NCPROTECT™

ADVANCED INFORMATION PROTECTION FOR SHAREPOINT® SERVER 2013, 2016, 2019 & SE

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 enterprise 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 SharePoint and Office 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 and data loss prevention controls
- Leverage MIP sensitivity labels or dynamically tag data based on its sensitivity level
- Extend access and protection policies to cloud and hybrid deployments for consistent security

STAYING ON-PREMISES OR MIGRATING TO THE CLOUD, DATA PROTECTION IS A PRIORITY

With modern collaboration apps, users can access data from an alarming variety of locations. While many companies are migrating to SharePoint Online and Microsoft 365, on-premises applications including SharePoint Server are still a staple in many organizations. SharePoint on-premises data protection requires the same robust security as Cloud tools to protect against data loss and insider threats.

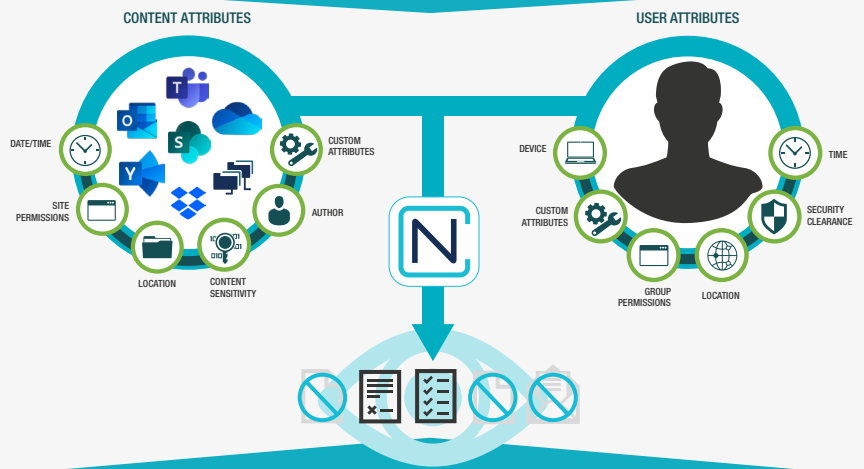
SIMPLE, FAST & SCALABLE DATA SECURITY

NC Protect provides advanced data-centric security for SharePoint Server 2013, 2016, 2019 and SE deployments, delivering enhanced information protection for on-premises environments that can be extended to hybrid and cloud M365 deployments should you migrate in the future.

NC Protect integrates with SharePoint on-premises to provide in-transit data protection. Plus unique capabilities to restrict Microsoft ribbon functionality, provide secure read only access, add digital security watermarks, encrypt or restrict attachments sent through Exchange Email, and more. All controlled from a centrally managed portal that requires no additional installation of a client-side application, reducing IT overhead and ensuring compliance and security policies are consistently applied.

NC Protect delivers advanced information protection for SharePoint that's simple, fast and scalable to safeguard sensitive data no matter where it travels.

CONDITIONAL ACCESS AND DATA PROTECTION BASED ON



Real Time, Contextual Access Control Determines:

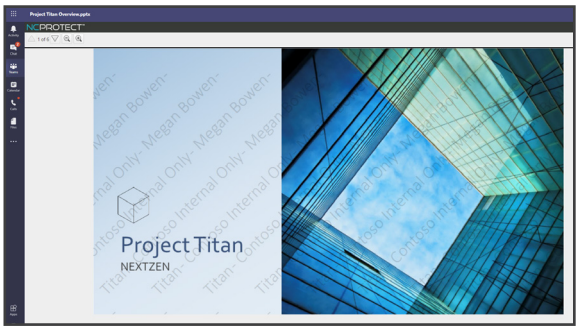
What a user sees when viewing and searching for files	Whether a user can open, edit, copy or download a file	If a file is encrypted when saved, copied, or emailed	If a dynamic watermark should be applied to a file	If a file can only be viewed in a secure application	What actions are enabled in the Microsoft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

DYNAMIC, GRANULAR INFORMATION PROTECTION FOR SHAREPOINT SERVER

NC Protect integrates natively into SharePoint Server to enhance the data security capabilities by leveraging dynamic attribute-based access control (ABAC) and protection policies to safeguard data at rest and in motion.

It enforces real-time conditional access, sharing and usage control of SharePoint files based on attributes such as file metadata, user location, device, time of day, etc. If the user context or data attributes change, NC Protect can automatically adjust access and protection based on your defined business and compliance policies.

NC Protect dynamically enforces access and security policies for each and every user and device, completely transparent to the end user to ensure secure document collaboration without impacting productivity.



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 information protection based on its sensitivity and your governance policies. It can also leverage MIP sensitivity labels in combination with other file and user attributes to control access to the file and apply further information protection.

RESTRICT

Utilize granular security policies to automatically restrict access to, protection of and sharing of content based on the policies associated with the file's classification or MIP sensitivity label.

With NC Protect, access is managed at the individual file level, meaning that a file in a SharePoint collection can be visible to one user and not another by leveraging the attributes - not the location of the file - even if they have administrative privileges.

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. It ensures access can be controlled for any data shared with external parties, even when it is removed from a site.

PREVENT

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 user does not have proper access to that category of document, then the file will be hidden from the view of the unauthorized individual.

Depending on the users access privleges, NC Protect will also prevent the printing, saving and copying of Microsoft Office documents or PDFs. Restrictions can also be applied to restrict the emailing of documents stored in SharePoint via Exchange servers to reduce data leakage.

CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers, managers or chain of command to assess the requested action. Business rules can be developed so that you can remediate compliance issues (i.e. review and classify, alter the classification of, or encryption of the content).

UNIQUE DATA PROTECTION CAPABILITIES

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

REDACT

NC Protect can redact sensitive or confidential information by removing or masking keywords or phrases (e.g. social security number) in a document when viewed in its native application (Word, Excel, PowerPoint and PDF) or when viewed in the NC Protect secure reader.

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 rescan, reclassify or reapply permissions if required. Integrate user activity and protection logs with SIEM tools like Microsoft Sentinel or Splunk 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 (ABAC) 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 on-premises, cloud and hybrid applications, regardless of user membership.

archTIS

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