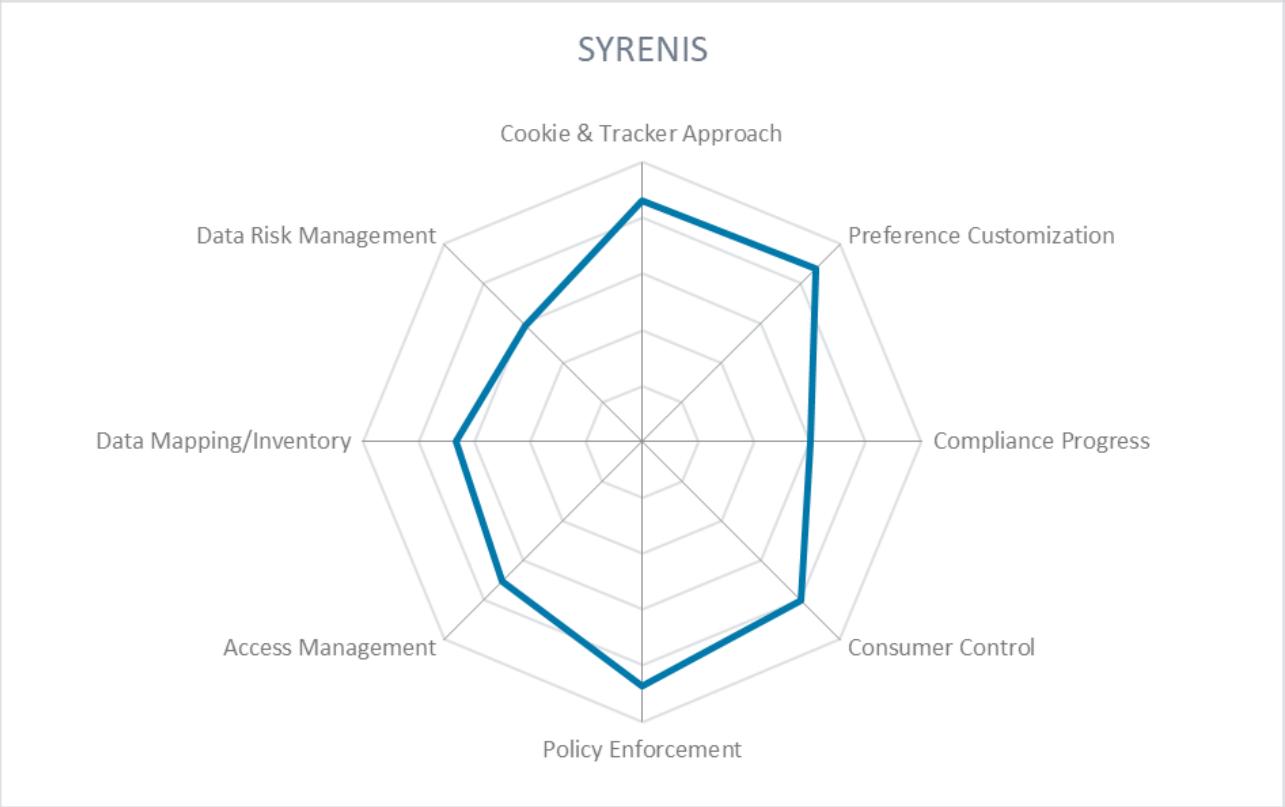
- Platform creates a single source of truth at meta-data level
- Strong automation capabilities
- Is IAB compliant
- Data visualizations assist in tracking compliance progress
- Solution serves as a single source of truth for consent and end-user data
- End-user access to self-service portal has authentication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

## Challenges

- Relatively long service roll-out of 1-6 months
- Data inventory services are mostly manual
- Could provide more support for data risk management

## Leader in




SYRENIS
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.12 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.

The Privacy Management Platform includes an automated customer privacy profile developed by an intelligent algorithm to determine applicable privacy regulations and develop a compliance plan. 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. 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 and its 2019 acquisition Nymity have developed proprietary frameworks to meet the privacy requirements of the major global regulations. TrustArc gives customers the tools to stay informed about privacy regulation with curated news stories available on the platform. TrustArc provides features to enable customers to track their own compliance, and customers may be certified through TrustArc's certification subsidiary, TRUSTe. 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 is a strong choice for all verticals.

| | |
|---|---|
| Security | ●●●●● |
| Functionality | ●●●●● |
| Interoperability | ●●●●○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |

TrustArc

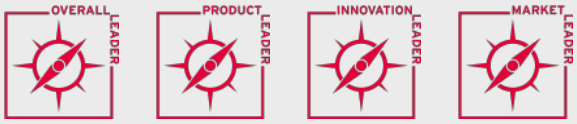
## Strengths

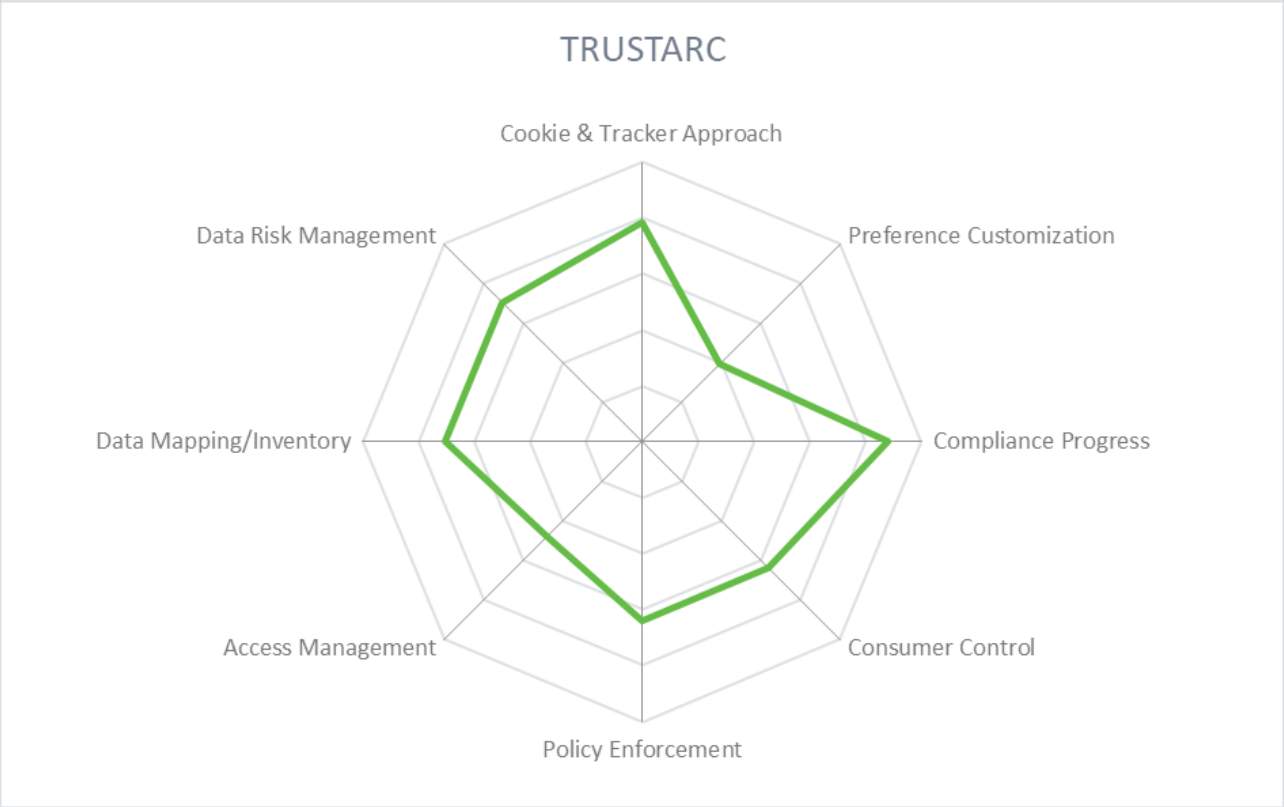
- Supports the IAB Framework
- Parent organization of independent certification organization TRUSTe
- Has options for automation and intelligent recommendation for compliance plan
- Data inventory is able to include text as well as video, image, and audio.
- Integrations with OAuth and SAML, as well as data analytics such as BigID and Sherpa

## Challenges

- Use of PAM for solution access management and support for the Kantara Initiatives would make this solution even stronger
- No integrations with SIEM environments

## Leader in




TRUSTARC
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

## 5.13 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. The CMP can be set to be compliant with GDPR, and many others including Brazil, Japan, Thailand, India, Russia, China, South Korea, and Canada.

Usercentrics gathers consent for cookie and tracker usage via web browser pop-ups, which controls when and which cookies fire, and generates auditable reports on the end-user's choices. A Privacy Shield blocks all third-party cookies until consent is captured. Usercentrics maintains a database of over 1000 cookie and tracker vendors that details the types of technology used, for what purpose, what types of data are collected, and location that data is processed in. This database is used to generate legal texts for customer privacy policy pages and is available in over 35 languages. End-users can choose to opt-in or out by cookie category, or per cookie vendor. Just-in-time consent is available. End-users can access their consent choices and view their history at any time by clicking on the persistent thumbnail on a customer website.

Usercentrics uses a TagLogger instead of a scanning technology to identify cookies and other tracking technology on a customer website. The TagLogger tracks URL calls originating from a website, which reveals third-party and piggyback tags. The TagLogger runs daily, and customers are informed of any tags or cookies on their website that are not already part of the privacy policy. An administrative dashboard displays analytics such as the aggregated opt-ins from end-users. Usercentrics provides insight to customers on their compliance progress by informing them directly of any changes in regulation.

The solution is deployed in the cloud by integrating a JavaScript into the customer website or tag manager. Data is hosted in Germany and Belgium, and Usercentrics offers a Self-Hosting solution to support customer control over location of data storage. No personal attributes of the end-user are kept, but the IP address, browser, and time are recorded as an anonymized Consent ID. To Usercentrics, fine-grained means that an end-user may have the ability to define their preferences as specifically as possible, and that customers may control the categorization of cookies and tags.

Although Usercentrics is a relatively new player, it has a strong presence with enterprise clients in a wide variety of industries. It provides detailed options for cookie tracking compliance, and preference management as it pertains to cookie usage.

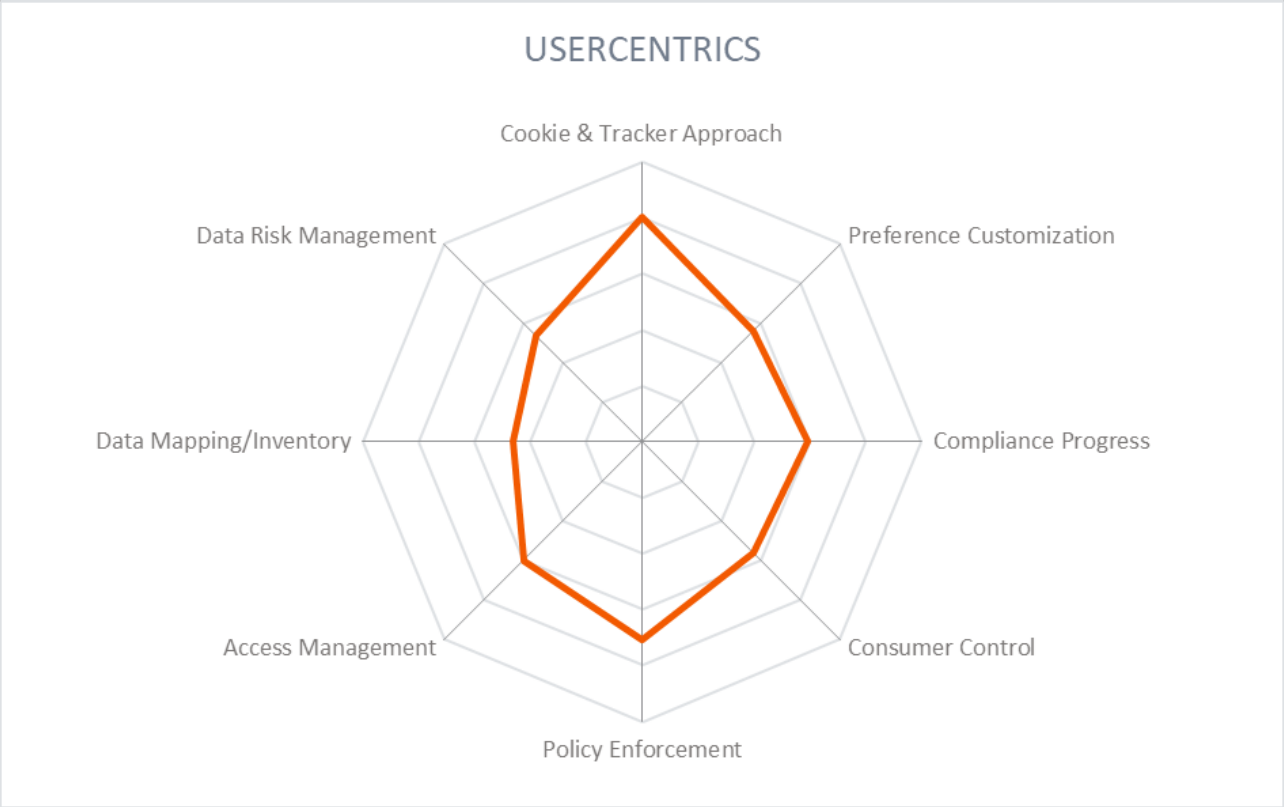
| | |
|---|---|
| Security | ●●●●○ |
| Functionality | ●●●●○ |
| Interoperability | ●●●○○ |
| Usability | ●●●●● |
| Deployment | ●●●●● |


## Strengths

- IAB TCF 2.0 certified
- Cloud provider is ISO 27001 certified
- Persistent thumbnail on customer website to view and update consent choices
- A/B testing is available
- Legal texts by cookie vendor are available for privacy policy generation
- In-house data analyst to test and provide insight on best practice for banner and opt-in optimization
- Privilege Access Management (PAM) functionality
- Supports consents for app content and cross-device content
- CCPA compliant as of August 2020

## Challenges

- Focused approach that specializes on managing for all data processing website and app technologies
- More integrations with access management standards such as SAML, OpenID Connect, or OAuth would make this product stronger


USERCENTRICS
Cookie & Tracker Approach
Preference Customization
Compliance Progress
Consumer Control
Policy Enforcement
Access Management
Data Mapping/Inventory
Data Risk Management

# 6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of Privacy and Consent Management or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

## 6.1 BigID – Data Intelligence Platform

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 cookie 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.

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 SFBX – AppConsent

SFBX, pronounced “safe box”, works to reestablish trust and transparency when data is exchanged between individuals and enterprises. Its CMP product, AppConsent, uses blockchain to collect, prove, and distribute consents across all digital channels. Use of the blockchain provides enterprises with an auditable proof of consent. The solution is IAB certified.

Watch this vendor to see if and how blockchain can add significant value to the process of collecting and managing consents.

## 6.3 Consenteye – Preference and Consent Management

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.

Watch this vendor increase its global reach for Privacy and Consent Management solutions.

## 6.4 Cybot – Cookiebot

Cybot is based in Copenhagen, Denmark, and was founded in 2012. 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. This generates a report of the existing cookies and trackers on a website for use in privacy policies. When individual end-users visit the privacy page, they may view their current consent state and make changes. The scan contributes to Cookiebot's ongoing global cookie repository with descriptions of each cookie's purpose. This information is automatically used on the customer's website to describe the cookie's purpose to the user. Among the information provided by the cookie repository is the data adequacy of the country the cookie or tracker sends data to, in order to inform end-users of a non-compliant destination for their data.

Watch this vendor for a robust cookie management solution with cutting-edge technology.

## 6.5 ForgeRock – Identity Platform

ForgeRock is a leading IAM and CIAM vendor. Its Identity Platform supports obtaining consent from end-users for the use of their PII during registration and when terms of service change. GDPR-compliant solutions can be built, but may require customization on the part of the customer to create consent management practices and processes.

Watch this vendor if you need a light consent management control, integrated with your comprehensive IAM or CIAM solutions.

## 6.6 TapMyData

TapMyData is a blockchain startup that fulfills an unmet need in Privacy and Consent Management

solutions. TapMyData aims to provide a secure communication line for organizations to respond to DSRs without exposing the recipient's data to unsecure email, post, etc., via a free app for end-users and a web portal for organizations. The solution has integrations with Salesforce and PrivacyTech players.

Watch this vendor to stay up-to-date on innovations in PrivacyTech delivering new protections to end-users.

# 7 Related Research

Leadership Compass: 79059 – CIAM Platforms
Leadership Compass: 79014 – Privileged Access Management
Leadership Compass: 80063 – Identity Governance & Administration
Whitepaper: 80136 – California Consumer Privacy Act: The Need for Data-Centric Security
Advisory Note 72557 – Maturity Level Matrix for GDPR Readiness
Executive View: 80328 – iWelcome IDaas and CIAM
Executive View: 80054 – Akamai Zero Trust Security
Executive View: 80046 – BigID
Leadership Brief: 80353 – Six Key Actions to Prepare for CCPA

# 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 in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment 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

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what 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 become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally

strong in particular areas.

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

### Product rating

KuppingerCole as an analyst company regularly conducts evaluations of 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 of 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**
- **Integration**
- **Interoperability**
- **Usability**

**Security** – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

**Functionality** – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

**Integration** – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

**Interoperability** – interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

**Usability** – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, 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 potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of

these areas will only result in increased human participation in deploying and maintaining IT systems.

- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

### Vendor rating

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

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

**Innovativeness** – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. 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. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. 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 overall markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

**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 become an acquisition target, with massive risks for the execution of the vendor's roadmap.

**Ecosystem** – this dimension looks at the ecosystem of the vendor. 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 – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

**Strong positive**
Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

**Positive**
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. 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. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., 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.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular market segment.
- **Lack of information supply**: Products of vendors which don't provide the information we have requested for the 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 of 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

# Copyright



**KuppingerCole Analysts** support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, 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 back 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.