NCPROTECT™

ADVANCED INFORMATION PROTECTION THAT'S SIMPLE. FAST. SCALABLE.

PERIMETER SECURITY ALONE IS NOT ENOUGH

With modern collaboration apps, users can access data from an alarming variety of locations. Between Microsoft 365, Teams, Nutanix Files, Dropbox, and other cloud sharing platforms, businesses are adopting new collaboration technologies faster than ever. As a result, data breaches due to negligent and malicious insiders, or insider threats, are on the rise.

With standard security technologies, once you're past the perimeter and have access to an application and file, it's yours to share, copy, download, etc. They don't cut it in a world where insider threats due to simple mistakes are becoming as prevalent as malicious actors outside your organisation.

Data protection policies must be firm enough to protect sensitive data and flexible enough to not impact productivity.

NC Protect allows you to put secure collaboration at the core of your enterprise. It's dynamic, attribute-based security adjusts with your users to protect information against insider threats.

DYNAMIC DATA SECURITY FOR SECURE COLLABORATION

NC Protect dynamically adjusts security based on real-time comparison of user and file context to make sure that users view, use, and share files, messages and chat content according to your organisation's regulations and policies.

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 life cycle 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.

PROTECT SENSITIVE INFORMATION WITH DYNAMIC SECURITY & GOVERNANCE

DISCOVER & AUDIT SENSITIVE DATA

Locate and classify all sensitive and confidential data (PII, IP, HR / Board docs, Contracts, etc.) using one set of rules for one to multiple on-premises and cloud environments. Encrypt or quarantine docs when required. Track access to data.

PREVENT DATA LOSS, MISUSE & HUMAN ERROR

Utilize dynamic file security that adjusts based on real-time comparison of user context and file content to enforce regulations and policies with configurable usage rights, sharing rules/controls, and unique security features such as custom watermarks.

EMPOWER USERS TO WORK ANYWHERE SECURELY

Automatically adjust access rights and control how business-critical information in chats, messages and files can be used and shared based on both user and data attributes such as file sensitivity, location, device and time of day.

DYNAMIC, DATA-CENTRIC DISCOVERY, PROTECTION AND COMPLIANCE

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 organization's 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 corporate information and collaboration systems.

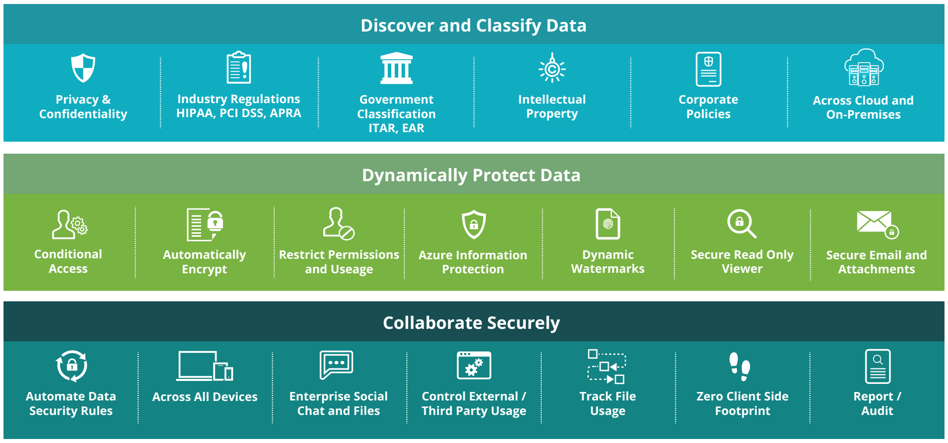
KEY BENEFITS

- Adjust protection based on file and user attributes to control who can access information, and if and how it can be shared
- 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
- Hide files from unauthorized users

Member of Microsoft Intelligent Security Association
Microsoft

CYBER SECURITY EXCELLENCE AWARDS
★ WINNER ★
2021

CYBERSECURITY BREAKTHROUGH AWARD 2020
DATA SECURITY INNOVATION OF THE YEAR



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

DISCOVER AND CLASSIFY DATA

Locate sensitive data using a single set of rules for one or multiple environments and automatically classify it based its sensitivity and your governance policies. Define who can classify or reclassify data, unlike standard metadata that can be modified by anyone with file access.

DYNAMICALLY PROTECT DATA

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.

COLLABORATE SECURELY

NC Protect works natively with Microsoft 365 products providing the ability to restrict functionality, including ribbon functions, methods for viewing files, sharing options 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. The platform is fully integrated with Microsoft 365 (SharePoint, OneDrive, Exchange, Teams, Yammer), Nutanix Files Dropbox and Windows files shares to centrally secure your collaboration tools.