PROTECTING SENSITIVE DATA WITH DIGITAL SECURITY WATERMARKS

How to Secure Your Digital Assets with Automated Security Watermarks: Use Cases and Tools

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Every day documents used for information exchange and collaboration have become a problematic source of damaging insider data leaks and breaches. The US National Guard, Facebook and WikiLeaks are prime examples of the serious damage insiders who perpetrate leaks can cause. Even with the best security tools in place, determined users always seem to find a way to circumvent security or accidentally share data with the wrong audience. This can lead to serious security incidents, resulting in financial losses, fines and damage to reputation.

Protecting intellectual property (IP) and trade secrets is paramount to any company's livelihood and competitive advantage. The defence supply chain has an added burden of protecting sensitive information that directly impacts national security and military secrets. This information must be handled and protected in accordance with a multitude of regulations to compete for and maintain Defense contracts.

However, it's not always feasible to keep IP and sensitive business-critical information solely within the company and its employees. Sharing sensitive information internally and with third parties is often necessary in the ordinary course of business. For example, previews of new products need to be shared with retailers and distribution partners. Defense manufacturing and shipping require collaboration with multiple vendors.

Digital security watermarks offer a simple yet powerful solution to mitigate the risks of data leakage caused by sharing IP and sensitive information. By clearly indicating a document's sensitivity, handler and intended audience, they act as a powerful deterrent, remind users of safeguarding requirements, and can prevent inadvertent sharing mishaps. In the event of a data leak, user-specific watermarks can prove invaluable in tracking the source and expediting remediation efforts.

This white paper delves into the advantages of using dynamic watermarks and how NC Protect facilitates the automatic watermarking of various file types, including Office documents (Word, PowerPoint and Office), PDFs, CAD files and more to provide additional security and control over your sensitive information.

SHARING SENSITIVE INFORMATION AND IP CAN BE RISKY

Frequently, manufacturers create and share IP such as product designs, schematics and sensitive images, with third parties as part of the supply chain process. These materials can include presentations, documents, and images that contain unreleased or proprietary designs, artwork or products. Leaked IP can significantly impact the manufacturer and their supply chain partner's marketing strategy, sales and competitive advantage.

Unfortunately, theft of intellectual property and sensitive often goes unnoticed until it is brought to the open market or used by a competitor. The problem is expansive and high stakes, with intellectual property theft costing the U.S. economy up to $600 billion annually.[1]

Top 3 Sources of IP Leaks

The age of digital transformation has made it easier for sensitive data and intellectual property to be leaked or breached. Below are the three most common sources of data leaks.

Insider threats: Intentional or accidental leaks originating from employees or contractors working on a project are called 'insider threats.' In the manufacturing industry, supply chain partners are also potential sources of leaks. Insider-perpetrated leaks can arise from simple negligence or mistakes or malicious intent motivated by financial gain, personal agenda, or a desire for notoriety. For example, a Dupont research chemist pled guilty in 2007 of misappropriating the company's intellectual property. He had downloaded 22,000 abstracts and accessed 16,706 documents outside the scope of his job.

Hacking and cyberattacks: Cybercriminals often target company networks or email accounts to access, steal and sometimes release sensitive files. Attacks are often initiated by foreign powers or competitors seeking to steal technology or new product information and reproduce it as their own.

Physical theft: Printed or photographed information can literally walk out the front door and subsequently be leaked online or shared with unauthorized individuals. The National Guard classified data leak in April 2023 is a prime example of both physical theft and an insider threat. It involved a National Guardsman with top-secret security clearance printing and photographing classified national defense information and posting it online for personal notoriety.

PREVENTING SENSITIVE DATA LEAKS WITH SECURITY WATERMARKS

Implementing strict security protocols and controls for employees, contractors and partners is critical to protect IP. These measures are necessary to ensure that information handlers comprehend the sensitivity of the information in their care and any policies that govern it.

One security control is dynamic watermarking technologies that are used to stamp documents with important information about the handler, providing the best possible protection. Displaying the handler's information throughout the document discourages the possibility of photographing and creates a digital thumbprint that can be used to identify the source of any data leak.

[1] https://www.forbes.com/sites/forbesbusinesscouncil/2023/09/25/the-costs-of-ip-theft-and-how-to-protect-your-companys-ideas/?sh=4a31633143f8

What is a digital security watermark?

Watermarks have come a long way from rubber stamping or adding the words ‘confidential’ or ‘draft’ in grayscale across a document via a word processor.

Today’s digital security watermarks embed important data into a document to track its point of origin and its handler using details about the user, time/date of access, machine it was accessed on, etc. They act as a digital thumbprint that travels with the document.

Why should you use security watermarks?

Applying digital security watermarks to sensitive documents can help prevent data loss, misuse and unauthorized sharing in a variety of ways. They can be used to augment data security practices to:

- Provide users with a visual reminder that they are handling sensitive information.
- Supplement user education and training relating to safely handling IP or sensitive information.
- Deter users from stealing documents or taking pictures with their mobile device.
- Track a document’s chain of custody in the event of a leak.
- Provide read-only access by displaying the watermarked document in a secure reader that disables print, copy and sharing capabilities.

What types of documents should you watermark?

Any document containing sensitive data you need to control or restrict access to is a good candidate for watermarking. Common types of data you should consider watermarking include:

- Intellectual property (IP)
- Manufacturing plans
- Product specs and designs
- Images
- Financial documents
- M&A documents
- Human Resources (HR) documents
- Healthcare Information
- Legal contracts
- Personally Identifiable Information (PII)
- Protected Healthcare Information (PHI)
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Export Control Data (e.g., International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR))
- Classified Information
- Information that falls under NATO standardization agreements (e.g., NATO STANAG 4774 and 4778))

PRACTICAL USES FOR DIGITAL SECURITY WATERMARKS

The potential uses for watermarks are endless and can vary according to an organization's individual needs, the type of data it manages, its industry and any associated regulatory requirements. Here are a few applications of digital security watermarks in enterprise and public sector scenarios.

ENTERPRISE USE CASES

- Sharing previews of upcoming products with partners that are not meant for public distribution, such as the release of a new toy or a script.
- Sharing and/or collaboration of IP and trade secrets with internal stakeholders and/or partners.
- Protecting HR documents that contain PII, salary or disciplinary information.
- Protecting documents lying on a printer in a public space.
- Sharing sensitive documents with third parties.
- Protecting images or information posted online.
- Clearly identifying that the information has additional specific handling instructions, such as "PROJECT X STAFF ONLY" or "UNCONTROLLED IF PRINTED."
- Applying relevant information such as the related industry, client, project or any other relevant document details.
- Adding disclaimers. For example, 'Document intended for Client X only, any use outside this purpose is not authorized.'
- Marking the current document status (Working / Draft / Final / Approved / Released) and recent history / current version + timestamp of a document. For example, 'This version is approved for public release by Person X.'
- Tracking the source of a leaked document – whether accidentally or deliberately shared with an unauthorized audience.
- Forensic tracking to identify the source of leaked sensitive information from a screenshot or photo.

GOVERNMENT & DEFENSE USE CASES

In addition to the use cases above, there are many specific use cases for Government, Defense and the Defense supply chain, including, but not limited to:

- Tagging of Freedom of Information Act (FOIA) documents when the data is publicly released.
- Securely sharing tactical information for military units (such as OP Orders, travel documents, etc.).
- Multinational coalition and intelligence sharing.
- Tagging and labeling CUI, FCI, ITAR and EAR-controlled data in accordance with U.S. government marking requirements (see DoD CUI requirements on left).
- Labeling and marking classified information according to individual government and coalition regulations such as the NATO STANAGS.

U.S. DoD CUI MARKING GUIDELINES

Controlled Unclassified Information (CUI) must be categorized and marked accordingly. With NC Protect, watermarks can be used to apply CUI markings and designation indicator labels alert recipients and users that CUI is present and of any limited dissemination controls.

Marking Unclassified CUI

Place "CUI" at the top and bottom of each page (headers/footers).

Portion markings are optional on unclassified documents, but if used, all portions will be marked.

The CUI designation indicator will be placed at the bottom of the first page or cover of all documents containing CUI:

Line 1: The name of the DoD Component (not required if identified in the letterhead)

Line 2: Identification of the office creating the document

Line 3: Identification of the categories contained in the document

Line 4: Applicable distribution statement or limited dissemination control (LDC)

Line 5: Name and phone number or email of POC

Marking Classified CUI

"CUI" does not go into the banner line.

The CUI designation indicator and the classification authority block will be placed at the bottom of the first page.

Portion markings are required on classified documents.

Classified documents will be marked IAW DoDM 5200.01 Volume 2.

CUI markings will appear in portions known to contain only CUI.

A warning statement will be placed at the bottom of the first page of multi-page documents alerting readers to the presence of CUI in a classified DoD document.

AUTOMATE DIGITAL SECURITY WATERMARKS WITH NC PROTECT

Manually applying watermarks is time consuming and prone to human error. For example, if a user forgets the step entirely or misclassifies a document. What if you could automatically ensure documents were watermarked properly?

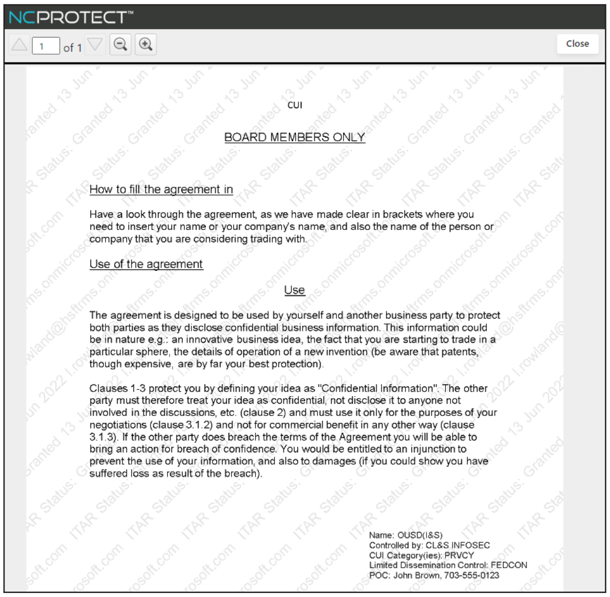
The archTIS NC Protect solution dynamically applies user-specific digital security watermarks to files, including Office documents (Word, PowerPoint and Office), PDFs, CAD files, images and more. It digitally stamps documents in their native application (e.g., Microsoft Word) with any combination of attributes automatically according to simple, configurable rules to meet business requirements.

The watermarks can contain attributes of the user who accessed the file, such as their name, date, and time of access, and other relevant information required to track the chain of custody and alert users of the document's sensitivity. Watermarks are persistent. Therefore, users can share and edit watermarked document contents – but cannot edit or remove the watermark itself. Visual markings for defense data such as headers, footers, and CUI labels can also be applied using NC Protect's watermarking capability (see screenshot on right).

For further protection, watermarked documents can be displayed in the Secure Reader, an in-app viewer that provides read-only access and disables functions such as print, edit, copy and save. It ensures your most sensitive documents can't be changed, downloaded or shared. You can track access to the document via detailed audit logs.

NC Protect's Digital Security Watermarks can be dynamically applied to the following standard file types:

- Microsoft Office documents (.txt, .csv, .doc, .docx, .xls, .xlsx, .ppt, .pptx)
- Images (png, .jpg, .jpeg, .tif, .tiff, .bmp)
- CAD files (dgn, .dwf, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cff2)
- PDF documents


NCPROTECT™
1
of 1
Close
ITAR Status: Granted 13 Jun 2022 l.rowland@hsftrms.onmicrosoft.com

CUI

BOARD MEMBERS ONLY

How to fill the agreement in

Have a look through the agreement, as we have made clear in brackets where you need to insert your name or your company's name, and also the name of the person or company that you are considering trading with.

Use of the agreement

Use

The agreement is designed to be used by yourself and another business party to protect both parties as they disclose confidential business information. This information could be in nature e.g.: an innovative business idea, the fact that you are starting to trade in a particular sphere, the details of operation of a new invention (be aware that patents, though expensive, are by far your best protection).

Clauses 1-3 protect you by defining your idea as "Confidential Information". The other party must therefore treat your idea as confidential, not disclose it to anyone not involved in the discussions, etc. (clause 2) and must use it only for the purposes of your negotiations (clause 3.1.2) and not for commercial benefit in any other way (clause 3.1.3). If the other party does breach the terms of the Agreement you will be able to bring an action for breach of confidence. You would be entitled to an injunction to prevent the use of your information, and also to damages (if you could show you have suffered loss as result of the breach).

Name: OUSD(I&S)
Controlled by: CL&S INFOSEC
CUI Category(ies): PRVCY
Limited Dissemination Control: FEDCON
POC: John Brown, 703-555-0123

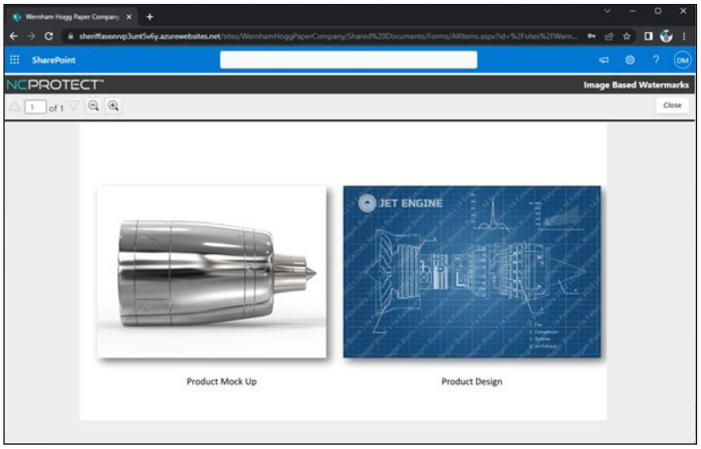
ADDING MULTIPLE WATERMARKS TO A DOCUMENT

While a single watermark is beneficial, adding a separate watermark to a sensitive image within a document or presentation or just the image itself, ensures it is protected in the same way.

In addition to watermarking a document, NC Protect can also individually watermark images and other elements within the document. This multi-watermark approach ensures sensitive or copyrighted images are independently marked as sensitive – automatically.

NC Protect's policies are automatically applied in real time based on the combination of user attributes, document sensitivity and environmental conditions at the time of access. Therefore, security controls and access rights can change depending on the situation. For example, suppose a user is in the office. In that case, they may be able to access the document in the Office application to edit it with the watermark automatically applied. If they are at home, it will be displayed in a secure read-only Reader app, and their information will be displayed as a watermark.

Dynamically watermark sensitive images in a document based on their classification with NC Protect. Force IP and sensitive data to be displayed in the built-in Secure Reader app to prevent users from printing, copying, or downloading files as shown in the screenshot below.


Wernham Hogg Paper Company
sheriffasexvvp3unt5v6y.azurewebsites.net/sites/WernhamHoggPaperCompany/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FWern...
SharePoint
DM
NCPROTECT™
Image Based Watermarks
1
of 1
Close
JET ENGINE
Product Mock Up
Product Design

ADVANTAGES OF NC PROTECT DYNAMIC SECURITY WATERMARKS

Dynamic. When an employee views or downloads a document, NC Protect will automatically watermark the document and/or sensitive images with the employee's name, date, time, client name, and any other data required by your organization.

Documents and Images. NC Protect can add multiple watermarks to a single document, including individual images within a document. Supported file types include Word, PowerPoint, Office, PDFs, CAD files and images.

Digital Thumbprint. Watermarks remind employees and partners of the content's sensitivity and discourage photographing. If someone takes the risk, watermarks provide a clear forensic trail of who, what, and when the leak occurred.

Persistent. Watermarks are applied in the native application (e.g., Word, PowerPoint, Excel). Users can share and edit the contents of watermarked documents, but not the watermark itself, for security and auditing purposes.

Read-only Access. Watermarked documents can be displayed in a built-in Secure Reader app that disables the print, download and copy functions if required.

Customizable. NC Protect's dynamic data-centric policies are flexible, allowing you to create fine-grain security and access rules to suit your business's specific needs.

Defense Visual Markings. Embed CUI Designation Indicator markings, including Owner Name, Controlled By, Category, Distribution/Limited Dissemination Control and POC, as well as headers/footers, manually or using automated policies.

Easy to Deploy. Seamless Integration with Microsoft 365, GCC, GCC High, SharePoint on-premises and File Shares. Simple deployment requires no additional software or agents for end users.

Protecting sensitive information has never been easier, faster, or more dynamic.

NC Protect helps proactively manage and mitigate IP data leakage, which can result in millions of dollars in lost revenue. It enhances data security and provides more secure collaboration in Microsoft 365, GCC, GCC High, SharePoint on-premises and File Shares to help protect your company's IP, brand reputation and bottom line.

Contact us for a demo today.

archTIS

Get the powerful information protection you need today.

CONTACT US

www.archtis.com/contact

Microsoft Partner

Member of Microsoft Intelligent Security Association Microsoft

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, SharePoint Server, NetApp ONTAP, Nutanix Files and Windows file shares.

For more information visit archtis.com. Follow us on twitter @arch_tis.

archTIS

archtis.com | info@archtis.com

Australia | United States | United Kingdom