NCPROTECT™

DYNAMIC DATA PROTECTION FOR MICROSOFT 365 & SHAREPOINT®

Executive Summary

Microsoft 365 enables users to access information from just about anywhere. Your data loss prevention and compliance strategies need to adapt to the modern workplace. Access and data protection policies must be robust enough to manage the risks but flexible enough to support a distributed, global workforce and third party users. This poses a challenge for IT and security teams.

NC Protect provides dynamic data-centric security to adjust access and file protection to augment Microsoft 365 security based on real-time analysis of content and user attributes to ensure that users view, use and share files according to your business policies - no mater where your data lives or travels.

Key Benefits

- Classify files with multiple labels and use third party classifications, including Microsoft Purview sensitivity labels
- 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

SIMPLE, FAST & DYNAMIC DATA PROTECTION FOR MICROSOFT 365 APPLICATIONS

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

The platform empowers enterprises to secure sensitive data, determining if, when and how it can be accessed, used and shared with granular control.

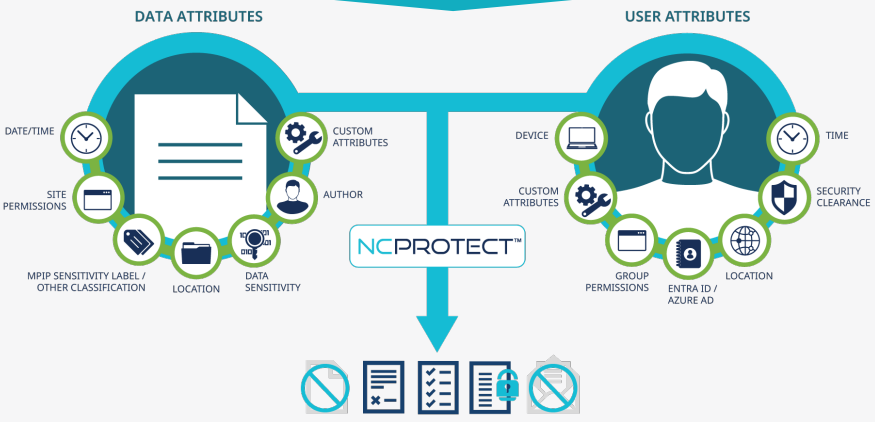
DYNAMICALLY SECURE COLLABORATION WITH ABAC POLICIES & UNIQUE SECURITY CONTROLS

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, 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



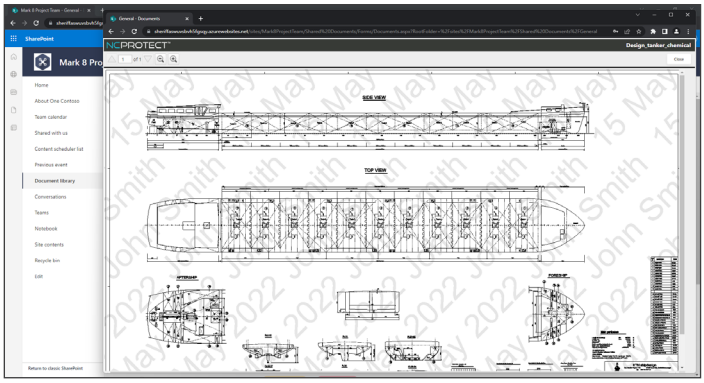
Real Time, Contextual Polices Determine:

If access to a file is approved or denied based on the policy and attributes	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

KEY NC PROTECT CAPABILITIES

NC Protect augments the native security in Microsoft 365 applications using the unique identity data builds over time. Using metadata, MPIP sensitivity labels, Entra ID properties and attributes such as file name, authorship and date stamps, as well as more transient context like IP location, device or time of day, it applies conditional access, usage and sharing policies 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.



CLASSIFY

Add unlimited labels to an individual file to aid in document classification and support complex taxonomies. Policies can also leverage Microsoft Purview Information Protection (MPIP) sensitivity labels and existing classifications from other vendors including Janusseal and Titus in combination with other file and user attributes.

RESTRICT

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 requiring encryption is identified, the content will be encrypted immediately, limiting access to only authorized 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 via downloads and email to minimize data loss/ exposure.

HIDE SENSITIVE FILES

Dynamically hide/obfuscate sensitive or confidential documents from unauthorized users in folders and searches. Only users with access rights will be able to see the files to minimize data exposure. Eliminates the need to create multiple sites and channels to accommodate different access rights.

SECURE READER

Force users to view sensitive documents in NC Protect's Secure Reader to prevent 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 user activity logs and policy changes. Integrate user activity and protection logs with Microsoft Sentinel, Splunk 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 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 supported Microsoft 365 apps regardless of user membership.

archTIS

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

Member of Microsoft Intelligent Security Association