DATASHEET

NUCLEUS CYBER

NCPROTECT™

AI-DRIVEN DATA SECURITY FOR FILE SHARES

EXECUTIVE SUMMARY

NC Protect™ (formerly Security Sheriff™) 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.

KEY BENEFITS

- Centralized, cost-effective policy 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.
- Detect potential violations and initiate workflows to remediate and minimize risk.
- Granular approach to security limits access at the item-level using secure metadata.
- Store document 'fingerprint' to enable policy rules to be applied if file share documents are emailed/socialized
- Audit trails and forensics track access to sensitive data to ensure transparency and accountability.

Unstructured Big Data Poses a Significant Risk

The numbers tell the story, 90 percent of data generated today is unstructured (customer purchase history, call center logs, emails, spreadsheets, documents, web content, blogs, wikis, etc.).[1] And information velocity is not slowing down with quintillions of bytes of data being created every day.

Many organizations have turned to document collaboration and management platforms including Microsoft SharePoint, Office 365, Dropbox and other cloud solutions to store and collaborate on this unstructured content. However, many companies still have legacy File Shares where terabytes of data are still being stored and accessed. Some will migrate that content over to systems like SharePoint; others will continue to store and archive information in existing repositories.

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

Ensure Data Compliance & Security for Your File Share Content

NC Protect offers centralized, cost-effective policy compliance management and data loss prevention for collaboration systems and files shares alike. It ensures data compliance and security by continuously monitoring and auditing data and documents on Windows Server File Shares against regulatory and corporate policies to protect against data breaches, unauthorized access and misuse. The same rules can also be applied to content on SharePoint, Office 365, Dropbox and more.

Managing compliance and security with NC Protect is as easy as 1-2-3.

DESIGN INTELLIGENT RULES

NC Protect's policy manager features hundreds of pre-defined checkpoints for US and international privacy policies (Privacy Acts, GLBA, COPPA), and other regulatory mandates including HIPAA, FISMA, PCI DSS and more.

Easily define and configure custom checkpoints to match your organization's unique privacy, confidentiality and security policies.

AUTOMATE COMPLIANCE

As NC Protect scans and identifies areas of risk, detects specific policy violations or confidential content, the flagged file is automatically classified via the addition of metadata.

SECURE INDIVIDUAL FLES

Once classified, user-defined business rules in NC Protect can automatically restrict access to a file, encrypt it, track the document's chain of custody, and prevent it from leaving the File Share.

[1] PC Magazine https://www.pcmag.com/news/364954/90-percent-of-the-big-data-we-generate-is-an-unstructured-me

Secure Content at the Document Level with NC Protect

NC Protect uses metadata-driven, item level security to restrict access to, encrypt, track and prevent the emailing of content based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection (DLP) capabilities for Windows Server File Shares. Organizations using Windows Server File Shares in addition to SharePoint for storage and collaboration can leverage NC Protect's rules across both platforms to centrally manage policies, classifications and controls.

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 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.

REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. It reports 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. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.

Advantages of Metadata-driven, Item-level Security

Nucleus Cyber's granular approach to security limits access at the item-level using secure metadata. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of folders on Windows Server File Shares. NC Protect looks at an entire folder of content and the data contained within the items, to identify individual documents and files to secure based on specific policies built in the policy manager. It then classifies, via secure metadata, and if desired, restricts access to and encrypts the item(s).

Since permissions are applied at the individual file level (using classification), as compared with solutions that secure or encrypt at the folder level, sensitive content can be stored, shared and collaborated on from any folder in the File Share. It ensures access to the file is restricted to only those who have permissions to it as defined by its classification.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com