DATASHEET

NUCLEUS CYBER

NCPROTECT™

ADVANCED INFORMATION PROTECTION FOR MICROSOFT 365 & SHAREPOINT®

EXECUTIVE SUMMARY

NC Protect™ dynamically adjusts file protection based on real-time analysis of content attributes and user attributes to ensure that users view, use and share files according to your business 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 access and protection based on file and user attributes in real time
- Automatically apply business policies to files as they move between people and locations
- Enable file protection that changes when the usage context changes
- Trim ribbon rules in Microsoft 365 apps according to user context or file content
- Add personalized user-specific watermarks to Word, PowerPoint, Excel and PDF documents
- Provide secure read-only access via a zero-footprint file viewer
- Apply user-specific file encryption/DLP policies to the copy of the file being opened or emailed by the user for more granular control.

Great for Collaboration, Problematic for Data Security

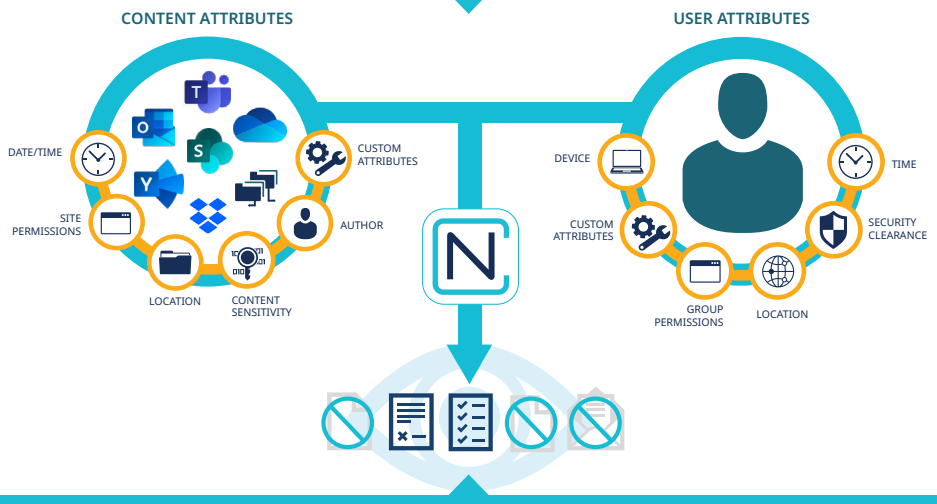
With modern collaboration apps, users can access data from an alarming variety of locations. Between Azure, Office 365 and other cloud platforms, businesses are adopting new technologies faster than ever and data loss prevention methodology needs to keep up. The data protection policy must be firm enough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

Simple, Fast, Scalable Security and Compliance for Microsoft Apps

NC Protect provides advanced data-centric security for Microsoft 365 applications including Office 365, SharePoint Online and on-premises, OneDrive, Teams, Yammer and Exchange emails. The platform empowers enterprises to automatically find, classify and secure unstructured data, and determine how it can be accessed with granular control in cloud, on-premises and hybrid environments.

NC Protect works natively with Microsoft products and enhances security to restrict the use of Microsoft functionality, including elements of the user interface, methods for viewing files, and encryption or restriction of attachments sent through Exchange Email. It requires no additional client-side application, reducing IT overhead and the risks involved in implementing new cloud services or BYOD policies. NC Protect delivers advanced information protection that's simple, fast and scalable.

REAL TIME, ATTRIBUTE-BASED ACCESS & SHARING CONTROL



DETERMINES:

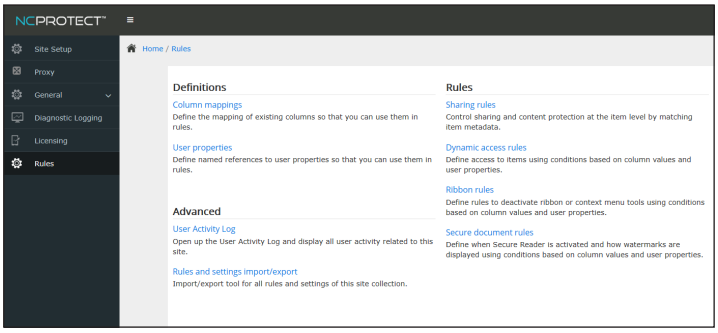
What a user sees when viewing and searching for files	Whether a user can open, edit, copy or download a file	If a file is encrypted when saved, copied, or emailed	If a dynamic watermark should be applied to a file	If a file can only be viewed in a secure application	What actions are enabled in the Microsoft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

DYNAMIC, GRANULAR INFORMATION PROTECTION WITHOUT THE COMPLEXITY

NC Protect augments native app security in Office 365 apps and SharePoint using the unique identity data builds over time.

Using metadata, MIP sensitivity labels and attributes such as file name, authorship and date stamps, as well as more transient context like IP location, device or time of day, NC Protect applies conditional, attribute-based access control (ABAC) and usage rights to support all business rules and enable secure collaboration.

NC Protect takes your data security policies and enforces them for each and every user and device, completely transparent to the end user.



DISCOVER & CLASSIFY

NC Protect scans and inspects files in on-premises and cloud collaboration apps for sensitive or regulated data according to defined policies. When detect, it automatically classifies the file and applies information protection based on it's sensitivity and your policies. It can also leverage MIP sensitivity labels in combination with other file and user attributes to control access to and apply information protection.

RESTRICT

Utilize granular security to automatically restrict access to, sharing of and protection of content based on the business rules associated with the file's classification or MIP sensitivity label. Access to a file can be restricted to a specific individual or group, even if a wider audience has access to the rest of the site where the item physically resides. Managing access at the file level is made possible by leveraging the data and user attributes, rather than the data location.

ENCRYPT

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 administrative privileges, making it safe to store confidential documents such as Board or HR documents. It also ensures access can be controlled for any data shared with external parties, even when it is removed from a site.

PREVENT

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.

AUGMENT SECURITY WITH DYNAMIC WATERMARKS & MORE

NC Protect works natively with Microsoft collaboration and security products to augment native features to enforce secure read-only access, hide sensitive files from unauthorized users, trim the application ribbon, apply dynamic personalized watermarks, and encrypt or restrict attachments sent through Exchange Email.

REDACTION

NC Protect can remove/redact sensitive or confidential information, such as keywords or phrases, in a document when viewed in its native application (Word, Excel, PowerPoint and PDF) or when the file is presented in the NC Protect secure reader for legal or security purposes.

AUDIT & REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. Report 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. Integrate user activity and protection logs with SIEM tools like Splunk or Microsoft Sentinel for further analysis and downstream actions.

ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

Nucleus Cyber's granular data-centric approach to security enforces a zero trust methodology through conditional, attribute-based access control at the item-level. Since access and information protection are applied to individual files, chats and messages, as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated on across Microsoft 365 apps, regardless of user membership.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com