DYNAMIC DATA LOSS PREVENTION IN SHAREPOINT

Achieving Real-Time, Attribute-based Access Control and Data Security with NC Protect

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

> *“Your role is to help foster safe behaviors, control information access, and verify ongoing compliance — all without hampering creativity, productivity, collaboration, or other daily activities.”*
>
> FORRESTER RESEARCH

This white paper introduces a new model for SharePoint data loss prevention and access control that enables collaboration without compromising security.

It aims to detail why dynamic security and access are a more effective approach for securing SharePoint content. By reading this paper, SharePoint administrators and site owners will gain a better understanding of how they can leverage user and file attributes and context to drive dynamic policy-based SharePoint security.

BALANCING USER ACCESS AND FILE PROTECTION

To protect sensitive information (trade secrets, acquisition plans, financial data, supplier and customer information, regulated information, etc.), many organizations decide to limit SharePoint collaboration and prohibit some users from accessing certain files from certain locations.

Or they decide to encrypt more files at rest because the consequences of a security breach are severe.

Both of these approaches limit collaboration, which causes users to find non-IT sanctioned ways and tools to bypass the applied restrictions.

The SharePoint Security Challenge

SharePoint is an excellent platform for collaboration. The problem is that with so many security and compliance requirements across an organization, it is nearly impossible to keep up with all the demands for file permissions without impacting collaboration flexibility. IT administrators continuously receive requests to modify file and user permissions that are in direct conflict with requests to adhere to compliance policies and security requirements. Complicating data security matters further are requests to:

- Identify where sensitive files reside e.g. which files contain personally
- identifiable information (PII)
- Secure files at rest and in motion
- Manage mixed SharePoint environments and versions
- Support a “Bring Your Own Devices” (BYOD) policy
- Implement cloud-based applications to access sensitive files
- Accommodate remote work and external/guest collaborators
- Adhere to changing global security regulations
- Prevent users from resorting to unsecured “shadow IT systems” to share files

Everyone is looking for an easier way to secure SharePoint without overburdening IT staff or overly restricting end users. It’s a balancing act between ensuring information security while enabling collaboration. And it’s tough when technology limitations often force administrators to decide between:

- Meeting compliance requirements and government regulations
- Maintaining certifications in SharePoint environments
- Employee productivity

SharePoint Data Security Approaches Today

There are two fundamental approaches that organizations use to secure content in SharePoint today: restrict user access and apply file encryption.

1. **Restrict User Access –** User access tools allow administrators to juggle inherited permissions, maintain multiple user groups or create unique silos for specific sharing scenarios. User access can be restricted to completely secure files to the point of rendering collaboration impossible.

Restricting user access also results in several SharePoint administration problems:

- Difficulty to manage and maintain users belonging to hundreds of groups
- Too many permissions requests and the need to handle exceptions
- Users bypass security to work around burdensome restrictions
- Complicated inter-rule interactions can yield unforeseen outcome

2. **Apply File Encryption –** File encryption tools are used to protect sensitive files that must not be mishandled . When user access has been relaxed, organizations can encrypt the files to ensure that the data is safe when it is being used.

When too many files are encrypted at rest, however, usability is often sacrificed:

- Files are not indexed or searchable, so they can be difficult to use
- Files cannot be scanned for content, so they may be inappropriately categorized
- Encryption key management and revocation requests can overload IT and inhibit sharing

User access restrictions and file encryption, combined with complicated permissions and exceptions, make it difficult to have secure and collaborative environments.

What Security Capabilities are Missing in SharePoint?

SharePoint offers some native tools to help, but they are static, leading to other challenges.

- User access permissions are static – they do not change as the user moves between networks, devices, and even countries.
- File encryption templates are static – they are generally applied to all files of a certain classification, regardless of how the content changes over time or how that file is used.
- Identification of sensitive content is limited – while advancements have been made with Microsoft's cloud based offerings, there is still limited out of the box options for identification and classification within SharePoint on-premises.

Static access permissions and file encryption templates do not work in the modern dynamic, 'always on' workplace.

Coupled with a lack of insight into nature of the information within files makes securing content within today's evolving SharePoint environments especially challenging when considering:

- Remote work, BYOD, and unsecured devices
- A large number of users and groups
- Mixed or legacy SharePoint environments (on-premises, cloud, hybrid) with inconsistent security tools
- A complex matrix of overlapping permissions such as security clearances or project teams or external collaborators and guest users
- How the sensitivity level of content changes over time
- Regulations that vary by country or data transmission methods

What is missing is dynamic security.

Dynamic security is an attribute-based approach that evaluates a range of constantly-changing user and file metadata and characteristics in real-time. As user and file attributes change, different security and protection policies are automatically applied that are appropriate for a given scenario at that point in time based on both the user and the file's context. This capability addresses the weaknesses of static user permissions and static file encryption templates that cannot take into account changing collaboration scenarios over time.

A dynamic, attribute-based model provides a much more flexible and fine-grained security approach that is simpler to administer and dramatically reduces the need for exceptions handling.

The key to dynamic security is combining both user and file attributes to create sophisticated policies. If any of these attributes change, appropriate policies respond in real-time.

DYNAMIC DATA LOSS PREVENTION FOR SHAREPOINT

Nucleus Cyber empowers you to leverage dynamic, attributed-based data protection without the complexity to enhance native SharePoint security.

The NC Protect solution provides content identification and classification, dynamic security and information protection. It can be overlaid on top of existing SharePoint environments (on-premises, cloud and hybrid), delivering additional security that is dynamic and automated.

NC Protect is a SharePoint-native solution that dynamically adjusts file security, encryption and rights management based on real-time comparison of user context and file content to make sure that users view, use, and share files according to your industry and business's regulations and policies.

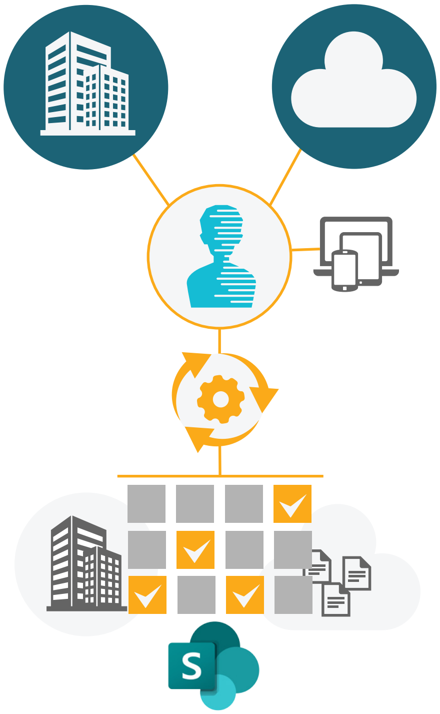
NC Protect's attribute-based policies are evaluated dynamically and in real-time . If user or file attributes change, these security and protection policies are applied to files and users in real-time.

NC Protect secures files at rest and in-motion without the overhead of complex user permissions and encryption, ensuring that the data is protected at the time it is used or shared . It restricts usage and visualization of data based on attributes such as the file's classification metadata and the user's current location, device, and security clearance, automatically encrypting it when the data leaves the safety of the corporate environment.

How NC Protect's Rules Engine Works

NC Protect uses a conditional logic rules engine that leverages user and file attributes to provide security and protection for SharePoint Online, on-premises and hybrid environments, and does not modify the underlying permissions and restrictions in existing environments.

NC Protect determines the access and security that should be applied based on a real-time evaluation of both the user's context and the file's content and properties.



Dynamic security is defined as the ability to apply appropriate security in real-time as users and documents change context Dynamic security is defined as the ability to apply appropriate security in real-time as users and documents change context

WITH NC PROTECT

Security policies are consistent in every environment

- Policies are equally applied to SharePoint data on-premises, online and in hybrid environments

Enhances Microsoft's security features

- Leverages Microsoft information protection and SharePoint security – no extra client apps needed

Zero end-user education

- Native to Microsoft Office 365 and SharePoint servers

Dynamic access accommodates the flexible workforce

- Data and user context combine to automatically apply Microsoft's controls

Zero-footprint secure reader capability empowers remote users

- Ensures the most secure documents never leave the business

POWERFUL, YET SIMPLE

Critically, this dynamic and policy- based approach requires the creation of far fewer rules than is required with static access and encryption rules

ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

NC Protect allows administrators to create a logical expression using a wide variety of properties from both the file and the user (figure 1).

Dynamic User Attributes

User properties or attributes, like department, location, security clearance and device type, as well as other properties can be pulled from any number of sources, AD groups, SharePoint groups, devices, custom properties, or even an external file.

Dynamic File Identity

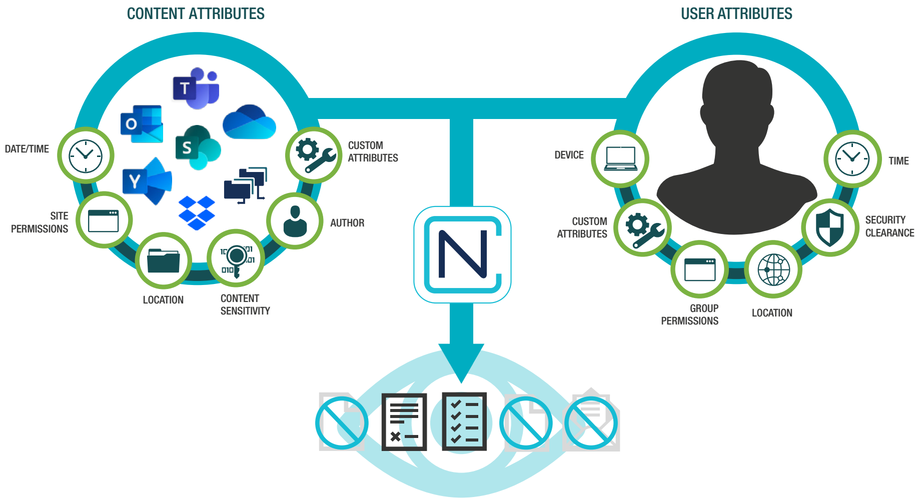
File identity or properties can include the original author, version number, location, projects, custom meta-data, for example, as well as classifications applied by any application, such as Azure Information Protection or NC Protect's built-in identification and classification capabilities.

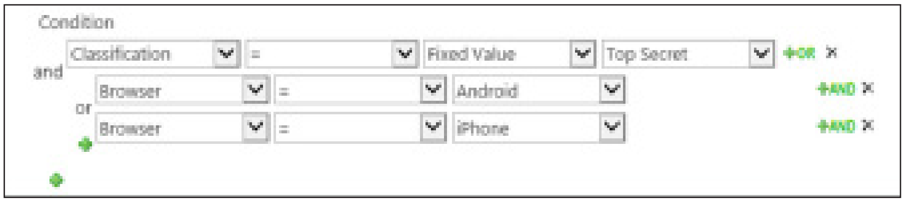
Custom Attributes

Organizations may also have custom user attributes that they want to include. Dynamic security enables organizations to consume these different attributes from many different locations and apply the appropriate policies in real-time.

NC Protect's simple application of dynamic rules provides a fine-grained solution to automatically control what each user can do with individual files and documents. When a user's context changes – for example going from the office to working from home – what the user can do with files automatically changes too.

Additionally, NC Protect's dynamic and attribute-based approach is transparent to the end user, who continues to use Microsoft's applications to access and collaborate upon files . NC Protect augments SharePoint's user interfaces and encryption which is natively integrated in Microsoft Office applications, which means that there is no additional user training, and no additional software installation required on users' devices.





Condition
and
Classification = Fixed Value Top Secret +OR ✕
or
Browser = Android +AND ✕
Browser = iPhone +AND ✕

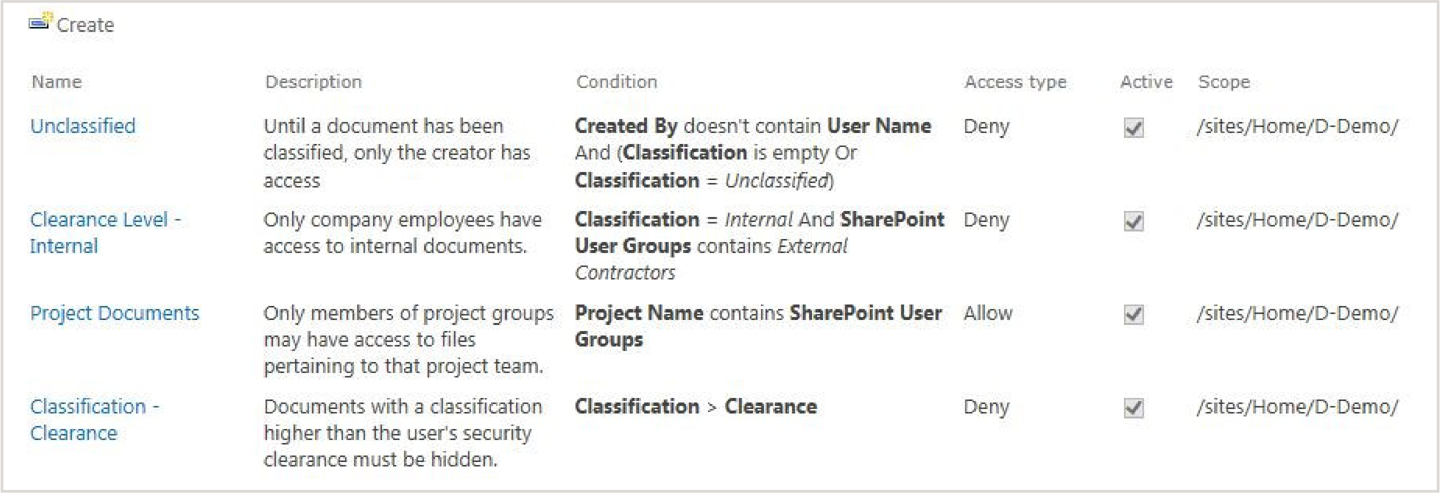
Figure 1: NC Protect's logical expression builder, showing user and file attributes to restrict access to Top Secret files from Android and iOS browsers

NC PROTECT’S DYNAMIC SECURITY RULES IN ACTION

NC Protect’s simple rules augment and automate the tools you already use to secure user access and apply file encryption. These work together to control the files a user can access, what they can do with the file, and how the file is protected when it leaves the secure SharePoint environment. Application of security and protection controls is based on a rule’s logical expression that is composed of user and file properties, which are then evaluated in real-time, whenever a user searches for or attempts to access or use a file.

Dynamic Access Rules

Dynamic Access Rules determine which files a user can discover when searching and viewing SharePoint documents. NC Protect augments the Microsoft user interface displaying the files, ensuring that users can never discover files that should not be used in a particular situation and context (figure 2).



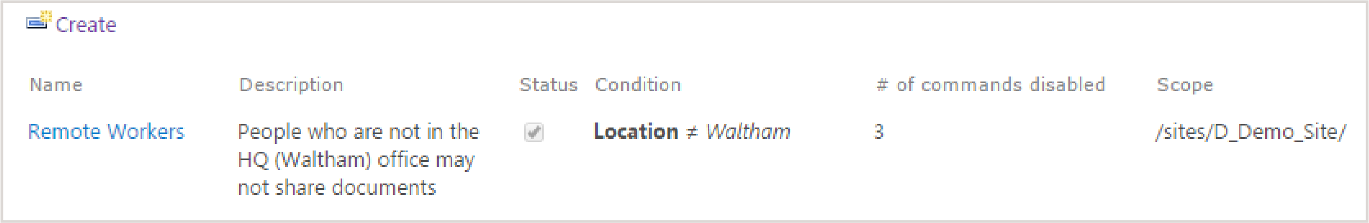
Create

Name	Description	Condition	Access type	Active	Scope
Unclassified	Until a document has been classified, only the creator has access	**Created By** doesn't contain **User Name** And (**Classification** is empty Or **Classification** = *Unclassified*)	Deny	☑	/sites/Home/D-Demo/
Clearance Level - Internal	Only company employees have access to internal documents.	**Classification** = *Internal* And **SharePoint User Groups** contains *External Contractors*	Deny	☑	/sites/Home/D-Demo/
Project Documents	Only members of project groups may have access to files pertaining to that project team.	**Project Name** contains **SharePoint User Groups**	Allow	☑	/sites/Home/D-Demo/
Classification - Clearance	Documents with a classification higher than the user's security clearance must be hidden.	**Classification** > **Clearance**	Deny	☑	/sites/Home/D-Demo/

Figure 2: NC Protect dynamic access rules example screenshot, showing restricted access based on file classification and user security clearance.

Ribbon Rules

Ribbon Rules deactivate individual items on Microsoft’s SharePoint toolbars so that certain actions are prevented in particular situations and context (figure 3).



Create

Name	Description	Status	Condition	# of commands disabled	Scope
Remote Workers	People who are not in the HQ (Waltham) office may not share documents	☑	**Location** ≠ *Waltham*	3	/sites/D_Demo_Site/

Figure 3: NC Protect ribbon rules example screen shot, showing restriction of three SharePoint ribbon rules for remote workers.

Secure Reader Rules

Secure Reader Rules dynamically apply security to files as they are removed from the SharePoint environment in two ways (figure 4):

1. Encryption

NC Protect tailors encryption as files leave the protected SharePoint environment. The encryption determines the usage rights and permissions a user has when opening or copying a file. NC Protect can apply a pre-defined rights management template, or it can specify a custom collection of rights and permissions. Once the file is opened on the user's device, it has been encrypted and usage permissions have been applied. This method of encryption and usage rights allows the file to be used on any device and by any application that is Microsoft encryption enlightened, such as Microsoft Office applications thereby negating the need to install additional software of end user's devices or force them to use an unfamiliar third-party app.

2. Zero-Footprint Secure Reader

NC Protect can prevent a highly sensitive file from ever leaving the protected SharePoint environment while permitting a user to view the content without transmitting the actual file. NC Protect's Secure Reader renders an image of the file that is transmitted with a personalized, custom watermark over a secure web browser connection. The user may look at the file and is reminded of the sensitive nature of the content, but the file cannot be copied or altered in any way.

Beyond these examples, NC Protect also provides the capability to dynamically encrypt files at rest and manipulate SharePoint file-level permissions based on scanned file content.

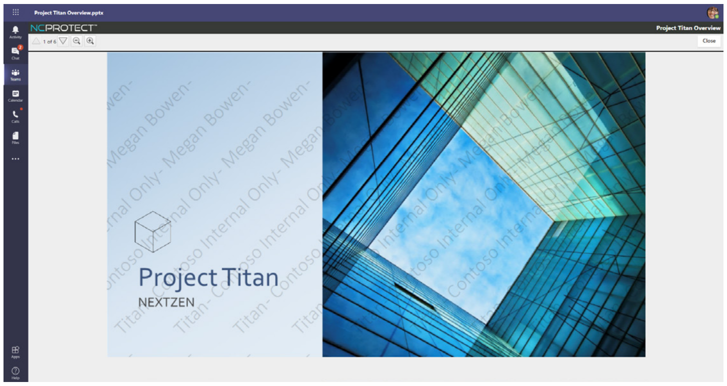
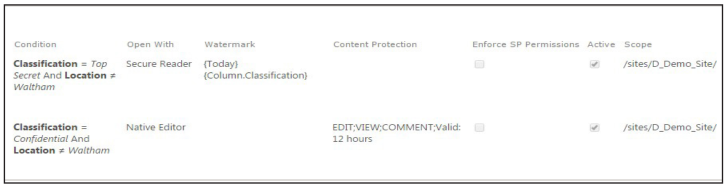


Figure 4: Screen shot of NC Protect Secure Reader, showing a secure, custom watermarked image presented through our secure web viewer.



Condition	Open With	Watermark	Content Protection	Enforce SP Permissions	Active	Scope

Classification = *Top Secret* And **Location** ≠ *Waltham*	Secure Reader	{Today}
		{Column.Classification}
				□	☑	/sites/D_Demo_Site/

Classification = *Confidential* And **Location** ≠ *Waltham*	Native Editor		EDIT;VIEW;COMMENT;Valid: 12 hours	□	☑	/sites/D_Demo_Site/

Figure 5: NC Protect secure document rules example screen shot, showing encryption and Secure Reader rules applied when workers access a file remotely.

CONCLUSION

User access restrictions and file encryption, combined with complicated permissions and exceptions, make it difficult to have secure and collaborative environments in SharePoint. Static access permissions, file encryption templates and a lack of insight into file content do not work in a modern dynamic "always on" workplace.

NC Protect's dynamic security provides unique and powerful capabilities not available from Microsoft that more easily secure on-premises, hybrid and cloud-based SharePoint environments. By examining both user and file attributes to apply appropriate security as users and documents change context in real-time, SharePoint administrators and site owners can ensure file security while enabling modern, "always on, work everywhere" collaboration.

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, Dropbox, 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