NCPROTECT™

DYNAMIC DATA DISCOVERY, CLASSIFICATION & SECURITY FOR WINDOWS FILE SHARES

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 applies security and encryption to file share content without the overhead of manually administered folder shares and NTFS permissions. Data can be automatically classified and encrypted based on the content and metadata associated with the file.

Organizations no longer need to rely on complex folder hierarchies but instead can easily ensure their sensitive data is appropriately protected with NC Protect.

Key Benefits

- Centralized, cost-effective compliance management and data loss prevention.
- Monitor and audit content against regulatory and corporate policies.
- Automatically classify, restrict access to and encrypt content based on the presence of sensitive data including PII, PHI, IP and other factors.
- Granular policy-enforced approach to security limits access at the item-level using file and user attributes.
- Supports common file types, including Word, Excel, PowerPoint, PDF, OCR, CAD files, images, text files and more.
- Audit trails and forensics track access to sensitive data to ensure transparency and accountability.

FILE SHARE DATA POSES A SIGNIFICANT RISK

Many organizations have turned to document collaboration and management platforms, including Microsoft 365 and other cloud solutions, to store and collaborate on unstructured content.

However, many companies still use traditional File Shares, where terabytes of data are stored and accessed. Some will migrate that content over to systems like SharePoint Online, while others will continue to store and archive information in existing repositories.

With so much focus on the cloud, how are access and compliance being managed on your File Shares? The same data privacy and security concerns that apply to newer technologies are equally important for file share systems.

NC Protect offers dynamic, real-time access control and data loss prevention. It continuously monitors and audits files and documents stored and shared on Windows File Shares against regulatory and corporate policies to protect against data breaches, unauthorized access, and misuse.

GET UNMATCHED DATA DISCOVERY, CLASSIFICATION AND PROTECTION

Stop relying on complex folder hierarchies to protect File Share data. NC Protect safeguards your file shares with data-centric security and encryption without the overhead of manually administered folder shares and NTFS permissions.

NC Protect takes a proactive approach to data security. It uses attribute-based access control (ABAC) and data protection policies to automatically discover, classify, restrict, and encrypt content. By dynamically adjusting access and security based on real-time comparison of user context and file content, NC Protect ensures that your business regulations and policies are adhered to, giving you peace of mind.

Discover

Scan and identify content for privacy and compliance factors, including privacy regulations (CCPA, GLBA, COPPA, GDPR, POPIA, etc.), protected healthcare information (PHI, HIPAA), FISMA, PCI DSS, defense data (ITAR, EAR, CUI) and more.

Easily create custom rules to match your organization's unique confidentiality and security policies for HR, financials, M&A, IP and more.

Classify

As NC Protect scans and identifies sensitive data or detects specific policy violations, the flagged file is automatically classified via the addition of metadata.

NC Protect audits a classified document's entire lifecycle, including who accessed the data and what they did with it.

Secure

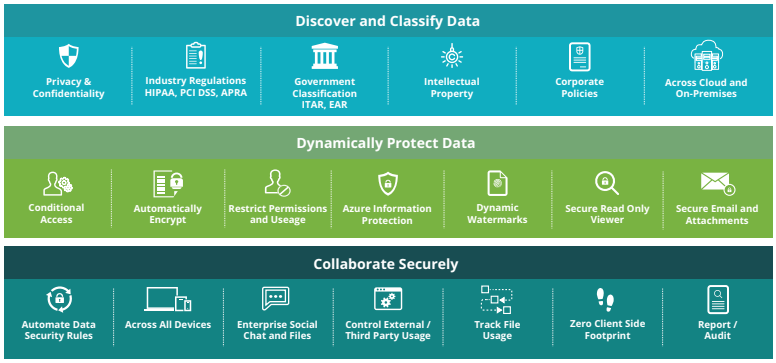
NC Protect also applies access and usage rights to automatically:

- Encrypt files at-rest and in-transit
- Prevent unauthorized sharing and editing of documents
- Start workflows for approvals and notifications
- Report on sensitive data issues, permissions and user activity

THE NC PROTECT DIFFERENCE: DATA-CENTRIC ACCESS CONTROL & PROTECTION

NC Protect allows you to discover and classify data, dynamically protect data and collaborate securely using dynamic attribute-based policies.

It enhances Windows File Share security to not just control access to sensitive data, but also apply conditional data-centric protections such as read-only access, user-based watermarks, encrypt or restrict attachments sent through Exchange Email, and more. It is entirely transparent to end-users and does not require any additional client-side applications.



CLASSIFY

With NC Protect users can easily configure secure metadata and define choice values to suit any business requirement. Authorized users can classify documents according to their content, unlike standard metadata that can be modified by anyone that is allowed access. Users can define the level of sensitivity of the document, e.g. confidential, private or secret, then depending on their selection additional levels of classification can be added as required, including selecting the audience, department or project.

RESTRICT

Based upon the business rules associated with its classification, access to a document or content item within a File Share can be restricted to a specific individual or group, even if a wider audience has access to the site or library where the item physically resides. With file level permissions, administrators can reduce the number of folder locations that get created (folder location proliferation) just to cope with another set of collaborative users. Managing file permissions with NC Protect is easy since they are based on the metadata values added at the time of classification.

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 File Share content by encrypting it. This means only properly credentialed users will be able to read the content – whether inside or outside of the File Share – even if they have administrator privileges, making it safe to store confidential documents such as Board and HR documents. It also ensures any documents that make it out of the file system can only be accessed by the credentialed users.

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 or or educate users of the risk. For example, if a document is going to be emailed to a group and a listed recipient does not have proper access to that category of document, then the email cannot be sent until the individual is removed from the distribution list. Users can also be prevented from printing, saving or copying the contents of Microsoft Office documents outside of the File Share.

Distribution rules can also be defined to enable secure document exchange via email with third parties. Office and PDF documents from File Share assets can be sent as secure, read-only PDF email attachments to external recipients using Adobe certificates (PKI).

CONTROL

Using workflows, NC Protect can trigger workflows to request approval from policy officers or managers, or to request explanations from users. Complete business rules can be developed to 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.

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

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 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 from any folder in the File Share. NC Protect ensures access to the file is restricted to only those who have permissions to access it as defined by its classification.

archTIS

Complior

archTIS SILVER Partner

archTIS.com | info@archtis.com

www.complior.se | +46 8 535 24 100