KuppingerCole Report

MARKET COMPASS

By Anne Bailey
June 18, 2020

Enterprise Information Protection

The KuppingerCole Market Compass provides an overview of the product or service offerings in a certain market segment. This Market Compass covers Enterprise Information Protection solutions. Because the perimeter of the corporation has changed to include personal and business devices, mass remote work, and increased collaboration, advanced methods for the protection of sensitive data have become necessary. This is an overview of the vendors that work to secure valuable assets – the sensitive data of an organization.

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

Content

1 Management Summary

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

This Market Compass covers vendors that provide Enterprise Information Protection (EIP). Information protection has quickly climbed to a high-ranking priority in enterprise security. At one point in time, enterprises hosted most major communication and documentation on-premises, without the complication of multiple devices, insecure communication, and extensive interface with entities outside the organization. This intricate pattern of internal and external interactions is now the reality of daily operations. Users login via mobile devices – private and corporately owned – and are often not on corporate premises as they access corporate information. User access must be managed in order to protected resources, but must be flexible enough to accommodate the extensive sharing of protected information. Perimeter protection is no longer adequate, leading to the release of many EIP solutions.

There are multiple trends that impact EIP: the recent mass migration to remote work, the need to manage user access to protected resources, the increasing need to accommodate the sharing protected information, and stringent regulation protecting the private information of individuals.

The market is still heterogeneous, with many vendors offering a variety of solutions to address similar use cases. The major use cases for enterprise information protection include protecting intellectual property, protecting PII data, and increasingly as an enabler for secure collaboration at a distance. A strong solution is one that protects enterprise data with flexible control of data that can accommodate the way that enterprise staff, business partners, and customers prefer to interact. Encryption is generally used to protect documents either at the folder level – in which all documents use the same encryption key – or at the file level where individual keys can be assigned on a per document basis. Document repositories can be used to protect information, and can be held on-premises or increasingly in cloud storage. Information protection that facilitates collaboration on documents is well-suited to a rights management solution where an author can determine who may access a document and what they can do with it. It is possible to manage access to documents by explicitly defining the rights of users to edit, save or print. These controls travel with the document and apply on internal infrastructure or cloud environments.

Solutions in this market segment often have robust rights management encryption capabilities, applicable at both the folder and file level. A policy framework and key management should also be part of the solution. Sensitive data often resides in multiple places in an organization, and is incorporated into files at rest, in motion, and in use. This requires high compatibility with file sharing platforms, many cloud providers, and file types. Full auditability should be available for any EIP solution. Advanced capabilities for this solution include data classification abilities along with the detection of sensitive information. In some cases a secure file repository may provide additional security. Email should also be protected, most commonly with encryption. Document versioning should also be supported.

2 Market Segment

This Market Compass covers solutions that protect enterprise information using primarily rights management, document repositories, encryption of files, with some utilization of data classification. The variety of methods that vendors use to protect information creates a dynamic market space.

2.1 Market Description

Information protection has quickly climbed to a high-ranking priority in enterprise security. At one point in time, enterprises hosted most major communication and documentation on-premises, without the complication of multiple devices, insecure communication, and extensive interface with entities outside the organization. This intricate pattern of internal and external interactions is now the reality of daily operations. Users login via mobile devices – private and corporately owned – and are often not on corporate premises as they access corporate information. User access must be managed in order to protect resources, but must be flexible enough to accommodate the extensive sharing of protected information. Perimeter protection is no longer adequate, leading to the release of many EIP solutions.

While a vulnerability from a security standpoint, storing and sharing business information is an increasingly important aspect of managing a business today. Businesses need to collect more information, they need to analyze more data and they increasingly need to share this information with business partners and customers. This is consistent across all verticals. Maintaining inventory levels requires candid communication with suppliers, and customer relations often depends on securely running a customer identity management system. Protecting enterprise information while still making it available for varied use is therefore paramount.

The market is still heterogeneous, with many vendors offering a variety of solutions to address similar use cases. The major use cases for enterprise information include protecting intellectual property, protecting PII data, and soon as an enabler for secure collaboration at a distance. A strong solution is one that protects enterprise data with flexible control of data that can accommodate the way that enterprise staff, business partners, and customers prefer to interact. Encryption generally used to protect documents either at the folder level – in which all documents use the same encryption key – or at the file level where individual keys can be assigned on a per document basis. Document repositories can be used to protect information, and can be held on-premises or increasingly in cloud storage. Information protection that facilitates collaboration on documents is well-suited to a rights management solution where an author can determine who may access a document and what they can do with it. It is possible to manage access to documents by explicitly defining the rights of users to edit, save or print. These controls travel with the document and apply on internal infrastructure or cloud environments.

Solutions are readily available that allow enterprises to securely share information and to positively identify devices and their users better than ever before. The task is to select an optimal solution that not only protects data, but fits the way our staff, business partners and customers prefer to interact; controls on data must be light-touch and must accommodate the way staff share information both internally and externally.

2.2 Market Direction

There are multiple trends that impact EIP: the recent mass migration to remote work, the need to manage user access to protected resources, the increasing need to accommodate the sharing protected information, and stringent regulation protecting the private information of individuals.

The enterprise is now definitively past the time when the corporate environment was well bounded and controlled by physical premises. The early months of 2020 saw the first instance where a vast portion of the global workforce was required to work remotely, putting stress on the infrastructure organizations had in place to facilitate collaboration and secure sharing of information. This wake-up call, as well as rising pressures on the climate from daily commuting and business travel will drive growth for this market. It is likely that more organizations will restructure workflows to allow more remote working opportunities.

The “post-perimeter” age of security means that every interface with enterprise data is a potential attack vector. Today, many users login via mobile devices – some of which they own – widening the number of devices that interact with potentially sensitive information while reducing the enterprise’s control over the device itself. In many cases they are not on corporate premises as they access corporate information. Perimeter protection is no longer adequate and more sophisticated protection mechanisms are required as the need to manage user access, not perimeter access, is increased.

Enterprises are increasingly collaborating with external partners and must share sensitive information outside of the organization. More transparent supply chains, joint projects, and much more requires the transfer and potential loss of critical information. This requires the ability to securely share documents in use, not simply finished documents, with fine-grained control over any user’s access to or manipulation of information in that document, and directly impacts the demand for solutions in this market.
Stringent regulation such as the GDPR in Europe, CCPA in the US, and others specific to various jurisdictions require the appropriate collection of, use, and ability to erase personal data. These regulations restrict the type, length, and reasons for storing data. The global spread of such regulations is a tangentially connected driver for the EIP market.

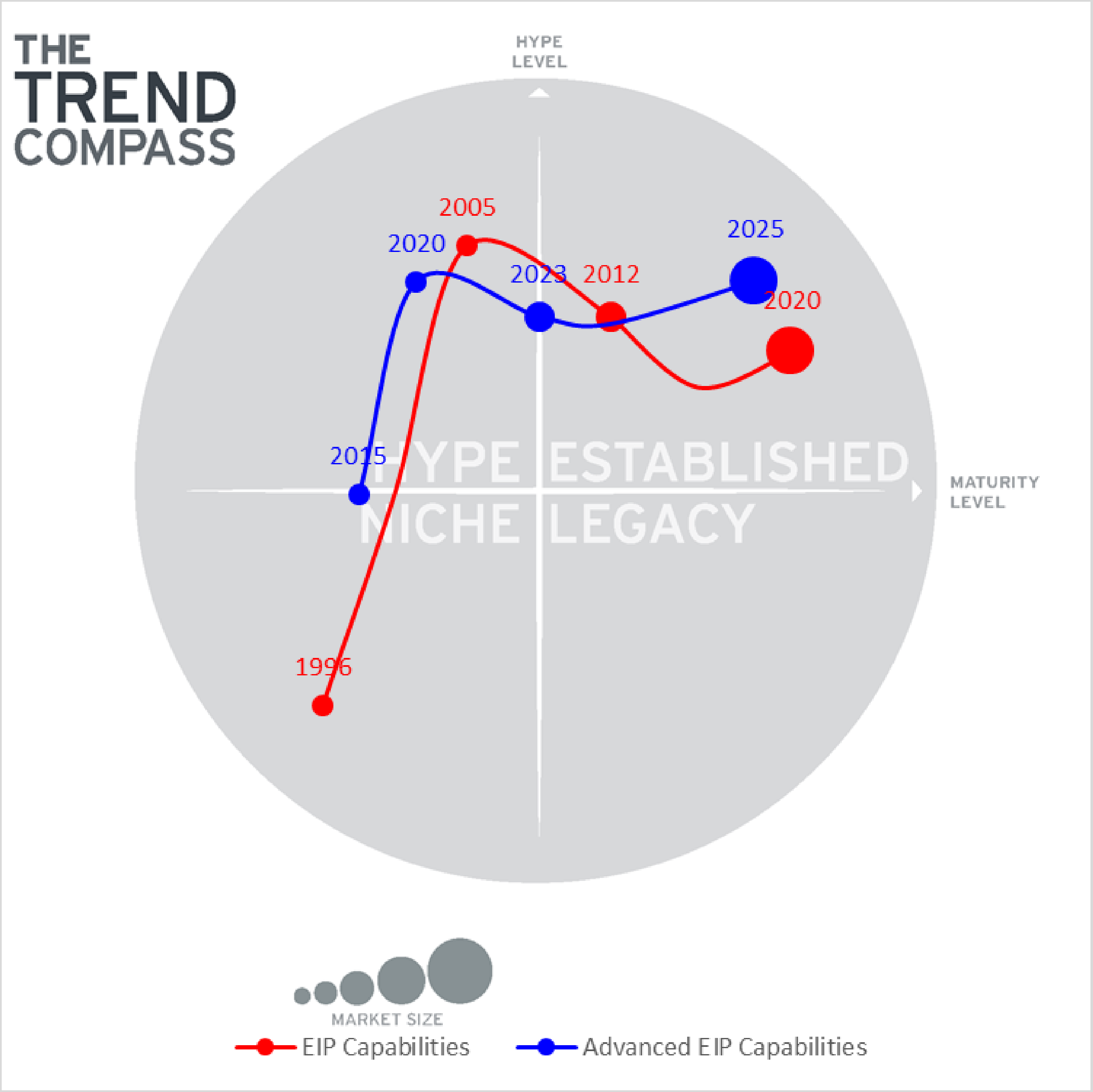


Figure 1: Trend Compass for Enterprise Information Protection Market

These environmental pressures have influenced the market direction for EIP solutions. This market segment appeared in the mid-nineties as a niche solution and have progressed into established solutions. Advanced capabilities for this segment will start to appear in 2020 responding to a high demand for secure remote workforces and collaborative workspaces.

2.3 Capabilities

The EIP segment has a collection of standard capabilities that most solutions include. However, advanced solutions are beginning to include other capabilities that change the focus of protection to the data level – like PII or PCI – or to the file or role level.

2.3.1 Basic Functionality

The basic functionality that should be provided by all solutions includes:

Capabilities	Description	Relevance
Rights Management	The solution should provide protection at the document level through applying encryption and document level entitlements.	Essential
Cloud and On-Premises Support	The solution should enable information to be protected in the cloud, and on-premises. Hybrid environments are also ideally supported.	Essential
Collaboration Platform Compatibility	The solution should offer wide compatibility with cloud-based workspaces such as Dropbox, GoogleDrive, OneDrive, etc.	Essential
Data Location	The organization using the solution should be able to control the geographic jurisdiction in which the protected data is held.	Essential
Encryption	Folder and file-centric encryption should protect information in motion and at rest.	Essential
Application Integration	The solution should work with other applications, standards, or technologies, with the ability to support programmatic access through a well-documented and secure set of APIs.	Essential
Key Management	The solution should establish secure encryption key distribution and management, possibly with HSM key storage for increased security.	Essential
Policy Framework	The solution should provide a framework of policies used to manage entitlements, with the potential to apply policies automatically.	Essential
File Type Support	The solution should support all major file types.	Essential
Device Support	The solution should support all major devices and operating systems.	Essential
Auditability	The solution should support secure logging of administrative activity and interaction with protected information.	Essential

2.3.2 Advanced Capabilities

Enterprise Information Protection is expanding to include a wider range of capabilities. These advanced capabilities offer increased robustness to a solution.

Capability	Description	Relevance
Classification	Solutions may apply a classification system to files to denote the level of protection needed.	Recommended
Document Versioning	Control over document versions should be provided for fine-grain management of past and present information in collaborative documents.	Recommended
File Repository	The solution may include a secure storage mechanism for files and information.	Optional
Detection of Sensitive Information	Sensitive information such as PII, PCI, and IP data in documents, emails, communication, etc. should be detected and the collaborators notified for further action.	Optional
Email Protection	Encryption of email messages, ability to retract access to documents in email attachments, data loss prevention (DLP) capabilities.	Recommended

3 Vendors and Products

The vendors in this market covered by this report are those that provide primarily a rights management solution for information protection, deployable in cloud, on-premises, or hybrid environments.

3.1 Vendors Covered

The vendors covered in this report are:

- AceroDocs is a 2016 startup based in Madrid, Spain. Its flagship product of the same name protects files as they are shared internally within the enterprise as well as externally.
- AWS or Amazon Web Services is based in Seattle, WA, USA. Its product Amazon WorkDocs is a secure file storage and content collaboration tool for organizations.
- CryptoMill Cybersecurity Solutions is a Toronto-based company founded in 2005. It provides multiple products in the EIP space, and this report focuses on its Circles of Trust product and concept, which creates groups of trusted team members and only grants authorized people the right to access protected files.
- Egress was founded in 2007 and is headquartered in London. It provides data security services and EIP, particularly for email and file sharing.
- Exostar was founded in 2000 and is based in Virginia. Exostar is a strong player in industry collaboration environments and actively supports identity management and document sharing, particularly in a multi-enterprise collaboration environment for specific industry sectors that require strong security and regulatory compliance, such as aerospace, defense, and life sciences.
- Fasoo was founded in 2000 and is headquartered in South Korea. It provides a suite of products to protect unstructured enterprise data, including the data-centric policy enforcement aspect, Enterprise DRM.
- SS&C Intralinks, founded in 1996 is a financial technology provider for the global deal-making, alternative investment, and capital markets communities. It offers a SaaS multi-tenanted secure, document-centric collaboration solution. Intralinks Unshare is an information rights management solution to provide administrators control over file permissions and access.
- Microsoft, based in Washington state, offers a comprehensive classification solution with Microsoft Information Protection. It leverages the Azure Rights Management Service (Azure RMS) and AD Rights Management Service (ADRMS).

- NextLabs was founded in 2003 and is based in California. NextLabs has a long history in collaborative rights management enabling sharing of protected documents to authorized users. Enterprise Digital Rights Management (EDRM) and SkyDRM provide end-to-end application protection for collaboration and protection of critical data.
- Prot-On, founded in 2010 and acquired by Groupo CMC in 2017, is an Information Rights Management solution for both the enterprise and the individual, with internal and external access control management. It also provides secure document collaboration services.
- SealPath was founded in 2010 and is based in Spain. SealPath provides enterprise rights management solutions that work integrated with DLP solutions, data classification, CAD, cloud collaboration tools, and document management systems with a focus on improving usability, collaboration, and protection automation.
- Seclore was founded in 2010 and is headquartered in Milpitas, California. Seclore is a mature provider of enterprise rights management technology for secure file sharing. It integrates with data classification and DLP products and unifies them into its Data-Centric Security Platform for a holistic approach to discover, classify, protect, and track enterprise information wherever it travels or resides.
- uniscon was founded in 2009 and is based in Munich, Germany. Its information protection services product is idgard®, which is deployed from uniscon’s proprietary secure cloud. It operates a secure document storage facility and incorporates a rights management approach for in-use document protection.

3.2 Featured Vendors

All vendors evaluated in this Market Compass have their unique strengths. Still, we have identified a few vendors that are notable for reasons which may not be apparent in the table above. Please note that being featured does not automatically mean that these vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company’s products will be necessary. Vendors featured here are for expertise in regulated industries, capabilities, innovation, and as the newcomer to the market.

3.2.1 Featured for Expertise in Regulated Industries: Exostar

Exostar is our featured vendor for expertise in regulated industries. Regulated industries typically have more stringent information access and management, security, and compliance regulation to follow as well as handling high volumes of sensitive data. Exostar has actively worked with global clients in the aviation, defense, finance, energy, government agencies, healthcare, and life sciences industries.

3.2.2 Featured for Capabilities: NextLabs and Seclore

NextLabs is one of two featured vendors for capabilities for its ability to provide a well-rounded product offering. It's on-premise and cloud options provide end-to-end application protection for collaboration and protection of critical data. It comprises of both rights managements and classification capabilities. Policies are dynamically determined by subject, environmental, and resource attributes, as well as by the action to be performed. This dynamic authorization aspect is patented.

Seclore is also featured for its EIP capabilities. Seclore's Rights Management solution integrates with DLP, data classification, and SIEM systems to automatically discover, classify, protect, and track sensitive data. Document repositories can be hosted anywhere; rights management and encryption will be applied regardless of the file type and works with various kinds of repositories. Policy management is via a built-in policy manager and can also be federated from the integrated repository or application.

3.2.3 Featured for Innovation: Fasoo

Fasoo is our featured vendor for innovation for the additional rights able to be imposed on documents. Fasoo's protection standard AES256 bit encryption assigns dynamic, adaptive access control to files and adds a unique embedded ID into each file for tracing, audit logging, and visibility. This unique ID stays with the file regardless of the file location or derivatives and is key to managing and controlling document versions across its entire product portfolio. Fasoo allows for total automation of the data security process, or allows users to make decisions on file protection such as an exception management capability. Fasoo Smart Print helps detect personal or other sensitive information and applies pre-defined policy before a file is printed, such as dynamic watermarking, masking, and blocking users from printing, assisting to minimize sensitive data loss. It's auditing capabilities allow administrators to see the image of the printout for stronger visibility and tracing of sensitive files. It also monitors user activity with the aid of a trusted clock, helping to avoid insider manipulation of a device's local clock.

3.2.4 Featured for Collaboration: Microsoft

The Microsoft Information Protection is well-positioned to solution facilitate secure collaboration on files. It has a combined offering of classification and rights management, leveraging workflows that are already familiar to the user. Microsoft has the benefit of offering a collaboration platform, Microsoft Teams, into which Microsoft Information Protection is can be fully integrated. Azure AD B2B facilitates secure collaboration with external partners, without the need to manage external identities.

3.3 Vendors to Watch

Those listed as “Vendors to Watch” offer similar products to the vendors included in this report, but do not fit into the market segment as we have defined it. Most vendors emphasize information classification as a primary capability of their product, rather than a rights management solution.

- Boldon James is a UK-based company, incorporated in 1985. It comes from a military messaging background and has expanded their expertise into classification tools for office products, email and remote device access management. Customers install the classifier product(s) in their corporate environment and select the classification approach (user, system prompt or automated). Keep an eye on this vendor if your organizational needs favor an information classification approach.
- Brainloop AG was founded in 2000, and brings extensive experience in secure collaboration for use in management board communication, M&A negotiations, and in IP protection. The product range provides a highly functional file and data protection regime with two-factor authentication, persistent IRM control, and 256-bit AES encryption. Brainloop provides a highly secure cloud storage solution that allows traceability on access by authorized users. Brainloop incorporates strong authentication facilities supporting IP range restrictions, MFA, device inspection and dynamic access control features. Watch this vendor to stay informed on the offerings of highly secure data vault solutions.
- ClearSwift is also a UK-based company, founded in 1982. It offers data loss prevention (DLP) solutions for email and web gateways, with information classification capabilities. Watch this vendor if you want a strong solution for email security.
- M-Files was founded in Finland and has offices in the US and across Europe. It is a content management system using a strong metadata approach to organizing and protecting content. Artificial Intelligence is used to automate classification and tagging of metadata, and permissions are set according to a user’s role, at the file level, and even by version as part of M-Files’ automated workflow offering. Although it is primarily a content management system, keep an eye on M-Files as an add-on for Office 365, Google products, Salesforce, Oracle, and more.
- Micro Focus, based in the UK, provides solutions that discover, manage, and secure sensitive information. It includes automatic policy application across systems and file types. For a strong pairing of analytics and classification capabilities, keep this vendor in mind.
- ProofPoint, based in California, is a cloud-based, classification solution. It classifies and protects information according to industry pre-defined policies, and provides encryption for email services.

Watch this vendor if you need a competitive edge to your email security.

- Secude was founded in 1996, and provides protection for SAP exports. As a long-term collaborator with SAP, Secude has deep knowledge on how to best support SAP security with encryption. Watch this vendor if you depend on SAP for your business processes.
- Titus is an Ontario-based company which uses classification as the foundation of its solution. Titus Classification for Microsoft Outlook is a purpose-built add-on to Outlook providing the capability to block an email being sent to an inappropriate recipient. It ensures sensitive documents are not emailed to recipients without the required authority. Watch this vendor if you need strong classification capabilities for your email security.
- Varonis Systems is based in New York, and provides a classification tool that identifies and protects sensitive data in files. It is supported by machine learning to monitor user access and recommend when access rights should be reduced. Watch this vendor if you’re interested in applying predictive recommendations to your information security strategy.
- Virtru was founded in 2012 and is based in Washington D.C., USA. It is a secure email and messaging service for data-centric protection. It adds an additional layer of encrypted protection to information being sent in enterprise apps, internally and to external partners. This is a vendor to watch for its contribution of the Trusted Data Format – an open standard for object-level encryption.

4 Ratings at a Glance

This section provides an overview of the various products we have analysed within this KuppingerCole Market Compass on EIP solutions. Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in table 1.

Product	Security	Interoperability	Usability	Deployment	Protection Model	Collaboration Model	Rights Management	Policy Framework	Mobile Device Support
AceroDocs	⚪	⚫	🟢	⚫	⚪	🔴	⚫	⚪	🟢
AWS Amazon WorkDocs	⚫	⚫	🟢	🟢	⚫	⚫	⚪	⚪	🟢
CryptoMill Circles of Trust	⚫	⚫	🟢	⚫	⚫	🟢	⚫	🟢	🟢
Egress Secure Workspace	⚫	⚪	🟢	⚫	⚫	🟢	⚫	⚫	🟢
Exostar ForumPass	🟢	⚪	🟢	⚪	🟢	⚫	⚫	⚫	⚫
Fasoo Enterprise DRM	🟢	⚫	⚫	⚫	⚫	⚫	🟢	🟢	🟢
Intralinks Unshare	🟢	⚫	🟢	🟢	⚫	⚫	⚫	⚫	🟢
Microsoft Information Protection	🟢	⚫	🟢	🟢	⚫	🟢	🟢	⚫	🟢
NextLabs EDRM and SkyDRM	🟢	🟢	🟢	⚫	🟢	⚫	⚫	🟢	🟢
Prot-On IRM-Prot-On	⚫	⚫	⚫	⚫	⚫	⚫	⚫	⚫	🟢
SealPath IRM	⚫	⚫	🟢	⚫	⚫	⚫	⚫	⚫	🟢
Seclore Data-Centric Security Platform	🟢	⚫	🟢	🟢	⚫	⚫	⚫	⚫	🟢
uniscon idgard	🟢	⚫	⚫	⚫	🟢	⚫	⚫	⚫	🟢

Legend 🟠 critical 🔴 weak ⚪ neutral ⚫ positive 🟢 strong positive

NextLabs is one of two featured vendors for capabilities for its ability to provide a well-rounded product offering. It's on-premise and cloud options provide end-to-end application protection for collaboration and protection of critical data. It comprises of both rights managements and classification capabilities. Policies are dynamically determined by subject, environmental, and resource attributes, as well as by the action to be performed. This dynamic authorization aspect is patented.

Seclore is also featured for its EIP capabilities. Seclore's Rights Management solution integrates with DLP, data classification, and SIEM systems to automatically discover, classify, protect, and track sensitive data. Document repositories can be hosted anywhere; rights management and encryption will be applied regardless of the file type and works with various kinds of repositories. Policy management is via a built-in policy manager and can also be federated from the integrated repository or application.

Fasoo is our featured vendor for innovation for the additional rights able to be imposed on documents. Fasoo's protection standard AES256 bit encryption assigns dynamic, adaptive access control to files and adds a unique embedded ID into each file for tracing, audit logging, and visibility. This unique ID stays with the file regardless of the file location or derivatives and is key to managing and controlling document versions across its entire product portfolio. Fasoo allows for total automation of the data security process, or allows users to make decisions on file protection such as an exception management capability. Fasoo Smart Print helps detect personal or other sensitive information and applies pre-defined policy before a file is printed, such as dynamic watermarking, masking, and blocking users from printing, assisting to minimize sensitive data loss. It's auditing capabilities allow administrators to see the image of the printout for stronger visibility and tracing of sensitive files. It also monitors user activity with the aid of a trusted clock, helping to avoid insider manipulation of a device's local clock.

The Microsoft Information Protection is well-positioned to solution facilitate secure collaboration on files. It has a combined offering of classification and rights management, leveraging workflows that are already familiar to the user. Microsoft has the benefit of offering a collaboration platform, Microsoft Teams, into which Microsoft Information Protection is can be fully integrated. Azure AD B2B facilitates secure collaboration with external partners, without the need to manage external identities.

5 Product Details

Spider graphs

In addition to the ratings for our standard categories we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the Market Compass. For this Market Compass, we look at the following 5 areas:

- **Protection Model**
  The capabilities used by the product for the protection of information.
- **Collaboration Model**
  The approach for supporting collaboration within and beyond the enterprise.
- **Rights Management**
  The built-in rights management capabilities, such as protection at the document level through applying encryption and document-level entitlements.
- **Policy Framework**
  The framework of policies used to manage entitlements for information and its flexibility for enterprise use cases.
- **Mobile Device Support**
  The breadth of support for mobile devices and providing access to protected information via such devices.

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

5.1 AceroDocs

AceroDocs is a 2016 startup based in Madrid, Spain. Its flagship product of the same name protects files as they are shared internally within the enterprise as well as externally. AceroDocs is a user-friendly, easy to implement offering for light and straightforward file protection.

The product is delivered as an app for Windows iOS and Android but can also be used via its web platform. Protection is applied per file regardless of if it is stored in a cloud environment or in physical repositories such as servers or USB. The file owner can encrypt a file and assign unique document permissions to individuals, assigned by email address. Encryption is applied in transit and at the file's destination. Once received, the recipient unencrypts it in their device app if an AceroDocs account holder, or on AceroDocs homepage if they do not have an AceroDocs account. Files are viewable on all major devices, and in a web browser if the recipient does not have the AceroDocs app via its drag and drop functionality.

This EIP product is suitable for finished documents, providing protection for .pdf, .txt, images, and MS Office files. The company is currently developing support for audio and video files, as well as collaboration capabilities for MS Office files. Its strengths come from the straightforward assignment of permissions, but lacks options for customization, automated application of policies, or strong authentication capabilities.

Security	● ● ● ○ ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Protection Model	● ● ● ○ ○
Collaboration Model	● ● ○ ○ ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ○ ○
Mobile Device Support	● ● ● ● ●

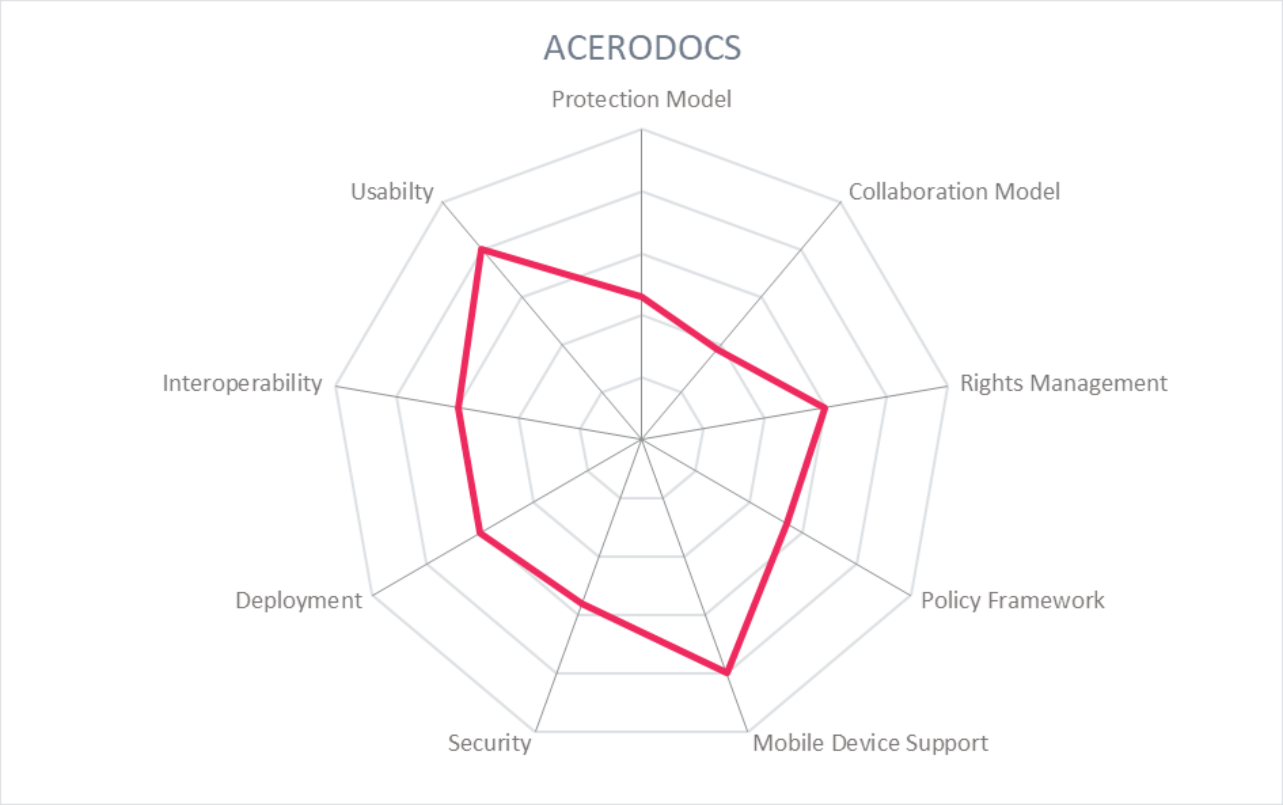
acerodocs

Strengths

- Containerized service simplifies delivery
- Uncomplicated user interface and straightforward protections
- Access may be revoked remotely at any time
- Protection for documents at rest and in motion

Challenges

- No email protection by default, but is an option in its plug-in for Outlook
- Limited protection of documents in use
- Limited customization of file protections, entitlements, or user authorization


ACERODOCS
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.2 Amazon Web Services

Amazon Web Services counts amongst the largest global suppliers of Cloud services. They offer a feature-rich service covering all aspects of Cloud services including compute services (Amazon EC2), Storage (Amazon S3), website hosting and collaboration tools. Part of this offering is the product Amazon WorkDocs (formerly Amazon Zocalo), which is a secure file storage and content collaboration tool for organizations. WorkDocs can be attached to an Enterprise AD or use a standalone directory for user authentication.

Amazon WorkDocs is a fully managed and extremely easy-to-use document storage and sharing service to enable content collaboration. Users are enrolled in the service with integration to their corporate directories and they can then access the corporate Amazon WorkDocs site. Uploading documents can be accomplished via Add Content and drag and drop click. Documents can be downloaded for use in their native application. A dedicated Amazon WorkDocs migration service application is offered to help first-time users migrate their on-premise file server content to WorkDocs, possible as a one-time data transfer or as regular migrations. Documents are stored centrally in the regionthe WorkDocs site is created in. WorkDocs is available in six regions worldwide. File tracking and auto-versioning are supported. It is a secure repository with 1 TB of default storage capacity. A mechanism to create approval workflows to track and manage document approval processes in an automated manner is one of the newer features for Amazon WorkDocs. File sharing is managed with a link share or invitation with usernames/email addresses, and rights to view, contribute to, or co-own are assigned at this time. Other rights managements include control at the file level for access, commenting, downloading or printing. Using IP address-based allow lists, administrators can define and manage groups of trusted IP addresses, and only permit users to access a WorkDocs site when they are connected to a trusted network. Off-line access is also supported. AWS maintains unlimited versioning and allows comments to be associated with specific versions to have a full log of document changes. 2FA for registered devices is supported. The AWS Business Productivity Series includes WorkDocs (file storage, sharing and collaboration), WorkMail (secure email and calendaring), and Amazon Chime (online meetings and video conferencing service). In addition, AWS offers WorkSpaces (virtual desktops) and AppStream 2.0, which offers cloud desktops and apps to end users. Amazon WorkDocs supports all major devices.

Amazon Web Services' approach using a secure repository with support from digital rights management is a flexible but slightly limited from a security perspective. It carries other benefits such as assisting organizations migrate from network file shares to cloud storage, task management for organized collaboration, Amazon WorkDocs Companion allows versioned editing in Microsoft Office, and Amazon WorkDocs Drive which is a desktop application that functions with the desktop's native File Explorer or Finder while still storing files in the cloud.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ○ ○
Policy Framework	● ● ● ○ ○
Mobile Device Support	● ● ● ● ●

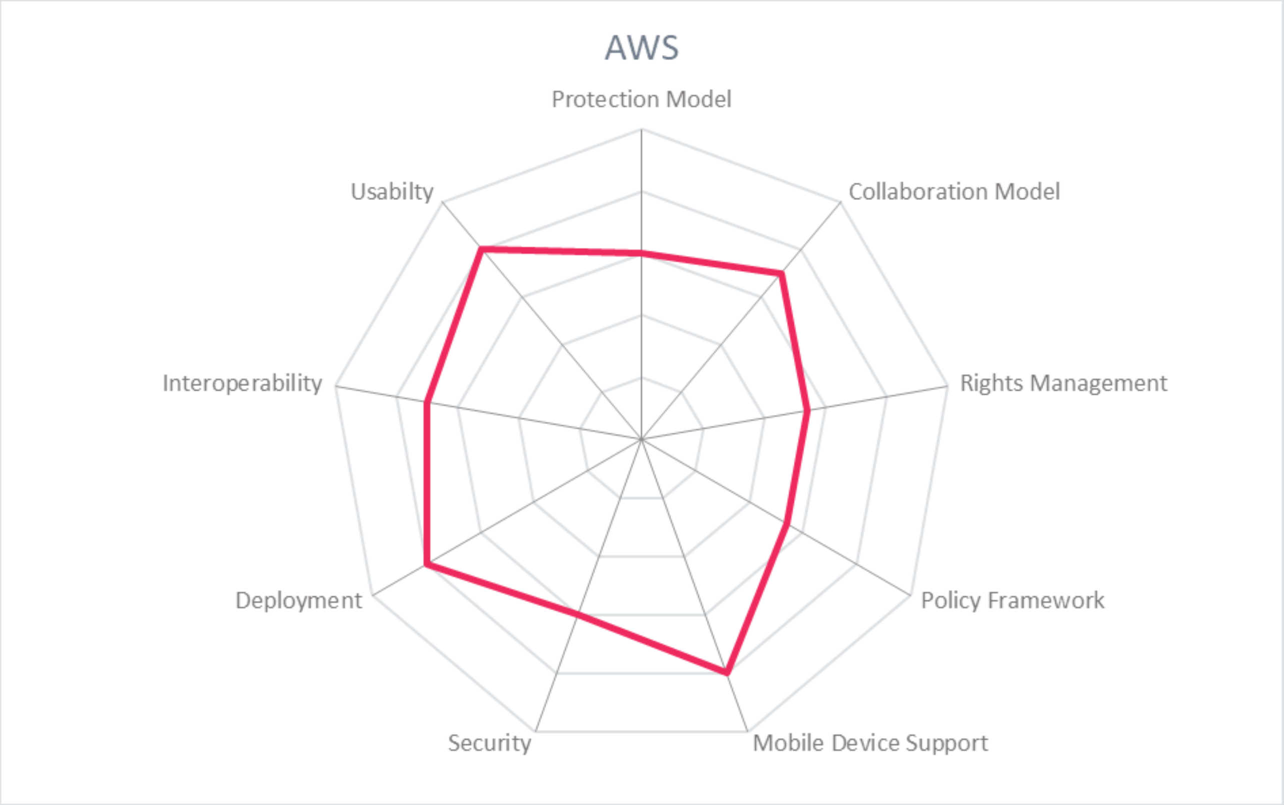
aws

Strengths

- Strong offering for AWS clients providing access to the main collaboration features in a secure way
- Broad market presence and global ecosystem
- Good support for mobile platforms via OAuth
- Desktop access to cloud files, and versioned editing capabilities in Microsoft Office
- Compliance with HIPPA, GDPR, PCI DSS is enabled, and is aligned with ISO compliance requirements
- Inexpensive price-point allowing widespread adoption of the service

Challenges

- Amazon WorkDocs supports AD and AWS/Microsoft AD, but does not yet have out-of-the-box support for users managed in Microsoft Azure AD
- SAML support for signed and encrypted data transfer should be considered


AWS
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.3 CryptoMill

CryptoMill Cybersecurity Solutions is a Toronto-based company founded in 2005. It provides multiple products in the EIP space, and this report focuses on its Circles of Trust product and concept, which creates groups of trusted team members and only grants authorized people the right to access protected files.

Circles of Trust is a hybrid solution that protects files regardless of their location, be it in the cloud, on a user’s device, or as an attachment to an email. The on-premise component is the Key Management Server, to provide customers with total control over its keys. A group of users are designated in the UI referred to as a circle of trust, and files are added to this group. Circles can be created manually or automatically based on existing organizational structures or processes, through AD and LDAP servers as well as for external collaborators who can authenticate with an email. Membership is dynamic with access able to be revoked at any time. Any file added to a circle is encrypted and remains so at rest or in transit protecting the document even if it is sent to an individual outside the Circle of Trust. One key is assigned per file, lifecycle management of that key is managed by the trusted group. Members of the circle may have read-only or editing rights, with further control over forwarding, copy/pasting, printing, or screen capturing rights. Policy control over Circles is very fine-grained, with the ability to customize approximately 70 features to create the desired secure collaboration environment. Multi-admin approval is required so that privileged users cannot unilaterally make critical changes. Individuals outside of the organization may be included to a circle, increasing the secure collaboration potential.

Circles of Trust’s simple user interface allows for intuitive usage, and it has a lean approach that only protects files that the organization deems necessary. MFA is an option for authenticating users. The solution integrates with all major cloud providers and is available on all major mobile devices with mobile app, or via a web browser. The solution provides protection independent of file type, size, and content.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ●
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ●
Mobile Device Support	● ● ● ● ●

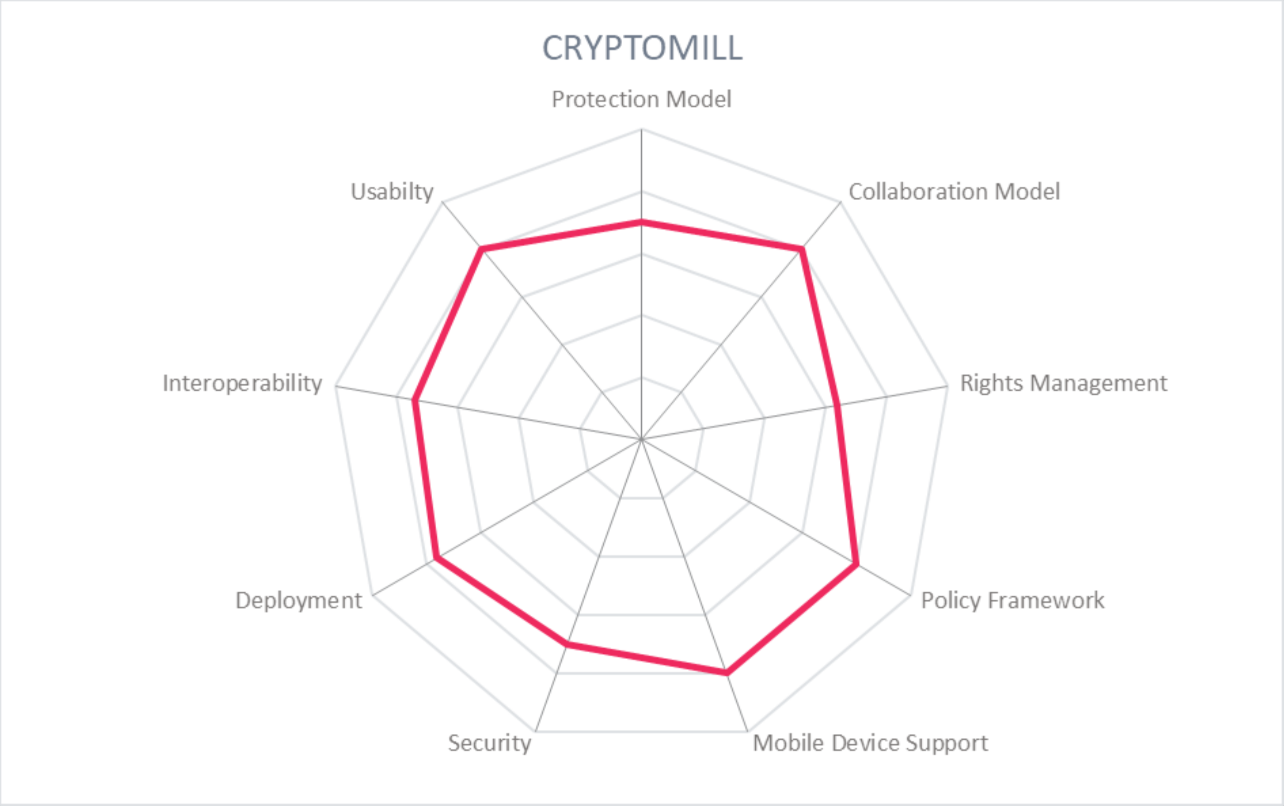
CryptoMill
Cybersecurity Solutions

Strengths

- Intuitive user interface
- Integrates with all major cloud providers and is available on all major mobile devices
- Circles of trusted users can be created manually or automatically
- Protection for information in use is possible, including offline editing
- Audit trails are recorded
- Trusted editing is fully functional offline
- Adherence to Privacy by Design principles

Challenges

- Approach may be too lean – lacks sensitive information detection capabilities
- No protection of email text
- No document versioning available


CRYPTOMILL
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.4 Egress

Egress was founded in 2007 and is headquartered in London. It provides data security services and EIP, particularly for email and file sharing. The Secure Workspace platform is a solution that allows secure sharing and collaboration on files with internal and external users.

Available in cloud or on-premise deployments, Secure Workspace is an extension for Microsoft Office that encrypts and protects files at rest, in motion, and in use. A plugin is provided for MS Office and is integrated into desktop and mobile applications to be non-disruptive to established workflows. Users are authenticated and assigned access rights, such as forwarding, copy/pasting, geolocation access, time of access, and downloading. Remote revocation of access is available at any time. All main operating systems and devices are supported, but support for cloud providers is limited to Azure, AWS, UKCloud, and UKFast.

Secure Workspace is a good solution for enterprises that rely only on MS Office. The simple deployment and ease of use is a positive for implementation. The solution is compatible with all SAML2 compliant identity providers, and SSO is supported for internal users. Audit trails and tracking of all interactions with a file is possible, including file opens, location, sharing, editing, and downloads.

Security	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ●
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

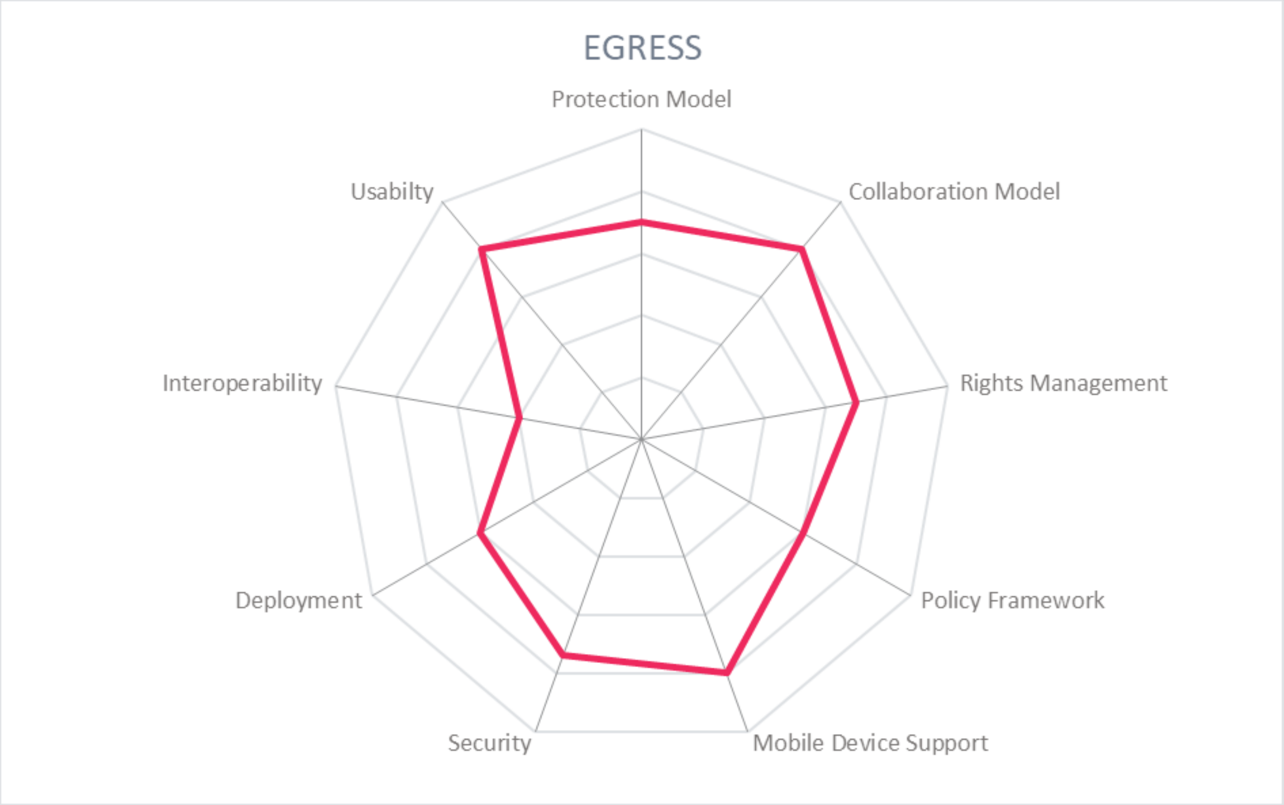
egress

Strengths

- Simple deployment with plugins and APIs
- Able to customize tool to match customer branding
- Free for third-party users to securely access protected files that are shared with them
- Protection for information in use is supported, including offline editing

Challenges

- Service is limited to MS Office Suite
- Only four cloud providers are supported: Microsoft Azure, AWS, UKCloud, and UKFast
- Lacks detection capabilities for sensitive information


EGRESS
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.5 Exostar

Founded in 2000 and based in Virginia, Exostar is a strong player in industry collaboration environments and actively supports identity management and document sharing, particularly in a multi-enterprise collaboration environment for specific industry sectors that require strong security and regulatory compliance. It currently serves industries including aerospace, defense, commercial aviation, energy, government contracting, healthcare, life sciences, manufacturing, and marine, supporting a global community of over 150,000 companies in more than 150 countries with trusted communication.

ForumPass is Exostar's cloud-based SaaS collaboration solution that offers multiple tiers of security to support business scenarios requiring controlled access to highly-sensitive documents and files. Exostar's identity and access management platform, Managed Access Gateway (MAG), provides for a multifactor authentication, single sign-on (SSO) user experience to access ForumPass. Authentication can be supported from Exostar's identity provider service (with in-person or remote identity proofing) or from a client's on-premise identity store via federated services with options for SSO. Documents can be protected via a full DRM solution – which incorporates technology from Seclore – with access controlled via policies that determine access rights on the basis of group membership or manually-granted permissions. Policies are attached to files which will control access and usage rights of users. Policies can be modified which will dynamically alter user permissions regardless of where the files may be stored. To properly support regionally-distinct compliance requirements, Exostar hosts ForumPass in both the U.S. and the U.K., offering customers the choice of data-at-rest location.

Exostar's expertise extends to identity and access management, security-as-a-service, multifactor authentication and industry certification compliance. Exostar is a Certification Authority, and issues credentials based on the National Institute of Standards and Technology (NIST) 800-63 standard, Levels 1 through 4. Exostar provides identity proofing and validation services for high-assurance environments, support PKI and two-factor authentication services such as one-time passwords (including mobile-based push authentication), common access cards, and other forms of enterprise identity. This is a strong solution for highly secure environments. ForumPass is cloud server agnostic, supports over 60 file types, and supports all major operating systems and devices.

Security	● ● ● ● ●
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ●
Deployment	● ● ● ○ ○
Protection Model	● ● ● ● ●
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ○

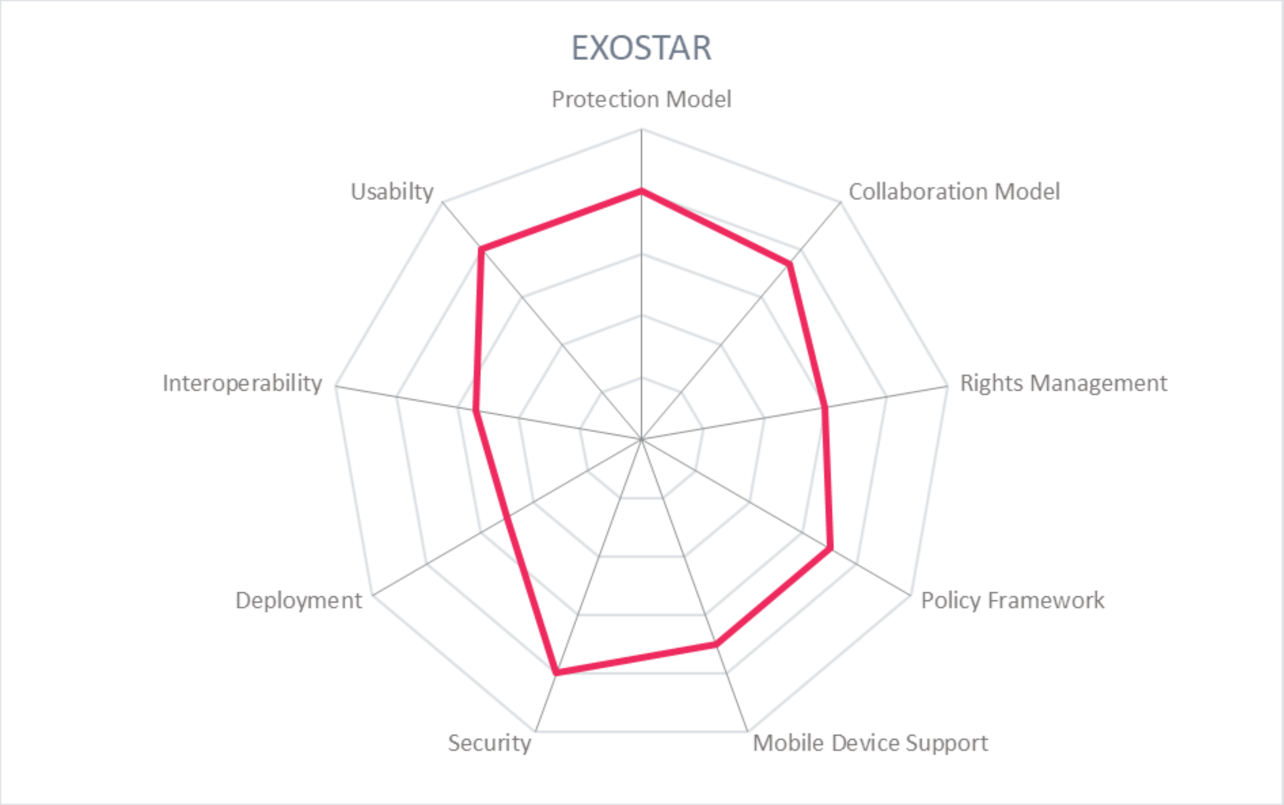
EXOSTAR®

Strengths

- Functionally complete managed service with strong encryption services
- Federated multi-factor authentication
- Innovative file-transfer support for fast transmission of large files
- Good protocol support: SAML, OAuth, OpenID Connect, WS-Fed, SCIM
- Strong customer assistance, with full SLA training and support
- Protection for documents in use, as well as in motion and at rest
- Compliant with regulatory standards such as U.S. NIST 800-171, NIST 800-63, Cybersecurity Maturity Model Certification (CMMC), and UK Official

Challenges

- Focus lies primarily on MS Office integration, built on Microsoft SharePoint
- A partial OEM, potentially adding complexity to delivery
- Browser-based client can view only
- Lacks detection capabilities for sensitive information


EXOSTAR
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.6 Fasoo

Fasoo was founded in 2000 and is headquartered in South Korea. It provides a suite of products to automatically discover, classify, and protect unstructured enterprise data, including the data-centric policy enforcement aspect, Fasoo Enterprise DRM (FED). This product enables enterprises to protect, control, and trace their data through file-level encryption and granular permission control.

FED is available in cloud or on-premise deployments, and offers protection for documents at rest, in motion, and in use. It relies on a secure combination of DRM Packager, Server, and Client where the Packager encrypts the file automatically as users create it locally or when downloaded from a repository or cloud-based system. The user is granted permission based on the pre-defined security policy for both the user and the document, and the data inside the file is unencrypted and passed to a rendering application (i.e. Microsoft Word) for use on the client. The file is always protected and under control at rest and in use, even in memory and temp files. Both users and devices must be authenticated to access a protected document. File rights include viewing, editing, printing, watermarks, screen capture, etc. and can be customized per user, device, and document.

Fasoo allows for robust authentication and offers SSO APIs and ready-made integrations into Active Directory, LDAP, and Identity and Access Management systems. Audit trails are provided, even in offline mode. The product provides functionality for a wide variety of file types, including CAD, and for all standard devices and operating systems.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ●
Policy Framework	● ● ● ● ●
Mobile Device Support	● ● ● ● ●

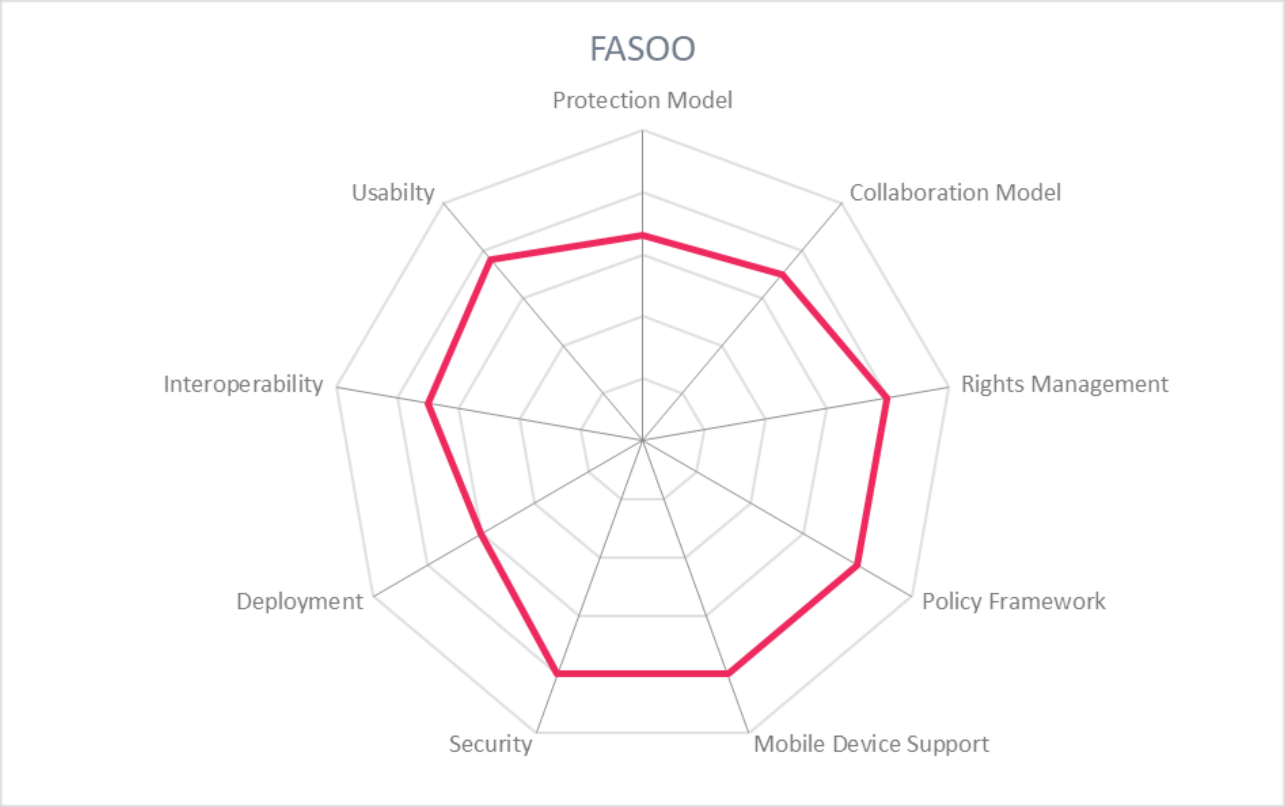
FASOO

Strengths

- Dynamic policy control allows for granular policy change even after encryption and distribution
- Fasoo Smart Print helps detect personal information and applies pre-defined policy including masking sensitive data and blocking users from printing
- Trusted clock, blocking screen-capture and secure copy/paste allow added file protection
- Strong ability to scale in large enterprises
- Files are protected at rest, in use and in motion
- Embedded ID in each file for stronger visibility, audit, and version control
- Automated Discovery, Classification, and protection of sensitive data in a single policy
- Exception management included

Challenges

- High security policies may disrupt flow of work, but can be mitigated through the proper use of exception policies
- Support for HSM could be considered
- The global partner ecosystem is still expanding


FASOO
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.7 Intralinks

Intralinks, an SS&C company, is a financial technology provider for the global deal-making, alternative investment, and capital markets communities. It offers a SaaS multi-tenanted secure, document-centric collaboration solution. Unshare is an information rights management solution to provide administrators control over file permissions and access. This product and others in Intralink's Trust Perimeter provide secure content sharing and collaboration within and between companies.

IRM is a managed service on Intralinks private Cloud service that allows users to securely collaborate using a wide variety of devices. Each file is encrypted with AES 256-bit encryption, and protected in motion, at rest, and in use. Users attempting to access a protected file must first authenticate. An Intralinks Workspace manages access to protected documents, logs access, and provides audit reports on authentication events. Files can be arranged in folders and the owner can invite others to collaborate in the workspace as an owner, editor, or viewer. External party users also have the option to add a comment to the file. Documents can be uploaded or 'dragged and dropped' and can be shared with recipients via email, with the recipient receiving a link rather than an attachment. Access to documents is controlled by the rights management settings associated with the document in question. IRM provides the ability to control the permissions assigned to users down to the document level for its lifetime. A redaction tool helps to detect sensitive information such as PII to quickly redact and share with external parties. Its archiving capability adopts bitlocker encryption, and its DealMarketing and DealVision products use document versioning, classification, and file repository as well as AI capabilities.

Intralinks has a strong model comprised of six disciplines and technologies that include data sovereignty, governance, and compliance, and four security levels: file, application, platform, and operations. Documents in-transit are protected via TLS and documents in-use rely on IRM with edit via MS Office and view/annotate via Adobe Acrobat. It can synchronize across multiple devices and allow documents to be shared with external parties. Intralinks has focused on providing a good user experience and extending the use of their service via an API facility.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

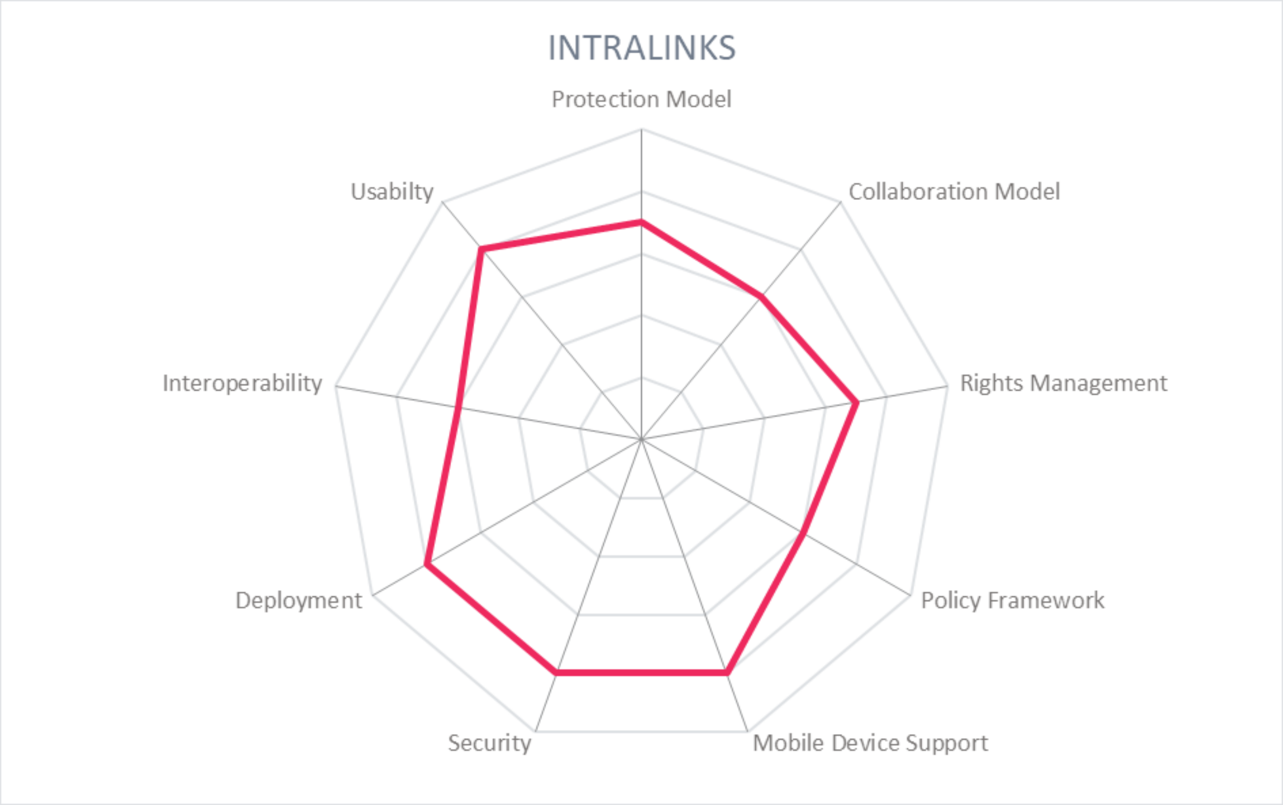
INTRA LINKS®

Strengths

- Strong encryption model
- Out-of-the box audit and reporting
- Third parties not required to download or install plugins to receive protected documents
- Files protected in motion, at rest, and in use

Challenges

- Relatively narrow business case for acquisitions, with potential to use in other contexts
- Smartphone device limited to iOS and Android
- No content inspection tool is currently provided


INTRALINKS
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.8 Microsoft

Microsoft, based in Washington state, offers a comprehensive EIP solution with Microsoft Azure Information Protection. It follows a classify, label and protect process. It also supports on-premise products such as Exchange server, SharePoint Server and windows file servers. Microsoft Information Protection is the only solution that provides built-in labeling and protection capabilities in Office on all platforms including iOS, Android, Mac, and web.

The Microsoft Information Protection solution provides a sophisticated classification system that can apply labelling to a document based on who created it, the context in which it was created, and/or the content within the document. Microsoft has focused on the user experience and made the product intuitive and easy-to-use. Users determine the classification of a document either themselves or via suggestions based on policies. The document then carries this label and encryption which ensures it is protected for its lifetime. Document owners can track statistics on who has accessed their documents and revoke permissions if necessary. The management console allows an administrator to create policies for security groups and set conditions such as “apply visual markings” to alert a user to a file’s classification. Manual, prompted, and automated classification mechanisms are supported. Mobile devices (iOS and Android) are supported. Microsoft’s device registration feature ensures network access from authorized devices – i.e., those that have been explicitly enrolled in the organization’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. Logging, auditing and reporting facilities are provided. PDF vendors including Adobe, Foxit, and Microsoft Edge PDF have built Microsoft Information Protection labeling and protection capabilities within their reader products.

The Microsoft Information Protection solution is an enterprise-ready secure information sharing facility that will suit any but the most exacting document protection requirements. For Office 365 users Microsoft Teams might be an adequate secure collaboration solution.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ●
Rights Management	● ● ● ● ●
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

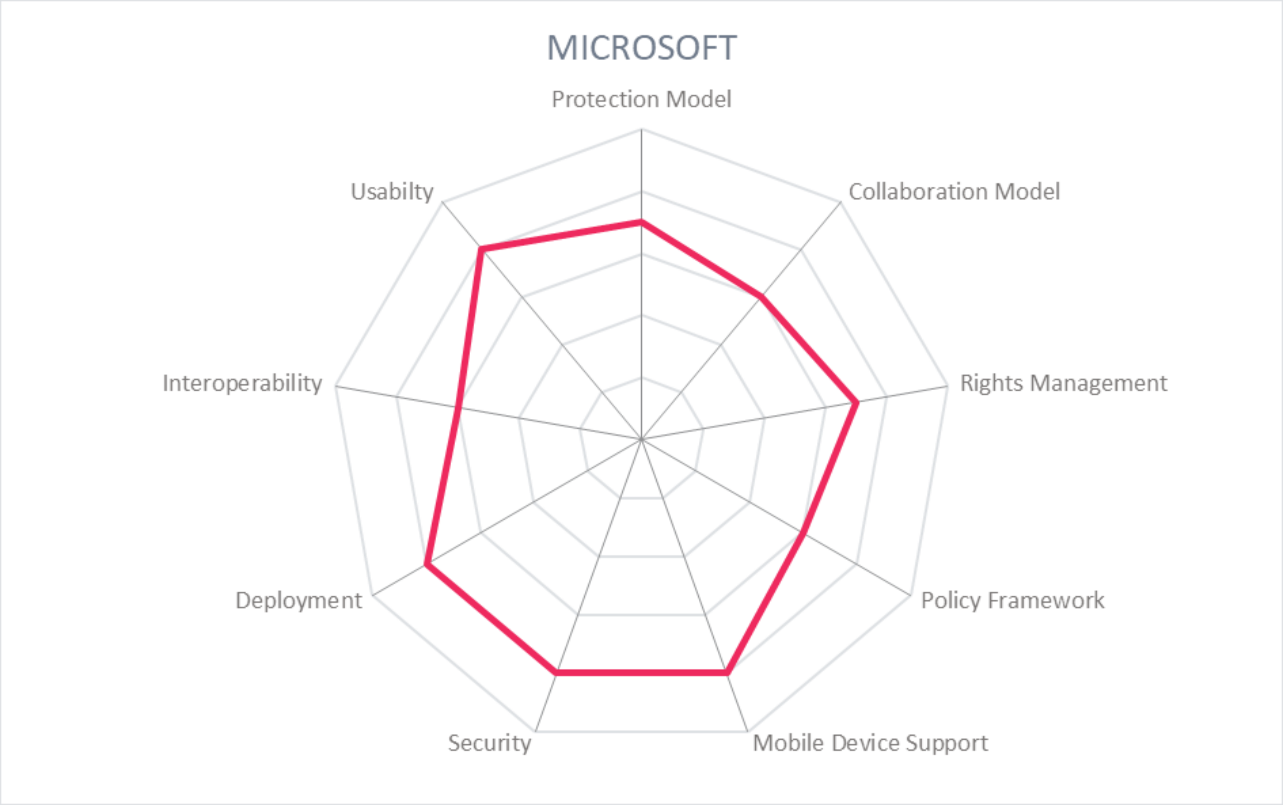
Microsoft

Strengths

- De facto standard for Office documents, and strong coverage for Windows, mobile, and web platforms
- Coverage for on-premise and cloud services (Azure only)
- Integration with an organization’s identity management environment
- Support for multiple encryption key management scenarios: BYOK, HYOK, etc.

Challenges

- Inability to upload custom images
- Integrated back-up is lacking


MICROSOFT
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.9 NextLabs

Founded in 2003 and based in California, NextLabs has a long history in collaborative rights management enabling sharing of protected documents to authorized users. NextLabs's products can be on-premise with Enterprise Digital Rights Management (EDRM) or on cloud services with SkyDRM, leveraging dynamic authorization with ABAC policy control. From a beginning in the aerospace and defense industries, NextLabs' industry focus has expanded to health and life sciences, manufacturing, government, financial services and energy market segments.

SkyDRM can be deployed as a SaaS, managed service, or be run on a customer's own private cloud or on-premise, in which Docker-based containers could be used. The NextLabs product offering consists of a Policy Management Server that utilizes 4GL policy language and component model for centralized policy. Policies are dynamically determined by subject, environmental, and resource attributes, as well as by the action to be performed. There are multiple data protection stages: first, the authorization data governance policies are managed based on business requirements in the central policy server. Secure project data rooms also make it possible to manage access rights on a smaller scale or per project. Next the protection itself, where users classify and protect sensitive data in addition to documents inheriting the access policies set in the business application being used. Batch protection of documents from a legacy server is possible. Audit trails are created with every action or reproduction of the document, monitored by the dynamic rights management server.NextLabs also provides a web-based Rights Management Server which provides secure access and usage controls to rights protected content of any kind without the need to install any client software, and often supports viewing in the native business application.

The NextLabs Rights Management Client is supported on Windows, Mac, Linux and Android and supports most major file types along with SAP data and Siemens CAD and 3D data files. Any federated identity is supported and user identities can be sourced from AD, AzureAD, or any LDAP-compliant directory. NextLabs has connectors and native integration into the major ERP, content management systems, cloud drives, CAD tools, etc. NextLabs' EDRM and SkyDRM are used in OEMs for both SAP and Siemens.

Security	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ●
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ●
Mobile Device Support	● ● ● ● ●

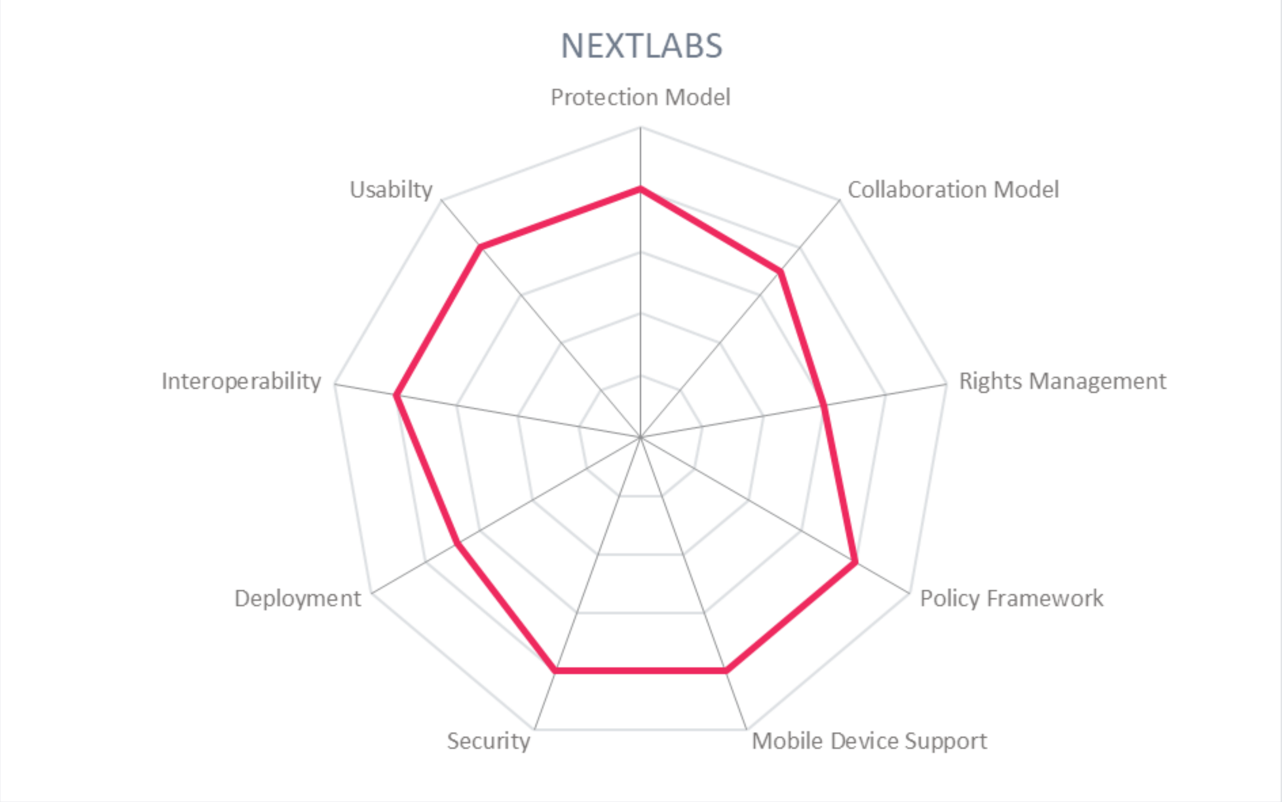
NEXTLABS®

Strengths

- Longevity on the market with a mature data sharing model
- Industry involvement and support for standards
- Fully integrated with SAP, Siemens
- Information classification capabilities available

Challenges

- Focus on the enterprise market means that scalable options might be cost-prohibitive for smaller organizations
- Authorization developments for smartphones could be utilized more
- Focus on regulated industries may restrict NextLabs’ reach


NEXTLABS
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.10 Prot-On

Prot-On, founded in 2010 and acquired by Groupo CMC in 2017, is an Information Rights Management solution for the enterprise and the individual, with internal and external access control management. It also provides secure document collaboration services. IRM-Prot-On's main emphasis is on information rights management, with complementary capabilities like data use tracking and classification.

The product's management server may be deployed on-premises or on Prot-On's cloud service. The on-premises version affords customers more control over security features such as key management, but the cloud service offers wide flexibility and a high level of security. Managed documents can be stored locally or on services such as Dropbox, OwnCloud and GoogleDrive. For cloud deployments, a REST API is provided. Policies can be defined by administrators and by users, policies that apply to multiple files can be supported with file-specific permissions, and any updates to a policy apply to all distributed copies of the relevant file through use of the central policy server. Prot-on solutions are widely used in financial services, the public and legal sectors, health and pharma industries and educations. It runs on all major operating systems, smartphones, and tablets, and supports the standard document formats.

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. Permissions associated with the file (users, groups and their access rights) are stored with the file as well as its metadata. Permissions are maintained even if multiple copies are made or 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 via an HSM. User logins are via username/password but social media logins via OpenID can be implemented. Prot-On maintains a directory of users; it can integrate with a company's directory service, importing user groups and authenticating to the corporate directory as users login via LDAP or via a SMAL assertion for cloud environments.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

Prot-On

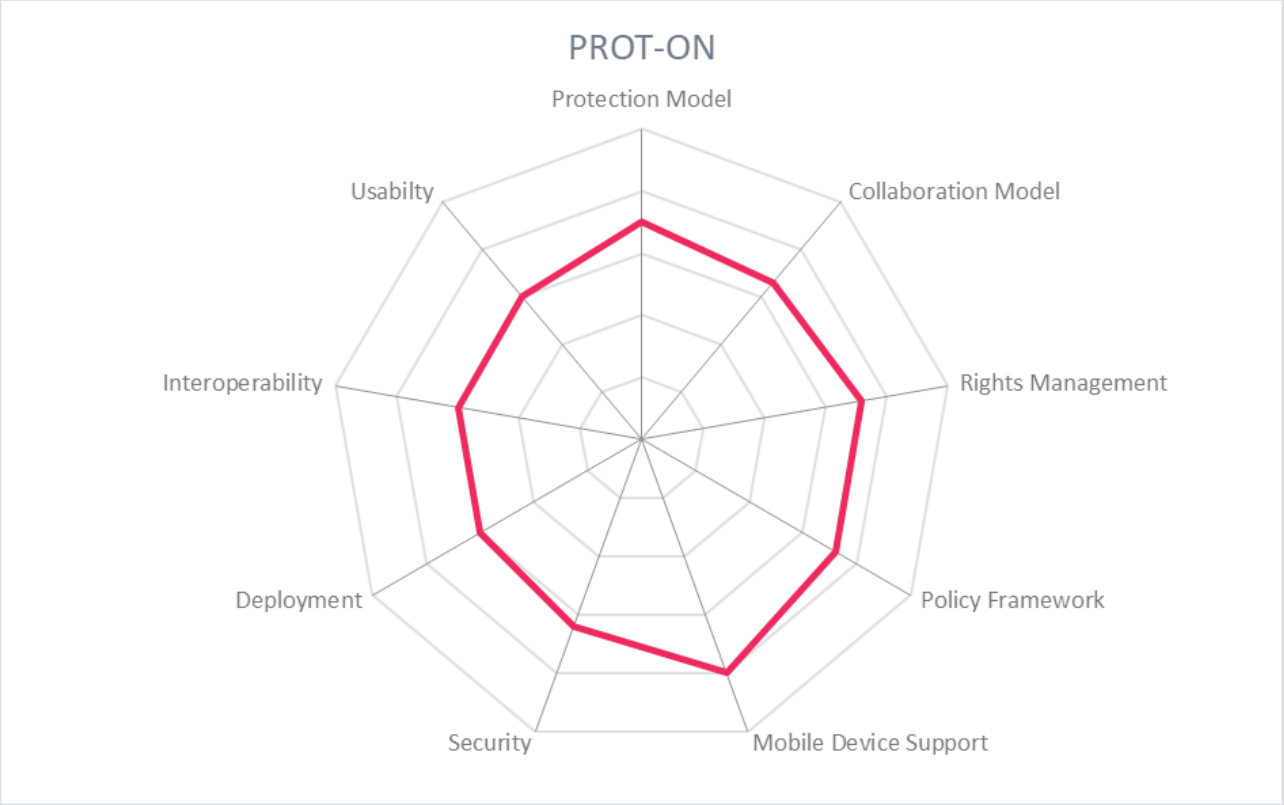
Protect what you share

Strengths

- Increased global reach
- A simple and easy-to-use file protection system
- A good balance between security and usability that suits most deployments
- Positive UX client screens for setting permission levels for users/groups
- Individual use is free
- Information is protected in use as well as at rest and in motion

Challenges

- A plug-in is required for Office applications to fully leverage the system’s capability
- Classification tools lack fine-grained access control
- The full span of the partner ecosystem and global reach is limited


PROT-ON
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.11 SealPath

SealPath was founded in 2010 and is based in Spain. Its main product, SealPath IRM, provides enterprise rights management solutions that work in an integrated manner with a variety of DLP solutions, classification, cloud, and document management systems with a focus on improving usability, collaboration, and protection automation. SealPath IRM automatically secures information stored in file servers, document management systems, and cloud collaboration tools at rest and in motion, and includes protection for emails and attachments.

SealPath IRM can be installed on a customer's servers on-premise with customer-managed keys with HSM, be deployed as a SaaS, or particularly for MSPs. The product protects files and individual documents with policy-based permissions that can be applied to Active Directory or LDAP groups for internal users and external users. Administrators and users can manage their own policies independently of IT admin to take advantage of the business knowledge that determines the best protection of documents. Administrators can restrict which users can create policies, share them, invite external users, and more. When integrated with classification and/or DLP tools, SealPath IRM can automate the implementation of these policies. These permissions follow documents regardless of their location and persists offline. Rights management can be applied to MS Office, PDFs, images, text, and industrial formats like CAD (including AutoCAD, Inventor, Siemens SolidEdge and others). These file types are encrypted and protected in transit, in use, and at rest. Rights include view, edit, copy and paste, print, and the ability to add users. Additional control and protection features include expiry dates, dynamic watermarks, and access restricted by IP address. Revocation of access and rights is possible at any time. Administrators can review the audit trails of all protected documents as well as statistics such as documents with the most risk, the top ten active users or documents, and more.

SealPath IRM contains the essential elements of Enterprise Information Protection. Security is bolstered by enabling customer key management when needed, protected by an HSM. SealPath IRM can work with identity management systems or with privilege accounts management tools through its integration with AD and LDAP. Collaboration is enabled with self-sign-up procedures for external users. Protected documents can be opened in the native app, or users can work with collaboration tools like Office 365 or SharePoint directly in the browser without needing to download the document to the desktop. All actions on a file are logged for audit and reporting purposes. All standard devices and operating systems are supported, and includes the option to use a browser version instead of a downloaded client.

Security	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

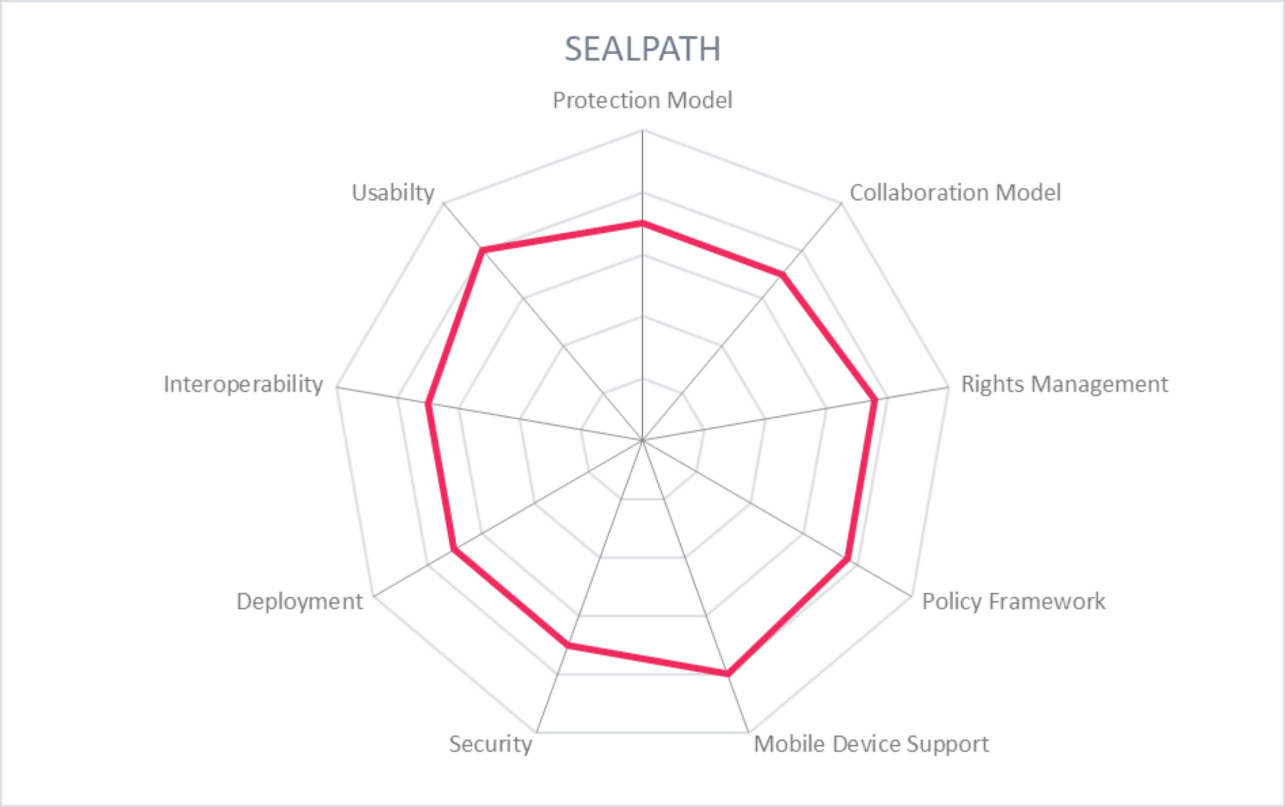
sealpath™

Strengths

- Broad set of supported systems and use cases
- Native integration with Office 365 for document and email protection
- Easy usability with drag-n-drop protection and dashboard for policy and rights management
- Access to protected documents can be controlled by IP address, so that very sensitive documents can be accessed by secure networks only
- Offline mode is possible without first needing to open protected documents online

Challenges

- Support for risk-based authentication would strengthen the solution
- Automated protection works at its best when used in conjunction with other classification or DLP tools


SEALPATH
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.12 Seclore

Founded in 2010 and headquartered in Milpitas, California, Seclore is a mature provider of enterprise rights management technology for secure file sharing and email communication. It integrates with data classification and DLP products and unifies them into its Data-Centric Security Platform for a holistic approach to discover, classify, protect, and track enterprise information wherever it travels or resides.

The platform offers on-premise or Cloud deployments (via AWS) which can be managed by Seclore or by a third-party provider. Document repositories can be hosted anywhere; rights management and encryption will be applied regardless of the file type and works with various kinds of repositories. Policy management is via a built-in policy manager and can also be federated from the integrated repository or application. A centralized policy server allows an administrator to define policies or allow individuals users to create their own policies to simplify the process to assign granular permissions for internal and external users. External users can access protected files via any browser or by downloading the Seclore-Lite agent to access the file.

Seclore’s focus on wide functionality and security make it a strong provider of EIP products. It offers out-of-the-box connectivity with Enterprise AD or LDAP corporate directory services. It also offers a built-in user repository for managing external users, if required. Users logged into the corporate infrastructure enjoy SSO to the Enterprise Digital Rights Management service. Seclore authentication can also integrate with Microsoft Azure, Okta, Ping Access and Google ID services. Seclore key management is server-based, encrypting individual documents via a tamper-proof mechanism. Clients can utilize their own HSM for key generation. All major operating systems, devices, and file types are supported.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ●
Deployment	● ● ● ● ●
Protection Model	● ● ● ● ○
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

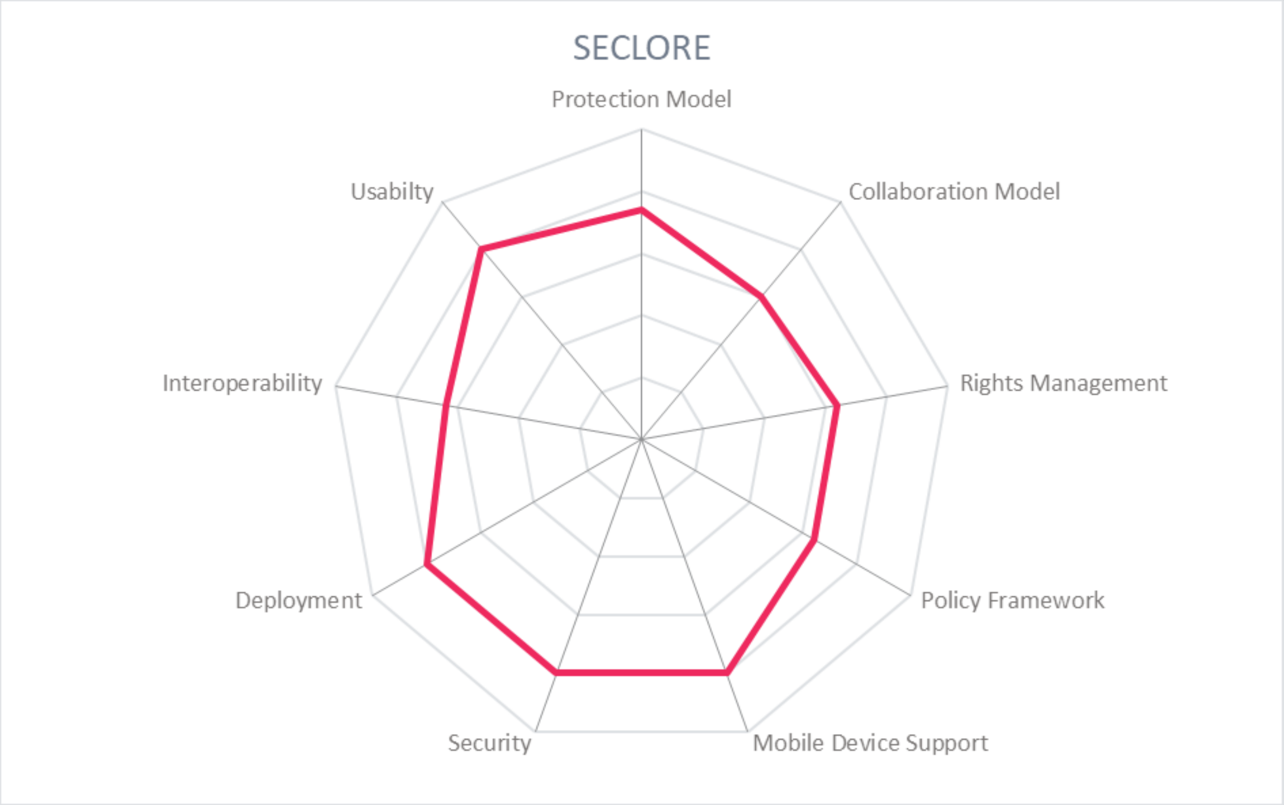
SECLORE

Strengths

- Established market solution with long market presence
- Flexible solution with many pre-built connectors and robust SDK
- Highly secure with standards-based encryption capability
- Flexible viewers for any device type
- Support for email security

Challenges

- Running all data through one platform may cause latency and performance issues


SECLORE
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

5.13 uniscon

uniscon was founded in 2009 and is based in Munich, Germany. Its information protection services is idgard®, which is deployed from uniscon's proprietary secure cloud. It operates a secure document storage facility and incorporates a rights management approach for in-use document protection.

The service is offered via managed service providers and could be installed on-premise if desired. uniscon's patented 'sealed cloud' technology is highly secure ensuring that only corporate staff can access protected information with dynamic deletion of files to ensure no access is provided to files being accessed. The idgard® product supports collaboration via the ability to establish project rooms and data rooms in the storage area with appropriate access controls. Documents at rest are protected via AES 256-bit encryption with dynamic key management for access control to documents, managed by document owners. Keys are stored in each individual's profile which is encrypted by a user-generated key. The managed service provider has no access to unencrypted files.
Users store all their secure documents in idgard® and email a link to collaboration partners. Recipients are required to enter a password, established by the document owner, to access the protected document. For two-way collaboration with external parties a guest-license can be issued to the remote user. Authentication to idgard® can be via the customer's AD or via idgard's® portal access control list. SAML is supported as is WebDAV and RestFUL API technology for interoperability.

uniscon brings high security and good integration potential to the EIP segment. It does not require the installation of any software, there are no set-up fees and the guest license is included. All common document types are supported with additional features provided, such as watermarking of PDFs. Policy management is via an easy-to-use GUI tool that allows the customer to manage access control by selecting from pre-defined policies and attributes. Wide support for devices is provided. Desktop systems access the idgard® portal via a browser session, and apps are available for mobile devices.

Security	● ● ● ● ●
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○
Protection Model	● ● ● ● ●
Collaboration Model	● ● ● ● ○
Rights Management	● ● ● ● ○
Policy Framework	● ● ● ● ○
Mobile Device Support	● ● ● ● ●

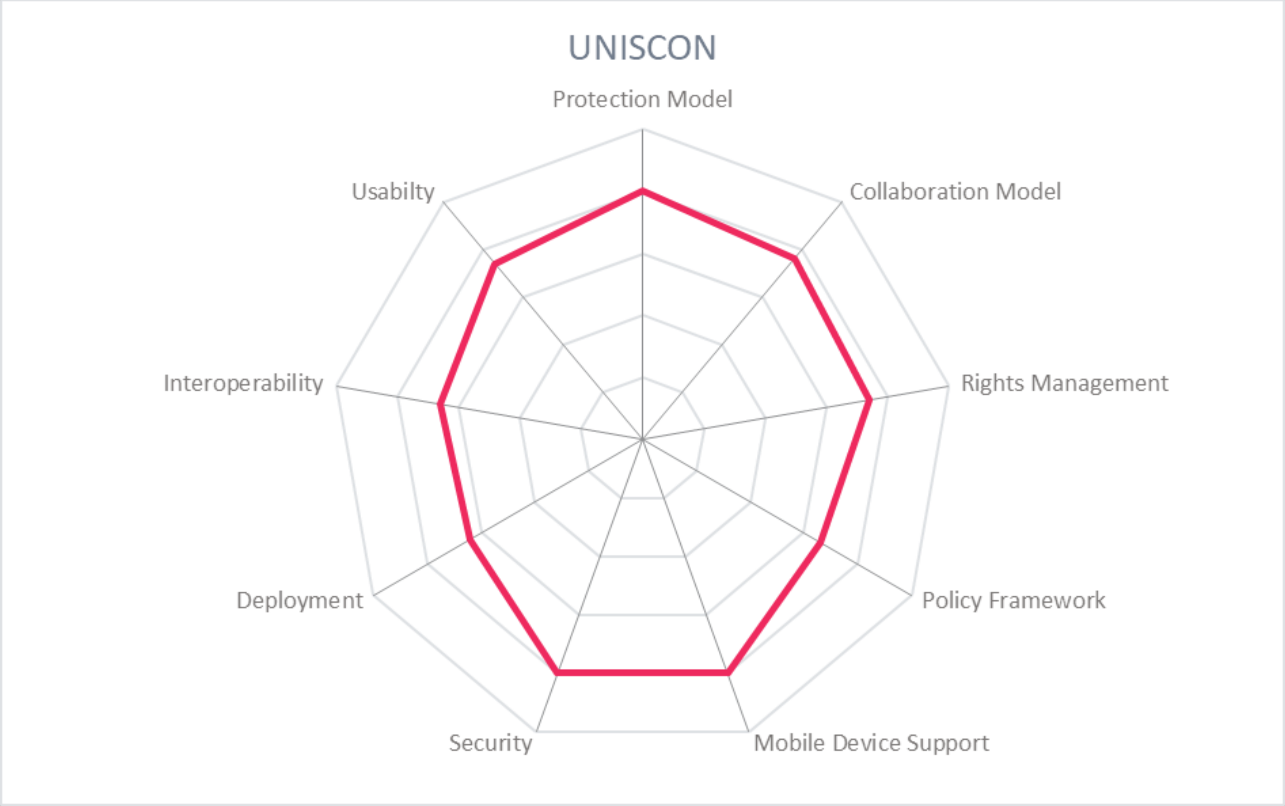
UNiSCON
Sealed Cloud Technologies

Strengths

- Secure login via username and password, SMS token, secure SIM card, certificates
- “Revision-proof” journal report
- Dashboard and real-time monitoring is supported
- Protection for documents in use, in motion, and at rest

Challenges

- Only manual classification is supported, no automatic
- Collaboration only via a secure data room, no flexible sharing of documents
- Limited document versioning issupported, with more functionality in the pipeline


UNISCON
Protection Model
Collaboration Model
Rights Management
Policy Framework
Mobile Device Support
Security
Deployment
Interoperability
Usabilty

6 Related Research

Executive View: Exostar Supplier Risk Management – 79074
Executive View: NextLabs Data Centric Security in the Hybrid Cloud—72531
Executive View: IRM-Prot-On – 71313
Executive View: Safe-T Software Defined Access – 79075
Executive View: Exploring the Microsoft Azure Information Protection Landscape – 72540
Advisory Note: Big Data Security, Governance, Stewardship – 72565
Leadership Brief: Introduction to the Information Protection Life Cycle and Framework – 80370
Leadership Brief: The Information Protection Life Cycle and Framework: Acquire and Assess – 80371
Leadership Brief: Data Security and Governance (DSG) for Big Data and BI Environments – 80109

Methodology

About KuppingerCole's Market Compass

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Ease of Delivery
- Interoperability
- Usability

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

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

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

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

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

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

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

Rating scale for products

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

- **Strong positive**
  Outstanding support for the subject area, e.g. product functionality, or security etc.)
- **Positive**
  Strong support for a feature area but with some minor gaps or shortcomings. Using Security as an example, this could indicate some gaps in fine-grained access controls of administrative entitlements.

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

- **Weak**
  Below-average capabilities in the area considered.

- **Critical**
  Major weaknesses in various areas.

Content of Figures

Copyright

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

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