

Fasoo Enterprise DRM

Enterprise Digital Rights Management

WHITEPAPER

Fasoo, Inc. | 6707 Democracy Blvd. Bethesda, MD 20817
Tel : (732) 955-2333 | Email : inquiry@fasoo.com

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

FASOO

Table of Contents

Executive Summary 3

1. The Challenge: How to Protect Unstructured Data? 4

2. The Fasoo Approach to Enterprise DRM 8

3. Fasoo Enterprise DRM Architecture 9

4. Policy Management 12

5. Tamper Resistance 15

6. Usage Log and Audit Trail 17

Conclusion 18

Executive Summary

Two major factors drive the powerful market resurgence of Enterprise Digital Rights Management (Enterprise DRM) we are witnessing today. First, data loss prevention (DLP) solutions have failed to stem the tide of insider threats and external breaches. And second, modern digital architectures eliminate the historic workflow frictions often inherent in traditional Enterprise DRM solutions.

Fasoo's advanced Enterprise DRM solution architecture enables the modern enterprise to implement centralized security and compliance policies for their sensitive data consistently and transparently across all networks, file-shares, devices, endpoints, and cloud services. Industry analysts and organizations alike recognize Fasoo's solution as the most robust approach to protecting access to sensitive content available in the market today. Its core strengths have been accentuated by the risks associated with the recent shift to remote work:

- Leading analysts point out that even extensive DLP coverage leaves “gaps in data flows where data can leak” and emphasize: “The better answer is a strategy focused on securing the data itself.” Securing and controlling the file itself while maintaining full visibility into how and by whom it is accessed is the only persistent approach to protecting sensitive data.
- Encryption is entering a “Golden Age”. Due to the growing concerns of data theft, privacy and government surveillance, security professionals are increasingly using all forms of encryption throughout their digital businesses.
- “Identity” is the new perimeter in a world of distributed Software as a Service (SaaS) and other cloud-based services. Centralized administration and maintaining control of access to data has become too critical to leave it to external service providers.

This white paper examines the challenges of document protection at scale in the era of remote access. It explains how automated individual access control, encryption, and rights management are combined to enhance security, governance, compliance, and productivity within the enterprise.

Find out on the following pages why Fasoo Enterprise DRM is the first choice of leading organizations looking to protect the entire document lifecycle of sensitive business information

1

The Challenge: How to Protect Unstructured Data?

The protection of unstructured data poses a major challenge for data security leaders in the enterprise. How can they secure their valuable Intellectual Property (IP), Personally Identifiable Information (PII), and other sensitive data with encryption and apply persistent security policies so that only authorized users can access them?

Organizations have lost track of how their unstructured data is shared, by whom, and with whom. Three developments are leaving unstructured data increasingly exposed to IP theft and other internal and external threats.

- The shift to remote work has put additional pressure on information security teams. Unmanaged devices on work-from-home networks are used to store, process, and share sensitive data.
- The adoption of multi-cloud environments is rapidly progressing.
- File-sharing internally and with third parties has become standard business practice.

These trends have created myriads of data protection blind spots along the supply chain. Large enterprises often collaborate with more than 20,000 third parties and partners. This collaboration amplifies the risk. Once information leaves the organization's environment, all visibility into and control over it is lost.

The shift to remote work, in particular, has exacerbated the challenges information security leaders and their teams face. Organizations become dependent on their partners' security controls and infrastructure, which in many cases may be insufficient to protect the information.

Remote Work and Outsourcing Put Core Digital Assets at Risk

Exposure of sensitive data due to missing or misconfigured VPN connections is common in remote work settings. Users frequently disconnect from their VPN for better system performance. The use of at-home personal printers adds to the risk, because the employer's or business partner's sensitive information isn't redacted, and there are no watermarks to identify the company or user. The organization has zero visibility into what is printed and who can view the material, which can lead to unintended information leaks and create another opportunity for IP theft.

Outsourcing is another example where sensitive information requires additional protection. Automotive manufacturers, for instance, rely on specialized external suppliers to manufacture critical components. Yet some automotive companies still send the necessary specification documents and CAD files to their outsourcing partners without the benefit of assigned access rights or security controls beyond encryption. This lack of protection increases the risk for IP theft along the supply chain.

The Challenge of Persistent Policy Enforcement

How can organizations enforce policy persistently at rest, in use, and in transit? When the document is used, it requires constraining the functions of rendering applications.

For example, if a user does not have permission to print a Microsoft Word document, the print function of Word must be disabled. Due to the wide variety of document formats and rendering applications, many enterprise DRM vendors struggle to keep up with application and document format updates.

A partial list includes Microsoft Office, Adobe Reader, CAD, GIS, graphics applications, and software development tools. Three different approaches can be taken to enforce policy at the endpoint (Table 1):

- **Embedding:** This approach requires source code modification or a rewrite of the whole rendering application. Rewriting all the relevant rendering applications in the enterprise to accommodate a DRM solution is not practical.
- **Plug-in:** Some rendering applications provide interfaces for third-party plug-ins. With others, such interfaces are missing or insufficient to support enterprise DRM functions fully. Another serious problem with the plug-in method is that it is not robust enough. Determined users may easily disable the plug-in.

- **Runtime overriding:** This approach 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 enables complete control over the features and functions of the applications and minimizes the risks from cracking attempts.

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

Historically, the challenges associated with persistent policy enforcement account for the reputation of many enterprise DRM solutions being complex to deploy. The implication was that they would impact existing workflows, result in productivity loss, impact interaction with stakeholders outside the company, and create additional burdens for the IT team.

This perception has changed over the past years, industry observers agree. According to Gartner analysts, enterprise DRM now “is one of the only mechanisms for retaining control of unstructured data transferred to business partners in secure collaboration scenarios.”

One vendor credited with driving much of this trend is Fasoo. Fasoo’s technology approach overrides an application’s memory space and provides strong document protection. It integrates smoothly with the end user experience for third-party applications where the Enterprise DRM vendor does not have access to the program code.

The unique characteristics of its technology make Enterprise DRM broadly applicable to a wide variety of applications and file formats. It provides strong security and interoperability with major network security and digital asset management components, thus protecting existing investments and reducing IT workload.

Fasoo's ability to scale across large enterprises, which are often a patchwork of identity management and client application systems, makes it stand out as the enterprise DRM solution of choice for large, globally distributed companies. Its flagship installation, for example, spans over 170,000 internal users and over 700,000 total users of affiliates and partners worldwide.

Experience with installations at this scale is rare among vendors in this segment. Historically, enterprises in major markets deployed DRM on a need-driven basis, for a given department or a specific set of users. Today, many organizations are seeking to deploy enterprise-wide DRM for all employees.

The technology has proved its mettle in securing documents against internal and external threats increased by remote work, cloud adoption and file-sharing. How can organizations build a comprehensive policy model for documents traveling all over the world?

Policy Management Model Considerations

To manage corporate information effectively, many have deployed Enterprise Content Management (ECM), Enterprise Resource Planning (ERP), Product Lifecycle Management (PLM), knowledge management, file servers, and other file sharing services. Documents stored in these systems would be the first targets for an enterprise DRM solution 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. Users also create documents at the desktop and have uploaded them to the repository yet. These unregistered documents need to be protected with Enterprise DRM as well. Enterprise DRM solutions can be differentiated by how their respective policy management model meets the security requirements of documents throughout their lifecycle. It will determine the effective reach of the security policy.

Conflicts and Lack of Interoperability

A single document can travel through many enterprise applications and be converted into different formats during its lifecycle. What would happen if an Enterprise DRM 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 enterprise-wide document protection solution only works with one ECM system, but not with other business application systems? This shortcoming 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 DRM solutions from different vendors in one organization. Attempting it frequently causes unwanted conflicts and is impossible to make interoperable.

The resulting productivity losses and budget overruns can be avoided with a neutral Enterprise DRM solution that works with any enterprise application system.

2

The Fasoo Approach to Enterprise DRM

Advanced information protection in the enterprise demands a data security solution built on a data-centric security model with people-centric policies. Fasoo Enterprise DRM has proven its effectiveness and scalability to meet this demand through numerous large-scale, enterprise-wide deployments. It protects, controls and traces an organization's unstructured data in an ever-changing enterprise IT environment and supports a wide variety of rendering applications, such as Microsoft Office, Adobe Reader, image editors, and numerous CAD applications.

Why Organizations Move to the Data-centric Security Model

Rather than relying on controlling access to networks and systems, more organizations move to apply security policies to data itself. This approach requires a security policy not only for data at rest or in transit, but also in use. Fasoo Enterprise DRM enables organizations to implement effective file-level security policies and granular permission control for all types of data. This capability ensures document protection throughout a file's lifecycle and no matter where it actually resides.

People-centric Policy Protects Productivity

Data security policies that slow down workflows and don't let users perform business operations on multiple devices without interruption are known to result in productivity losses. They also introduce new risks when users compensate with "creative" workarounds.

A people-centric security policy on data helps maintain the sensitive balance between security and productivity. One key characteristic of such a policy is that it can be flexible and dynamically enforced based on rich context including content, user, device, time, location, etc.

Fast and friction-less exception management is another essential element, because it prevents delays, keeps time-to-resolution at a minimum, and frees up valuable IT resources for more critical tasks. Fasoo Enterprise DRM supports dynamic binding of policy with rich context and allows exception on-demand or through approval.



3

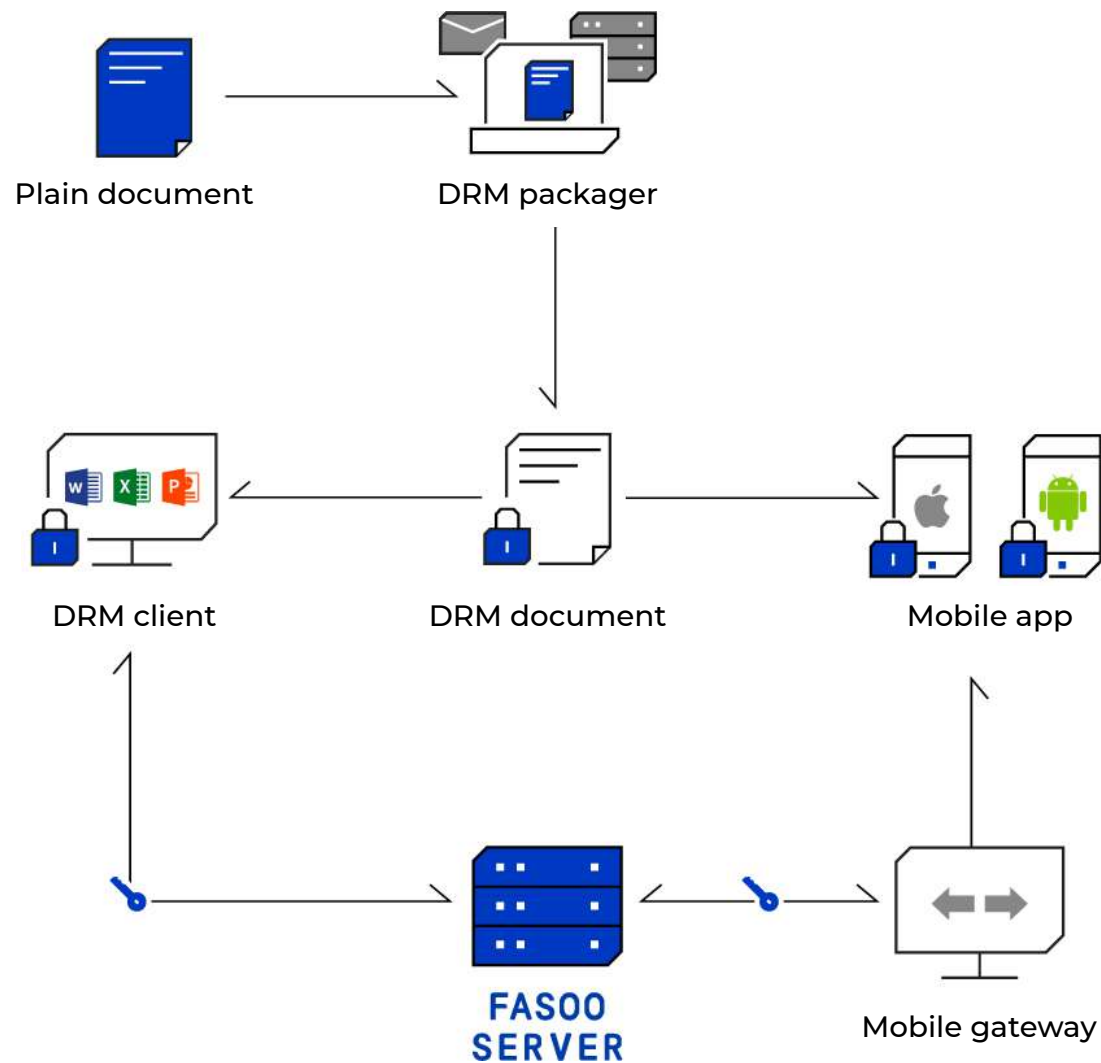
Fasoo Enterprise DRM Architecture

Fasoo Enterprise DRM 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 predefined 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 the United States National Institute of Standards and Technology (NIST). This cryptography mechanism is the basis of Fasoo Enterprise DRM products and extends to accommodate different requirements.

Figure 1. Fasoo Architecture



Application Support

The DRM Client in a Windows environment supports most common native applications, rather than third-party viewers or editors. 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.

Integration

Packaging and authentication should be integrated into existing enterprise application systems when implementing Enterprise DRM. A Packager should be integrated into the document flow for convenience and security. 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. Several prebuilt Packagers exist for common ECM platforms.

Authentication

Fasoo Enterprise DRM 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, and to use SAML-based authentication. For ad-hoc external users, a proprietary authentication, Fasoo Email Based Authentication (FEBA), is built into the relevant Fasoo Enterprise DRM 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.



4

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.
	No_Print/Print_Watermark/Print	Allows “print”, “print only with watermark” or prevents “print”.
	No_Screen_Capture/Screen_Capture	Allows or prevents “screen capture”.
DRM-disabled	Un-package	Allows everything without any restriction, even retrieval of a plain document.

The licensing policy can grant offline access for business travelers and remote workers, restrict view count for highly sensitive documents, and limit devices used only for specific users.

Blocking Screen Capture

Fasoo Enterprise DRM 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 is one of the standard permissions to a document, so a policy can allow it for specific documents or users. Fasoo Enterprise DRM 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. 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 illegitimate remote access. Fasoo Enterprise DRM makes it possible for users to take advantage of SBC with full DRM capabilities.

Deter Theft through Watermarks

Once a document is printed, the printout can get into the wrong hands, and it cannot be protected by software. Fasoo Enterprise DRM deters users from leaking important information through printouts by adding a visible watermark on each page that includes text or images of identifying information, such as company, division, title, user name, IP address, and the time a user printed the document. 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. Watermark print is a standard permission on any DRM-enabled document 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.

Fasoo Enterprise DRM also provides screen watermarks to trace documents captured with a camera or phone on monitors or mobile screens. It discourages users from leaking important information since the screen watermark contains the company name, user ID, IP address, time, and other information to help trace the source of the information.

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.

Policy Exception Setting

Fasoo Enterprise DRM allows exceptions on-demand or through approval. Users can request a one-time elevation in permissions to a specific document or class of documents to enable them to do their job. Exceptions can be requested and granted to exempt printing watermarks, applying screen watermarks, and even having extended offline access to documents. Approval authority can be distributed to department heads, allowing those closest to business operations to make decisions. These capabilities provide 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 (encrypting). 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. Policy for any DRM-enabled document can be changed or revoked at any time, regardless of its location or how many copies exist. Additional policy settings allow for using a document even without connection to the DRM Server, which is useful when users travel where a network is not available or when work-at-home connections may not be robust.

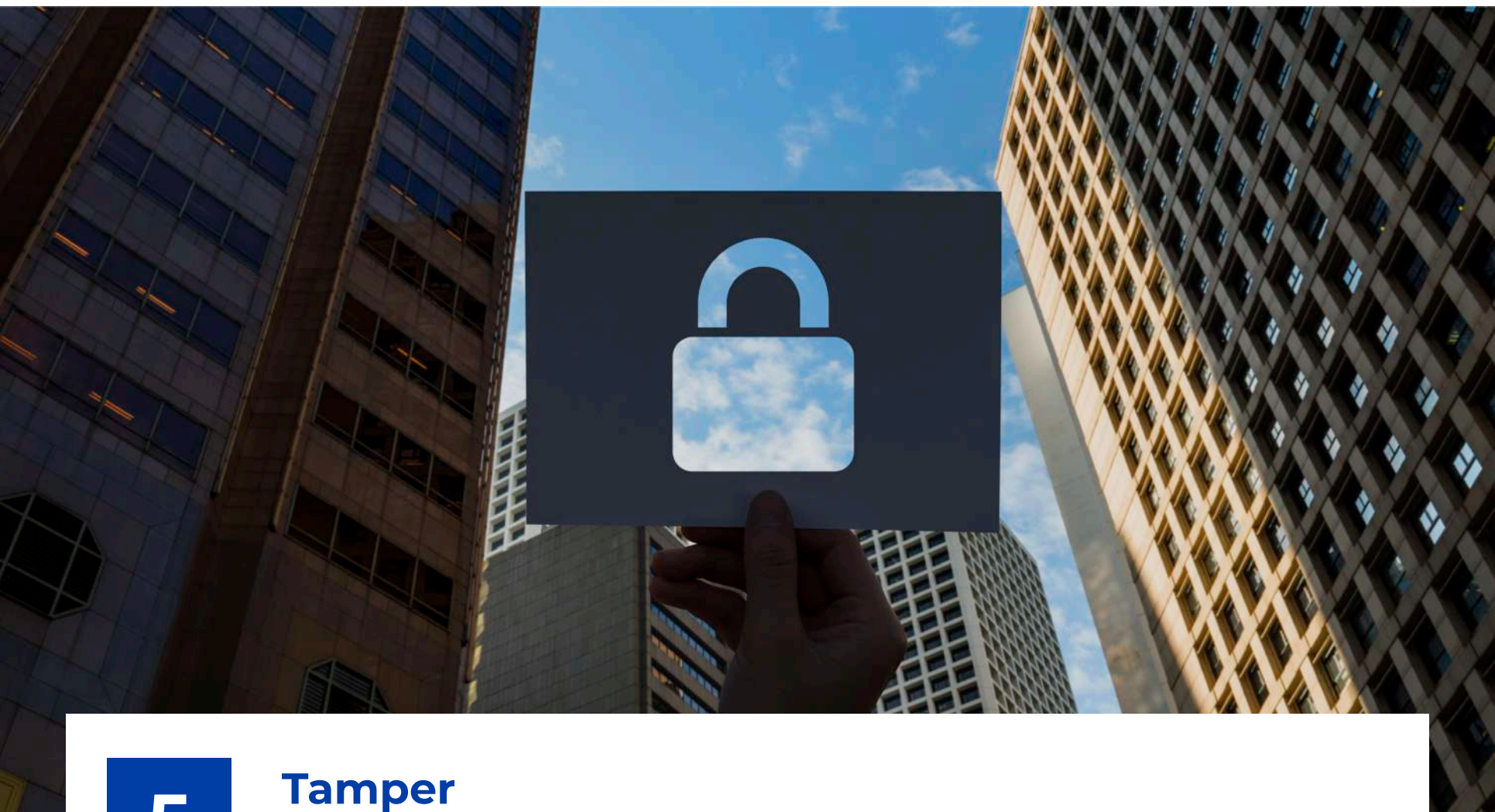
Intelligent Policy Management: Context-Aware Protection (CAP)

Depending on the content of a document, selective packaging (encrypting) 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. With Fasoo's CAP, the Packager runs only if the target document contains a certain content pattern, such as a social security or credit card number. For example, if a document includes 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 predefined policy can be applied to automatically encrypt the file 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.

Fasoo supports DLP integration for customers who want to deploy both technologies. The context-aware capabilities sense the content of documents while in use, and protects them throughout the entire document lifecycle.

Mobile Support

Fasoo Enterprise DRM extends access to protected documents on smartphones and tablets, including editing with proper permission. DRM-enabled documents on mobile devices are safe persistently, even if the devices are lost or stolen. A screen watermark can be added to deter taking a picture of the screen with a digital camera or the mobile device itself.

**5**

Tamper Resistance

Fasoo Enterprise DRM 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 or other insecure environments, such as email or a messaging application.

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 Enterprise DRM 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 Enterprise DRM encrypts all exported files, which inherit the policy of source documents.

Trusted Clock

Fasoo Enterprise DRM 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.

6

Usage Log and Audit Trail

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.

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. Exceptions to logging can be enforced through policy to accommodate workplace and privacy requirements stipulating user activities are not logged.

Fasoo Enterprise DRM offers suitable tools for a document owner or administrator to review and audit activities of users and documents. This includes document tracking so that a document owner can easily see all derivatives of a document and how those derivatives travel. Every policy change on the server is also logged so that security breaches by arbitrary changes of policy can be identified.

Enhanced monitoring enables administrators to detect usage patterns of DRM-enabled documents and alerts IT to risks of possible data breaches, based on predefined rules. Results are viewable in a dashboard with comprehensive statistics of document activities.

This shows detailed user and file activities involving sensitive documents and serves to strengthen an organization's overall security posture.

As organizations use Fasoo Enterprise DRM, they may need to adjust and optimize existing security policies by analyzing variations of exception ratios among groups.

If a department is constantly requesting an exception to print specific documents, for example, the organization may want to make that permission permanent. Monitoring capabilities show administrators these exceptions to enable adjusting policies as needed to accommodate the changing needs of the business.

Conclusion

The shift to the cloud and remote work in the enterprise has put sensitive unstructured data at risk in new ways that traditional perimeter and endpoint security solutions cannot match. This development drives the adoption of data-centric security solutions. More organizations now deploy data-centric document protection to mitigate internal and external risks, such as IP theft.

Fasoo Enterprise DRM enables organizations to protect documents persistently on any device, at any time, throughout the entire document lifecycle. It is scalable to meet the needs of large, global enterprises, and it is agnostic to digital asset management, server software and Data Loss Prevention (DLP) systems. It interoperates with all market-leading applications and platforms and protects a wide range of document formats, from office documents to image files to CAD drawings.

Fasoo is available on Windows, macOS, Android and iOS systems. Fasoo Enterprise DRM easily integrates into existing ECM, ERP, PLM, and other information systems, and meets the numerous security requirements of different phases of the document lifecycle. Context-aware protection capabilities increase security and significantly reduce the burden on IT and document owners.

Fasoo Enterprise DRM plays a crucial role as an early warning system that alerts administrators to irregular or unusual user activities. It has become a core security infrastructure that global organizations rely on to maintain the confidentiality of intellectual property and other sensitive business information. This secures a company's strategic business advantage, protects its intrinsic value, and ensures regulatory compliance.

Fasoo's technology leadership is rooted in its deep understanding of customer requirements and future trends. Its Enterprise DRM technologies combine data-centric document protection with people-centric policy management and oversight in close alignment with existing enterprise infrastructure, information security, and regulatory compliance needs.

What kind of documents is your team looking to protect? Contact us now to learn how your industry leverages Fasoo Enterprise DRM to protect sensitive data:

Email: inquiry@fasoo.com | Web: www.fasoo.com