KuppingerCole Report

LEADERSHIP COMPASS

by Graham Williamson | July 2015

# Secure Information Sharing

There are multiple options for organisations with intellectual property and restricted information that must be shared between staff and business partners to adopt in order to avoid inadvertent release of restricted information to unauthorized personnel. This document will help in the selection of an optimal solution.

by **Graham Williamson**
gw@kuppingercole.com
July 2015

Leadership Compass
**Secure Information Sharing**
By KuppingerCole

## Content

## Content Tables

## Table of Figures

## Related Research

Advisory Note: The new ABC for IT: Agile Businesses, Connected - 70998

Advisory Note: Connected Enterprise Step-by-step - 70999

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Executive View: AWS – Security and Assurance - 71280

Executive View: Covertix SmartCipher™ - 71267

Executive View: Druva inSync - 71131

Executive View: Exostar Services for Life Sciences - 70878

Executive View: Executive View Microsoft Azure RMS - 70976

Executive View: NextLabs Control Center - 70847

Executive View: Prot-On - 71268

Executive View: Seclore FileSecure - 71295

Executive View: TITUS Classification Suite - 70951

Leadership Compass: Access Control / Governance for SAP environments - 71104

Leadership Compass: API Security Management - 70958

Leadership Compass: Infrastructure as a Service - 70959

Leadership Compass: IAM/IAG Suites - 71105

Leadership Compass: Access Governance - 70948

Leadership Compass: Cloud User and Access Management - 70969

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Dynamic Authorization Management - 70966

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

# 1. Management Summary

Business professionals are often faced with an overwhelming amount of information, both structured and unstructured, and making efficient use of this data is becoming increasingly more difficult. Determining the balance between security and business efficiency in the adoption of new technology can be daunting. There is an increasing need to share data, not just within the organisation but with business partners as well as customers. In the digital business this increased communication has significant benefits to each line of business, improving efficiency and reducing costs. At the same time there are increasingly scary revelations of data breaches and loss of intellectual property. So in order to support business processes it is important to be able to provide access to sensitive data but it is also important that cyber security requirements are adequately observed.

In approaching the selection of a vendor for the provision of secure information sharing solution it is important to take an information lifecycle approach whereby the processes around data generation, its transformation and classification, as well as data storage and data destruction, are well defined. This requires policy to be established to advise on the proper location of records, the ownership and the value of data, and for retention periods to be determined and documented. The focus needs to be on deriving value for data assets which means ensuring data quality, improving the communication of data and deleting data when it's no longer required.

Solutions to the management of access to shared data are diverse. Each of the products featured in this Leadership Compass are different and takes a unique approach to the task of secure information sharing. The products fall into two broad approaches:

- Secure repository with strong access control on file access. These solutions typically use encryption to protect documents and provide a key-management solution. In some cases a single repository is supported, this might be an on-premise storage facility or it might be a cloud-based managed service. In other cases a captured environment is used whereby documents are encrypted so that they can be stored anywhere but they can only be accessed by a client that can decrypt them. Vendors of this type of system typically provide a secure control system to manage and log access to documents, regardless of where it occurs. A subcategory of secure repository system is the gateway approach that restricts access protected files based on a set of pre-configured policies.
- Rights management approach whereby solutions validate user permissions to access/modify a document at the time access is requested. Most solutions in this space support AD Rights Management and Azure Rights Management, some adopt their own information rights management solution and some solutions use client software to manage external storage or emailing. For vendors in this space the provision of classification capabilities are important to customers since documents need to be appropriately codified for a rights management system to be effective.

While the diversity of solutions makes it more difficult to compare products it makes the selection of a solution to a particular requirement easier, provided the requirements are well-understood.

Customers of secure information sharing solutions must first decide the type of environment that best suits their requirements. The typical characteristics of a secure data sharing environment are:

- Enable the use of cloud services: flexibly and with maximum control of the access rights of both internal and external users.
- Protect information held in cloud services ensuring it is protected from unauthorized access.
- Facilitate sharing of restricted information via available channels e.g. email, cloud storage, physical devices, social networks etc.
- Protect information held in any type of file including unstructured data and rich media.
- Allow access by business partners but in a flexible and controlled way supporting full compliance with the legal agreements.
- Allow collaboration in industry networks: (such as networks of healthcare professionals), allowing members of these networks controlled access to shared information.
- Provide support for new working models: with freelancers, mobile workers, and other forms of collaboration.

To cover all these requirements a comprehensive solution is needed that might require the combination of more than one product. Core functionality can be provided by one product and ancillary services can be added-on via another product. Ancillary services might be document classification, mobile device support, or secure email.

This document should be used to identify potential solutions to a specific problem; vendors are positioned in regard to their product functionality, market presence and innovation. The relative position of each vendor's offering in the accompanying graphs is less important than the description of each vendor's offerings which describes each product's specific focus.

## 1.1 Overall Leadership

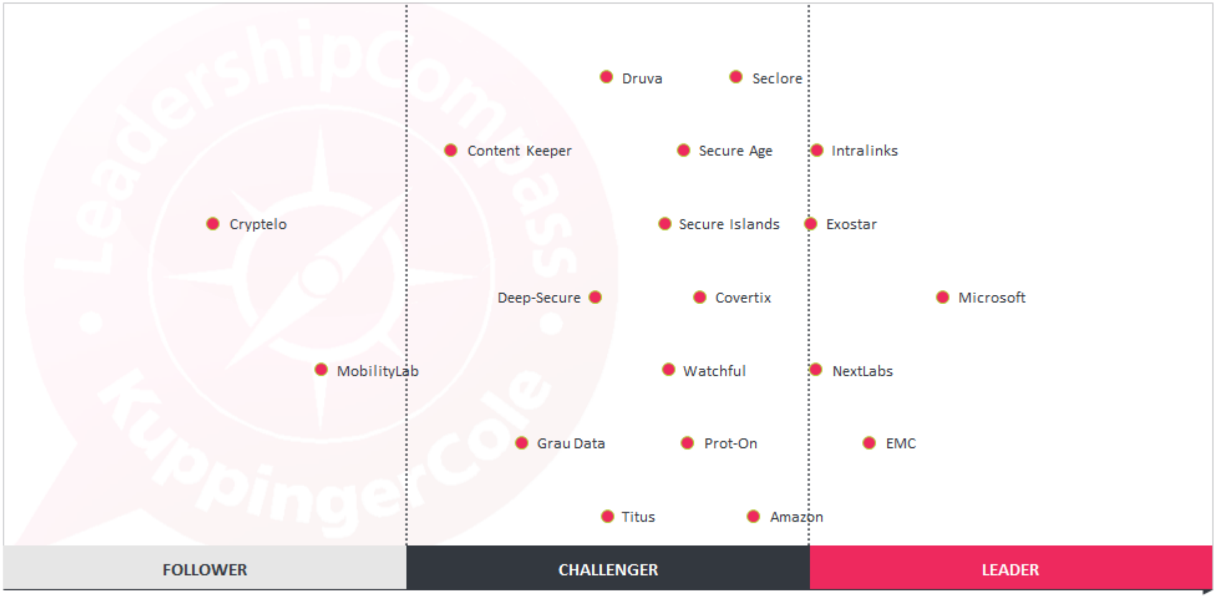


**Figure 1: Overall Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

In the Overall Leaders chart, as expected the large players are in front. This results from their market size and, in the case of Microsoft, their dominant position in the rights management market. EMC, also a large player with a wide partner base, have a functionally rich secure data sharing product specifically focused on providing an easy-to-use tool to give end-users the ability to control access to their documents[1]. Intralinks provide a comprehensive solution with a strong IRM-by-design focus. NextLabs provide fine-grained access to protected documents by combining a secure data storage capability with a rights management, attribute based access control solution. Taking a different approach is Exostar who specialise in supporting secure data sharing in specific industry environments.

It is perhaps not surprising that Microsoft's leadership is so dominant. Microsoft's rights management solution is mature and it is well integrated into two areas of product dominance – authentication services (based on AD) and office documents where Microsoft enjoys a leadership position. It can also be seen that Microsoft is clearly looking to maintain their leadership in rights management with the integration of Microsoft Identity Manager (formerly FIM) with AzureAD. AD RMS settings can be synchronised to Azure Rights Management which provides extended entitlements for the management of user permissions in the Cloud.

The Overall Leadership rating also shows a number of other vendors challenging the Leaders category. These include the very functional AWS WorkDocs product (formerly Zocalo), Seclore with their comprehensive enterprise rights management solution, Covertix with their cross platform support and monitoring functions, the Prot-On secure document environment, the Secure Age managed storage solution, the Secure Islands enterprise IRM approach and Watchful with their innovative classification functionality. Also in the Challenger section are five companies with different approaches to secure information sharing. They didn't score as highly as more conventional solutions but offer strong solutions in their target market sectors: Druva provides tight integration at the file system level, good endpoint enablement and dashboard functionality, Deep Secure have a modular approach to providing strong security over their data sharing environment, Titus provide a very comprehensive classification solution, Grau Data provide a very secure data-at-rest solution offering clients full control over keys and Content Keeper who provide a managed gateway approach to protecting data from users, and users from data.

In the Follower section we have two vendors; this is primarily due to their nascent status and small market presence. Mobility Lab are a start-up in Russia with an impressive, high-security solution focussed on end-client usability. Cryptelo is headquartered in the Czech Republic, their Drive product takes a server-based document approach with strong encryption facilities.

[1] Note: Prior to publication EMC sold the Syncplicity product to Skyview Capital.

## 1.2 Product Leadership

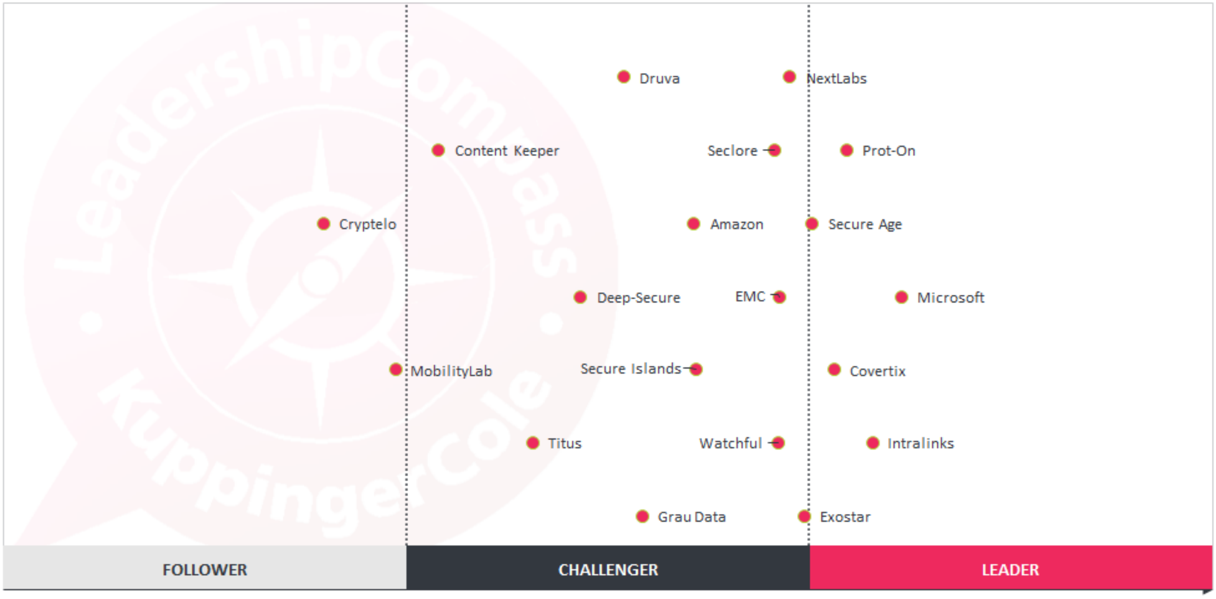


**Figure 2: Product Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

Product Leadership is the view where we look specifically at the functional strength and completeness of vendors' products. Again, we see Microsoft in a leadership position because of their rights management technology. Prot-On is also in the Leader section; they offer a cloud-based solution providing complete control over data at rest, in-motion and in-use with a custom-designed key management solution. Intralinks is in the Leader section with their Via product, a multi-tenanted SaaS solution. Covertix also do well in the Product space due to their file access control across multiple platforms. SecureAge is shown just inside the Leader section in the Product space because of their coverage of the secure data lifecycle – protection at rest, in motion and in use.

Closely following in the Challenger section are: Exostar who provide the "go to" solution in their specific industry environments, the NextLabs offering which combines a powerful policy management capability with a good end-client support, Seclore who offer a powerful and comprehensive rights management solution focussed on external collaboration, the EMC Syncplicity product focussed on a frictionless user expericne across a wide variety of file types, Watchful providing a comprehensive classification-based offering with good mobile device support, Amazon with their easy-to-use, advanced collaboration WorkDocs environment, Secure Islands provide a rights management solution with good classification capabilities and email/storage management support, Grau Data offering a strong encryption capability and support for secure data standards, Deep Secure with a military-grade solution based on a secure-server offering, the Druva server-focussed solution with strong encryption and a dual key capability that gives customers full control, Titus with a strong classification approach to document sharing with solutions for both desktop and mobile devices, and Content Keeper taking a different approach based on a gateway solution (both Titus and Content Keeper appear lower in the leadership graph only because their solutions do not align with the classical definition of SIS used to construct this Leadership Compass).

In the Follower section the MobilityLab solution provides an innovative solution in their file sharing tool and support for Citrix and Symantec App Center and the Cryptelo offering, a versatile server-based solution with an innovative approach to encryption key generation. MobilityLab and Cryptelo are small contenders at the moment which is largely responsible for their positioning in the Follower sector.

Again, to select a product it is important to map customer requirements to specific features. There are many examples in which a selected vendor's products weren't "feature leaders" but were still the best solution for a customer's requirements.

### 1.3 Market Leadership

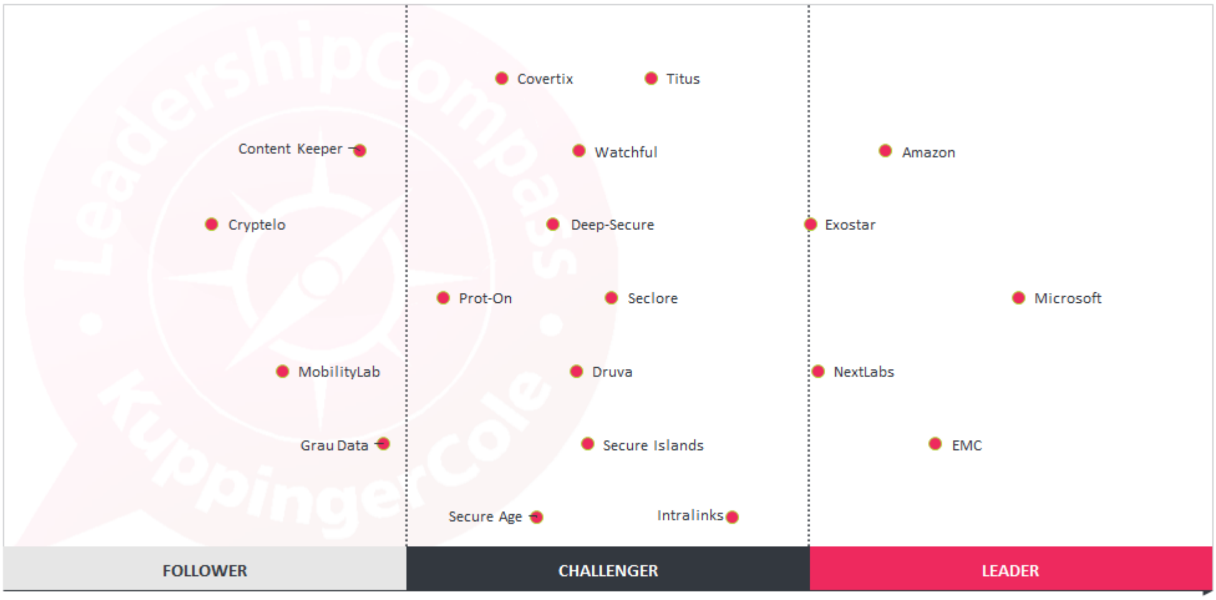


**Figure 3: Market Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

As expected the Market Leadership chart is dominated by Microsoft due to the size of their product ecosystem and their dominance in the rights management market. Also in the leader segment is EMC Syncplicity, again influenced by their size; this should be considered in light of the recent sale of the product to Skyview Capital. Amazon Web Services are in the Leadership space because of the global market presence and WorkDocs solution. Nextlabs, with their cross-sector rights management server enjoys a significant market penetration in the United States but with a growing customer base in Europe and Asia Pacific. They are followed closely by Exostar with their industry-focussed solutions primarily sold in North America and Europe.

In the Challenger space is Intralinks with their very competent Via product providing a secure sharing environment to a global customer base, primarily in North America but with good coverage in Europe and expanding sales in APAC. The mid-section of the Challenger space is crowded: Seclore and Titus both have a global reach, Secure Age is primarily in Asia, and Watchful Software has strong European sales but growing North American reach. Secure Islands have good penetration into Fortune 500 companies. Deep Secure is very focussed on the European market as is Druva: they both enjoy significant market share in their specific market sectors.

In the Follower section Content Keeper, MobilityLabs and Grau Data all have good market penetration in their respective regions. Cryptello is focused on the European market at the present and is in start-up mode.

Again, the positioning of vendors as Leaders, Challengers and Followers simply demonstrates the breadth of the market.  Rating based on the size of their customer base and partner ecosystems disadvantages some vendors which are regional in nature. Such vendors can be a better fit than larger contenders, especially in the vendor's home markets.

### 1.4 Innovation Leadership

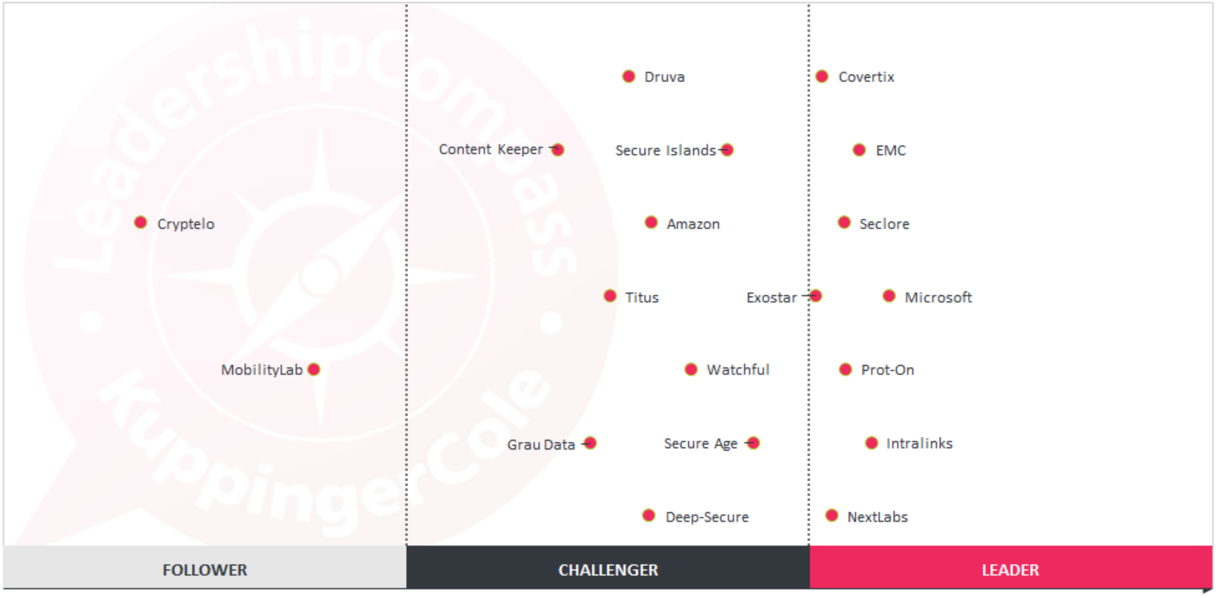


Figure 4: Innovation Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].

Microsoft is also a leader in the innovation space as a result of their developments in AD and Azure rights management, the de-facto standard for IRM solutions. EMC do well with their comprehensive support for mobile devices. Intralinks offer a comprehensive solution encompassing infrastructure, applications and processes. Seclore follows closely in the innovation space with strong email control and audit functions that are available in the product. Prot-On demonstrate innovation in their user interface and easy control of document permissions by users. Covertix also score highly on the innovation scale with their policy management solution and support for cross-boundary and device sharing capabilities. NextLabs is rated highly for their policy framework and content inspection classification Exostar is also in this sector primarily because they have developed some innovative solutions providing improved functionality such as their optimised file transfer technology.

In the Challenger section Secure Age are recognised for their wide support for encryption technology. Druva has an innovative solution with their endpoint enablement and file system integration. Watchful are strong in the support of typical document sharing processes and adaptive classification options. Amazon WorkDocs focusses on ease of use, Secure Islands offer an innovative "interceptor" approach to integrations with popular applications. Deep Secure scores well in the innovation stakes with their flexible “guards” for various data exchange technologies that allows customers to define a solution to fit specific requirements. Grau Data are innovators in their target market with a powerful secure storage capabilities. Titus have a unique classification offering recently extended to mobile devices. Content Keeper are unique in their ability to protect data at the application level, they focus on keeping content secure behind a network device with flexible configuration functionality

Cryptelo at this point, are offering a core product that will fit many customer requirements very well, so just because they do not score highly on the innovation area in no way indicates their capability to suit most secure information sharing tasks. WorksPad from Mobility Lab should also feature on any potential supplier list especially for users in Russia and Commonwealth of Independent States, they offer a highly secure offering with good device support.

## 2. Methodology

KuppingerCole’s Leadership Compass is a tool that provides an overview of a particular IT market segment and identifies the leader in that market segment. It is the compass that assists you in identifying the vendors and products in a particular market segment, which you should consider for product decisions.

This report provides an overview of several solutions for access control and access governance for SAP environments. The range of products and vendors covered in this report is limited to those that were able (and willing) to participate in time.

It should be noted that it is not advisable to pick solutions and vendors based only on the information provided within this report. Customers must always define their specific requirements and analyse in greater detail what they need. This report does not 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.

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market segment. These products to a large extent deliver 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 new ideas, devices, or methods in the particular market segment. They provide several of the most innovative and upcoming features we hope to see in the particular 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 area, 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 best choice for specific use cases and customer requirements but are of limited value in other situations.

In addition, we have defined a series of tables which

- Compare, for instance, the rating for innovation with the one for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path from established vendors, but also established vendors which no longer lead in innovation. These tables provide additional viewpoints on the vendors and should be considered when picking vendors for RFIs (Request for Information), long lists, etc. in the vendor/product selection process.
- Add additional views by comparing the product rating to other feature areas. This is important because not all customers need the same product, depending on their current situation and specific requirements. Based on these additional matrices, customers can evaluate which vendor fits best to their current needs but also is promising regarding its overall capabilities. The latter is important given that a product typically not only should address a pressing challenge but become a sustainable solution. It is a question of helping now, but also of being good enough for the next steps and future requirements. Here these additional matrices come into play.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view of vendors and their products.

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

## 3. Product Rating

KuppingerCole as an analyst company regularly does evaluations of products and vendors. The results are, amongst other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance. KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- 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 IT Model (#70129 Scenario Understanding IT Service and Security Management). 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 state of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the state 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 the portfolio. Thus, when we use the term integration, we are referring to the extent in 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 insure 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. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy) for more information about the nature and state of extensibility and interoperability.

**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, overall we have strong expectations 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 both 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 increase costs, but inevitably lead 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 is of highest importance. This is because lack of excellence in any or all of these areas will lead to inevitable identity and security breakdowns and weak infrastructure.

## 4. Vendor Rating

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

- Innovation
- Market position
- Financial strength
- Ecosystem

**Innovation** – this is measured as the capability to drive innovation in a direction, which aligns with the KuppingerCole understanding of the particular 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. Innovation, as well as being part of the vendor rating, also looks at the innovation in the particular market segment analysed in this KuppingerCole Advisory Report.

**Market position** – measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active, e.g. being weak in one segment doesn't lead to a very low overall rating. This factor takes into account the vendor's presence in major markets. Again, while being part of the vendor rating, this mainly looks at the market position in the particular market segment analysed in this KuppingerCole Advisory Report. Thus a very large vendor might not be a market leader in the particular market segment we are looking at.

**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 or, in the case of IaaS, even the delivery of their IT services.

**Ecosystem** – this dimension looks at the ecosystem of the vendor for the particular product/service covered in this Advisory Report. 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 this report, most of these ratings apply to the specific product/service and market segment covered in the analysis, not to the overall rating of the vendor.

## 5. Vendor Coverage

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

However, there might be vendors, which don't appear in this document for various reasons:

- Limited market visibility: There might be vendors and products/services that 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 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 report will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analysing. In these cases we might decide not to include the product in that KuppingerCole report.

The target is providing a comprehensive view of the products/services in a market segment. KuppingerCole will provide regular updates on their documents.

For this Leadership Compass document, all major vendors we approached responded to the questionnaire. However, there are a number of point offerings in the market that have a limited market visibility and were not included in the leadership analysis for this KuppingerCole Leadership Compass. Some of these vendors are listed in the final section of this document and might become part of the next edition of this document, depending on how they evolve.

## 6. Market Segment

The scope of the Secure Information Sharing problem is quite broad. At its core information must be protected, this usually means encryption; but it must also be made available to appropriate users, this usually means some form of information rights management (IRM). Vendor solutions featured in this document can be segmented into the following categories:

Secure Data Repositories

These solutions deploy a storage mechanism for documents and files. Files are encrypted so that if the storage repository is compromised the files cannot be read. The major benefit is that all documents to be shared amongst a collaborative group can be held in one place and it’s relatively easy to manage encryption keys, and potentially signing keys, amongst the group. Very strong key administration with HSM key storage can be deployed. Version control is also facilitated by having just one copy of a document in a single repository.
In some cases these solutions allow files to be stored anywhere (on-premise or public Cloud) but with management from a secure data centre by providing a special client that users install on their devices. These deployments do require a key management solution to ensure that keys are distributed securely and that a mechanism to archive encryption keys is maintained.

Rights Management

Some solutions adopt an information rights management (IRM) approach whereby documents or data files are coded in order to control access. These solutions apply classification coding to files to manage user access rights to the data (read, edit, print etc.).  Only users with appropriate permissions will be allowed to access the files and then only the actions a particular user is permitted to do, will be allowed. Rights management solutions typically exert a high degree of control over documents with the author determining with whom a file can be shared (typically relying on a directory group) and who will be allowed to alter or annotate the document.

Rights management solutions focus on sharing data, but in a secure way. Rights management provides controlled access to data providing strong management of data-in-use. Documents can be shared while at the same time protected from editing, printing, screen-scraping or saving. IRM solutions can also encrypt data to provide protection of data-in-motion and data-at-rest.

Classification

Rights management solutions are very dependent upon a robust document classification facility. For customers with significant information infrastructure appropriately classifying documents can be a daunting task. These deployments presume a level of planning to determine an appropriate classification model and a policy to control auto-classification functions and exfiltration rules. In some cases classification will be at the discretion of the author, in other case documents will be classified according to a set of rules i.e. all HR documents are classified "secret", finance documents force authors to classify etc. Auto-classification is offered by some vendors; a set of keywords can be established and content inspection can be used to classify documents automatically. Documents with personally identifiable information for instance, can be restricted.

It's also necessary to ensure the company's infrastructure can execute the required policies. For instance, restricting emailing of "internal" documents requires a mail client that can enforce the rule, or limits on saving data to external storage needs network technology that restricts access to internal storage devices.

Gateway

Gateway solutions apply data sharing security via an appliance that sits between the user and the data repository and only permits approved communication between the two.

Content inspection technology is typically employed to ensure sensitive documents and files are not passed externally and to ensure documents stored on the network are adequately protected. Access to repositories can be restricted to specific groups and PKI can be used for access control. Documents will typically not be encrypted at rest since the gateway is securing access to the repository to approved persons only. Content inspection is also more difficult when the data is encrypted.

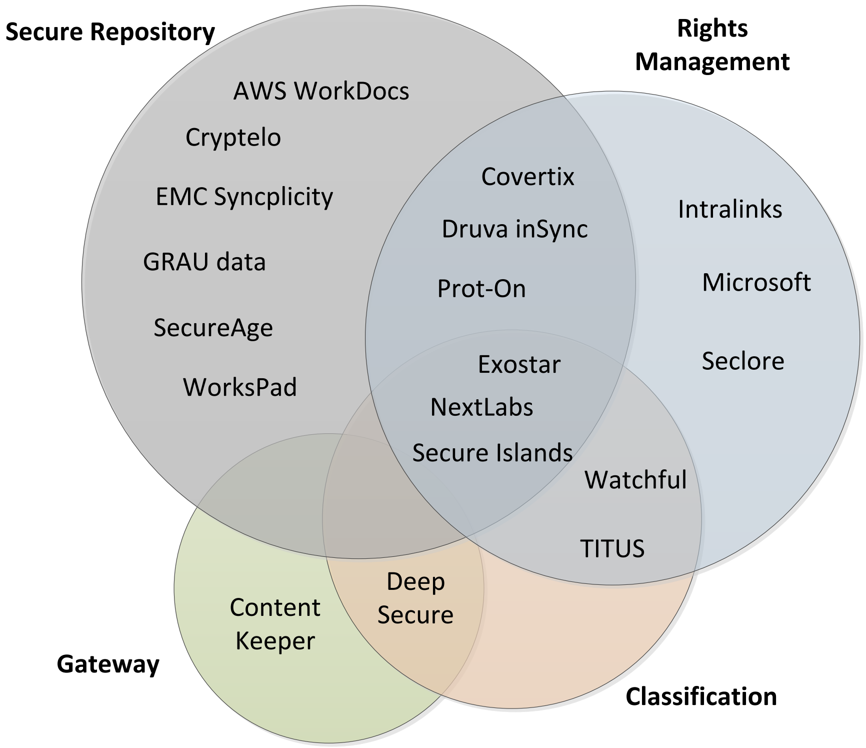


Figure 5: Product Categorization Summary

At this time there is no overarching standard governing secure information sharing.

The European Network and Information Security Agency (ENISA) has issued the European Information Sharing and Alert System. The National Institute of Standards and Technology (NIST) has developed the Security Content Automation Protocol (SCAP) initiative.

Various information rights management solutions are available, including Microsoft RMS, and a Content Management Interoperability Standard (CMIS) has been issued.  There is also the Web Distributed Authoring and Versioning (WebDAV) that has been developed.

These initiatives are to be applauded and are adding to the appreciation of, and solutions for, the task of secure information sharing. This Leadership Compass advises on the support for these initiatives where this information has been made available. Customers should define their integration requirements when evaluating solutions to their specific business requirements.

A useful framework for evaluating product on the market is the Confidentiality, Integrity and Availability (CIA) model:

**Confidentiality – keep secret**

Typically encryption is deployed to ensure data at rest is protected from access by unapproved persons. This does require the exchange of keys which must be accomplished in a way that matches to level of protection afforded the data in question. For instance, in a high security environment keys must be distributed via a secure out-of-band process. Ways that vendors featured in this document protect access to data varies from strong encryption of document repositories to IRM-based document classification mechanisms to gateway access control solutions.

**Integrity – keep accurate**

Maintaining a document's integrity typically involves digital signatures. Again key management is a concern and the longevity of the keys necessary to sign and verify a signature is problematic. A key store is required to validate a document after the signing certificate's expiry.

**Availability – efficient sharing**

Supporting business processes by making available protected documents is at the core of this Leadership Compass. It is unsatisfactory for persons wanting accesses to confidential information having to go through a complex or time-consuming procedure in order to access the required data. While many systems are built around making it difficult to gain access to controlled documents, this is the antithesis of a well-designed secure data sharing facility.

## 7. Specific Features Analysed

Respondents provided detail on their products emphasising the specific features they offer to assist clients in their data sharing activities. Specific detail was requested on the following features:

### 7.1 Core Functionality

Data at Rest

The product must interoperate with mechanisms to protect data that is stored in databases, directories or file stores.  For databases encryption is the preferred protection. Typically asynchronous encryption is employed whereby a key pair is generated, data is written to storage with one key and the other key is used by approved users to decrypt the data when it is retrieved from storage.

For directories secure look-up protocols such as SLDAP are used whereby only requests from approved sources will be actioned. Typically approved sources will be issued a certificate that will be used to digitally sign look-up requests.

File stores are typically protected via Windows Integrated Authentication that can be used be protect against unintended access or modification of data.

Data in Motion

A mechanism is required to ensure data being transmitted between data stores and users cannot be intercepted and understood but unauthorised users. Typical mechanism are server-side SSL encryption or client-side public Key infrastructure (PKI) using asynchronous keys.

Protection of data-in-motion can also be achieved by the use of a gateway device that can ensure data will only pass to approved users. Nefarious activity will be stopped by policies in the gateway appliance.

Data in use

Data sharing products must have some mechanism to protect data being used from corruption or inadvertent access. This can be achieved via the use of secure client software that must be loaded on systems used by members of the collaboration community. The management system then checks to see if the user is a member of an approved group before access is allowed. Other systems use an information rights management approach that codifies documents and ensures that users accessing them have the appropriate permissions to either read or modify them. Fine-grained control can be implemented with IRM systems restricting edit, print, screen scraping or saving of a document.

Strong authentication for data-in-use protection can be achieved via public key infrastructure whereby a user will only be able to open a document when they provide the appropriate key. Keys are normally stored in a certificate held on a client device or a token storage device such as a smartcard.

### 7.2 Discretionary Functionality

Document classification

One of the detractors to the use of rights management schemes is the need to apply classifications to documents.  Classification can be manual (either forced or discretionary) or automated via content inspection or keyword assignment. In some cases sophisticated classification mechanisms can combine attributes such as source application, system location and AD attributes to generate a classification. While automated classification mechanisms can significantly improve adoption rates they typically require a culture change within the organisation to readily accept the attendant constraints.

Key Management

For encryption and digital signing features it is necessary to generate, distribute and archive keys. Respondents were requested to indicate their key management capabilities

Mobile Device support

Increasingly user groups require access capabilities from mobile devices. Some solutions provide a downloadable app. Others rely on web-browser access. The level of authentication and the functionality supported on mobile devices is dependent upon the supported method of access. An app provides the capability to authenticate users and devices and edit/save/print constraints can be applied based on document classification.

Document Types

In any data sharing environment it is important that solutions support the type of documents being shared. While some environments only protect office documents, project teams might want to share Microsoft Project files, SAP users might need to share SAP files or architects might need to share CAD files.

### 7.3 Other Functionality

When evaluating the products, besides looking at the overall functionality we also considered:

- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models

## 8. Market Leaders

Based on our evaluation of the responses to our survey, we've positioned the vendor's product offerings in terms of their market strength in the Secure Information Sharing market segment. The market leaders are shown in figure 5.

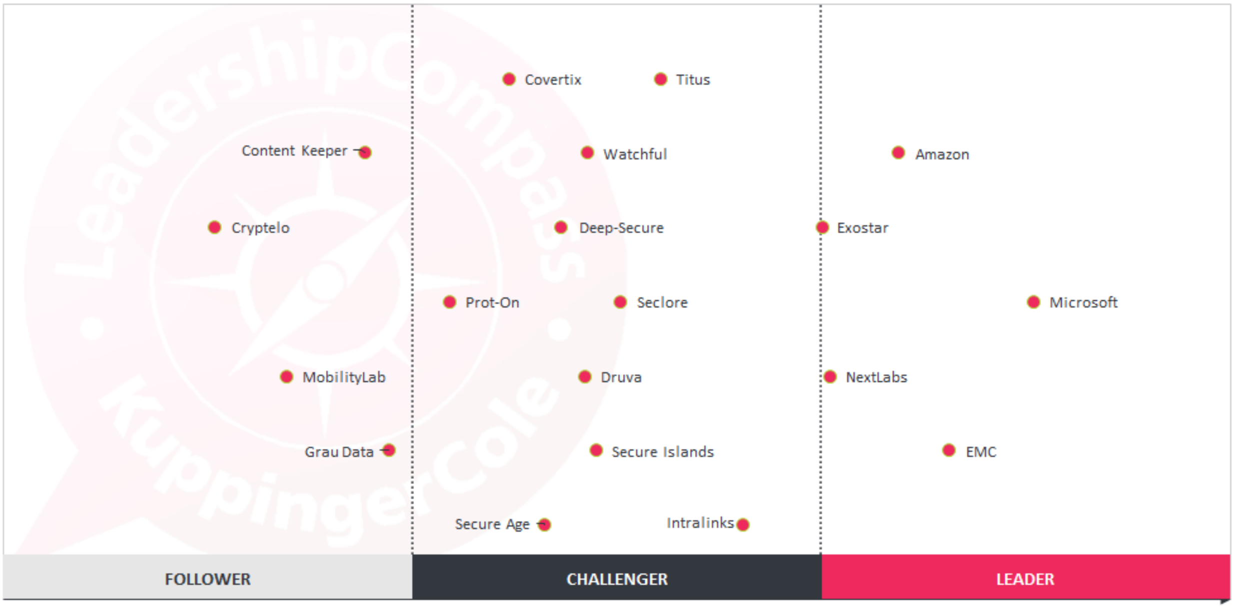


**Figure 6: Market Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

As expected the Market Leadership chart is dominated by Microsoft due to the size of their product ecosystem and their dominance in the rights management market. Also in the leader segment is EMC Syncplicity, again influenced by their size; this should be considered in light of the recent sale of the product to Skyview Capital. Amazon Web Services are in the Leadership space because of the global market presence and WorkDocs solution. Nextlabs, with their cross-sector rights management server enjoys a significant market penetration in the United States but with a growing customer base in Europe and Asia Pacific. They are followed closely by Exostar with their industry-focussed solutions primarily sold in North America and Europe.

In the Challenger space is Intralinks with their very competent Via product providing a secure sharing environment to a global customer base, primarily in North America but with good coverage in Europe and expanding sales in APAC. The mid-section of the Challenger space is crowded: Seclore and Titus both have a global reach, Secure Age is primarily in Europe, and Watchful Software has strong European sales but growing North American reach. Secure Islands have good penetration into Fortune 500 companies. Deep Secure is very focussed on the European market as is Druva: they both enjoy significant market share in their specific market sectors.

In the Follower section Content Keeper, MobilityLabs and Grau Data all have good market penetration in their respective regions. Cryptello is focused on the European market at the present and is in start-up mode.

Again, the positioning of vendors as Leaders, Challengers and Followers simply demonstrates the breadth of the market.  Rating based on the size of their customer base and partner ecosystems disadvantages some vendors which are regional in nature. Such vendors can be a better fit than larger contenders, especially in the vendor's home markets.

Market Leaders (in alphabetical order):

- Amazon
- EMC Syncplicity
- Exostar
- Microsoft
- NextLabs

## 9. Product Leaders

The second view we provide is about product leadership. This view is mainly based on the analysis of product features and the overall capabilities of the various products.

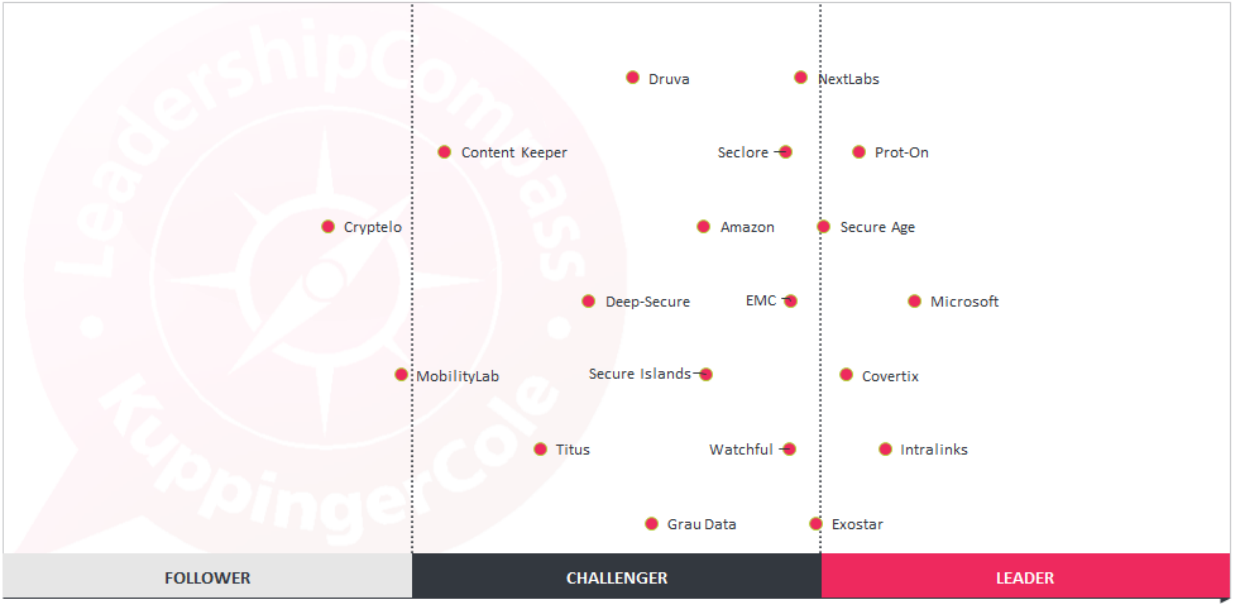


**Figure 7: Product Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

Product Leadership is the view where we look specifically at the functional strength and completeness of vendors' products. Again, we see Microsoft in a leadership position because of their rights management technology. Prot-On are also in the Leader section; they offer a cloud-based solution providing complete control over data at rest, in transit and in-use with a custom designed key management solutions. Intralinks is in the Leader section with their Via product, a multi-tenanted SaaS solution. Covertix also do well in the Product space due to their file access control across multiple platforms. SecureAge is shown just inside the Leader section in the Product space because of their coverage of the secure data lifecycle – protection at rest, in motion and in use.

Closely following in the Challenger section are: Exostar who provide the “go to” solution in their specific industry environments, the NextLabs offering which combines a powerful policy management capability with a good end-client support, Seclore who offer a powerful and comprehensive rights management solution focussed on external collaboration, the EMC Syncplicity product focussed on a frictionless user expericne across a wide variety of file types, Watchful providing a comprehensive classification-based offering with good mobile device support, Amazon with their easy-to-use, advanced collaboration WorkDocs environment, Secure Islands provide a rights management solution with good classification capabilities and email/storage management support, Grau Data offering a strong encryption capability and support for secure data standards, Deep Secure with a military-grade solution based on a secure-server offering, the Druva server-focussed solution with strong encryption and a dual key capability that gives customers full control, Titus with a strong classification approach to document sharing with solutions for both desktop and mobile devices, and Content Keeper taking a different approach based on a gateway solution (both Titus and Content Keeper appear lower in the leadership graph only because their solutions do not align with the classical definition of SIS used to construct this Leadership Compass).

In the Follower section the MobilityLab solution provides an innovative solution in their file sharing tool and support for Citrix and Symantec App Center and the Cryptelo offering, a versatile server-based solution with an innovative approach to encryption key generation. MobilityLab and Cryptelo are small contenders at the moment which is largely responsible for their positioning in the Follower sector.

Again, to select a product it is important to map customer requirements to specific features. There are many examples in which products weren’t “feature leaders” but were still the better solution for a customer’s requirements.

Product Leaders (in alphabetical order):

- Covertix
- Intralinks
- Microsoft
- Prot-On
- SecureAge

## 10. Innovation Leaders

The third angle we took when evaluating products concerned innovation. Because of the emerging nature of the Secure Information Sharing market Innovation is, from our perspective, a key capability. Innovation drives customer satisfaction when they receive new releases that meet their developing requirements. Thus, a look at innovation leaders is important part of analyzing product features.

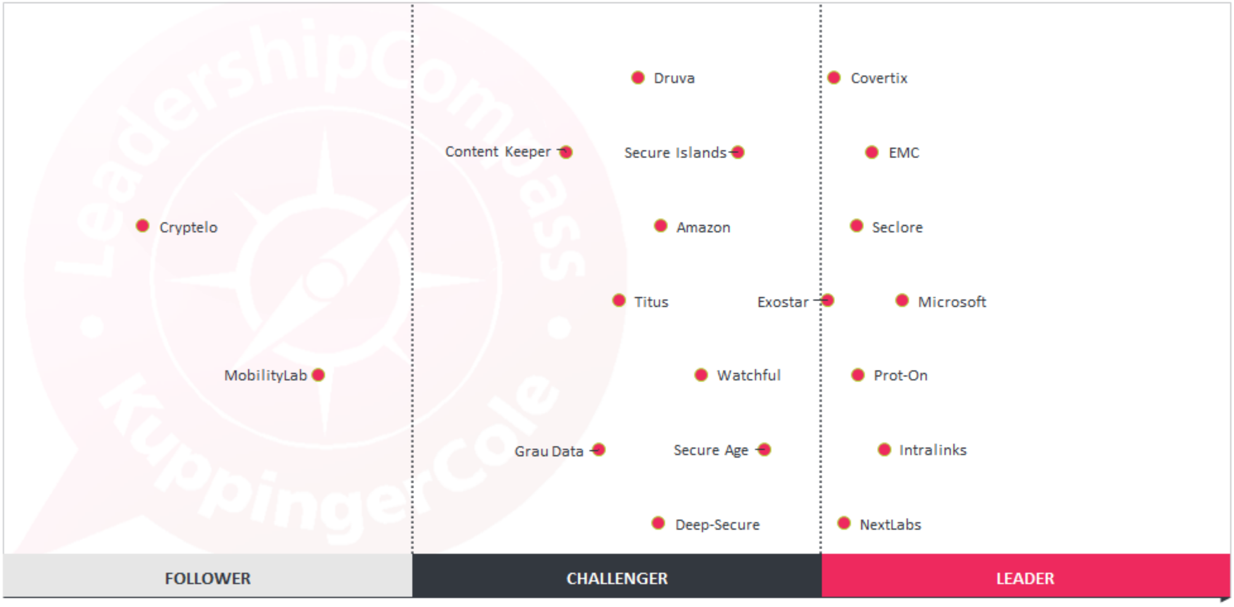


**Figure 8: Innovation Leaders in the Secure Information Sharing market [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

Microsoft is also a leader in the innovation space as a result of their developments in AD and Azure rights management, the de-facto standard for IRM solutions. EMC do well with their comprehensive support for mobile devices. Intralinks offer a comprehensive solution encompassing infrastructure, applications and processes. Seclore follows closely in the innovation space with strong email control and audit functions that are available in the product. Prot-On demonstrate innovation in their user interface and easy control of document permissions by users. Covertix also score highly on the innovation scale with their policy management solution and support for cross-boundary and device sharing capabilities. NextLabs is rated highly for their policy framework and content inspection classification Exostar is also in this sector primarily because they have developed some innovative solutions providing improved functionality such as their optimised file transfer technology.

In the Challenger section Secure Age are recognised for their wide support for encryption technology. Druva has an innovative solution with their endpoint enablement and file system integration. Watchful are strong in the support of typical document sharing processes and adaptive classification options. Amazon WorkDocs focusses on ease of use, Secure Islands offer an innovative “interceptor” approach to integrations with popular applications. Deep Secure scores well in the innovation stakes with their flexible “guards” for various data exchange technologies that allows customers to define a solution to fit specific requirements. Grau Data are innovators in their target market with a powerful secure storage capabilities.

Titus have a unique classification offering recently extended to mobile devices. Content Keeper are unique in their ability to protect data at the application level, they focus on keeping content secure behind a network device with flexible configuration functionality

Cryptelo at this point, are offering a core product that will fit many customer requirements very well, so just because they do not score highly on the innovation area in no way indicates their capability to suit most secure information sharing tasks. WorksPad from Mobility Lab should also feature on any potential supplier list especially for users in Russia and Commonwealth of Independent States, they offer a highly secure offering with good device support.

Innovation Leaders are (in alphabetical order):

- Covertix
- EMC Syncplicity
- Exostar
- Intralinks
- Microsoft
- NextLabs
- Prot-On
- Seclore

## 11. Product evaluation

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

## 11.1 AWS

Amazon Web Services is the largest global supplier of Cloud services. They now offer WorkDocs (formerly Zocalo) as a secure collaboration tool for organisations.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Leverages AWS strengths for secure document storage<br>• Maintains good key management for document/file encryption<br>• Good support for mobile platforms via OAuth and OpenId Connect. | • Does require use of AWS storage infrastructure<br>• Microsoft Azure clients will need to deploy an AD instance as a repository of user attributes. |

Table 1: Amazon Web Services

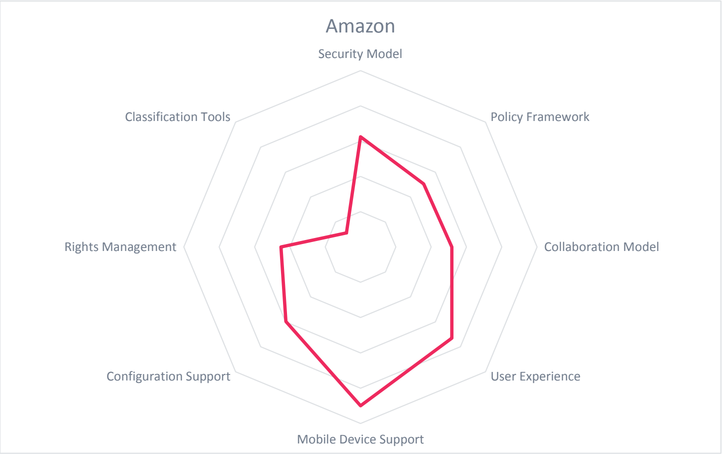
WorkDocs provides a simple environment for end users that allows them to share files and folders, set contributor or viewer permissions on their documents, limit downloads, set "public" files or share with external parties. Users can request feedback and set deadlines via a notification workflow. The intent is to dramatically reduce the number of documents sent as email attachments.

A central hub provides document control and versioning. Supported platforms include PCs, Macs, tablets (IoS, Android and Kindle) and smartphones (IoS, Android). The Amazon WorkDocs app is loaded onto a user's tablet or smartphone and a number of device-optimised features are then available. Users can then download files, annotate them and save them back to the WorkDocs storage. Off-line access is also supported with encryption of files on the external device. All AWS features such as 2FA for registered devices are supported. WorkDocs can also be used within Amazon WorkSpace virtual desktop service. All data is encrypted at rest and in-transit. Policies control user sharing behaviour and audit logs track document activity. WorkDocs is available at AWS datacentres globally.

Key management is a strength of AWS with good direction on managing root keys and access (user) keys. Most clients using WorkDocs will elect to use temporary security credentials. In this instance keys are short-lived and will auto-renew. For heavier users of AWS, rotation of access keys is supported and recommended. AWS are strong in the governance space with extensive administrator controls and Cloud environment management tools.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | neutral |
| **Integration** | neutral |
| **Interoperability** | neutral |
| **Usability** | strong positive |

Table 2: Amazon Web Services Product Rating



## 11.2 Content Keeper

The Content Keeper Secure Internet Gateway is a security appliances that sits between web-servers and data repositories to provide comprehensive content filtering and malware threat monitoring. The device provides a click and configure administrative console that allows administrative personnel to configure the device to allow or deny access to URL groups that are deemed inappropriate or offensive. For instance any site in the "adult content" group can be disallowed with a single click, which would block any attempt to access such a site. The Web 2.0 control feature allows granular access to the popular social networking sites. For instance, the Facebook chat might be enabled but the upload of picture and video could be prohibited. Policies can be restricted to individual users, IP address ranges or AD groups.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Very fast content filtering to provide transparent security for users<br>• Effective blocking of inappropriate sites<br>• Pre-defined management console with graphical depiction of system status | • Not a storage encryption device - does not secure data at rest<br>• Fine-grained attribute-based access control could be attractive to users |

Table 3: Content Keeper

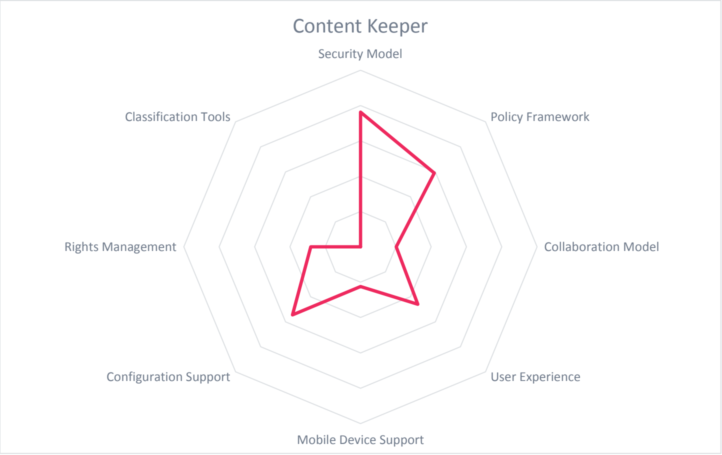
Typical applications for the gateway are: authentication verification of SSL sessions to authorised service providers, content filtering on keywords, and policy management for secure data sharing.

Content Keeper maintains a collaborative filtering service that provides push notifications of real-time threats to all client devices in the collaborative group. For instance, in a school environment an inappropriate website identified by one school can be disabled for all schools in the sharing environment.

All configuration is via the Management Console which is a browser-based and allows authenticated personnel to establish policies and generate reports. Data is aggregated from multiple Content Keeper devices and can be used to feed BI analytics and management dashboards. Policies can be time-of-day aware, granting access to a specific protocols or URLs for a period of time, tuning access off when the access period expires. This can be useful for project or for maintenance purposes.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | neutral |
| **Integration** | weak |
| **Interoperability** | neutral |
| **Usability** | neutral |

Table 4: Content Keeper Product Rating



## 11.3 Covertix

The SmartCipher product suite from Covertix provides a highly functional file and date protection regime that is independent of the device, network or platform on which it is used.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Complete and comprehensive file access control across multiple platforms<br>• Policies inbuilt to files to maintain access control from all potential devices and access locations<br>• Mobility solution is clientless<br>• Azure AD supported for identity attributes | • Requires file modification to store policy information<br>• A SmartClient app is required on all user's PCs to enforce policies<br>• Mac OS system still in development |

Table 5: Covertix

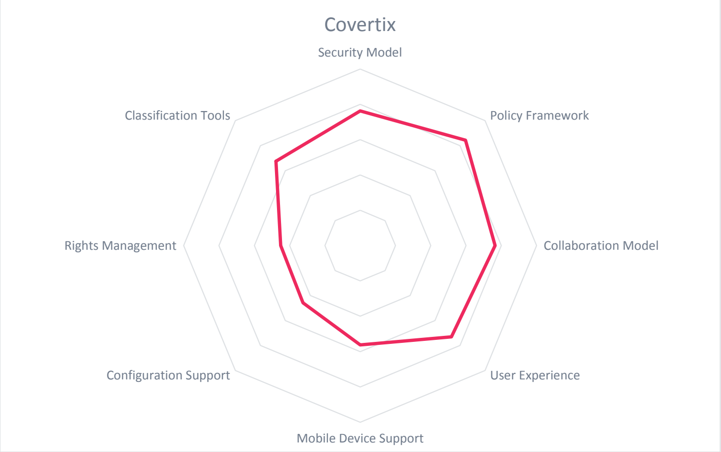
On-premise it can securely manage documents and files in the corporate data store managing and monitoring data at rest or in motion on the company's network. SmartCipther Mobility extends file protection to external devices without the need to download an app. SmartCipther Collaborator provides tools to securely share information with business partners, contractors and clients. SmartCipher Cloud provides file protection for documents stored in popular on-line storage services such as Dropbox, Google Drive and OneDrive. Addons are provided for Microsoft SharePoint and Citrix Xenapps.

Covertix provides monitoring and protection of files seamlessly across diverse platforms. Access to documents is controlled via policies established by the corporation which are then observed across the organisation's computing environment. Facilities are provided for the automatic identification of PII data, for file control and for document protection. Actions on files such as save, edit, copy/paste and print are controlled by polices enmeshed in the files. This provides the ability to manage access in real-time and revoking access immediately when appropriate.

Covertix provides audit reporting and policy violation alerts. Indeed deploying monitoring as a first step is often recommended with phasing-in full file and folder-level security when organisational or departmental policies have been developed. Once the monitoring facility is deployed reports on file types, sensitivity, location, file usage and access detail can be generated.

| | |
|---|---|
| **Security** | strong positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 6: Covertix Product Rating



## 11.4 Cryptelo

Cryptelo is a relatively new supplier to the secure data sharing sector. Documents are stored securely in the Cryptelo Drive Cloud application.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Very high AES-256 elliptic curve cryptography using a unique key for each access<br>• Employs a standard browser with no need to install client software<br>• Intuitive user interface for document monitoring and management | • Lack of native application support could hamper document modification<br>• No mobile device app support |

Table 7: Cryptelo

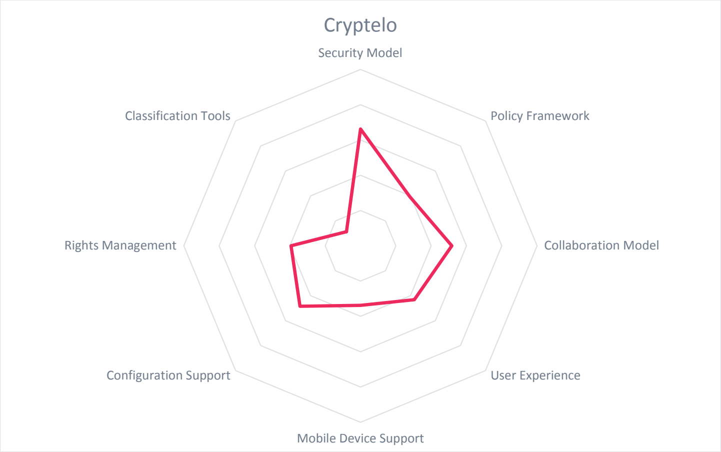
The Cryptelo Drive product is a server-based document repository with very high encryption standards. Cryptelo offer an in-Cloud solution ideal for document sharing to external business partners or valued customers. It can also be deployed on-premise for greater control over key creation and storage. The file/document repository provides very high-level encryption protecting documents at rest and in motion; encryption/decryption occurs on the client device.

No client software installation is required; Cryptelo supports all mainstream browsers. The user interface allows users to see activity on documents in each folder to which the user has access. The document owner is indicated and users with appropriate permissions can access protected files and perform the actions which have been allowed by the owner.

The central storage of documents facilitates sharing with real-time updates. As soon as a modification is made to a document others with permission to access the document will see the changes.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | critical |
| **Interoperability** | weak |
| **Usability** | neutral |

Table 8: Cryptelo Product Rating



## 11.5 Deep Secure

Deep Secure offers tailored solutions to a customer's specific requirement combining multiple security components in such a way as to satisfy most secure data sharing requirements. Solutions typically include an information exchange gateway utilising a variety of "guards" to enable data sharing functionality.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Highly secure infrastructure is supported with full PKI capabilities and HSM support<br>• Central policy management controls the way in which secure information is communicated from sender to recipient | • Relies on constraining communication rather than classification and secure sharing functionality<br>• Limited support for mobiles – enabling communications to a secure mobile application would be useful |

Table 9: Deep Secure

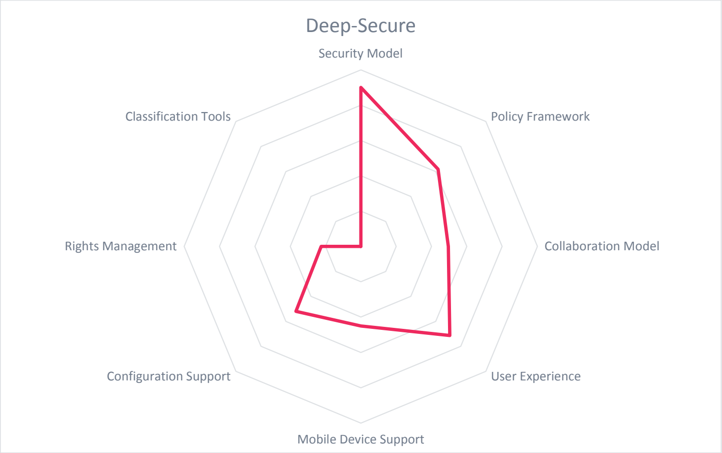
Deep Secure offer Mail, Web, XML, Chat, Directory and File guards to protect information at multiple levels. For instance, security labelling is one such level whereby a "guard" will compare a document's security label against policy to determine if the document/data in question can be passed to the requestor. User authentication relies on the client's identity and access management environment and typically uses digital signatures to secure communication.  "Guards" have extensive file format knowledge to protect data leakage from, as well as malware insertion into, protected networks. Guards utilise a common policy manager. Deep Secure content inspection guards provide deep content inspection for email, messaging systems. Web browsing web-service applications, file transfer and directory replication. Guards can be used to compare security labels, obfuscate email addresses, remove attachments and validate digital signatures and decrypt messages.

There are two sides to the Deep Secure offering: protecting the communication of secure data and protecting storage of secure data. Communicating data securely is enabled via sender/recipient groups that provide a flexible way to apply sophisticated policy-based access control. For data repositories Deep Secure support server-based solutions that offer a wide range of security levels support from a highly secure operating system such as Oracle Solaris for on-premise solutions to inexpensive Centos server deployed in the Cloud.

Features include application layer proxies for access control to protected resources and content verification services for inspection of encrypted traffic in real-time. The deployed solution can be PKI based with both digital signing and encryption supported.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | weak |
| **Interoperability** | neutral |
| **Usability** | positive |

Table 10: Deep Secure Product Rating



### 11.6 Druva

Druva offer an innovative solution around their inSync product. It can be deployed on-premise or on an enterprise-level private Cloud offering on the AWS Cloud service. Druva InSync provides tight integration with enterprise file systems (NFS) and mobile devices (iOS, Android). Centralised policy management from the administrator console is supported, global deduplication technology is supported as well as user storage quotas.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| ● Unique split-key encryption mechanism means no external access to unencrypted data is possible<br>● Support for native OSs on Windows and mobile devices.<br>● Tight file server integration with de-dup and dashboard analytics | ● Automated classification of documents would be advantageous for some implementations.<br>● Support for Azure AD is not available at the moment but is planned<br>● Cloud deployment is limited to AWS at the moment |

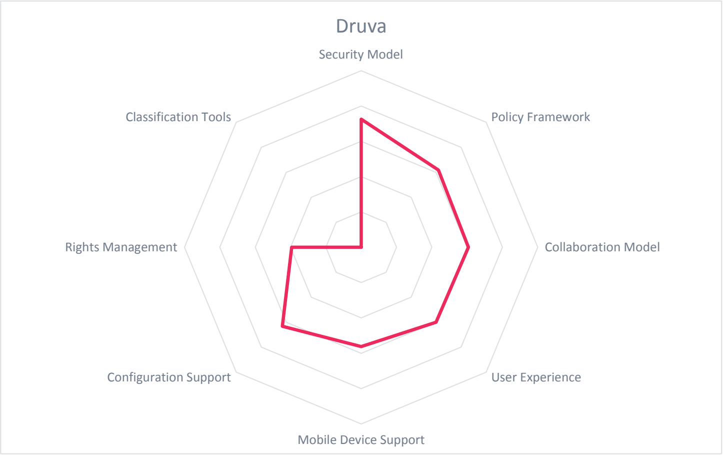
Table 11: Druva

Druva is particularly strong in the endpoint enablement area providing users unprecedented control over their file folders, determining with whom they should be shared and providing dashboard visibility over endpoint protection.  User control over backups is comprehensive with users able to indicate who can view backup files and for how long backups should be retained. This provides control over a major source of intellectual property loss. Data governance is facilitated by a dashboard indicating data storage statistics and data sharing events. Users can share data securely via sending links to the data in question or via adding approved users as collaborators on folders. Editing of shared documents is supported across Druva supports network storage facilities for on-premise storage node or Amazon S3 for a Cloud-based storage node. Supported directory services include AD and 3rd party identity service providers via SAML.

Druva consider their encryption mechanism a competitive advantage with session-based keys generated at run-time with no capability for an external agent getting access to unencrypted data. Data at rest is encrypted via 256 bit AES, data in motion is encrypted via 256 bit SSL and data in use at the endpoints with the inSync DLP features.  A split-key encryption mechanism is utilised with a unique key generated on session commencement which is then encrypted with the administrator's key. A session key cannot be accessed by Druva and ceases to exist when a session ends.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | neutral |
| **Usability** | positive |

Table 12: Druva Product Rating



### 11.7 EMC Syncplicity (Note: EMC has recently sold the Syncplicity product to Skyview Capital)

The Syncplicity tool provides file synchronisation and file sharing functionality and can be configured to synchronise any folder on a user's computer.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Easy-to-use data sharing functionality with fine-grained control over folders<br>• Good use of dashboard technology to advise users on data sharing access<br>• Supports LDAP and SQL queries | • Confusion between Syncplicity and Panorama product offerings<br>• Azure AD support should be considered |

Table 13: EMC Syncplicity

Syncplicity Panorama provides content viewing across file shares, home directories, SharePoint and Documentum. Syncplicity natively supports rights management i.e. copy/print, screen capture and location restrictions as well as watermarking. Document formats include all Office files and PDFs. In-app editing and annotation is supported. Automatic version control is supported with native clients for Windows, Mac, iOS, Android and Windows 8 (x86 and RT). Office 365 integration is provided via the Syncplicity Windows 8 app. Both Cloud deployments and hybrid deployments are supported. A policy-based approach is used with real-time access control based on group membership and folder settings. Both file and object (EMC Atmos and Amazon S3) storage. All documents are encrypted with AES-256 bit encryption. Data in transit employs SSL 256-bit encryption; keys are transported via an encrypted HTTPS/TLS tunnel.

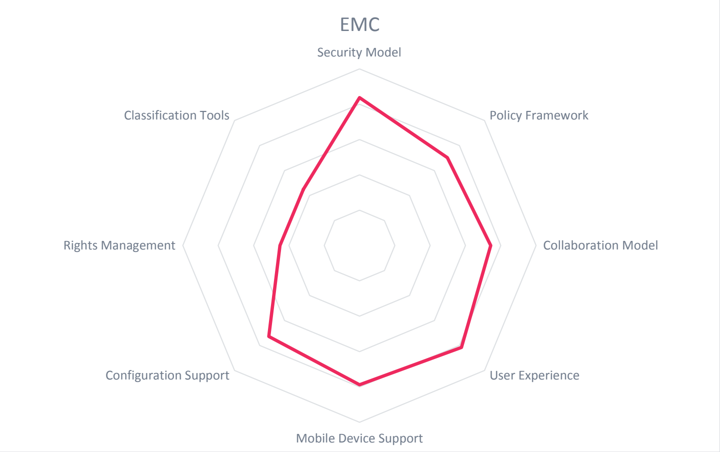
A wide range of image and video formats can be securely shared as well providing a frictionless user experience while avoiding data leakage. Visual search provides users a display of their shared folders with visual depiction of the users or groups with access to the folders. Point and click management of folder sharing is supported. Access statistics for shared documents can be viewed via the graphic user interface which can also display geographic access details.

Data is stored in secure repositories either in SSAE16 protected data centres or in secure on-premise facilities. Authentication of remote devices can be achieved via RESTful APIs using standards such as OAuth2.0. Third party mobile device management tools such as MobileIron and AirWatch are supported.

Supported directory services include AD with ADFS for provisioning, group management. Integration with any SAML 2.0 gateway is also supported. A policy management facility is provided whereby policies can be attached to groups from a library of over 30 policies. Prioritized policy sets accelerate policy evaluation.

| | |
|---|---|
| **Security** | strong positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 14: EMC Syncplicity Product Rating



## 11.8 Exostar

Exostar is a leader in industry collaboration environments and actively supports identity management and document sharing in supply chain and R&D. Exostar's solutions support the aerospace and defense, life sciences and healthcare sectors which are heavily dependent upon secure distribution of documents to a highly distributed user base. The underlying document management technology is SharePoint.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Functionally complete managed service with strong encryption services<br>• Data-in-use protection via one-time password technology<br>• Innovative file-transfer support for fast transmission of large files | • Azure AD not supported as the present time<br>• Browser-based client can view only<br>• Only iOS fully supported via Secure mShare |

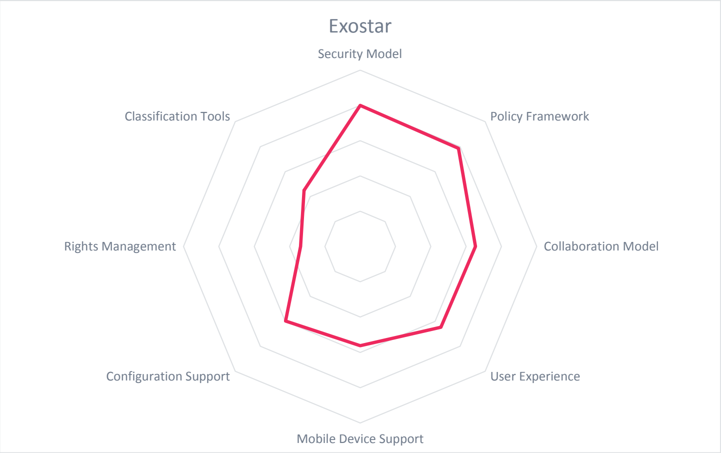
Table 15: Exostar

ForumPass (FP) provides a document and file sharing solution that enables both internal and external sharing of documents under a single management environment.  FP offers multiple tiers of security to support business scenarios requiring highly sensitive documents and files. FP sits behind Exostar's Identity Hub, with access controlled by Exostar's Managed Access Gateway (MAG). Both products are offered as Cloud-based SaaS offerings. Authentication can be supported from Exostar's identity provider service or from a client's on-premise identity store via federated services. Users with a valid session will experience SSO to other service providers in the federation. SAML 1.x, 2.0 and WS-Fed are supported, with Exostar handling any necessary protocol translation. Exostar offer a full certificate authority service and identity proofing and validation service for high-assurance environments, they support PKI and two factor authentication services such as one-time passwords and common access cards. Documents can be protected via a full DRM solution with access controlled via policies that determine access rights on the basis of group membership or manually granted access rights. Policies are attached to files which will control access and usage rights of users. Policies can be modified which will alter the user permissions regardless of where the files may be stored. Exostar's Governance Council and application owners generate applicable policies which are managed by Exostar. DRM provides usage audits and reporting,

ForumPass supports WebEX services to an extended collaboration network. Operating the WebEX Meeting Centre in Restricted mode will exclude external participants and sessions will be encrypted. File transfer is via a patented UDP-based protocol enabled via a self-installing plug-in. For networks blocking UDP packets fall-back to TCP or secure file transfer proxies is supported.

| | |
|---|---|
| **Security** | strong positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 16: Exostar Product Rating



### 11.9 Grau Data

Grau Data has a long reputation as a provider of secure storage solutions. DataSpace provides a high-availability, highly secure way to share data. The Web interface is HTML5 so it is customisable via style sheets and it is compatible with all the major smart devices. Native iOS and Android apps are also available. SAML and OAuth2 are supported for authentication.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Intuitive user interfaces provide easy-to-use access to DataSpace features<br>• Wide support for mobile devices via the HTML interface<br>• Dual key protection for files in the document store | • Mobile applications provide view capabilities only<br>• DataSpace creates its own user repository rather than relying on enterprise identity stores<br>• HSM support is planned for 2015 |

Table 17: Grau Data

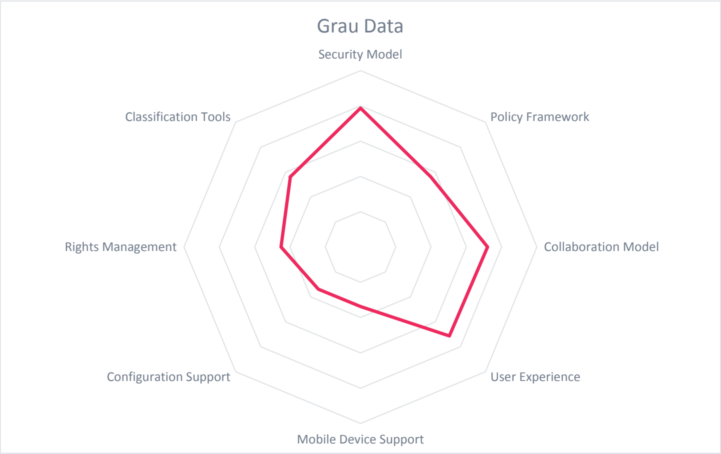
DataSpace users manage file storage via a screen that displays their folders on the left-hand side with the associated access rights in the centre pane. Document owners add and delete users to access groups is via a GUI with drag-n-drop functionality. Checked-out documents are then opened in their native apps and saved back to the secure storage when finished. Document versioning is supported. There is also a user admin tool that allows administrators to create and manage members of groups. A TouchUI facility is provided for devices with touch-screens, the interface is optimised for touch screen operation. The product comes with extensive tutorials.

Document permissions (read, edit, print etc.) are assigned to roles and roles are assigned to users. Roles can be assigned to global or private groups as well. File-level permission can be assigned via an ACL to a shared folder. DataSpace support the CMIS content management interoperability services standard by OASIS and should integrate with any other compliant document store. It is fully tested against the WebDAV, the HTTP extension for distributed authoring which means that any WebDAV client should interoperate against the DataSpace document repository.

At the file level DataSpace divides files into “chunks” which are then encrypted and sent to any storage device the client chooses. Multi-levels of encryption are supported with full client-control over keys. DataSpace supports ownCloud clients. Optionally the DataSpace repository can be fully encrypted via the Boxcryptor.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | neutral |
| **Usability** | neutral |

Table 18: Grau Data Product Rating



### 11.10 IntraLinks

Intralinks is a supplier of a managed document sharing service. With Intralinks VIA users can collaborate securely and productively, using any device. Customer can select where their documents are stored, Intralinks maintain datacentres in the UK and USA. The Intralinks platform is a cloud-based, multi-tenanted SaaS solution purpose-built to enable secure content sharing and collaboration within and between companies. It can synchronise across multiple devices and allow documents to be shared with external parties. Intralinks VIA provides an easy-to-use platform. Documents and be unshared as easily as they are shared.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Strong encryption model<br>• Drag 'n drop user interface<br>• Choice of UK or US based document repository | • Lack of global solution at the present time<br>• Smartphone device limited to iOS & Android<br>• Mobile device editing is limited to a web-browser |

Table 19: Intralinks

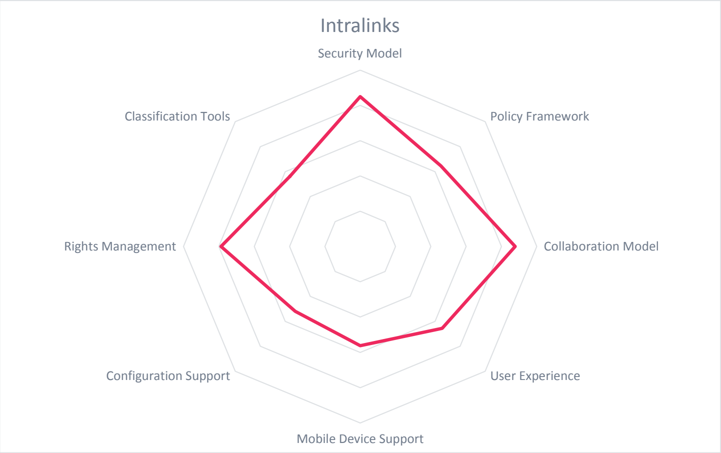
Intralinks adopts an "IRM by design" approach marks and encrypts documents to keep them secure and to allow sharing policy to be applied.  The Intralinks solution is "plug-in free" allowing documents to be opened in their native format while still being protected in Intralinks secure environment which will enforce access rights to editing printing and downloading functions. Each business group can manage policies via the administrator portal. This includes managing IRM settings, white/black lists and synchronising desktops and mobiles.

Intralinks offers a strong authentication model that includes customer managed keys ensuring that organisations keep control over their encryption keys and that no one outside the company can get unencrypted access to documents unless specifically granted permission to do so. For data-at-rest documents are 256-bit AES encrypted with a unique key comination, clients can mange their own master keys. For data-in-transit  2048-bit RSA TLS is used and 256-bit AES packet encryption can be deployed. For data-In-use Intralinks uses existing IT policies and provides full traking and anlystics with features such as remote expiry of documents.

Intralinks manages identities via a user's email address. Administrators' provision users into their business groups and users can invite participants to set up their own accounts.  Intralinks offers clients for Windows and MAC users as well as apps for iOS and Android.

| | |
|---|---|
| **Security** | strong positive |
| **Functionality** | strong positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 20: Intralinks Product Rating



### 11.11 Microsoft

The Microsoft secure information sharing offering is based on Azure Rights Management Service (Azure RMS) and AD Rights Management Service (ADRMS). Azure Rights Management supports information rights management (IRM) in Exchange On-line, SharePoint Online and Office 365. It also supports on-premise products such as Exchange server, SharePoint Server and windows file servers running File Classification Infrastructure.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Defacto standard for Office documents<br>• Coverage for on-premise and Cloud services (Azure only)<br>• Implicit trust between organisations in Cloud-based environments | • ADRMS requires explicit trust to be defined between AD domains<br>• Operational constraints on non-Azure Clouds |

Table 21: Microsoft RMS

Azure is Microsoft's Cloud service. It provides several services to reduce the risk of a network compromise and improve protection of assets from inappropriate access. The device registration feature ensures network access from authorised devices i.e. those that have been explicitly enrolled in the organisation's list of mobile devices approved to access the network. The multi-factor authentication feature registers a personal device, usually a smartphone, to approved users and a message will be sent to the device as part of the login process to act as the "something you have" factor. Both ADRMS and Azure RMS provides document-level control and it is the defacto standard for Office documents. Azure RMS is now part of the Office 365 product and provides protection for all Office documents. It is included in the Enterprise Mobility Suite, AD RMS is the on-premise deployment.

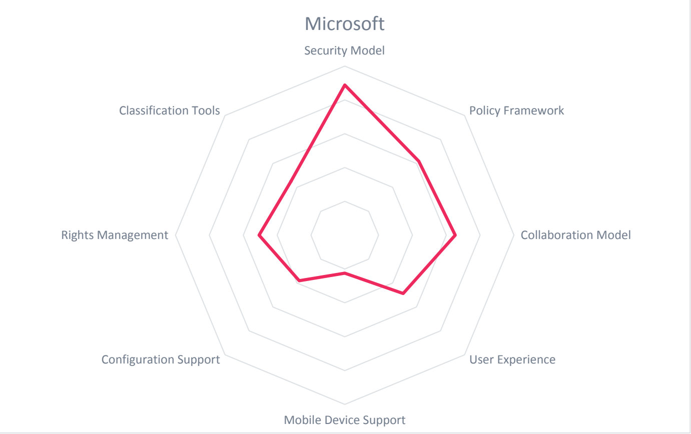
The Rights Management Sharing App for Windows is a free app for organisations that use Azure RMS or AD RMS. Ii allows users to interoperate with partners rating their documents with using Microsoft IRM.

Microsoft also provide an SDK for service providers to incorporate into their apps thereby imposing IRM constraints on document sharing. This includes the Word, Excel and PowerPoint Office formats as well as PDFs, JPEG & PNG images, and text formats such as CSV and XML. There is also a generic file protection encapsulation format (PFILE). Microsoft Outlook is an "enlightened" email application and will observe restrictions such as "do not forward".

On-premise customers can choose to store ADRMS keys in the standard CAPI cryptographic storage facility or use their own SQL database or hardware security module (HSM). In the Cloud keys are stored in the Azure environment or a hosted hardware repository whereby customers provision their own keys.

| | |
|---|---|
| **Security** | strong positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | strong positive |

Table 22: Microsoft RMS Product Rating



### 11.12 MobilityLab

WorksPad is a data and document sharing tool that is available for on-premise installations. It is designed to provide secure, policy-based access to internal corporate information by mobile users.

Users of the application are able to gain access to shared documents and grant/deny access to others via an easy-to-use screen. The WorksPad administrator can apply access permissions via a policy profile. This can be used to control actions such as opening documents, sending by email or printing.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Easy-to-use interface for document sharing control<br>• Support by major mobile device management tools<br>• Direct File Sharing tool for real-time collaboration | • Restrictions such as copy/paste and deny-print are planned<br>• On—premise solution only |

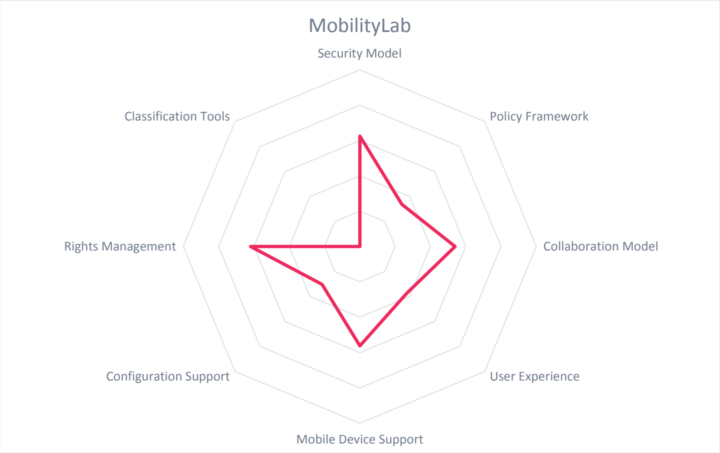
Table 23: WorksPad

Mobile devices are supported via the WorksPad apps which provide a protected, secure environment for collaborative workforces across PCs as well as iOS and Android devices. WorksPad provides a multi-screen operation bringing PC-like operation to tablets. File and screen sharing can restrict opening of files in third party apps, restrict emailing of files and stop copying functions. Office formats for Word, Excel and PowerPoint are supported as well as PDF and TIFF files. Microsoft environments are supported via the SMB network file protocol and SharePoint document stores. A file synchronisation agent is also provided.

MobilityLab has developed a real-time collaboration tool, called Direct File Sharing that enables meeting attendees or work teams to share documents directly via services such as Wi-Fi. Security is enabled via the use of security token to control access by corporate mobile devices and prohibit sharing with external users. Authentication is based on user and group detail that is maintained in an MS SQL database on the MobileSputnik server. Initially user data is imported from AD and then WorksPad-specific functions are added. WorksPad maintain a data repository of users. Direct File Sharing is based on the AllSeen Alliance Framework. WorksPad supports Good Dynamics mobile device management, Citrix Worx and Symantec Appcentre.

| | |
|---|---|
| **Security** | neutral |
| **Functionality** | neutral |
| **Integration** | weak |
| **Interoperability** | weak |
| **Usability** | positive |

Table 24: WorksPad Product Rating



### 11.13 NextLabs

NextLabs provides data classification, access control, secure storage and rights management in one solution. Their product offering leverages attribute-based policies to control access to applications and rights protected data wherever they reside, as well as data segregation and loss prevention capabilities.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Longevity on the market with a mature data sharing model<br>• Industry involvement and support for standards<br>• Web-based solution without client install<br>• File-type agnostic with support for engineering data such as 2D , 3D and CAD | • Currently limited support for mobile devices |

Table 25: NextLabs

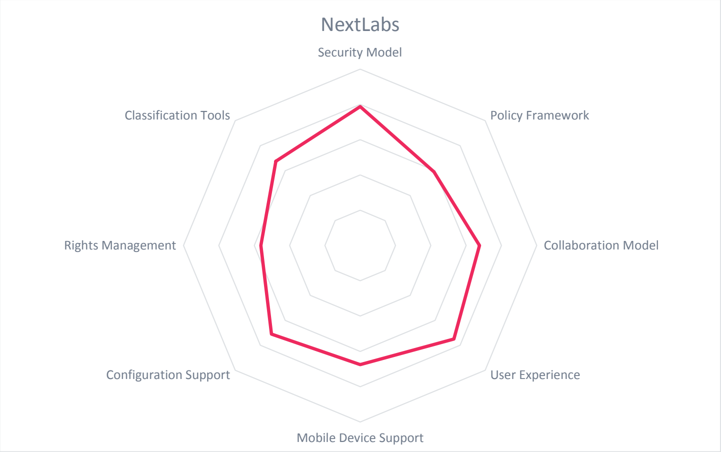
The NextLabs product offering consists of a Rights Management Server, providing a secure document sharing solution for users via HTML5 applications, and a Rights Management Client which provides data classification and rights management controlling access to a wide number of file formats and applications. Both products leverage the NextLabs Control Center which is used to centrally manage policies and provide audit facilities. The Control Center Policy Platform maintains a user identity repository of approved users and an events module to manage and report on events. The Information Control module manages data classification, access control, encryption and communications with the Control Center. Classification can be user-driven or rule-based. The Information Control Enforcement module performs the rights management; it consists of enforcement connectors for supported file stores. NextLabs also provide a web-based Rights Management Server which provides secure access and usage controls to rights protected content of any kind with rich functionality without any client software

The NetLabs Rights Management Client is supported on Windows, Mac, Linux and Android. They also provide integration with key enterprise applications including SAP, Siemens Teamcenter, Dassault Enovia, PTC Windchill, SharePoint, Office 365, file servers and cloud storage such as Dropbox. User identities can be sourced from AD, AzureAD, or any LDAP-compliant directory or HR systems such as SAP.

NextLabs provide a strong authorisation module that meets various industry regulatory requirements such as the North America Electricity Reliability Corporation (NERC) and export compliance protection required by agencies such ITAR, EAR, BAFA and the UK Export Controls Act. NextLabs also work with with various standards bodies including NIST, OASIS, OpenLiberty and TSCP.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | positive |
| **Interoperability** | positive |
| **Usability** | neutral |

Table 26: NextLabs Product Rating



## 11.14 Prot-On

Prot-On provide a complete offering with the management server deployed on-premise or on Prot-On's Cloud service. The on-premise version affords customers more control over security features such as key management but Cloud storage deployment on services. Managed documents can be stored locally or on services such as Dropbox, OwnCloud and GoogleDrive. For Cloud deployments a REST API is provided.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| ● A good balance between security and ease-of-use that suits most deployments.<br>● Easy-to-use client screens for setting permission levels for users/groups<br>● Multi-channel sharing with seamless management of internal and external users | ● Lack of classification tools for document repositories |

Table 27: Prot-On

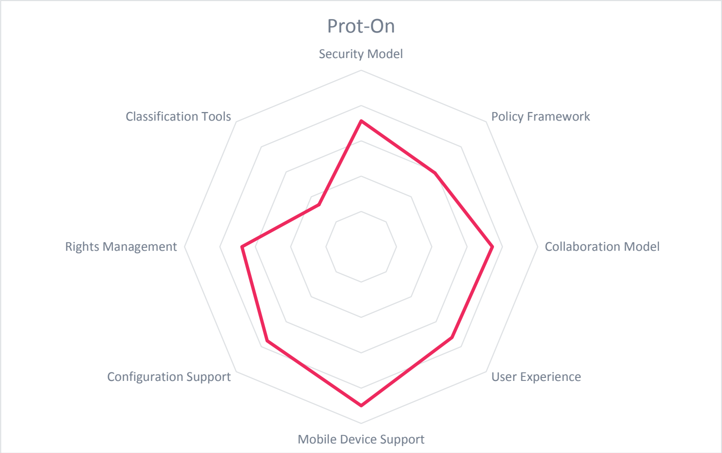
When a file has been processed via the Prot-On service it is encrypted and stored with a file extension identifying it as a "proton-ized" file. It is this file that is shared with other users, not the original. Permissions associated with a file (users, groups and their access rights) are stored separately from the file in the Prot-On key server. Multiple copies can be made and the permissions will be maintained, even if the filename is changed. Encryption keys are stored in the Prot-On key database. For files marked for off-line use keys are stored in the Prot-On Client. Customers wanting a highly secure data sharing environment will use Prot-On on premise and manage their own keys. User Logins are via username/password but social media logins via OpenID and OAuth can be implemented.

A user with Read permissions to a file will only be allowed to view the file, copy/paste functions will be disabled as well as screen capture apps. Edit permissions will allow users to modify the file with the file saved back to the same location. Copy provides the ability to make another copy of the file. Print permissions only allows pointing of the document, no modifications. "Manage" permissions allow a user to change the access rights associated with a document.

Supported files types include Office documents, PDF, image files, CAD drawings most multimedia files and a wide variety of text files. Windows and Mac clients are provided as well as Android, iOS and Blackberry mobile apps. Microsoft Office applications require a plug-in to access a Prot-On-ized file. Other file formats such as.pdf, text and image files are accessed through the Prot-On viewer. The Drag'n Drop service allows browser access to Prot-On-ized files.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 28: Prot-On Product Rating



## 11.15 Seclore

Seclore are a mature provider of enterprise rights management technology for secure file sharing. They offer on-premise or Cloud deployments (AWS) which can be managed by Seclore or by a third party provider. Documents repositories can be stored anywhere; rights management will be applied regardless of the document transport or storage mechanism. The Seclore FileSecure product encrypts files and applies usage polices that enforce users or groups access permissions. External users can access protected files via any browser or download the Seclore-Lite agent to access the file, but not in the native application. Watermarks can be imposed on files sent externally.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Flexible solution with a large number of pre-built connectors and robust SDK<br>• Highly secure with standards-based encryption capability<br>• Flexible viewers for any device type | • Limited tools for classification of documents<br>• Document versioning/archiving would be a useful addition |

Table 29: Seclore

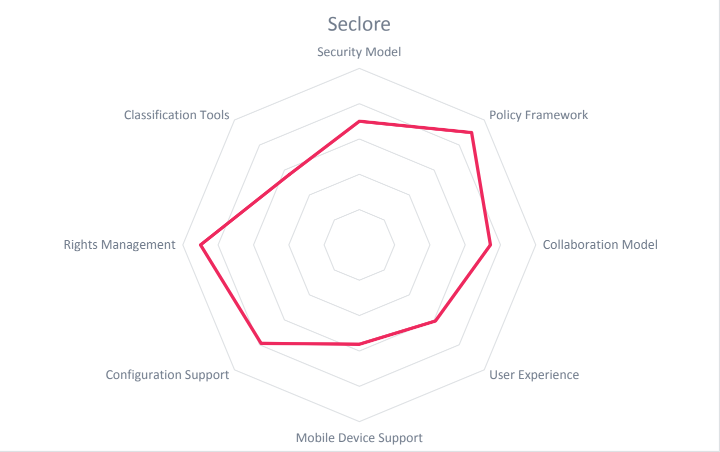
The FIleSecure desktop client is Windows-based and LiteViewer for Windows provides viewing on Windows systems. There is a FileSecure Lite agent for Mac devices and a File Secure Lite for Mobiles priovidind a native app for Android and iOS devices. A browser-based viewer is also available. Microsoft Outlook and Lotus Notes mail clients are fully supported and will allow classification of messages and attachment of usage rights. Popular document management tools such as SharePoint, FileNET and Documentum are fully supported. Supported file formats include OpenOffice, Microsoft Office, PDF, CSV and image files. All activities performed on a protected file are logged.

A centralised policy management function is provided whereby an administrator can establish access permission policies that can restrict individual users from creating their own policies. To simplify the authentication process, even for external users, the FileSecure identity system federates identities from on-premise or cloud systems which are typically a combination of Microsoft AD, on-prem systems (HR) or cloud identities (Google, any SAML authorization system. If a user is not in a federated IdP the identity will be created in the built-in Seclore identity management system.

A secure key management process is used that creates keys with a randomised algorithm. The key store is kept in an encrypted file on the Seclore server. Keys are not stored with documents. If a user has off-line privileges an encrypted key store will be established on the client machine encoded for the user's machine and will use their login credentials. A user-supplied HSM can be used for key management.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 30: Seclore Product Rating



## 11.16 Secure Islands

The Secure Islands provides an enterprise IRM solution that protects files of any type from any data repository (on-premise or Cloud based) by generating a classification (either automatic or user-driven) and encrypting the document with its enforcement actions. The system tracks documents thought its lifecycle of collaboration storage (internal and external) and archiving.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • Full support for Microsoft RMS on-premise or on Azure<br>• Support for any storage mechanism including common public Cloud storage<br>• Easy-to-use console management for policies and data analytics | • Focussed on Microsoft RMS<br>• Wider directory support would be useful i.e. more than just AD |

Table 31: Secure Islands

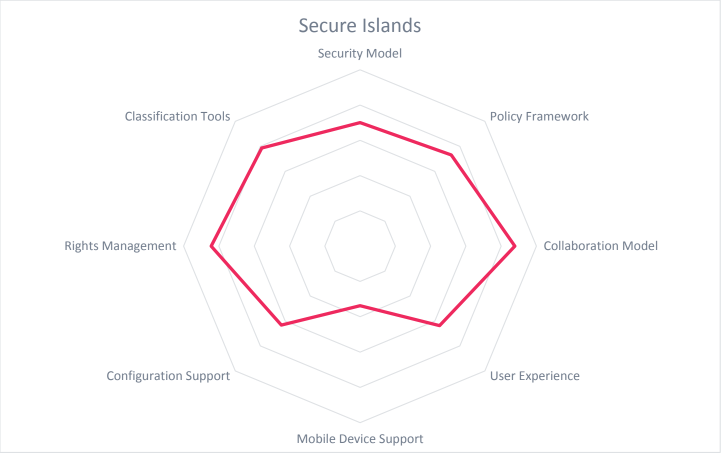
All major data repositories are supported including OneDrive, Google Drive, Box.net, Citirx ShareFile and Dropbox. SharePoint Online and Office 365 are supported as well as any collaboration tool that supports CIFS and WebDAV. The Endpoint Suite agents can automatically classify sensitive data accessed by users whether it be via email, an enterprise application or documents kept in a Cloud service.  This is achieved via the deployment of “interceptors” for common applications and a data crawler for classification of files in data repositories. A software development kit is available for custom application interceptor development. This means that deterministic classification and protection of all files in the business can be deployed regardless of whether the data is being generated at a client end-point, an application or sourced from an on-premise or Cloud repository. Desktop and mobile devices are supported. On mobiles the Secure Island’s technology allows files to be emailed via native email apps without installing any applications. An app is available for Android and iOS that extends the viewing, editing and creation of documents on the mobile device.

The IQProtector management server enforces Microsoft RMS in any file or document. It utilises AD on-premise, or Azure AD in the Cloud, for user identity and permissions information.

The policy management console provides an intuitive management screen for setting policies. For instance a policy to automatically classify all financial reports might be set whereas for HR documents a recommendation might be issued. It also displays a real-time dashboard of document access, and provided metrics on data accessed internally or sent externally.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | positive |
| **Interoperability** | neutral |
| **Usability** | positive |

Table 32: Secure Islands Product Rating



### 11.17 SecureAge

The SecureAge Technology offers a managed storage service that allows authorised users to work in a secure collaborative environment. With SecureData each user can set sharing privileges for their documents and can work on other documents to which they have been granted access. SecureData works in the background to ensure that data at rest is encrypted (AES 256) and that data in transit uses a TLS session.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • User-transparent file encryption/decryption regardless of storage location<br>• Android and iOS mobile device support via the LockCube product | • Support for SecureData in public Clouds such as AWS and Azure would be beneficial.<br>• A robust document classification system observing RMS constraints would be useful |

Table 33: Secure Age

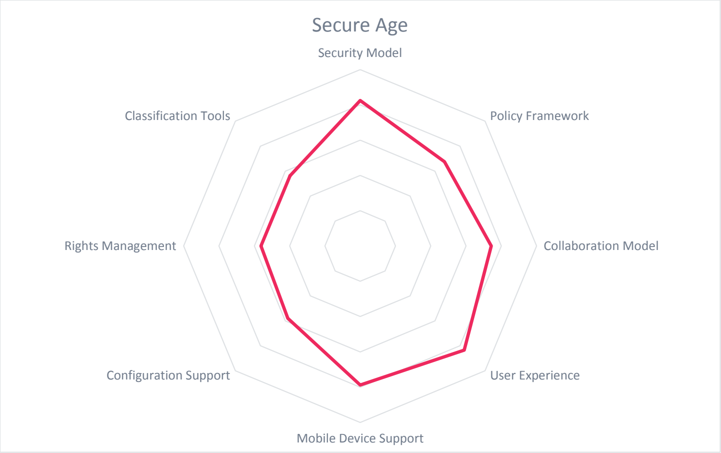
SecureData solution combines an Application Whitelisting function with a data protection capability that is proactive i.e. user or policy-based, pervasive, covering all file types and persistent, for the entire file lifecycle. This means that applications are protected from malware with data automatically encrypted at rest and in motion. Clients are available for both Windows PCs and Macs.

The on-premise solution provides end-point protection (desktop and laptop). Files are decrypted inreal-time and useable in their native application; the encryption and decryption process is transparent to users. When authorised users save data or documents encryption will be used to ensure unauthorised access to the data is useless. Other trusted users will be able to access the data with the decryption happening in the background. Public key infrastructure is used, with certificates held in a local or network directory. AD is used as the source of identity information. SecureAge operate two data centres in Singapore for storage of SecureData settings and management facilities.

SecureAge also offer the LockCube product. It is a user-managed data store whereby a network drive is set-up which is automatically encrypted. Users simply store and retrieve their data as normal and LockCube encrypts it and provides access to other authorised users. Android and iOS devices are supported.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | neutral |
| **Interoperability** | positive |
| **Usability** | positive |

Table 34: Secure Age Product Rating



## 11.18 TITUS

Rather than concentrate on secure data stores and data encryption TITUS have focused on data classification and entitlement. With the TITUS client installed, when a document or file is saved it can be classified either automatically, via a set of rules established by the administrator, or by the user who can select one of the pre-defined classifications for the document. The classification framework is managed via a centralized administration console which allows administrators to have consistent configurations and policies across the products in the suite.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| • The TITUS solution instils a DLP culture within the organisation<br>• Comprehensive classification and rights management for the Microsoft environment<br>• Good mobile device support with TITUS Docs and TITUS Mail apps | • Solution is Microsoft-centric and less-comprehensive in hybrid environments |

Table 35: Titus

The Classification for Desktop application supports all files types supported on the Windows environment and the Classification for Microsoft Office product provides extra capabilities for managing access to Word, Excel and PowerPoint files.

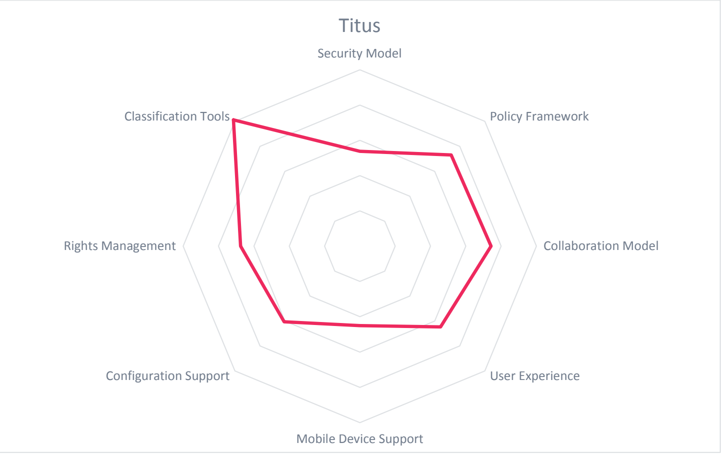
TITUS Message Classification is a purpose-built add-on to Outlook providing the capability to block an email being sent to an inappropriate recipient. Recipients of documents are assigned access rights and they will be warned if they attempt to violate them. For instance, if a recipient attempts to email an internal document to an external user the system will typically remove the attachment and notify the administrator depending upon the established policy.

TITUS Classification for Mobile extends the classification capabilities to mobile devices. It configures a protected area on the mobile device that is encrypted and can be wiped by an administrator or via pre-defined rules such as number of days inactive. The mail client provides a standard interface which users will be familiar with but adds color-coded classification levels to each entry.

TITUS Classification Suite is Microsoft-centric and supports all variants of Windows Server and Windows clients from Vista to Windows 8.1. The product requires .NET Framework and TITUS Mail works with Exchange 2003 to 2013. Classification for Mobile is compatible with Azure and Active Directory Rights Management. Supported file types include Office documents, media files, PDFs zip files etc.

| | |
|---|---|
| **Security** | neutral |
| **Functionality** | neutral |
| **Integration** | neutral |
| **Interoperability** | neutral |
| **Usability** | positive |

Table 36: Titus Product Rating



## 11.19 Watchful

The Watchful RightsWATCH product automatically classifies and protects any file format in accordance with corporate policy based on content, context or metadata-aware policy rules. The product extends the Microsoft Right Management facility to ensure that sensitive and confidential information is identified and classified appropriately. This allows the exchange of documents in a collaborative environment without the need to add external users to the organisation's identity store.

| Strengths/Opportunities | Weakness/Threats |
|---|---|
| ● Good mobile device support with coverage of Android, iOS, Blackberry and Windows.<br>● Comprehensive data sharing based on Microsoft rights management | ● Comprehensive in the Microsoft environment but might be less appropriate in hybrid environments |

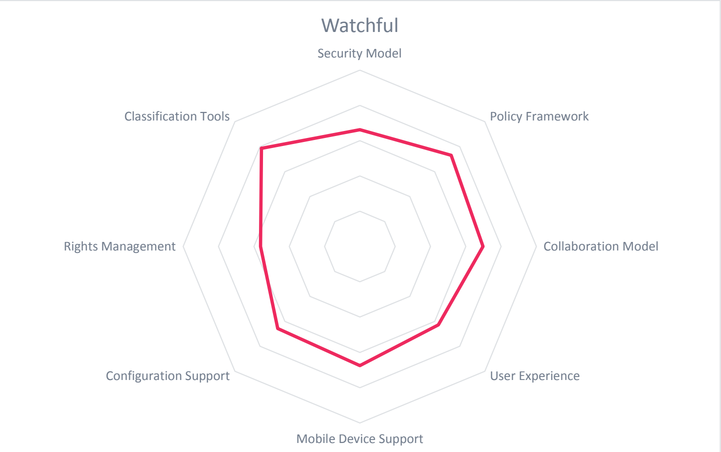
Table 37: Watchful

Documents are shared via email or Cloud-based storage; this aligns with typical user workflows and fits well into most collaborative environments.  Document permissions such as view, edit, print, save, attach etc. are attached to documents and recipients will be able to work with shared documents to the extent allowed by their classification. Encryption of sensitive data can be enforced if required by an organisation/s information control policy. Keys are stored in the RMS server or an HSM. Supported file types include Office documents, media files, PDFs zip files etc.

The Watchful approach is to enable classification via both user rating and automated policy-based classification. A policy can then be established to automatically re-classified a document at a future point in time. Classifications are observed regardless of the platform; the credentials of a user accessing a classified document will be compared with the classification policy for the document in order to apply the appropriate restrictions to the user's permissions. Classification can be applied automatically based on real-time content analysis searching for key words such as Company Confidential, Internal Use Only, Restricted or Top Secret. This can be extended to PII data such as credit card numbers or identity codes. Classifications can be inferred from normal document usage i.e. internal-use only, or from meta-data such as file path or file size. Policy administration can be distributed whereby a business unit sets the policies for their unit without affecting other corporate documents. The product also supports visual markings such as watermarks that can be automatically applied depending upon policies established by the organisation's information control policy. Restrictions can be applied based on individual user attributes or role-based group membership.

| | |
|---|---|
| **Security** | positive |
| **Functionality** | positive |
| **Integration** | positive |
| **Interoperability** | neutral |
| **Usability** | strong positive |

Table 38: Watchful Product Rating



# 12. Products at a glance

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

## 12.1 Ratings at a glance

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 39.

| Product | Security | Functionality | Integration | Interoperability | Usability |
|---|---|---|---|---|---|
| Amazon Web Services | positive | neutral | neutral | neutral | strong positive |
| Content Keeper | positive | neutral | weak | neutral | neutral |
| Covertix | strong positive | positive | neutral | positive | positive |
| Cryptelo | positive | positive | critical | weak | neutral |
| Deep-Secure | positive | positive | weak | neutral | positive |
| Druva | positive | positive | neutral | neutral | positive |
| EMC Syncplicity | strong positive | positive | neutral | positive | positive |
| Exostar | strong positive | positive | neutral | positive | positive |
| GRAU DATA | positive | positive | neutral | neutral | neutral |
| Intralinks | strong positive | strong positive | neutral | positive | positive |
| Microsoft | strong positive | positive | neutral | positive | strong positive |
| MobilityLab | neutral | neutral | weak | weak | positive |
| NextLabs | positive | positive | positive | positive | neutral |
| Prot-On | positive | positive | neutral | positive | positive |
| Secure Age | positive | positive | neutral | positive | positive |
| Seclore | positive | positive | neutral | positive | positive |
| Secure Islands | positive | positive | positive | neutral | positive |
| TITUS | neutral | neutral | neutral | neutral | positive |
| Watchful Software | positive | positive | positive | neutral | strong positive |

**Table 39: Comparative overview of the ratings for the product capabilities.**

In addition we provide in table 40 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

| Vendor | Innovativeness | Market Position | Financial Strength | Ecosystem |
|---|---|---|---|---|
| Amazon Web Services | neutral | strong positive | strong positive | positive |
| Content Keeper | neutral | weak | weak | weak |
| Covertix | positive | weak | weak | positive |
| Cryptelo | weak | critical | weak | weak |
| Deep-Secure | neutral | neutral | neutral | positive |
| Druva | neutral | neutral | neutral | positive |
| EMC Syncplicity | positive | strong positive | strong positive | positive |
| Exostar | positive | positive | positive | strong positive |
| GRAU DATA | neutral | weak | weak | neutral |
| Intralinks | positive | neutral | positive | positive |
| Microsoft | positive | strong positive | strong positive | strong positive |
| MobilityLab | weak | critical | weak | neutral |
| NextLabs | positive | positive | strong positive | positive |
| Prot-On | positive | weak | weak | neutral |
| Secure Age | positive | weak | neutral | positive |
| Seclore | positive | neutral | neutral | positive |
| Secure Islands | positive | neutral | neutral | positive |
| TITUS | neutral | positive | positive | neutral |
| Watchful Software | neutral | neutral | neutral | positive |

Table 40: Comparative overview of the ratings for vendors.

In the area of Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets such as Russia or Spain or even within these markets. Usually the number of existing customers is also limited in these cases.

In the area of Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base, but is also based on some other criteria. This doesn't imply that the vendor is in a critical financial situation; however the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

## 12.2 The Market/Product Matrix

Beyond that analysis, we've compared the position of vendors regarding combinations of our three major areas of analysis, i.e. market leadership, product leadership, and innovation leadership. That analysis provides additional information.

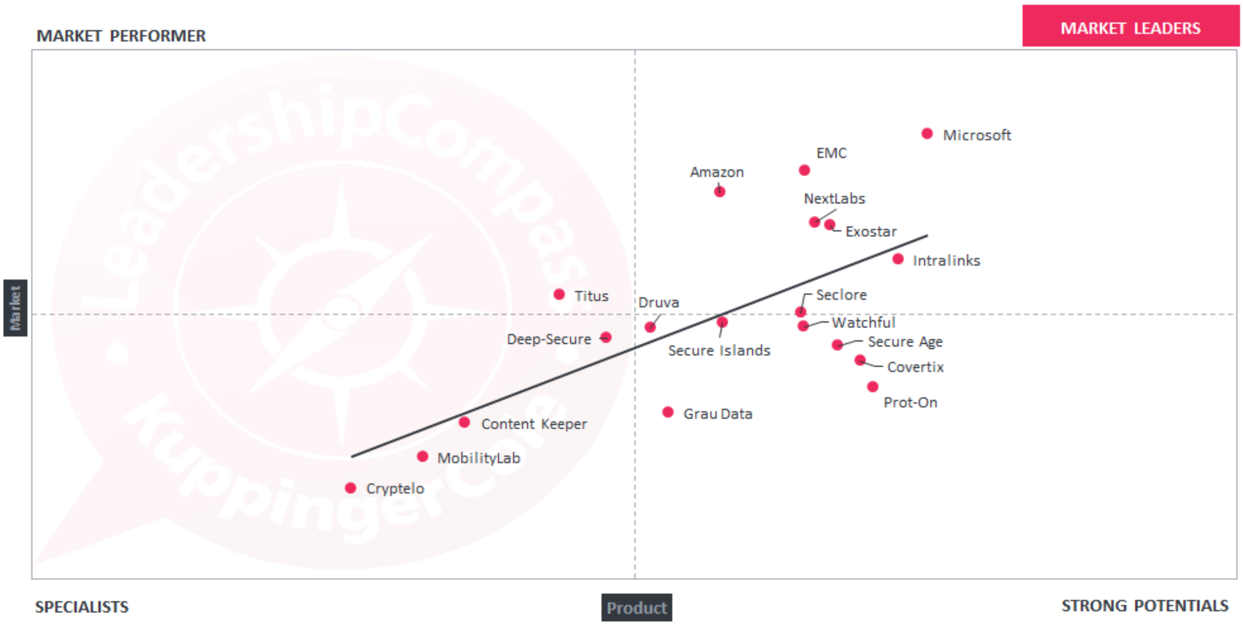


**Figure 9: Market/ Product Matrix Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "over-performers" when comparing Market Leadership and Product Leadership.**

In this comparison it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

We've defined four segments of vendors to help in classifying them:

Market Leaders: This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

Strong Potentials: This segment includes vendors which have strong products, being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be caused by various reasons, like a regional focus of the vendors or the fact that they are niche vendors in that particular market segment.

Market Performers: Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically such vendors have a strong, established customer base due to other market segments they are active in.

Specialists: In that segment we typically find specialized vendors which have – in most cases – specific strengths but neither provide full coverage of all features which are common in the particular market segment nor count among the software vendors with overall very large portfolios.

In the Market Leaders segment, we see Microsoft, EMC, Amazon, Exostar, NextLabs and Intralinks. Vendors towards the upper right are the ones that have both strong product features and a significant market presence.

It is interesting that there is only one vendor in the Market Performers section at the present time, which is Titus – a vendor focusing on the specific capability of information classification.

The Strong Potentials section of the graphic is very busy with the majority of vendors. Vendors in this quadrant are not leading-edge in product functionality but have a good sales presence. Seclore is on the borderline.

Finally, there is the Specialists section with three vendors.  This sector is characterized by products that are rather new and still evolving. Deep Secure, Content Keeper, Cryptelo and MobilityLab are all moving their products into the mainstream from a background in specific applications. All specialists might be a perfect fit for some customers due to the fact that they provide rather specialized tools that might suit some use cases better than standard authorization tools.

### 12.3 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there are some marked differences between the two views. This distribution and correlation is typical for emerging markets with a significant number of innovative vendors.

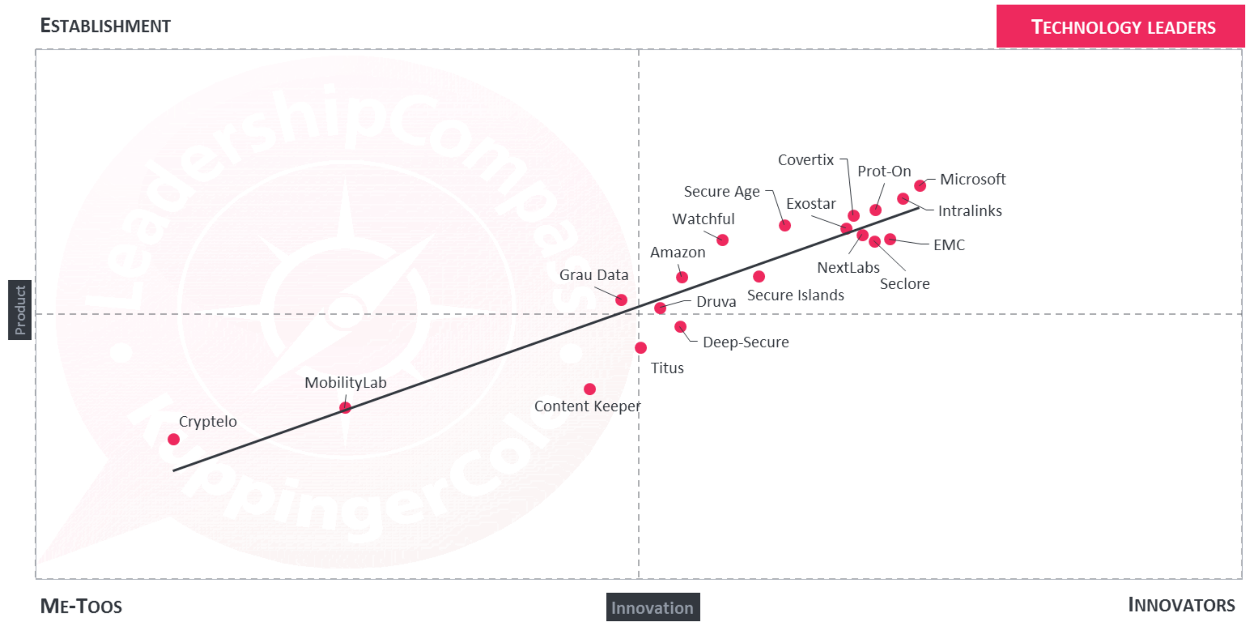


**Figure 10: Product/Innovation Matrix. Vendors below the line are less innovative, vendors above the line are, compared to the current Product Leadership positioning, more innovative.**

Again we've defined four segments of vendors. These are

Technology Leaders: This group contains vendors which have technologies which are strong regarding their existing functionality and which show a good degree of innovation.

Establishment: In this segment we typically find vendors which have a relatively good position in the market but don't perform as strong when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market and thus do not count that strong for the Innovation Leadership rating.

Innovators: Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because vendors therein might be a fit especially for specific customer requirements.

Me-toos: This segment mainly contains those vendors which are following the market. There are exceptions in the case of vendors which take a fundamentally different approach to provide specialized point solutions. However, in most cases this is more about delivering what others have already created.

There is a good percentage of vendors in the upper right segment of the matrix, which we define as the Technology Leaders segment. These vendors show good to excellent innovation and provide strong product capabilities.

On the other hand the Establishment segment is bare except for Grau Data which is close to the Leader quadrant.  This is fully understandable because Secure Information Sharing products have not been around long enough to become "established".

Also, only few vendors make it into the Innovators segment – most of the innovative ones already have a significant market share.

The Me-Too section contains vendors that are providing standard Sharing functionality but are also taking a somewhat different approach to the market. Vendors in this segment are regional players or vendors providing solutions with specialist functionality such as Titus.

## 12.4 The Innovation/Market Matrix

The fourth 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 but might also fail, especially in the case of smaller vendors.

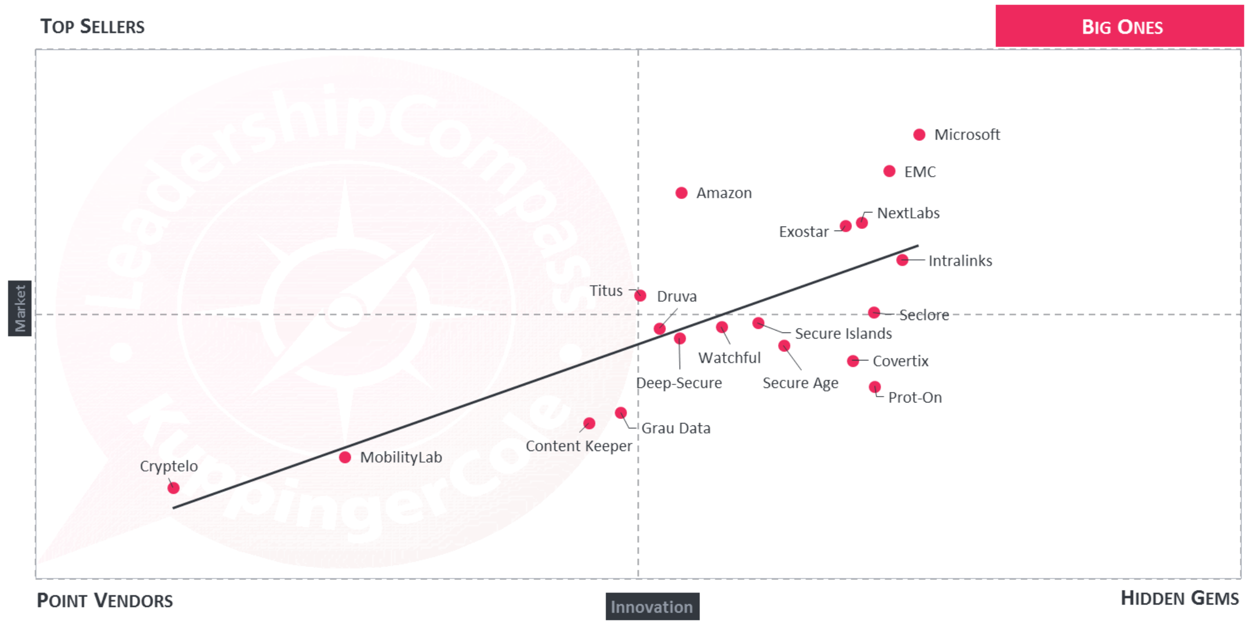


**Figure 11: Innovation/Market Matrix. Vendors below the line are performing well in the market compared to their relative weak position in the Innovation Leadership rating, while vendors above the line show based on their ability to innovate, the biggest potential for improving their market position.**

The four segments we have defined here are

Big Ones: These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

Top Sellers: In this segment we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of “customer customers”, i.e. a loyal and powerful group of contacts in the customer organizations.

Hidden Gems: Here we find vendors which are more innovative than would be expected given their Market Leadership rating. These vendors have a strong potential for growth, however they also might fail in delivering on that potential. Nevertheless this group is always worth a look due to their specific position in the market.

Point Vendors: In that segment we find vendors which typically either have point solutions or which are targeting specific groups of customers like SMBs with solutions focused on these, but not necessarily covering all requirements of all types of customers and thus not being among the Innovation Leaders. These vendors might be attractive if their solution fits the specific customer requirements.

Again, this matrix contains the two large players in the Big Ones section as well as the gateway vendors who command a wider market share.  These vendors both hold a significant market share and execute well in adding innovative features to their products.

The Top Sellers segment we find empty.  This is because the top sellers in this segment are also innovative which moves them into the upper quadrant.

More interesting is the Hidden Gems segment. As expected we see the main innovators here: Covertix and Prot-On are excellent examples here. Also a number of other vendors shows a significant potential for market expansion.

The Point Vendors segment contains the specialized vendors. Again, these vendors might be a good choice for many customers and should not be overlooked in preference for the larger players in general Secure Information Sharing market segment, with Grau Data being close to entering the Hidden Gems segment.

## 13. Overall Leadership

Finally, we've put together the three different ratings for leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 12.

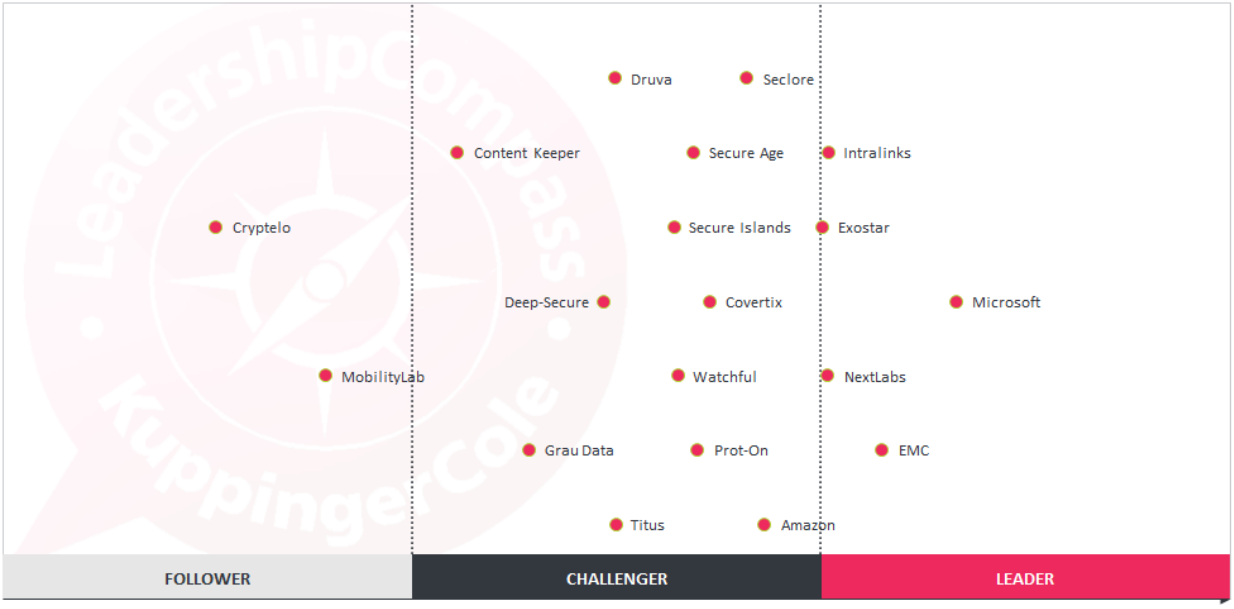


**Figure 12: Overall Leadership for the Secure Data Sharing market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better].**

In the Overall Leaders chart, as expected the large players are in front. This results from their market size and, in the case of Microsoft, their dominant position in the rights management market. EMC, also a large player with a wide partner base, have a functionally rich secure data sharing product specifically focused on providing an easy-to-use tool to give end-users the ability to control access to their documents[2]. Intralinks provide a comprehensive solution with a strong IRM-by-design focus. NextLabs provide fine-grained access to protected documents by combining a secure data storage capability with a rights management solution. Taking a different approach is Exostar who specialise in supporting secure data sharing in specific industry environments.

It is perhaps not surprising that Microsoft's leadership is so dominant. Microsoft's rights management solution is mature and it is well integrated into two areas of product dominance – authentication services (based on AD) and office documents where Microsoft enjoys a leadership position. It can also be seen that Microsoft is clearly looking to maintain their leadership in rights management with the integration of Microsoft Identity Manager (formerly FIM) with AzureAD. AD RMS settings can be synchronised to Azure Rights Management which provides extended entitlements for the management of user permissions in the Cloud.

[2] Note: Prior to publication EMC sold the Syncplicity product to Skyview Capital.

The Overall Leadership rating also shows a number of other vendors challenging the Leaders category. These include the very functional AWS WorkDocs product (formerly Zocalo), Seclore with their comprehensive enterprise rights management solution, Covertix with their cross platform support and monitoring functions, the Prot-On secure document environment, the Secure Age managed storage solution, the Secure Islands enterprise IRM approach and Watchful with their innovative classification functionality. Also in the Challenger section are five companies with different approaches to secure information sharing. They didn't score as highly as more conventional solutions but offer strong solutions in their target market sectors: Druva provides tight integration at the file system level, good endpoint enablement and dashboard functionality, Deep Secure have a modular approach to providing strong security over their data sharing environment, Titus provide a very comprehensive classification solution, Grau Data provide a very secure data-at-rest solution offering clients full control over keys and Content Keeper who provide a managed gateway approach to protecting data from users, and users from data.

In the Follower section we have two vendors; this is primarily due to their nascent status and small market presence. Mobility Lab are a start-up in Russia with an impressive, high-security solution focussed on end-client usability.  Cryptelo is headquartered in the Czech Republic, their Drive product takes a server-based document approach with strong encryption facilities.

Overall Leaders (in alphabetical order):

- EMC Syncplicity
- Exostar
- Intralinks
- Microsoft
- NextLabs

## 14. 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 for that market. Some had 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 Identity Provisioning or are not yet mature enough to be considered in this evaluation. We provide short abstracts on these vendors.

### 15.1 Bolden James

With an impressive customer-base Bolden James is a specialist in data loss protection and classification-based secure data sharing. Their background in military messaging provides a highly secure collaboration environment allowing for labelling, protective marking and release control of files and documents. They also provide network interconnection tools for interoperability between disparate security classification environments.

### 15.2 Brainloop AG

Brainloop offer a complete package with data store encryption, dual key, rights management integration that allows you to work natively if you use Microsoft Office or Lotus Notes. Brainloops Dox is a clouid-based solution that facilitates secure collaboration across multiple devices and supports adherence to regulatory controls and company policy in the protection of intellectual property.

### 15.3 Citrix Systems GmbH

The Citrix Workspace Suite is a collaboration solution for mobile workforces. The product offers the ability to share documents across multiple devices using a unified app. Windows, web, SaaS and mobile apps can be delivered to any supported device with SSO access for users. Citrix's strength is in efficient delivery of on-demand services to end-point devices.

### 15.4 Covisint/Compuware GmbH

Covisint built their reputation in the automotive industry B2B environment. Now an independent company they are offering their Cloud platform tools for trusted access to information, anywhere to a wider customer base. They are particularly strong in the integration of devices and should be considered by any organisation with secure IoT requirements

### 15.5 Google

Google Apps for Work builds on Google Docs and Gmail to provide a secure collaboration environment that includes office products, calendar, storage and webinar capabilities via Google Hangouts. This provides a secure and consistent user experience across laptops, tablets and smartphones.

### 15.6 Jericho Systems

As a provider of data segmentation for privacy solution to the Department of Homeland Security Jericho Systems should be considered in any classification-based secure data sharing solution. Their "data labelling and data segmentation" technology enables fine-grained access control in a policy-based environment. This allows for consistent and auditable data collaboration that minimises privacy risk.

### 15.7 Nexor

Nexor are a long-time supplier of secure messaging infrastructure that is used in critical infrastructure protection and defence intelligence environments. Their Trustworthy Technology solutions should be considered for robust, cross-domain data sharing environments particularly in situations requiring certification to standards.

### 15.8 SecSign Technologies

Secure solutions based on two factor authentication solutions is the focus of SecSign. The SecSign Portal provides a secure environment for the storage of protected documents and the SecSignID provides a secure authentication service to control access to protected documents. They should be considered for solutions requiring strong client authentication.

### 15.9 Secude

Secude is a Swiss-based supplier of security software providing classification-based DLP as well as audit and reporting functions for governance and compliance. They specialise in the SAP environment with their Halocore product intercepts data being exported from SAP and encrypts it, applying RMS metadata for access control decisions. Data can either be protected automatically based on standard policies or the user can be prompted to select a classification which is then applied to the file. Access to the SAP data is then controlled via Microsoft Rights Management and alerts can be issued when sensitive data is downloaded.

Beyond the integration with Microsoft Rights Management, Halocore as a stand-alone solution can also provide classification capabilities in tight integration with existing SAP entitlements and access control information. Furthermore, it supports auditing access to sensitive information that is exported from SAP environments, including integration with SAP HANA and SAP Business Intelligence solutions.

### 15.10 Senetas

Senetas are a supplier of level 2 router technology and is a strong contender for gateway solutions with fast throughput requirements. As a gateway device it provides robust security for restricted systems and is ideally suited to big-data analysis requirements and CCTV environments.

## 15. Copyright

# The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought Leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization.

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

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
**www.kuppingercole.com**