# NCPROTECT™

# DYNAMIC INFORMATION PROTECTION FOR MICROSOFT 365 & SHAREPOINT®

## Executive Summary

Adoption of cloud collaboration tools and remote work has exploded and traditional data loss prevention methods are struggling to keep up. With Microsoft 365 applications users can access data from a variety of channels including file shares, chat and email – in the office, at home and in public spaces.

Data protection policies must be firm enough to protect data and flexible enough to allow your users to work when, where and how they need to.

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

## Key Benefits

- Discover and classify files based on the sensitivity of their contents
- Dynamically adjusts access and protection based on file and user attributes in real time
- Enable file protection that changes when the usage context changes
- Control who can access information, and if and how it can be copied, printed or shared
- Obfuscate/Hide files from unauthorized users
- Add user-specific security watermarks to Word, PowerPoint, Excel and PDF documents
- Enforce secure read-only viewing of sensitive information with a built-in Secure Reader
- Encrypt individual files only when the situation requires
- Trim ribbon rules in Microsoft 365 applications to restrict functions

## SIMPLE, FAST, DYNAMIC SECURITY AND COMPLIANCE FOR MICROSOFT 365 APPLICATIONS


NC Protect provides advanced data-centric security across Microsoft 365 applications including SharePoint Online, Office, OneDrive, and Exchange, SharePoint on-premises and hybrid environments.

The platform empowers enterprises to automatically find, classify and secure sensitive data, and determine how it can be accessed, used and shared with granular control.

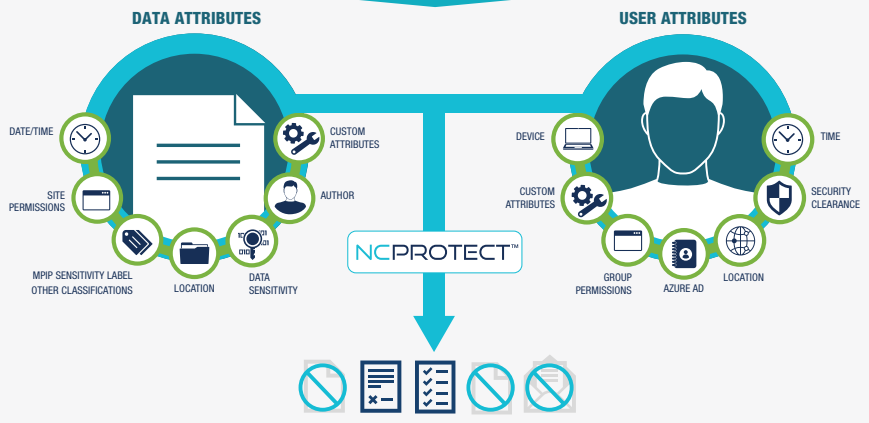
## DYNAMICALLY SECURE COLLABORATION WITH ABAC POLICIES & UNIQUE SECURITY CONTROLS

NC Protect works natively with Microsoft products and enhances security with attribute-based access control (ABAC) and protection polices. It restricts usage and visualization of data based on the file's classification and the user's current location, device and access rights.

It adds unique security capabilities to enforce secure read-only access, hide sensitive files from unauthorized users, redact sensitive or classified information, trim the application ribbon, apply dynamic security watermarks, and encrypt or restrict attachments sent through Exchange Email.

NC Protect requires no additional client-side application, reducing IT overhead and the risks involved in implementing new cloud services or BYOD policies.

## REAL TIME, ATTRIBUTE-BASED ACCESS CONTROL & DATA PROTECTION




### Real Time, Contextual Polices Determine:

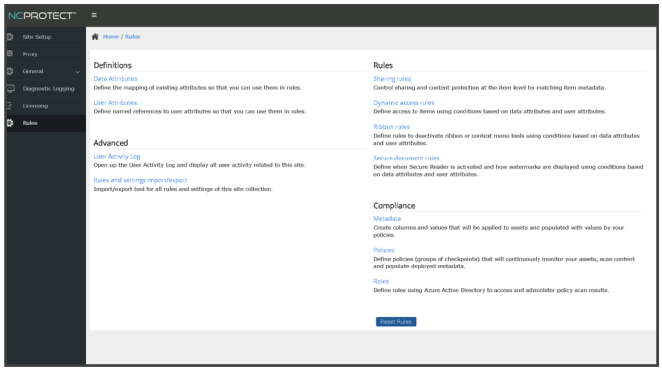
| | | | | | |
|---|---|---|---|---|---|
| What a user sees when viewing and searching for files | Whether a user can open, edit, copy or download a file | If a file is encrypted when saved, copied, or emailed | If a dynamic watermark should be applied to a file | If a file can only be viewed in a secure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

# KEY CAPABILITIES

NC Protect augments native security in Microsoft 365 applications using the unique identity data builds over time.

Using metadata, MPIP 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 enforces data security and compliance policies for each and every user and device, completely transparent to the end user.




## DISCOVER & CLASSIFY

NC Protect scans and inspects files for sensitive or regulated data according to defined policies. When detected, it automatically classifies the file and applies access controls and information protection based on it's sensitivity and your policies.

NC Protect's policies can leverage Microsoft Purview Information Protection (MPIP) sensitivity labels and existing classifications in combination with other file and user attributes. You can add unlimited additional security labels using NC Protect to augment other classifications.

## RESTRICT

NC Protect's attribute-based access control (ABAC) policies use data and user attributes (e.g., classification, geolocation, device, time of day), not data location, to determine access rights in real time. Access to a file can be restricted to a specific individual or group, even if a wider audience has access to the site or folder.

Granular security policies automatically restrict access to, sharing of and protection of content based on the policies and the context of the user at the time of access.

## ENCRYPT

If a sensitive document that requires encryption is identified, it can encrypt the content immediately – limiting the audience to only credentialed users. The contents of an email and any attachments sent through Exchange can also be encrypted automatically. The optional NC Encrypt module offers SharePoint column encryption, key management, and BYOK support.

## PREVENT

Define rules in NC Protect to prevent the distribution of sensitive information or confidential documents in emails and chat to minimize data loss/exposure.

## HIDE SENSITIVE FILES

Dynamically obfuscate data to hide sensitive or confidential documents from unauthorized users in folders, chats and searches. Only users with access rights will be able to see the content exists to minimizing data exposure and the need to create multiple sites and channels to accommodate different access rights.

## SECURE READER

Forced users to view sensitive documents in NC Protect's Secure Reader for read-only access. It prevents users from being able to download, copy, edit or print sensitive data.

## DYNAMIC SECURITY WATERMARKS

Dynamically add security watermark(s) customized with user and/or file attributes to sensitive and confidential Word, PowerPoint, Excel, PDF and image files for security and auditing purposes. Watermarks can incorporate attributes such as user name, email, time and date that the file was accessed. They deter users from taking photos and create a digital thumbprint for tracking and forensics purposes.

## REDACTION

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 Secure Reader for legal or security purposes.

## AUDIT & REPORT

Provides centralized reporting on classified data and user activity logs. Report on the number of issues identified by classification level, review scan results and rescan, reclassify or reapply permissions if needed. Integrate user activity and protection logs with Splunk, Microsoft Sentinel and other SIEM tools for further analysis and downstream actions.

## ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

**archTIS' 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.**

archTIS

Australia | United States | United Kingdom
archtis.com | info@archtis.com

Member of Microsoft Intelligent Security Association
Microsoft Security