Fasoo Enterprise DRM

Enterprise Digital Rights Management

WHITEPAPER

Fasoo, Inc. I 7315 Wisconsin Avenue, Bethesda, MD 20814
Tel : (732) 955-2333 I Email : inquiry@fasoo.com

Fasoo Co., Ltd. (Headquarters) I 396 World Cup Buk-ro, Mapo-gu, Seoul 03925, Korea
Tel : +82-2-300-9000 I Fax : +82-2-300-9400 I Web : www.fasoo.com

FASOO

Table of Contents

Introduction

The latest technology allows us to communicate and collaborate at the speed of light, but makes it easy to lose intellectual property, trade secrets, personally identifiable information (PII), personal health information (PHI) or PCI regulated data with just one click or tap. An increasingly mobile and remote workforce uses a mix of organization-managed and personal (unmanaged) devices from home, while on the road and from higher-risk global locations. Cloud and mobile computing have brought new challenges as companies adopt BYOD policies to reduce cost and allow users the flexibility to choose the best experience for themselves. Conventional information security tries to protect network and system boundaries, but cloud and mobile computing blur those lines making it difficult or even meaningless to define the perimeter of a corporate network. Information security must enable mobility, remote work and the consumerization of devices, applications, collaboration tools, and social networking for business and personal use.

According to Search Technologies, about 80 percent of the data created today is unstructured content stored in documents. Most organizations consider these documents secure while inside a controlled boundary, such as a content management system, collaborative repository, email inbox or shared file folders. Authorized users download these documents to desktops, laptops and mobile devices, where they can easily copy and forward them anywhere. Once someone has a document, they can do anything with the information in it, since there are no restrictions on what can be done with the data or where it can be sent.

Authorized users can be an insider threat as they may accidentally or deliberately share sensitive information with unauthorized users. Most organizations manage insider threats as part of general security practices, but often ignore information security, relying on general security guidelines and regulations without appropriate technical measures. In addition to cloud, mobile and insider threats, advanced persistent threats (APT) have become the latest concern of CISOs. As cyber-attacks are constantly diversifying and evolving, it is a complicated game of cat-and-mouse, and hackers are frequently one step ahead in the game. There have been many efforts to detect and mitigate insider threats and APT, but it is difficult to prevent and detect them, leaving organizations vulnerable to data breaches. You should implement a security framework that assumes your network will be penetrated, your systems infected by malware and your data stolen.

Enterprise Digital Rights Management (EDRM), also known as Information Rights Management (IRM) or Enterprise Rights Management (ERM), is a data-centric security solution that protects information itself rather than focusing on perimeter and device security. It protects, controls and tracks documents containing sensitive information, whether at rest, in transit or in use.

Challenges

Managing and controlling unstructured data is by far one of the most challenging issues of data security for enterprises. All PII and other sensitive information, corporate or otherwise, should be protected with encryption and persistent security policies so that only authorized users can access them. Sensitive information is shared, often unknown by the organization and is notoriously unprotected in an era where:

- Remote workforces are more common
- Adoption of multi-cloud environments is increasing
- File-sharing internally and with third parties are standard business practices
- Unmanaged devices are growing

These trends and common business practices increase the exposure and risk of unstructured data.

It is common business practice for large enterprises to collaborate with over 20,000 third parties and partners. The foundational security challenge with external collaboration exists: once the information leaves the environment, all visibility and control disappear. And today, with a growing remote workforce, the exchange between internal employee and third parties can be lost. Known or not, the institution then becomes dependent on the security controls and infrastructure of the partner, which in many cases may be insufficient to maintain protection of the information.

Outsourced and Remote Workforces

A good example of risks associated with outsourcing is within financial services where printing of customer statements and checks is common. Sensitive information in most cases is sent to the outsourced partner without the benefit of assigned access rights or security controls beyond encryption. And because the information being transmitted and received by the outsourced partner is personally identifiable in nature, it is subject to legal and regulatory mandates. The print jobs also contain financial account information such as unredacted credit card numbers, therefore vulnerable to theft for unauthorized charges.

Remote workforces increase the risk of sensitive data exposure from insufficient VPN resources or users disconnecting from VPNs in favor of better system performance. Use of at home personal printers may put you at risk because sensitive information isn't redacted and there are no watermarks to identify the company or user. Worse yet, the organization has zero visibility into what is being printed and who can view the material.

Policy Enforcement

The one key challenge in implementing EDRM, in contrast to perimeter security solutions or encryption, is to enforce policy persistently even when a document is used. Achieving this requires constraining the functions of rendering applications to achieve persistent control. For example, if a user does not have the permission to print a Microsoft Word document, the print function of Word must be disabled. Organizations use many document formats and rendering applications and EDRM vendors face challenges keeping pace with application and document format updates. The partial list includes Microsoft Office, Adobe Reader, CAD, GIS, graphics applications and software development tools.

There are three different approaches to enforce policy at the endpoint as described in Table 1. The embedding approach can be used if it is possible to modify the source code or rewrite the whole rendering application for EDRM. There are a lot of rendering applications used in the enterprise and in reality, only the manufacturer can modify them. A company cannot use as many EDRM solutions as the number of rendering application vendors. Rewriting rendering applications for EDRM is not practical considering the cost and the fact that users seldom want to switch their applications.

Some rendering applications provide interfaces for plug-ins to third parties, but not all are equipped with such interfaces. Sometimes the interfaces are insufficient to implement EDRM functions fully. Another serious problem of the plug-in method is that it is not robust enough. Determined users may easily disable the plug-in, such as through Visual Basic tampering. Operating system (OS) filtering is a kind of plug-in at the OS level. Similar to the plug-in method, it does have limitations on security and EDRM functionality. Kernel mode filtering in Windows for example can control the application to some extent, but crackers may obstruct or crack communication while reading or writing plain data.

Runtime overriding controls access to the behavior of rendering applications at runtime. Rendering applications communicate with the OS through APIs and these APIs can be overridden in memory at runtime. This method is capable of controlling the complete features and functions of the applications, and minimizing risks of losing data from cracking attempts. Developing commercial quality products using the runtime overriding method requires lots of expertise, effort and time.

Table 1. Comparison of DRM Client Technology

	Embedding	Plug-in	Runtime overriding
Security	High	Low	High
Applicability	Very limited	Limited	Any application
Cost	Low	Medium	High

Little progress has been made towards the standardization or interoperability of EDRM. If there is such a standard and every rendering application vendor follows that, the enforcement of policy at the endpoint will no longer be an issue. Until then the efforts to develop a secure rendering environment should continue to meet the changing requests from customers.

Policy Management

Another big challenge is to build a complete policy model for documents traveling literally all over the world. Many organizations have deployed Enterprise Content Management (ECM), Enterprise Resource Planning (ERP), Product Lifecycle Management (PLM), knowledge management, file-servers, etc., to manage corporate information effectively. Documents stored in these systems would be the first targets for EDRM to reinforce existing access controls (ACL). The basic model is to DRM-enable a document upon download, so that the repository's ACL can be extended beyond its protective confines. This appears simple, but gets complicated if that document is meant for legitimate external sharing. Users also create documents at the desktop and have not uploaded them to the repository yet. These unregistered documents need to be protected with EDRM as well. EDRM solutions can be differentiated depending on policy management models to meet the security requirements of documents throughout their lifecycle. It will determine how widely and persistently the security policy can reach.

The Information Lifecycle and EDRM

A single document can travel through many enterprise applications and be converted into different formats during its lifecycle. What would happen if an EDRM solution were only applicable to a fraction of document types? A user would need to convert the DRM-enabled document in one format to a plain document in another unsupported format during a workflow. What if an EDRM solution only works with one ECM system, but not with other business application systems? This would result in multiple islands of security domains. Information needs to travel across the security domains without losing security. It is not practical to deploy EDRM solutions from different vendors in one organization. It may cause unwanted conflicts and is impossible to make interoperable. An effective EDRM solution should be neutral and work with any enterprise application system.

Fasoo Data Security Framework

The Fasoo Data Security Framework helps organizations enhance their information security based on a data-centric security model with people-centric policies. This multi-layered strategy protects, controls and traces an organization's unstructured data in an ever-changing enterprise IT environment.

Data-centric Security Model

Organizations should apply a security policy to data itself rather than controlling access to networks and systems. Unstructured data causes many security issues since it is constantly created and used by many different users, moved and stored in multiple locations, while structured data is generally stored and managed in secure environments. It is not easy to design a security model for unstructured data. Organizations should incorporate a security policy not only for data at rest or in transit, but also in use. The Fasoo Data Security Framework allows organizations to protect, control and trace their data based on a data-centric security model no matter where it actually resides. This enables organizations to implement effective file-level security policies and granular permission control for all data types throughout its lifecycle.

People-centric Policy

A data security policy should maintain a balance between security and productivity to allow different users to perform business operations on multiple devices without interruption. This is why security policy on data should be people-centric. The policy should be flexible and dynamically enforced based on rich context including content, user, device, time, location, etc. Even though a flexible policy is in place, organizations need to allow exceptions to minimize productivity issues. Data security policies are constantly challenged by the unpredictable nature of data usage in a business environment. The Fasoo Data Security Framework supports dynamic binding of policy with rich context and allows exception on-demand or through approval. The framework offers a unique methodology to adjust and optimize existing security policies by analyzing variation of exception ratios among groups.

Multi-layered Approach

A security framework that has a data-centric security model with people-centric policy may not be secure enough if it has only a single layer of policy enforcement. Exceptions are inevitable in a dynamic business environment and exclusions can be easily found in real implementations. Exceptions are a temporary deviation from policy and exclusions are an exemption from applying security policy. The Fasoo Data Security Framework consists of a three-tiered suite of solutions to strengthen information security. Fasoo Data Radar discovers and classifies the data and reapplies policy to data unprotected by policy exceptions and exclusions. The Fasoo Enterprise DRM (FED) suite plays a pivotal role to enforce security policy on data. Fasoo RiskView enables organizations to visualize risks by correlating logs of authorized data usage with other user activity. This approach enhances and completes an organization's security framework.

The Fasoo Data Security Framework is ideal for a diversified collaboration environment in cloud and mobile, effective for insider threat management and a last resort against possible APT.

Solution

EDRM solutions help companies maintain the confidentiality of sensitive corporate intellectual property and customer personal information. This secures a company's strategic business advantage, protects its intrinsic value and complies with government and industry security regulations. While nearly every company acknowledges the need for strong protection of its digital assets, they face significant hurdles in deploying full-fledged solutions company-wide. Given the challenging global economic climate, companies are limiting capital expenditure and seeking to lower operating expenses to control costs. This may limit a willingness to spend on new IT investments, yet many corporate boards and business decision makers advocate an increase in spending on data-centric security solutions to help mitigate the risk of insider threats and advanced persistent threats (APT) on their most important digital assets.

EDRM was historically viewed as complex to deploy, as it would impact existing workflows, employee productivity and interaction with stakeholders outside the company. The general market perception on EDRM was about creating additional work for IT departments. While the overall benefits of EDRM are recognized, these perceptions continue to impact adoption rates. Nevertheless, Fasoo has carefully crafted and executed its competitive strategy to thrive and grow in this promising but challenging landscape. Fasoo is uniquely positioned as an independent vendor of EDRM products. The solution has unique technology characteristics that make it broadly applicable to a wide variety of applications and file formats, while providing strong security and interoperability with major network security and digital asset management components. Fasoo is unique in its proven ability to deploy very large scale EDRM installations and leverages the strength of its unique technology, ongoing R&D improvements, comprehensive product capability, and effective use of competitive intelligence.

Fasoo EDRM supports numerous rendering applications, such as Microsoft Excel, PowerPoint, Word, Adobe Reader and numerous CAD applications, covers the entire document lifecycle, and provides an open security platform for existing enterprise systems. It has proven its effectiveness and scalability through numerous large-scale, enterprise-wide deployments.

Strategy

Fasoo's technology approach is driven by security and practical considerations. It overrides an application's memory space and provides strong document protection that integrates smoothly with the end user experience for third party applications where the EDRM vendor does not have access to the program code. This is a difficult approach for several reasons, including risk of performance impact and the need to keep pace with application and document format updates. Fasoo has developed the technical strength and deployment process to execute this well. Another unique Fasoo strength is its ability to scale across large enterprises, which are often a patchwork of identity management and client application systems. Fasoo has significant experience with securing information for large, globally distributed companies. For example, its flagship installation spans over 170,000 internal users and over 700,000 total users of affiliates and partners worldwide. Other competitors rarely have experiences of installations at this scale. Historically, enterprises in major markets have deployed EDRM on a need-driven basis, for a given department or a specific set of users. Today there is a drive to employ EDRM uniformly for all employees. Fasoo's strategy of combining a highly interoperable product with customization services has positioned it well to organically fulfill this growing demand.

Strategic Intent

Fasoo has a detailed understanding of competing technology approaches and the strengths and weaknesses of current market incumbents. Its product and service strategies all leverage this intelligence. Fasoo has a strong understanding of customer requirements and future trends. Its technologies are aligned with existing enterprise infrastructure and security needs. Fasoo's strategy is to be a provider of data-centric security that is not only agnostic to digital asset management, server software and Data Loss Prevention (DLP) systems, but also interoperates with all market leading applications and platforms and is scalable to meet the needs of large, global enterprises.

Characteristics and Specifications of Fasoo Enterprise DRM

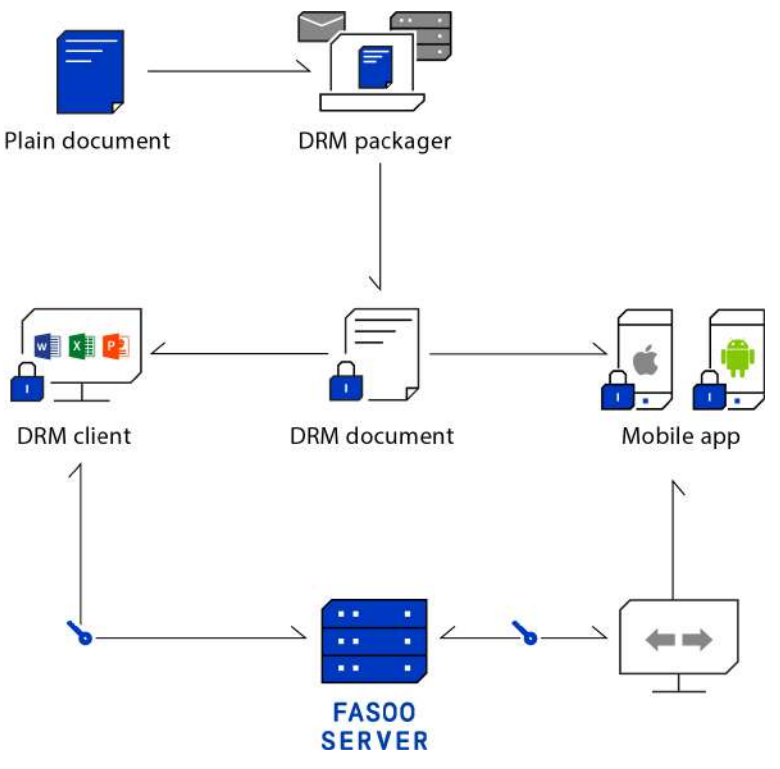
Architecture

Fasoo EDRM modules share the same core architecture. Features vary between modules to meet the unique security requirements of the discrete stages of the document lifecycle. The core Fasoo architecture consists of four major processes (DRM Client, Packager, DRM Server and rendering applications) and three key objects (document, DRM-enabled document and License).

A document is converted into a DRM-enabled document by packaging (encrypting) it with a Packager. The DRM-enabled document cannot be read without a DRM Client. When a user tries to open a DRM-enabled document, the DRM Client requests a License from the DRM Server. The DRM Server issues a License according to the pre-defined security policy for the user and the document. The DRM Client un-packages the DRM-enabled document and sends the data to a rendering application, such as Microsoft Word. The DRM Client controls the rendering environment and prevents any attempt to remove the decrypted data without a proper License.

Fasoo uses FIPS 140-2 validated cryptographic modules to meet the requirements of organizations that are part of or do business with the United States government. These meet the requirements of the Cryptographic Module Validation Program (CMVP) run by United States National Institute of Standards and Technology (NIST). This cryptography mechanism is the basis of Fasoo EDRM products and extends to accommodate different requirements.

Figure 1. Fasoo Architecture



The following steps describe packaging in detail:

- Encrypt a plain document with a document key (AES)
- Encrypt the document key with the server public key (RSA)
- Encrypt the metadata with a metadata key (RC4)
- Assemble a DRM-enabled document with encrypted metadata and encrypted document

The metadata includes a document ID, server URL, encrypted document key and other document related data. The document encryption algorithm can be interchanged to another if the functional features are the same, but the current AES algorithm is the best one in widespread use.

When a license is requested from a DRM Client, it provides the DRM Server with the encrypted metadata, user and device information. The DRM Server generates a License based on the licensing policy. A License is encrypted with a License key (RC4). The License contains a document key encrypted by a symmetric key associated with the device information and permissions the user can have on that document. This cryptography mechanism is the basis of Fasoo products and extends to accommodate different requirements.

Application Support

The DRM Client in a Windows environment supports most common native applications, rather than third-party viewers or editors. The DRM Client becomes transparent to users, since they use native applications to access documents. Using an additional viewer or editor may limit usability and eventually affect productivity. The DRM Client overrides the Win32 API to control rendering applications. It is capable of controlling the complete features and functions of the applications and minimizes risks of losing data from cracking attempts. Fasoo supports most of the common document formats and rendering applications used in most organizations, such as Microsoft Word, Excel, PowerPoint, Project, Visio, Notepad, WordPad, Paint, Adobe Acrobat, Adobe Reader, Adobe Photoshop, Adobe Illustrator, AutoCAD, Catia, Creo, I-deas, NX, Pro/E, and many others. New applications are being added regularly and the most current list is available upon request. The Fasoo DRM Client API is also available for those who want to develop a rendering application compatible with the DRM Client. Fasoo is not limited to the Windows PC platform as it is available on macOS, Android and iOS systems. A browser accessible trusted viewer is available to enable an authorized user to access documents from any device. These approaches will allow organizations to have some flexibility for cross-platform and multi-device environments.

Integration

Packaging and authentication should be integrated into existing enterprise application systems when implementing EDRM. A Packager should be integrated into the document flow for convenience and security. As users download documents from a repository, the documents should be automatically packaged. This simplifies users' interactions and ensures that all documents are encrypted. Authentication should be integrated so that users only need to log on once and for consistent policy management. Fasoo provides ready-to-install interface modules for many systems. When interfaces are unavailable, it is necessary to develop custom-made interface modules with available APIs. Fasoo provides a Packager API and single sign-on (SSO) API for various development environments, including C, C#, C++ and Java (JNI) on platforms such as Windows, Linux, Sun Solaris, IBM AIX, and HP-UX.

Authentication

Fasoo EDRM does not have its own authentication system. Instead, an SSO API and ready-made interface modules are provided for integration into Active Directory and other LDAP-compatible systems. For ad-hoc external users, a proprietary authentication, Fasoo Email Based Authentication (FEBA), is built into the relevant Fasoo EDRM products. FEBA allows robust and secure authentication without managing directories for random external users. Fasoo's authentication APIs can support numerous 3rd party, federated and proprietary authentication systems.

Policy Management

DRM policy defines what a user can do with a document on a specific device. A user must be authenticated first and an authenticated device is associated with a user. A user can have multiple devices but the number can be restricted as a part of policy. A License is a token to open a DRM-enabled document on a specific device with specific permissions and time constraints. A License is issued from a DRM Server based upon the licensing policy. Licensing policy is a function of user, device, document and other contexts, such as time and location. Various combinations of permissions can be assigned to a document, as in Table 2.

Table 2. DRM Permissions

	DRM Permission	Description
DRM-enabled	View_Only/Edit	Allows authorized user to open a DRM-enabled document for “view on the screen only” or “view, edit and save”. Edited and derivative DRM-enabled documents will have the original permission.
DRM-disabled	No_Print/Print_Watermark/Print	Allows “print”, “print only with watermark” or prevents “print”.
	No_Screen_Capture/ Screen_Capture	Allows or prevents “screen capture”.
	Un-package	Allows everything without any restriction, even retrieval of a plain document.

The licensing policy is able to grant offline access for business travelers and remote workers, view count for very sensitive documents and limit devices used only for specific users.

Blocking Screen Capture

Fasoo EDRM blocks all known third-party screen capture tools and the Print Screen function of Windows. Even attempts to capture screens through virtual machines or remote access tools are blocked. Screen capture tools are very useful sometimes, for example, if you are making a product demonstration kit or user manual with screenshots. Screen capture is one of the standard permissions to a document, so a policy can allow it for specific documents or users. Fasoo EDRM blocks only the window of the DRM-enabled document, not the whole screen. Screen capture permission can be extended to server-based computing (SBC) environments, such as Citrix XenApp and Microsoft Remote Desktop Services. Users can download sensitive documents in an SBC environment as long as they have permission to access the documents. This includes taking screenshots while the document is open. Fasoo EDRM products should be

deployed in the application systems and multi-user versions of the DRM Client should be installed on the SBC servers to control access. Fasoo Smart Screen (FSS) controls screen capture in a XenApp or other SBC client environment. Without FSS, a DRM-enabled document without screen capture permission cannot be viewed on the remote client since it may be considered an illegal remote access. Remote access from SBC clients with FSS is treated as an exception, and FSS blocks all other remote access attempts. To force users to install FSS, an SBC connection is allowed only with FSS. Fasoo EDRM makes it possible for users to take advantage of SBC with full DRM capabilities.

Watermark

Once a document is printed, the printout can get into the wrong hands and it cannot be protected by software. A visible watermark on printouts may contain identifying information and can be used to trace the user that printed the document. Watermarks are also useful to widely release sample content but make it inappropriate for anyone to use it. Fasoo EDRM can enforce visible watermarks on each page that include text or images of identifying information, such as company, division, title, user name, IP address and the time a user printed the document. Fasoo EDRM inserts visible watermarks before a document gets to the printer driver using a Win32 API overriding method, so there is no printer dependency. Visible watermarks can be inserted on any printer including virtual printing environments. Watermark print is a standard permission on any DRM-enabled document. Fasoo EDRM also provides screen watermarks to trace documents captured with a camera or phone on monitors or mobile screens.

Flexible Policy Setting

Any policy can be defined for each document or document group with various combinations of permissions and constraints for each user or group. Users can be grouped arbitrarily, for example, by roles, positions, or departments. Documents can be grouped by classifications with any criteria. Most organizations prefer to define a set of templates first and assign one of them to a document for convenience.

Exceptional Policy Setting

Even though a flexible policy exists, organizations need to allow exceptions to minimize productivity issues. Data security policies are constantly challenged by the unpredictable nature of data usage in a business environment and Fasoo EDRM allows exception on-demand or through approval. A user can request a one-time elevation in permissions to a specific document to allow them to do their job. This provides a layered security approach allowing flexibility within the enterprise security model.

Dynamic Policy Control and Offline Access

Policy is bound to a document when a license is issued, not when packaging. This late binding makes it possible to change policy at any time, if necessary, and apply it to any document, even if it is already packaged and distributed. A typical License is a one-time License. Whenever a DRM-enabled document is opened, a DRM Client requests a new License and the DRM Server will issue one based on the most recent policy. Policy for any DRM-enabled document can be changed or revoked at any time, regardless of its location or how many copies exist.

One drawback of this late binding is that it requires every device to have a connection to the DRM Server. There are some occasions when this is not possible. In such cases, multiple licenses with a time limit can be used, instead of a one-time license. Multiple licenses can be used repeatedly until the time limit expires. As a result, the document can be used even without connection to the DRM Server. Another way of supporting offline access is to issue a special offline license with a time limit. This will change all licenses on the device to multiple. This feature is very useful when users travel where a network is not available. To avoid the abuse of this feature, an approval process may be required prior to issuing such a special offline license.

Intelligent Policy Management: Context Aware Protection (CAP)

Depending on the content of a document, selective packaging is possible. A Packager is usually integrated with document workflow and is turned on automatically. This may result in excessive security because all documents are encrypted. There may be cases when packaging is not enforced and left to the user. Usually this results in insufficient security. With Fasoo's CAP, the Packager runs only if the target document contains a certain content pattern, such as a social security number. A pattern can be defined in the form of a regular expression or basic text. A document can be classified into pre-defined categories, based on content patterns. For example, if a document contains social security numbers, addresses and phone numbers then

it can be classified as a document with PII. If a document contains the code name of a special project, then it can be classified as top secret. A pre-defined policy can be applied automatically without user intervention. It can reduce the burden of packaging documents that may not have sensitive information. It also minimizes the risk of documents left un-packaged by the negligence of users.

DLP and EDRM vendors are collaborating to provide combined offerings. Fasoo supports DLP integration for customers who want to deploy both technologies. By integrating EDRM with DLP, DLP senses the content of documents at end-points or network boundaries, and EDRM encrypts the sensitive documents. The context aware capabilities sense the content of documents while in use, and protects them throughout the entire document lifecycle. This tight integration can offer a more flexible and robust policy, while applying EDRM policy through the document lifecycle.

Tamper Resistance

Fasoo EDRM has many tamper resistant features including secure copy and paste, secure export and trusted clock. Some codes are also inserted to prevent memory hacking, reverse engineering and attempts to disable DRM processes.

Secure Copy & Paste

Windows clipboard is controlled to prevent copying from a DRM-enabled document to a plain document. Copying is allowed between secured documents if the user has proper permission. Secure Copy and Paste is allowed when the user has at least edit permission to the source and target document. Secure Copy and Paste is unique to Fasoo EDRM and provides convenience without losing security. “Secure Copy and Paste” is a patent pending technology of Fasoo.

Secure Export

There are several ways to export the content of a file, such as printing to file and exporting content to other formats. Fasoo EDRM encrypts all exported files, which inherit the policy of source documents.

Trusted Clock

Fasoo EDRM maintains a trusted clock, rather than relying on a local PC clock. This ensures that a user cannot circumvent time restrictions by changing the system clock.

Usage Log and Audit Trail

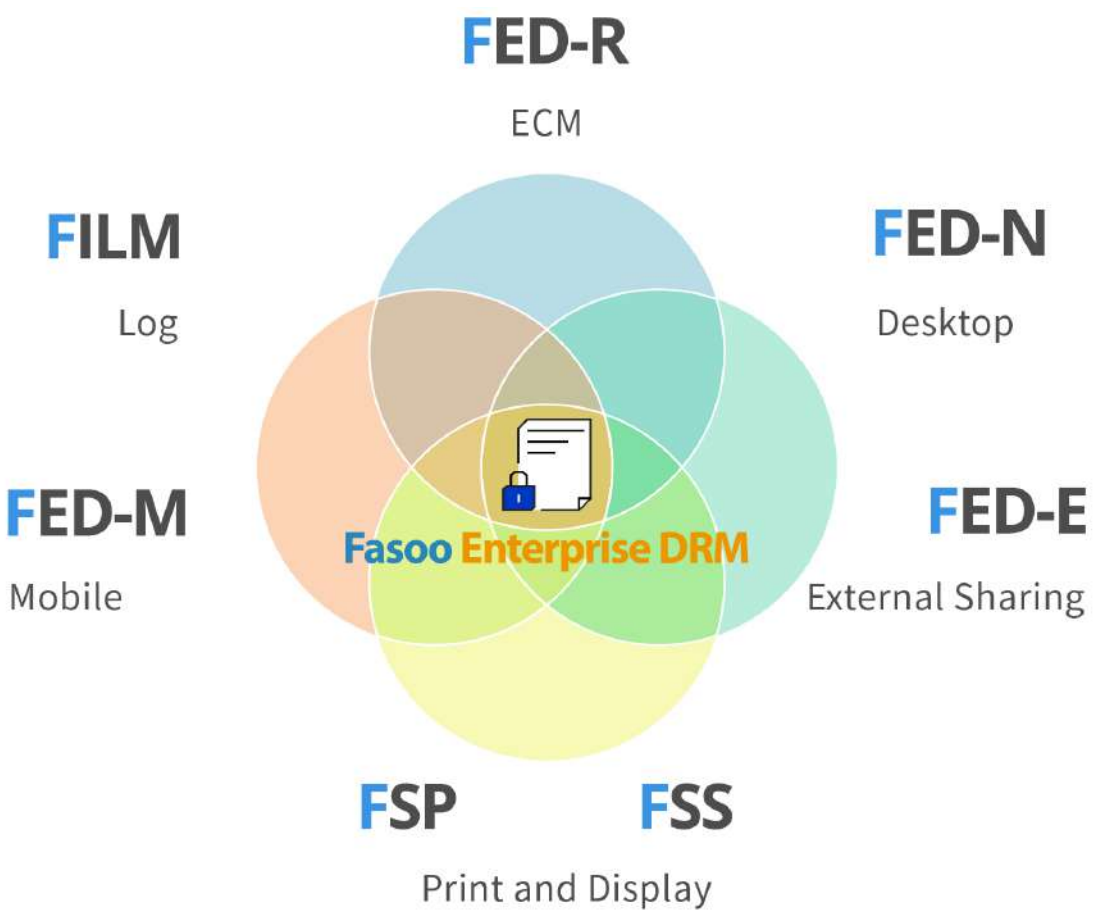
All user activities of DRM-enabled documents are captured in usage logs and sent to the DRM Server. Even when the document is used offline, the usage log will be sent to the DRM Server when the device is reconnected. Fasoo EDRM offers suitable tools for a document owner or administrator to review and audit activities of users and documents. Every policy change on the server is also logged. Security breaches by arbitrary changes of policy can be identified.

User and file activities related to sensitive data could be useful to run forensic analysis, yet it is still considered a procedure done by law enforcement and other highly trained specialists. Organizations need a better decision-making framework for proactively seeking and acting on potential security threats. Fasoo Integrated Log Manager (FILM) allows organizations to set a clipping level for usage patterns and alerts them to the risk of possible data breaches by detecting inappropriate patterns and activities in advance. It will not only work as a preventive measure to strengthen overall security of an organization, but also shows detailed user and file activities of sensitive documents.

FILM also allows an organization to adjust and optimize existing security policies by analyzing variation of exception ratios among groups. If a department is constantly requesting an exception to print specific documents, the organization may want to make that permission permanent, since it is a business requirement of that department.

Fasoo Enterprise DRM Suite

The Fasoo FED suite consists of several modules that can be used alone or combined together to extend the coverage.



Document Security Domain

After numerous EDRM deployments, Fasoo developed the concept of a Document Security Domain (DSD). A DSD refers to a boundary within which security policies for documents are maintained. Throughout the whole lifecycle of a specific document, it moves along several DSDs.

Let's examine the lifecycle of a price list and the security policy related to it. While the document is edited by a sales manager on a desktop and circulated for approval, the document should be accessible only by people involved in the approval process. After the approval process, the price list will be uploaded to an ECM system and become available to all internal sales people. At this stage the user boundary should be widened to all internal sales but it should be read-only. If a new partner joins as a distributor, the document needs to be shared with them. The partner should be allowed to view, but not to redistribute to anyone else.

In this example, the document belongs to at least three different DSDs throughout its workflow. Crossing a DSD, the security policy may change and the responsibility for document security may belong to a different person. The system to authenticate users also needs to change.

DSDs can be categorized into three major types: Server DSD, Ad-hoc DSD, and PC DSD. FED modules are designed to meet different DSD requirements for security and manageability reasons.

The PC DSD stands for the domain where documents are created and edited but not uploaded to a content repository. The documents may not be the final version and official yet, but still may contain a lot of sensitive information and should be secured. To support this domain, EDRM should be enabled at the creation of a document. The security policy of documents at this stage can be defined best, based on the author's security privilege.

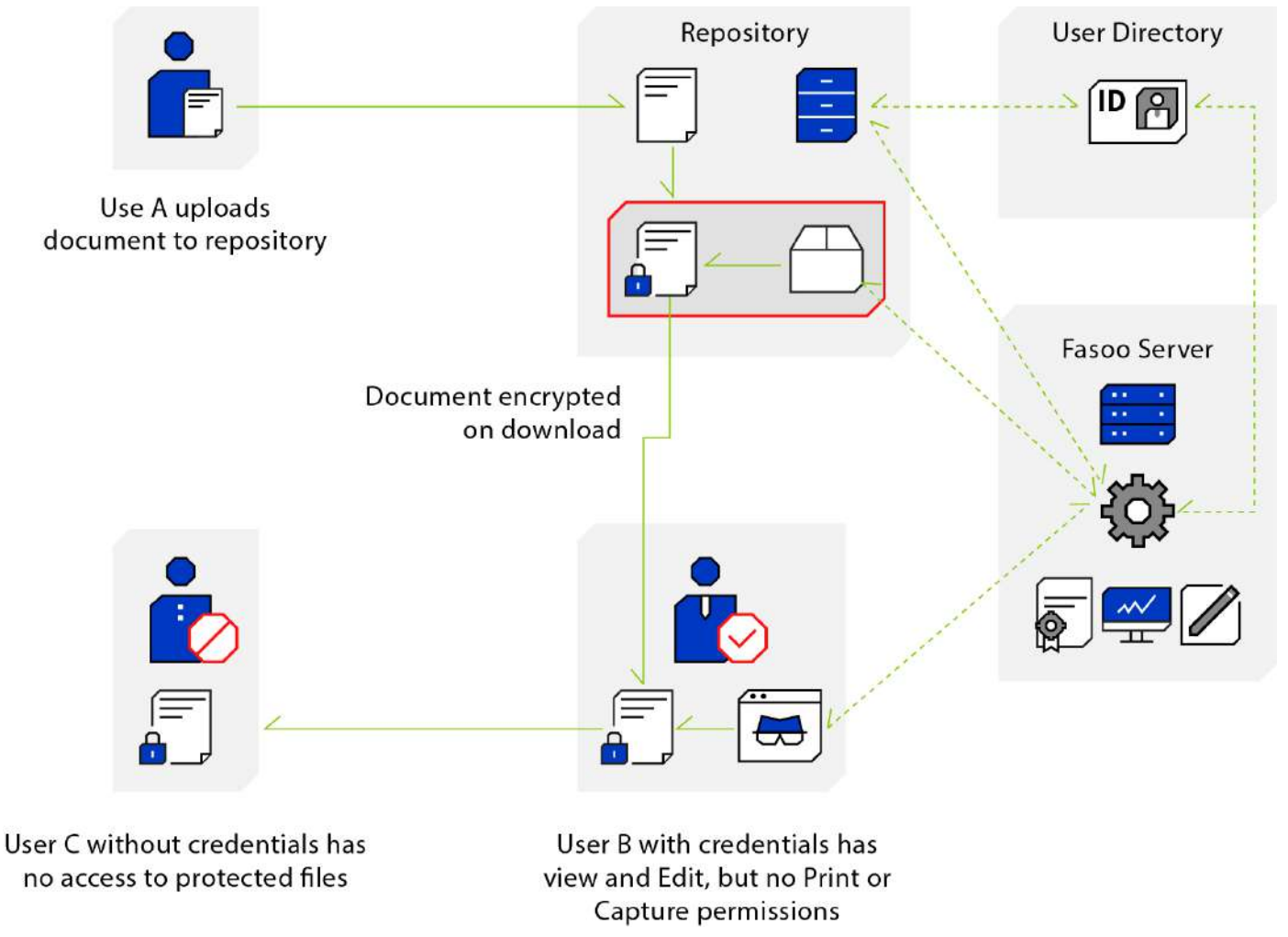
When the documents are checked into a document repository, the document is controlled by the ACL of the repository. The security policy cannot be maintained if the documents are downloaded from the repository, which is why EDRM is required to protect documents in repositories. The Server DSD is the domain controlled by a server-based system, such as an ECM system. The security policy of this domain is generally the extension of the ACL from the repository with additional security options that are available only with EDRM. User authentication should be integrated with the server to extend the existing ACL systematically. The administrator of the server will be responsible for the security of Server DSD documents.

At some point in a document lifecycle, the document needs to be sent to a person who is not within the current authentication boundary. In this case neither the PC DSD nor Server DSD authentication can be applied to external users. The Ad-hoc DSD has evolved to serve this domain and requires a new authentication system to cover a random user boundary.

Server DSD FED Product, Fasoo Enterprise DRM for Repository

Fasoo Enterprise DRM for Repository (FED-R) protects, controls and tracks documents that have left the protective confines of a document repository. Figure 2 illustrates FED-R integrated with a document repository, which can be an ECM, ERP, PLM or any sort of application server. The user authentication is integrated so a user only has to log into the target application system. A Packager is installed on the repository to package files as a user downloads them. Documents are kept unencrypted in the repository. There might be a security risk that plain documents are on the server, but it's important to ensure that encrypted documents do not interfere with indexing or workflows in the system. This is a tradeoff between security and usability. Daily routine policy management can be done mostly on the application server not on the FED-R Server. FED-R provides tools to integrate with existing authentication systems and the Packager works on multiple platforms.

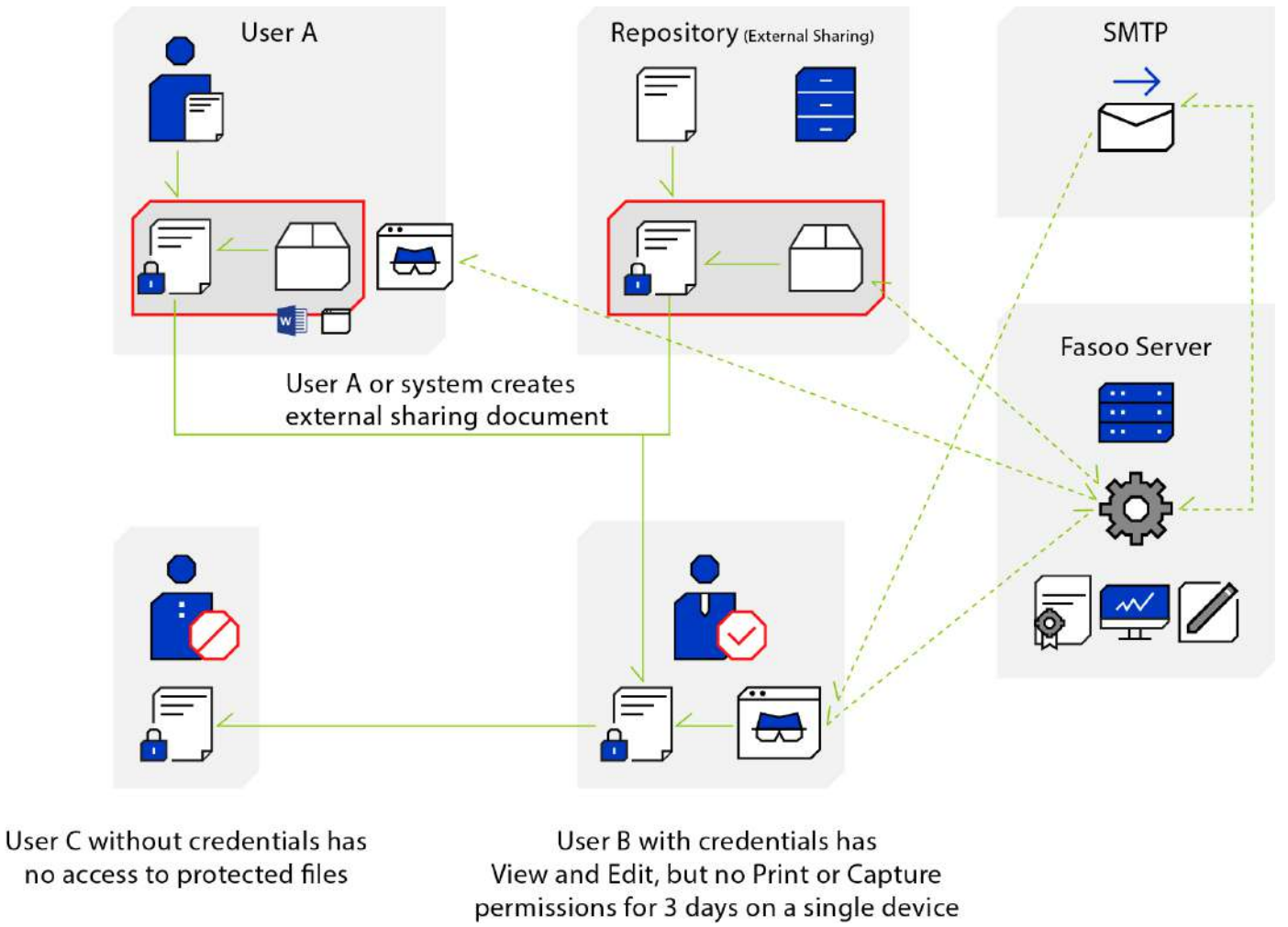
Figure 2. General Flow of Data and Components for FED-R



Ad-hoc DSD FED Product, Fasoo Enterprise DRM for External

Fasoo Enterprise DRM for External (FED-E) protects, controls and tracks documents and email messages sent outside the organization. It is designed for ad-hoc, unmanaged users. The Ad-hoc DSD's main concern is how to authenticate users. The user boundary cannot be known in advance and is continuously changing. FED-E offers a patent pending authentication method, called FEBA, where an email ID is used as its user ID and is validated and associated with device information. FEBA makes it simple to manage such random users with sufficient security. FED-E includes a standalone Packager, Microsoft Outlook plug-in Packager and API that can be embedded in existing systems. The FED-E Server usually resides inside the front-end firewall, DMZ, so that external users can access it. FED-E enables sharing confidential documents through any media with anyone who has an email ID. Figure 3 shows the processes involved in sending and receiving FED-E documents.

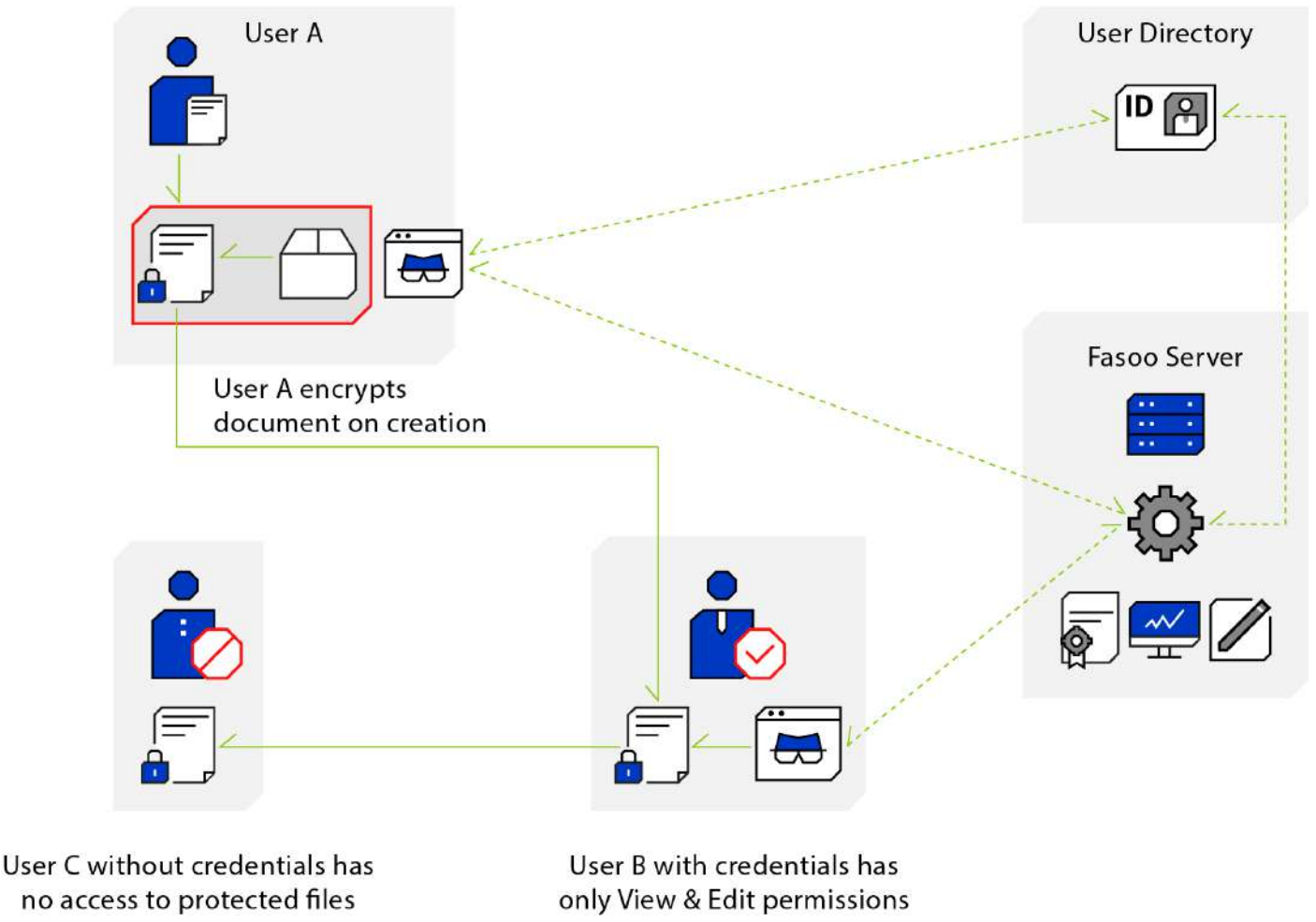
Figure 3. General Flow of Data and Components for FED-E



PC DSD FED Product, Fasoo Enterprise DRM for Node

Fasoo Enterprise DRM for Node (FED-N) protects, controls and tracks internal communication documents created or edited at a PC. FED-N packages documents when users create them or edit existing documents on desktops or laptops. The FED-N policy can be established by user, group, position or role. The default policy of an author will be applied to a newly encrypted file. The author can change the policy of that document if she has full permission to it. FED-N can easily be deployed after synchronizing with an existing authentication system or without any integration.

Figure 4. General Flow of Data and Components for FED-N



Extended FED Products

Fasoo Smart Print

Fasoo Smart Print (FSP) is a comprehensive print management solution that provides the functionality of both printer-related cost reduction and security. It deters users from leaking important information through printouts by adding a visible watermark to the printout. The watermark contains company name, user ID, IP address, printing time, etc. and helps trace the source of the information in case of a data breach. All printing activities and printed contents are logged to help identify and narrow down the source of the leak. It also enables CPP (cost per page) reduction like toner control and paper usage control. It can allow or block printing jobs based on the predefined permission or content within a document, mask sensitive content and provide pull printing for additional printout security.

Fasoo Smart Screen

Fasoo Smart Screen (FSS) deters users from leaking important information by adding a visible watermark to the monitor screen. This can discourage someone from taking a picture of the screen with a digital camera or smartphone. The screen watermark contains company name, user ID, IP address, time, etc. and helps trace the source of the information. FSS also blocks screen capture tools and print screen functions, and even stop attempts to capture a screen through virtual machines and remote desktops.

Fasoo Enterprise DRM for Mobile

Fasoo Enterprise DRM for Mobile (FED-M) protects documents on smartphones and tablets by extending EDRM functionality to mobile devices. DRM-enabled documents on mobile devices are safe persistently, even if the devices are lost or stolen. This includes adding a screen watermark to deter taking a picture of the screen with a digital camera or the mobile device itself.

Intelligent Real-time Encryption

Real-time Encryption detects content patterns of regular expressions or keywords such as PII, credit card numbers, etc. and secures the relevant documents selectively according to the detected pattern. This includes the ability to prevent document access depending on the policy.

Fasoo Integrated Log Manager

Fasoo Integrated Log Manager (FILM) monitors usage patterns of DRM-enabled documents, detects and alerts risks of possible data breaches based on predefined rules while using FED products. FILM also provides the results in a dashboard and comprehensive statistics of document activities.

Fasoo Data Security Solutions

Fasoo Data Radar

Helps organizations discover unstructured data, classify and protect it using encryption. It enables organizations to:

- Discover sensitive data on endpoint devices and in document repositories
- Classify data based on content patterns defined by regular expressions or keywords
- Protect data using encryption
- Generate reports required for data governance and regulatory compliance

Fasoo Enterprise DRM

FED controls who can access data on what device, when, and in what context to meet an organization's confidentiality requirements. It tracks authorized and unauthorized access to data, send alerts where necessary, and responds to data security triggers to prevent a possible data breach. It enables organizations to:

- Provide persistent data security throughout its entire lifecycle
- Enable cross-platform and multi-device support with extensive application coverage
- Restrict unauthorized copy and paste attempts of protected content
- Prevent unauthorized screen capture attempts while protected documents are in use
- Enforce the policy of protected documents on its derivative files
- Limit file access using validity time/period or device ID
- Revoke access to protected documents when required
- Leverage existing repository ACLs by integrating with backend systems
- Enforce policy when data is being created on PCs
- Authenticate unmanaged external users efficiently using email validation
- Provide innovative methodologies for security policy optimization

Fasoo RiskView

Allows an organization to visualize risks by correlating logs of authorized data usage and with other user activity. It enables organizations to:

- Correlate logs of FED, Fasoo Data Radar and other various systems
- Analyze statistics of retention and usage of sensitive data
- Define a risk index based on multiple data breach related scenarios
- Visualize a risk index of users and groups
- Help business managers determine level of intervention for risk management

Summary

Fasoo EDRM enables an organization to protect documents persistently on any device at any time throughout the entire document lifecycle. It can protect numerous document formats, including ordinary office documents, graphics and engineering drawings. Fasoo is not limited to the Windows PC platform as it is available on macOS, Android and iOS systems. A browser accessible trusted viewer is available to enable an authorized user to access documents from any device. For each document, EDRM can control detailed permissions such as view, edit, print, print watermark, screen watermark and screen capture. Further constraints can be imposed, such as number of devices, valid access period and number of views.

Organizations have deployed many systems to share documents internally. Documents are no longer controlled and vulnerable to loss once downloaded or checked out from application systems such ECM, ERP, PLM and many others. EDRM easily integrates into existing internal systems and meets the numerous security requirements of different phases of the document lifecycle. It is also equipped with the patented email-based authentication technology to protect documents shared externally with partners or customers. Documents created and used on a PC can be secured by EDRM before they are shared internally or externally. Printouts and screens can be overlaid with watermarks to help trace the source of a breach. This alerts users to data sensitivity and makes them more cautious about handling their printouts and taking pictures of their screens.

By adding context-aware protection, Fasoo has taken EDRM to another level. It makes EDRM smarter and easier to use. It can set security policy automatically according to the content of a document. The policy can be adjusted without user intervention based on access time, device location and document usage history. This context-aware protection makes EDRM more secure without impacting usability and lessens the burden of the EDRM administrator significantly.

EDRM can alert administrators to irregular or unusual user activities by collecting and analyzing log data intelligently in real time. It has become a core security infrastructure of organizations and is the best solution to protect data from insider threats and APTs.