DATASHEET

NUCLEUS CYBER

# NCPROTECT™

## DYNAMIC DATA-CENTRIC SECURITY FOR MICROSOFT OFFICE 365 & SHAREPOINT®

### EXECUTIVE SUMMARY

NC Protect™ dynamically adjusts file protection based on real-time analysis of file content and comparison of user and file context to ensure that users view, use and share files according to your business's regulations and policies.

NC Protect secures files in-transit without the overhead of complex user permissions or limitations of encryption at rest, 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 access rights, automatically encrypting files when the data leaves the safety of corporate information and collaboration systems.

### KEY BENEFITS

- Adjust protection based on file and user context – including email recipients
- Automatically apply business policies to files as they move between people and locations
- Enable file protection that changes when the usage context changes
- Restrict ribbon rules according to user and/or file context in all Microsoft Office apps
- Apply file encryption at the time of access to maintain O365 collaboration features that are negatively impacted by encryption at rest
- Dynamically add custom user-specfic watermarks to Word, PowerPoint, Excel and PDF documents
- Provide secure read-only access via a zero-footprint file viewer

## Great for Collaboration, Problematic for Data Security

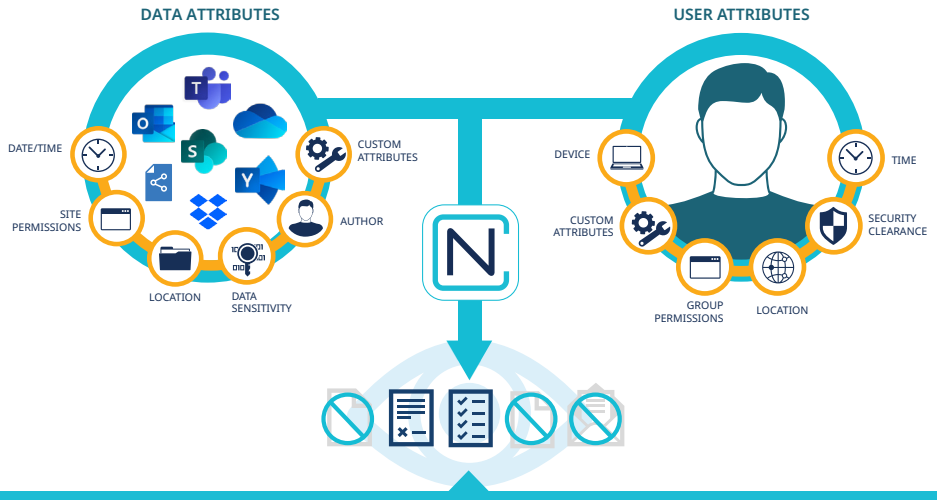
There is little doubt that collaboration tools are changing how people collaborate with colleagues and external parties. With modern collaboration apps, users can access data from an alarming variety of locations. Between Azure, Office 365 and other cloud platforms, businesses are adopting new technologies faster than ever and data loss prevention methodology needs to keep up. The data protection policy must be firm enough to accommodate the adoption of new cloud services – and flexible enough to allow your users to work when, where and how they want.

## Data-Centric Security and Compliance for Office 365 Apps

NC Protect offers centralized, cost-effective policy compliance management and data loss prevention (DLP) for Office 365, SharePoint and OneDrive . It ensures data compliance and security by continuously monitoring and auditing files against regulatory and corporate policies to protect against data breaches, unauthorized access and sharing, and misuse.

Policies for encryption and usage rights can be automatically enforced based on the content and context of the collaboration scenario. It provides an unmatched level of data-centric protections without impacting productivity to facilitate secure collaboration and reduce the risk of Shadow IT.

## CONDITIONAL ACCESS AND DATA PROTECTION BASED ON

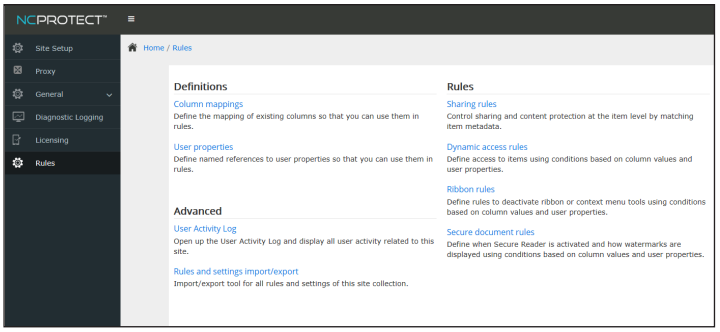



## REAL TIME, CONTEXTUAL ACCESS CONTROL DETERMINES:

| | | | | | |
|---|---|---|---|---|---|
| What a user sees when viewing and searching for files | Whether a user can open, edit, copy or download a file | If a file is encrypted when saved, copied, or emailed | If a dynamic watermark should be applied to a file | If a file can only be viewed in a secure application | What actions are enabled in the Microsoft UI |

## NC Protect Delivers Integrated, Conditional Access Control at the Document Level

NC Protect works natively with Azure Information Protection (AIP) and other Microsoft products to provide granular information protection to data within Microsoft collaboration tools by controlling file access and use combined with restricting certain collaboration functionality as needed, including elements of the SharePoint user interface, an application's method for viewing files, and encryption or restriction of attachments sent through Exchange Email. NC Protect can also apply dynamic, custom watermarks to editable and read-only Microsoft Office files for auditing and security purposes. It requires no additional client-side application, reducing IT overhead and the risks involved in implementing new cloud services or BYOD policies.




### DISCOVER

Locate all sensitive and confidential data (PII, PHI, HR, IP, etc.) to create an 'information footprint' of your sensitive data using a single set of rules for one or multiple on-premises and cloud environments.

### CLASSIFY

Once sensitive information is detected the file can be automatically classified based on the sensitivity of the content and pre-defined governance policies. You can also define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

### RESTRICT

Based upon the business rules associated with its classification, access to a file within can be restricted to a specific individual or group within the site, even if a wider audience has access to the rest of the Team where the item physically resides. With file level controls, users and administrators can reduce the number of Teams needed to enable secure collaboration with a subset of site members. Managing access down to the file level is made possible by leveraging the data and user attributes rather than the data location.

### ENCRYPT

Data loss prevention is a critical issue for many organizations. In addition to securing a document based on its classification (metadata), NC Protect can further secure content by encrypting it to ensure only properly authorized and credentialed users will be able to access the content even if they have Team owner privileges. This additional security makes it safe to store confidential documents such as internal only, Board or HR documents. It also ensures access can be controlled for any data shared with external parties, even when it is removed from the Team.

### PREVENT

To further extend the tracking process you can also define rules in NC Protect to prevent the distribution of sensitive information or confidential documents to minimize the risk of data loss. For example, if a file is added to a site and member does not have proper access to that category of document, then the file can be hidden from the view of the unauthorized individual. Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of the Office 365, SharePoint or OneDrive.

### CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers or managers or to request justifications from users. Complete business rules can be developed so that you can remediate compliance issues and task the proper individual(s) in the organization to review and potentially classify, alter the classification of, or encrypt the content.

### TRACK & REPORT

Dynamically add a custom watermark to Word, PowerPoint, Excel and PDF documents for security and auditing purposes. A dynamic Results Viewer provides centralized reporting and management of classified data. It reports on the number of issues identified by classification level and allows policy officers to review the results and rescan, reclassify or reapply permissions if needed. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.

Member of Microsoft Intelligent Security Association

Microsoft

CYBERSECURITY BREAKTHROUGH AWARD 2019 — ACCESS MANAGEMENT SOLUTION OF THE YEAR

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

## ADVANTAGES OF INTELLIGENT, ITEM-LEVEL SECURITY

Nucleus Cyber's granular data-centric approach to security enables conditional access control down to the item-level using secure metadata and user attributes. Since access and usage rights can be applied to specific content or individual files (using classification), as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on from any site regardless of user membership. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of sites to support individual collaboration scenarios.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com