WHITE PAPER

Dynamic Security in SharePoint with NC Protect™

Applying user and file context to automate fine-grained SharePoint security

NUCLEUS CYBER

Table of Contents

Introduction

This white paper proposes a new model for SharePoint security that enables collaboration without compromising security. This document will show why dynamic security is so important to secure SharePoint. By reading this paper, SharePoint administrators will gain a better understanding of how they can apply user and file context to drive dynamic policy-based SharePoint security.

The Security Challenge

SharePoint is an excellent platform to leverage for collaboration. The problem is that with so many security 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 file security matters further are requests to:

- Secure files at rest and in motion
- Manage mixed SharePoint environments and versions
- Roll-out a "Bring Your Own Devices" (BYOD) policy
- Implement cloud-based applications to access sensitive files
- Accommodate mobile users and external 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 security while enabling collaboration. And it's tough to decide which is more important:

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

"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

BALANCING USER ACCESS AND FILE PROTECTION

Many organizations decide to limit collaboration and prohibit some users from accessing some 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 creative ways to bypass the applied restrictions.

SharePoint 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
   - 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 is Missing in SharePoint?

Microsoft offers quite a few tools to help, but they are **static**.

- 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.

Static access permissions and file encryption templates do not work in the modern dynamic, 'always on' workplace and with today's evolving SharePoint environments especially when considering:

- User mobility, BYOD, and unsecured devices
- A large number of users and groups
- Mixed or legacy SharePoint environments with inconsistent security tools
- A complex matrix of overlapping permissions such as security clearances or project teams
- Regulations that vary by country or data transmission methods

What's missing is dynamic security.

Dynamic security is a policy-based approach that evaluates a range of constantly-changing attributes in real-time about users and files. As user and file contexts change, different policies are automatically applied that are appropriate for both the user and the file's context. This capability addresses the weaknesses of static user permissions and static file encryption templates.

This dynamic and policy-based model provides a much more 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.

WITH NC PROTECT:

Security policies are consistent in every environment

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

NC Protect automates Microsoft's features

- Leverages Microsoft RMS 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

Dynamic Security and Data Loss Prevention for SharePoint

Nucleus Cyber's NC Protect software provides dynamic security. It can be overlaid on top of existing SharePoint environments, delivering additional security that is dynamic and automated.

NC Protect is a SharePoint-native solution that dynamically adjusts file security 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 simple policies are evaluated dynamically and in real-time. If user or file attributes change, these security policies are applied to files and users in real-time.

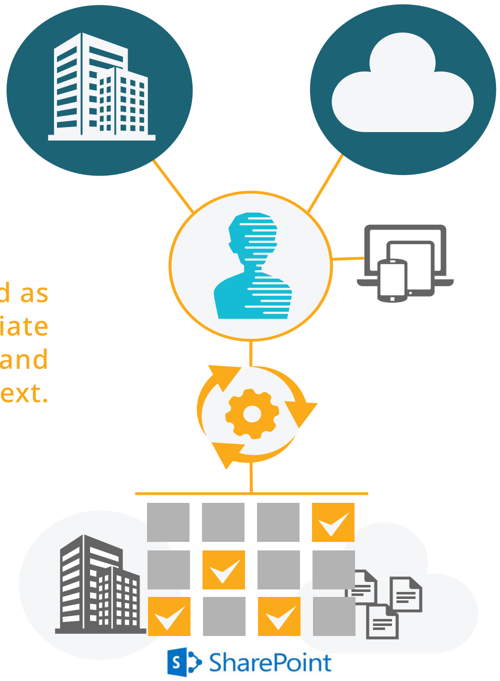
NC Protect secures files at rest without the overhead of complex user permissions and encryption, ensuring that the data is protected at the time it is used or shared. It restricts usage and visualization of data based on the file's classification and the user's current location, device, and security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

How NC Protect's Rules Engine Works

NC Protect uses a logical expression-based rules engine that works with all SharePoint versions, 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 properties.

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



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.

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 Properties

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

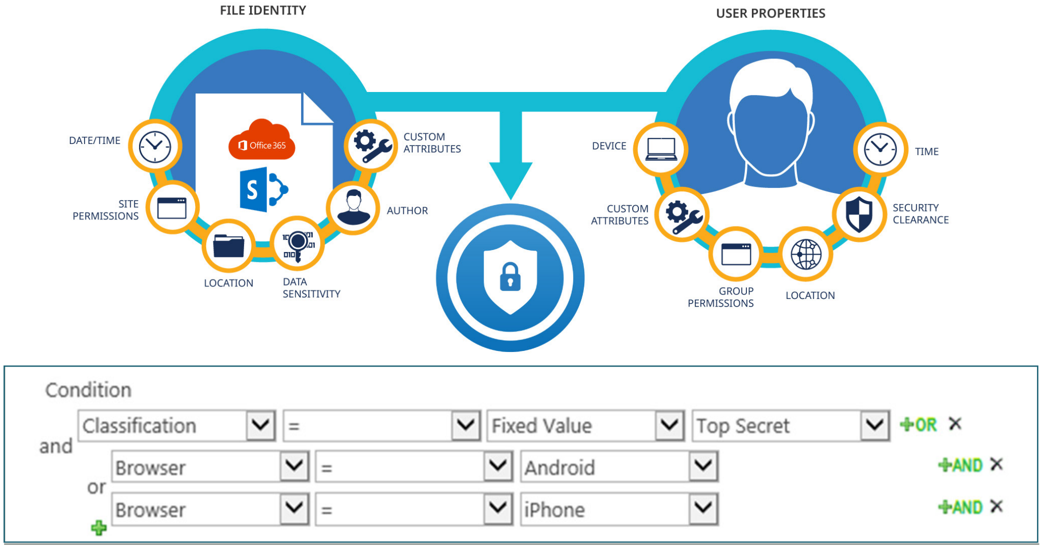
File identity or properties can include the original author, version number, location, projects, custom meta-data, for example, as well as classifications applied by any application, such as Azure Information Protection or NC Protect Compliance Module.

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 he or she can do with files automatically changes, as well.

Additionally, NC Protect's dynamic and rule-based approach is transparent to the end user, who continues to use Microsoft's applications to access and collaborate upon files. NC Protect manipulates SharePoint's user interfaces and RMS encryption, which means that there is no additional user training, and no additional software on users' devices.



Condition

and Classification = Fixed Value Top Secret +OR ✕

Browser = Android +AND ✕

or

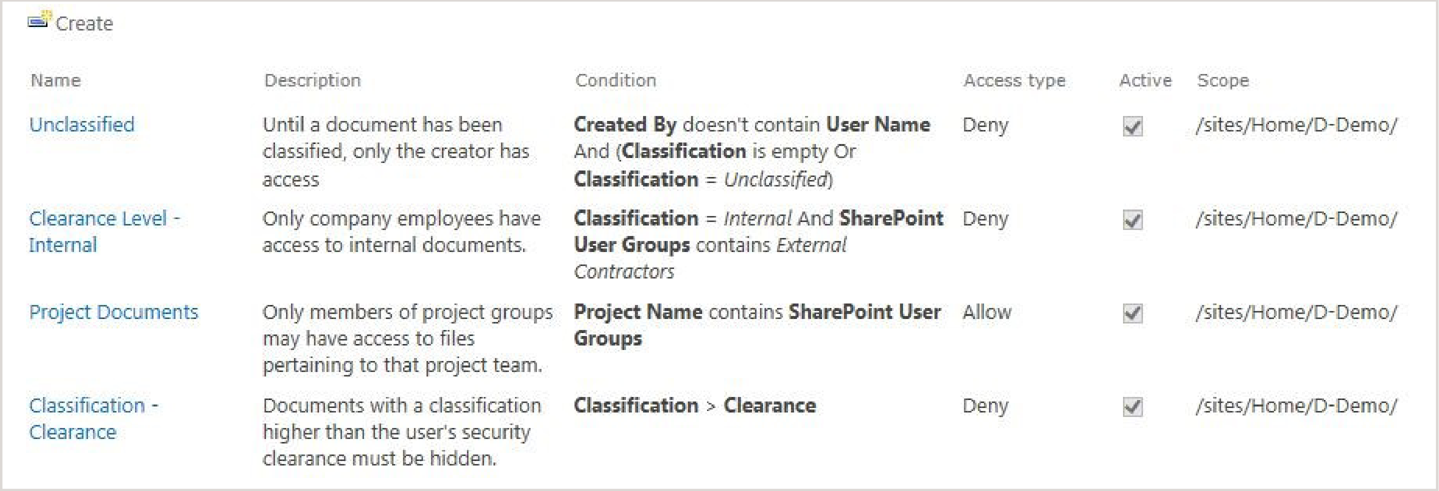
Browser = iPhone +AND ✕

Figure 1: NC Protect's logical expression builder, showing user properties and file properties 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 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. All of these rules determine the response to a logical expression that is composed of user and file properties, and they are evaluated in real-time, whenever a user searches for or uses a file.

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

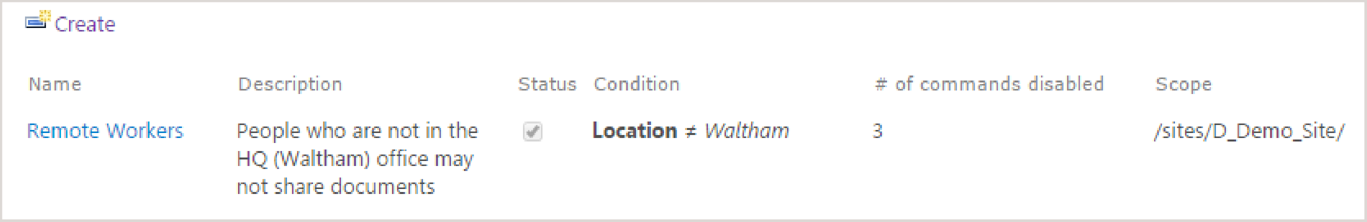


Create

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



Create

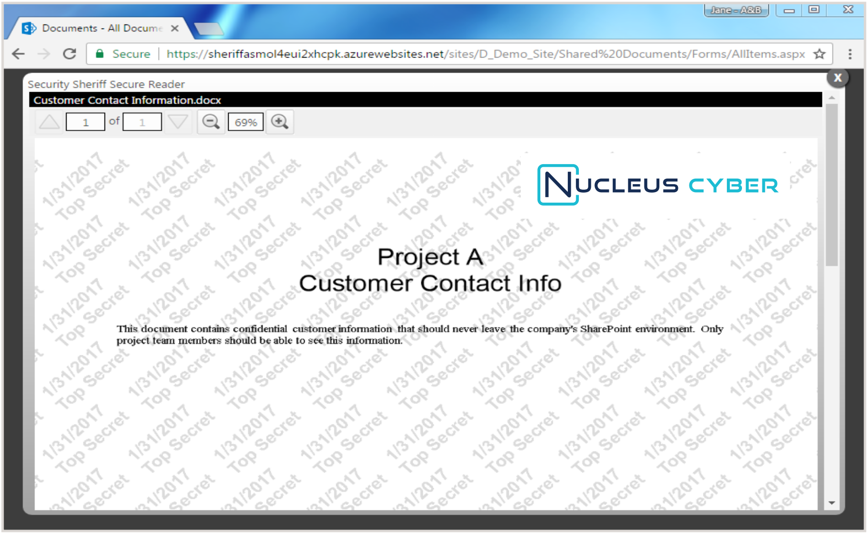
Name	Description	Status	Condition	# of commands disabled	Scope
Remote Workers	People who are not in the HQ (Waltham) office may not share documents	☑	**Location** ≠ *Waltham*	3	/sites/D_Demo_Site/

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

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

1. **RMS Encryption:** NC Protect tailors RMS encryption as the files leave the protected SharePoint environment, determining the permissions a user has when opening or copying a file. NC Protect can apply a pre-defined RMS template, or it can specify a custom collection of RMS permissions. Once the file arrives on the user's end device, it has been encrypted and that user has appropriate permissions that are managed by Microsoft RMS. This means that the file can be used on any device and by any application that is Microsoft enlightened and that there are no additional applications or tools that need to be installed and managed on end devices.

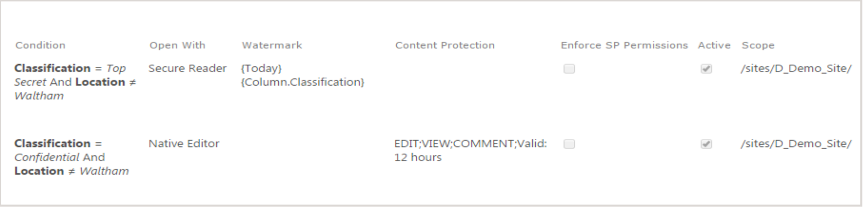
2. **Zero-Footprint Secure Reader:** NC Protect can prevent a highly sensitive file from ever leaving the protected SharePoint environment while permitting a user to view the content without transmitting the actual file. NC Protect's Secure Reader renders an image of the file that is transmitted with a customizable 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.


Documents - All Docume
Jane - A&B
Secure
https://sheriffasmol4eui2xhcpk.azurewebsites.net/sites/D_Demo_Site/Shared%20Documents/Forms/AllItems.aspx
Security Sheriff Secure Reader
Customer Contact Information.docx
1
of
1
69%
NUCLEUS CYBER
1/31/2017
Top Secret

Project A
Customer Contact Info

This document contains confidential customer information that should never leave the company's SharePoint environment. Only project team members should be able to see this information.

Figure 4: Screenshot of NC Protect Secure Reader, showing a protected image presented through a secure web browser.



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 screenshot, showing RMS encryption and Secure Reader rules applied when workers access a file remotely.

Note: 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. These rules are not the focus of this whitepaper, and are not explored in depth here.

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 and file encryption templates do not work in the 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 combining both user and file context to apply appropriate security as users and documents change context and in real-time, SharePoint administrators can ensure file security while enabling modern, "always on, work everywhere" user collaboration.

ABOUT NUCLEUS CYBER

Nucleus Cyber is the AI-driven security solution for the intelligent workplace providing dynamic, granular data security that leverages existing infrastructure investments. The NC Protect platform dynamically adjusts file security based on real-time comparison of user context and file content to enforce data governance policies for more secure collaboration. It minimizes data loss and misuse risk for a wide range of digital environments including SharePoint, Office 365, file shares, enterprise social systems and the cloud. For more information visit www.nucleuscyber.com or follow @nuclüescyber.

CONTACT US

info@nucleuscyber.com
www.nucleuscyber.com

in nucleuscyber
@nucleuscyber