

# White Paper on Document Security: **HEXAGONAL SECURITY**

---

Enadoc Hexagonal Security provides additional innovative features to Traditional Triangular Security when it comes to keeping company information secure from external and internal threats.



## A. Introduction

With the advent of emerging technologies that make it easy for modern day tech users to snap and share in an instant, the need to implement document security measures for your organization's files has never been more pressing. Companies are constantly finding ways to ensure that files which are the product of their research, team work, and hard work are not put to waste through internal leaks and security breaches. As a company that gives prime focus on document management solutions, we make sure that the documents you work so hard to keep organized are also safe from prying eyes- whether in real life or virtually. This is why Enadoc prides itself in its document security measures, called Hexagonal Security, a set of features that differentiate our product from other enterprise-level document management software.

This white paper serves as an explanation to how security is applied to files within traditional document management systems, common security concerns faced with evolving technologies, and most importantly, how Enadoc Hexagonal Security addresses these concerns.

## B. Passive and Active Security

Generally, security for IT systems is implemented using two techniques, Passive Security and Active Security.

### PASSIVE SECURITY

The goal of implementing passive security measures is to prevent unauthorized access to information. In document management, this is done through systems encryption. Encryption allows system admins to protect documents regardless of where those are stored. Anyone who tries to open or read the files require decryption. Encryption is most used to protect against external threats such as hacking, where outside sources will try to sniff around or steal information by getting access to files.

### ACTIVE SECURITY

On the other hand, active security is implemented to assign the level of access that certain users have to certain files. In document management, this is done by assigning user names & passwords and implementing role-based security. Assigning user names, passwords, and role-based security give access to authorized users, but with varying access levels. In this case, encryption (as discussed in Passive Security) will have no impact on internal authorized users as the decryption process is part of a solution internal users might not even be aware of. While this simplifies the user experience for getting file access, this also signifies that there is no control over internal users who want to leak or steal confidential information.

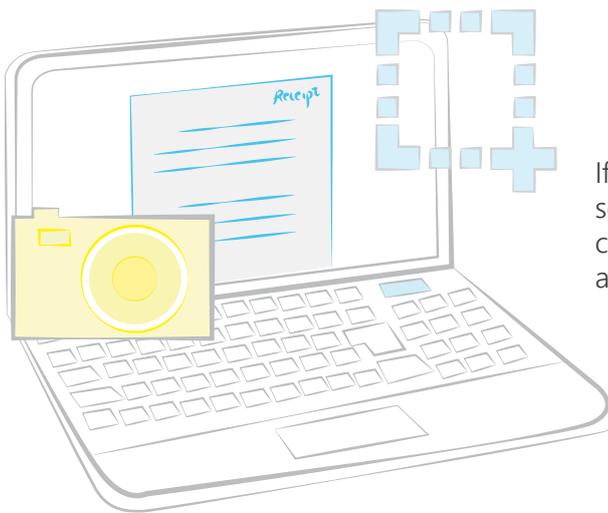
## C. Issues with Traditional Triangular Security

The three techniques discussed above, encryption, assigning user name and passwords, and role-based security is called Traditional Triangular Security. These features are available with most document management solutions.

However, challenges in current IT environments have transformed along with vast changes in technology and new paradigms require innovative thinking and adaptable solutions to manage it.

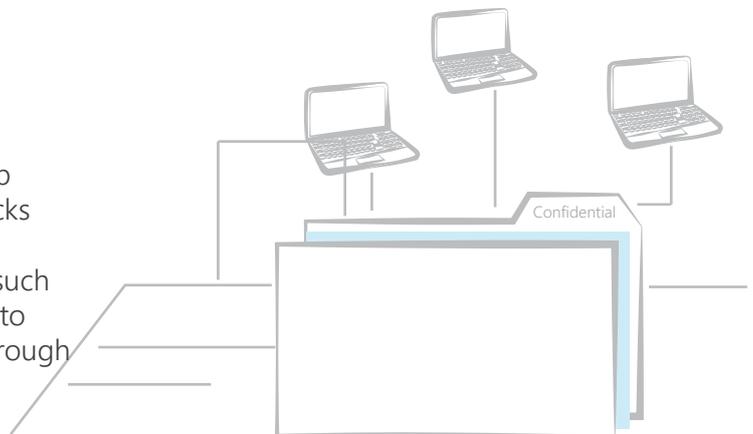


For an example, the following are three issues that seem to become a big challenge to CIOs:



If someone accesses a document on screen, they can take a screen shot or take a photo of the screen with a mobile camera. This is very challenging as all the security measures applied have big flaws once users can do this.

In earlier days, highly confidential documents cannot be found in the drawers of offices of top management, rather, they sit in a room with locks and log books, not ideal for anyone's breakfast reading material. Now, with the digitization of such documents, all users with authority and access to the document can read them without going through any security process.



Imagine super confidential documents- such as confidential business plans of new products, or for banks, individual statements of accounts- to be everyday reading for your system admins. Certainly, top management would not want unauthorized access to such confidential information.



A third issue is filtering what information gets passed down from the same document, to people in different roles. Imagine a situation where company HR has to review the contract of their CEO/MD and the document is sent to legal for review, which again will be reviewed by some junior lawyer who will be exposed with information which may be not for his/her eyes. Managing this requires dynamically removed information such as salary details, bonuses, etc. In paper form, this was achieved by blackening out certain info. However, digitally, there seems to be no effective solution. According to a Gartner report, 16.9 percent of the time, information leaks happen within a company. These are some main issues Enadoc aims to address with its security measures.

## D. Enadoc introduces Hexagonal Security

Enadoc Security brings three additional methods to the traditional triangular security systems, making it more secure than others. Technically, we call this Hexagonal Security.

### THE THREE NEW TECHNIQUES

#### DYNAMIC WATERMARKING

This is an interesting feature that displays current users, login info, and some other information on the displayed image, discouraging current users to screen capture or mobile capture from the computer screen.

#### DYNAMIC REDACTION

Under the same category as dynamic watermarking, this is a technique that dynamically blacks out certain portions of documents based on the user security level. The areas that need to be redacted will be marked at the time of uploading documents and differently-marked zones will be marked with different security levels. This will control which zones are to be shown when different users access the same document. The selectable security levels for the zones at the time of upload will be from the current security level of the document to the highest level, L7.

#### DOCUMENT CLASS

This is similar to a passive security methodology that controls the access to actions on documents. This interesting feature will inherit certain controls regardless of system security.

For example, a document may belong to a class called "Cannot Print or Email" which will impose this control over the document, irrespective of the users who access the document. Even a super admin cannot print or email this document, unless the document is re-classified into a different class.

Reclassifying the said document into a different class will require multifactor authentication, which means based on our implementation, we can setup more than two or three users needed to authenticate such a re-classification.

Enadoc also has a notification engine which can be configured to notify a set of different users indicating that such an action is taking place.



## SECURITY LEVELS

In Enadoc, documents can be classified from Security Level 1 to Level 7, as compared to defining user security levels which only go from Level 1 to Level 6.

With the addition of Level 7 to document security levels, users will not be able to access the Level 7 documents unless they go through an authentication process. Specific users with a Level 6 security level with the feature "Can list the above level documents" enabled can list Level 7 documents but will not be able to open them.

In effect, users who want to access such documents will have to request a declassification of the document. The process of declassification will require multifactor authentication.

As earlier mentioned, multifactor authentication requires two or three users to authenticate a request for declassification. The notification engine can be configured to notify a set of different users indicating that such action is taking place. Enadoc will then be able to preset the documents to get re-classified to the originally assigned security level after a certain period.

A similar message will be sent, such as this:

"Hello notifying committee,

The ABCD Count document has been requested to be declassified to Level 6 by Users Andy, Charlie, and Bravo. The document will be declassified over the next 10 minutes and will remain there for 30 minutes before reclassifying back to Level 7.  
Thank you."

### E. Other security features

Aside from the key security features mentioned above, Enadoc enforces the following security-related measures:

## SECURITY CODES ON DOCUMENTS

When documents are printed or exported, security codes/barcodes can be imprinted on the document for easy tracking/validation by Enadoc should there be a requirement.

## NOTIFICATION ALERTS

Transaction-based email alerts can be system-generated. Rules can be created to send an email alert for the selected person(s) each time when uploading data. Similarly, concerned users are notified when someone tries to access documents from specific document classes.



## DIGITAL AND ELECTRONIC SIGNATURES

Enadoc can integrate digital certificates from external service providers and authorities based on customer requirements.

## ACTIVE DIRECTORY INTEGRATION

Enadoc can integrate with Microsoft Active Directory to enable Single Sign-On and to authorize and authenticate corporate end users.

## SECURITY LOGS

Enadoc maintains logs of all system and end user activities. Administrative roles can access the audit logs through standard reporting interface and system log files.

## COMPLIANCE WITH STANDARD SECURITY FEATURES

Enadoc can be easily implemented in enterprise IT infrastructure with corporate security measurements including firewalls and secure protocols such as SSL and HTTPS.

### **F. Conclusion**

Enadoc Hexagonal Security is designed to meet the challenges faced by organizations when it comes to keeping documents secure. More than the documents, it is the ideas and information contained in these documents which companies try to preserve. The presence of malice in unwanted security leaks is clearly intolerable for every organization. It's time to move to a document management solution that keeps your documents safe and secure. 





## ABOUT ENADOC

### *What is Enadoc?*

Enadoc is an enterprise document imaging system, which provides a variety of document management features including document conversion to digital format, index creation, search, distribution, and workflow management. Enadoc runs on a web browser and has a user-friendly interface, which makes it easy to navigate for the first-time user.

### *How does Enadoc work?*

The software operates on the premise of Capture. Tag. Find. Do.

**Capture.** Scan and digitize physical or paper files.

**Tag.** Assign keywords, called "tags", to your document so you can find them later on.

**Find.** Locate your document using a visually-stimulating, innovative feature, the Tag Cloud.

**Do.** Easily print, download, or share your documents with colleagues, clients, and partners.

### *What makes Enadoc stand out from other document management systems?*

The value of a document management system lies in its ability to retrieve key information in the fastest and best way possible. Enadoc promises a successful file search experience through its key feature, the Tag Cloud. The Tag Cloud is an innovative tool in document management systems that is intuitive and hassle-free, making the search process easy for users.

**To learn more about Enadoc, visit our website: [www.enadoc.com](http://www.enadoc.com)**

---



Enadoc is a U.S.-based document management solution company focused and specialized on electronic document management solutions and document processing services. Our Cloud offerings are hosted with Amazon Web Services, designed to ensure 24/7 availability, high security, disaster recovery capabilities, and protection for your records.

#### **ENADOC LLC**

3 Bethesda Metro Center  
Suite 700  
Bethesda  
Maryland 20814

M: +1 301 332 8923

