DATASHEET

NUCLEUS CYBER

NCPROTECT™

INTELLIGENT DATA-CENTRIC SECURITY FOR SHAREPOINT® AND OFFICE 365®

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 secures files in-transit without the overhead of complex user permissions and encryption, 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 corporate information and collaboration systems.

KEY BENEFITS

- Adjust protection based on file and user context – including email recipients
- Automatically apply business policies to files as they move between people and locations
- Encrypt individual files only when the situation requires
- Enable file protection that changes when the usage context changes
- Dynamically restrict ribbon rules by user and/or file context in all Microsoft Office apps
- Restrict details of all files and properties so users can't discover security policies

DISCOVER & SECURE SENSITIVE DATA

Do you know where your unstructured content in your organization is being created, shared and stored? Are you sure that your sensitive data is adequately protected and only available to the appropriate individuals?

NC Protect locates and classifies sensitive and confidential data (PII, IP, HIPAA, HR, etc.) using a single set of rules for one or multiple on-premises and cloud environments. Automatically encrypt or quarantine files when required.

PREVENT DATA LOSS, MISUSE & HUMAN ERROR

NC Protect complements the powerful content publishing and collaborative features in SharePoint and Office 365 by enabling users to monitor content at rest and restrict content in transit to protect against data loss and misuse.

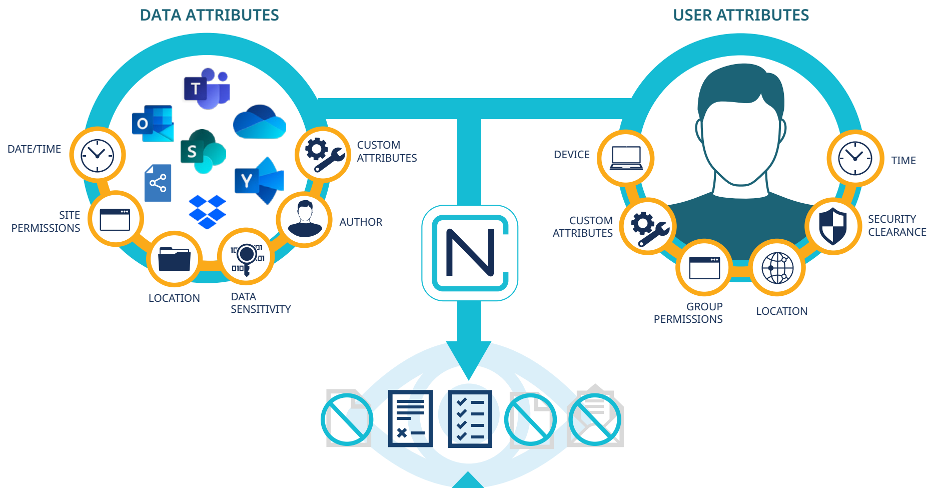
Dynamically adjust file access security and in-transit encryption based on real-time comparison of user context and file content. Ensure users share and use files according to your regulations and policies across all devices and locations.

ENABLE AN INTELLIGENT WORKPLACE

AI-driven security applies your information protection rules to automatically make decisions on what users can do with business files to reduce employee mistakes, data loss and unauthorized access.

With NC Protect, IT administrators can manage user access without creating more security groups, more sites, libraries or folders. Instead, IT administrators define access rules and usage rights to efficiently and dynamically control access and user actions.

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

PERIMETER DATA SECURITY ALONE DOESN'T WORK ANYMORE

With modern collaboration apps, users can access data from an alarming variety of locations. Between Azure, Office 365 and other cloud platforms, businesses are adopting new technologies faster than ever and data loss prevention methodology needs to keep up. The data protection policy must be firm enough to accommodate the adoption of new cloud services – and flexible enough to allow your users to work when, where and how they want.

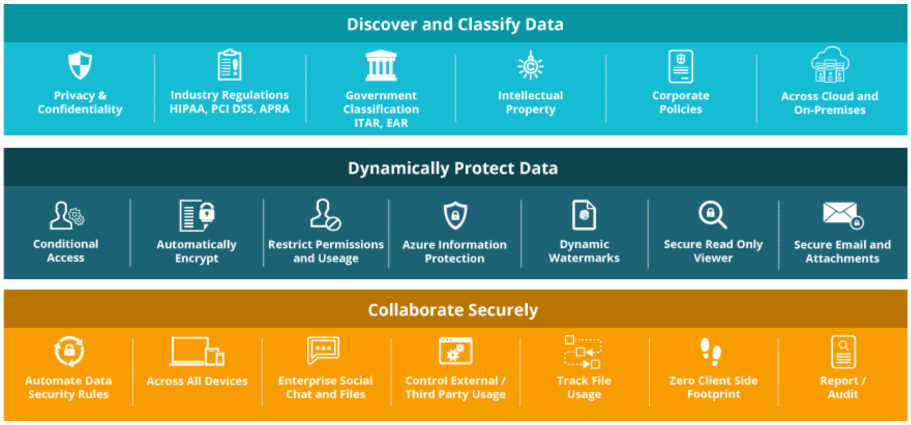
REAL-TIME AUTHENTICATION FOR THE EXPANDED ATTACK SURFACE

NC Protect augments authentication using the unique identity a file builds over time. It starts the moment a file is first saved, with its content, name, authorship and date stamps. And then through its lifecycle it gains additional transient context such as the file location or information repository and classification levels.

Real-time authentication reflects the user's current context, blending traditional user permissions with granular business information such as security level or project team. Additionally, NC Protect leverages even more transient context such as IP address, device, browser or time of day.

NC Protect takes your data security policies and enforces them for each and every user and device, completely transparent to the end user.

Data-centric Security, Protection and Compliance



Discover and Classify Data

Privacy & Confidentiality

Industry Regulations HIPAA, PCI DSS, APRA

Government Classification ITAR, EAR

Intellectual Property

Corporate Policies

Across Cloud and On-Premises

Dynamically Protect Data

Conditional Access

Automatically Encrypt

Restrict Permissions and Useage

Azure Information Protection

Dynamic Watermarks

Secure Read Only Viewer

Secure Email and Attachments

Collaborate Securely

Automate Data Security Rules

Across All Devices

Enterprise Social Chat and Files

Control External / Third Party Usage

Track File Usage

Zero Client Side Footprint

Report / Audit

Secure Data In-Use and In-Transit

NC Protect leverages dynamic access, usage denial rules and a secure viewer to ensure that only approved users can access and share your business content. Keep control of your sensitive information on-premises, in hybrid environments or in the cloud. Apply protection rules centrally or locally, ensuring compliance, while enabling content experts to fine- tune rules.

Secure Data at Rest

NC Protect locates and classifies all data on-premises and in the cloud, encrypting or quarantining when required, and reporting status and compliance violations to stakeholders. It automatically inspects, classifies, and restricts data according to industry regulations and your business policies.

Encrypt When Required

Microsoft or proprietary encryption can be automatically applied when needed, and read/write privileges are automatically manipulated, so the user can concentrate on the content rather than the policies governing collaboration. Data is automatically protected even after it leaves the business.

Lower Cost of Ownership

NC Protect works natively with Microsoft products, restricting usage of Microsoft functionality, including the SharePoint ribbon, an application's methods for viewing files and encryption or restriction of 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. Organizations using SharePoint and Office 365 in addition to Teams, Yammer, Exchange and Dropbox for storage and collaboration can leverage NC Protect's rules across all platforms to centrally manage policies, classifications and controls.

ADVANTAGES OF INTELLIGENT, ITEM-LEVEL SECURITY

Nucleus Cyber's granular data-centric approach to security enables conditional access control down to the item-level using secure metadata and user attributes. Since access and usage rights can be applied to specific content or individual files (using classification), 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 SharePoint or Office 365 regardless of native user sharing rights. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of sites to support individual collaboration scenarios.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com