NCPROTECT™

SIMPLE. FAST. DYNAMIC.

ADVANCED INFORMATION PROTECTION

TRADITIONAL SECURITY IS NO LONGER ENOUGH

With the rapid adoption of Microsoft 365 and other cloud platforms, and legacy on-premises tools still in use, users can access data from an alarming variety of locations. As a result, data breaches due to negligent and malicious insiders are on the rise as traditional data loss prevention tools struggle to keep up with modern collaboration.

With most security technologies, even zero trust tools, once you're past the perimeter and have access to an application and file, it's yours to share, copy or download freely. Worse, security incidents caused by insiders are hard to detect - often taking months. A reactive approach is no longer sufficient as security incidents due to simple user mistakes are becoming just as prevalent as those caused by external actors and they are just as damaging to your bottom line.

It's time for a proactive data-centric approach to access and security. NC Protect delivers dynamic, attribute-based access control (ABAC) and data protection that adjusts with your users' context to protect sensitive information against accidental and malicious data loss and misuse. It ensures only the right people – access the right information – at the right time – enforcing the principles of zero trust at the data layer.

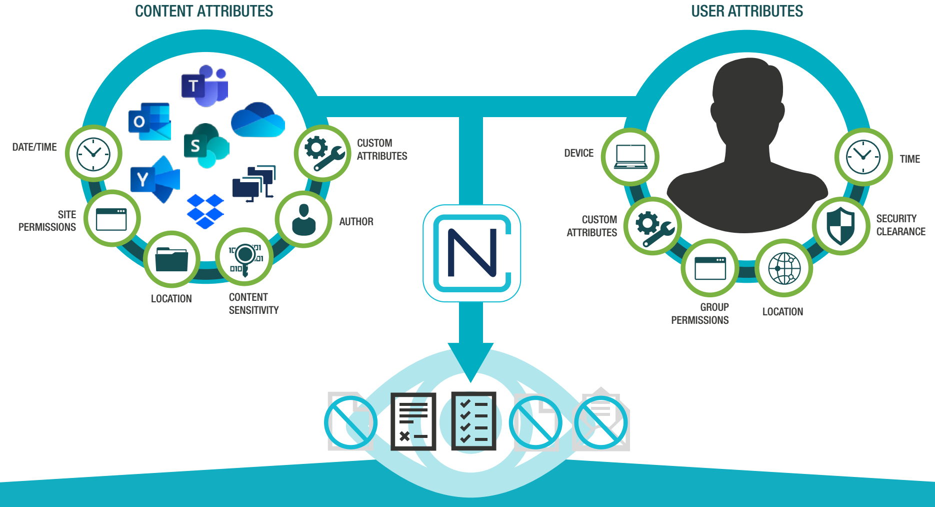
DYNAMIC DATA-CENTRIC SECURITY FOR SECURE COLLABORATION

NC Protect dynamically adjusts access and security based on a real-time comparison of user and file context to ensure that internal users and guests view, use, share files, messages and chat content according to your organization's regulations and policies. The platform empowers enterprises to automatically find, classify and secure unstructured data on-premises, in the cloud and in hybrid environments.

Real-time access and data protection policies evaluate the user's current context, blending traditional user permissions with granular user attributes such as security level, clearance or project team and content attributes such as the sensitivity of the document, classification, or Microsoft Purview Information Protection (MPIP) sensitivity label. NC Protect can also leverage additional attributes such as IP address, device, browser, time of day, etc., to approve access, restrict usage and sharing, or deny access based on the scenario.

It takes your data access and security policies and enforces them for each and every user and device, every time access is requested, completely transparent to the end user. NC Protect allows you to take advantage of all the productivity and collaboration capabilities the Microsoft suite has to offer with zero trust ABAC powered data security.

CONDITIONAL ATTRIBUTE-BASED ACCESS AND DATA PROTECTION



Real Time, Contextual Access and Protection Policies Determine:

- 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 read-only application
- Which ribbon actions are enabled in the Microsoft application UI

DYNAMIC, DATA-CENTRIC DISCOVERY, PROTECTION AND COMPLIANCE

NC Protect ABAC policies dynamically adjust access and protection based on real-time analysis of file content/ sensitivity and user context to ensure that users view, use and share files according to your organization's regulations and policies.

It 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.

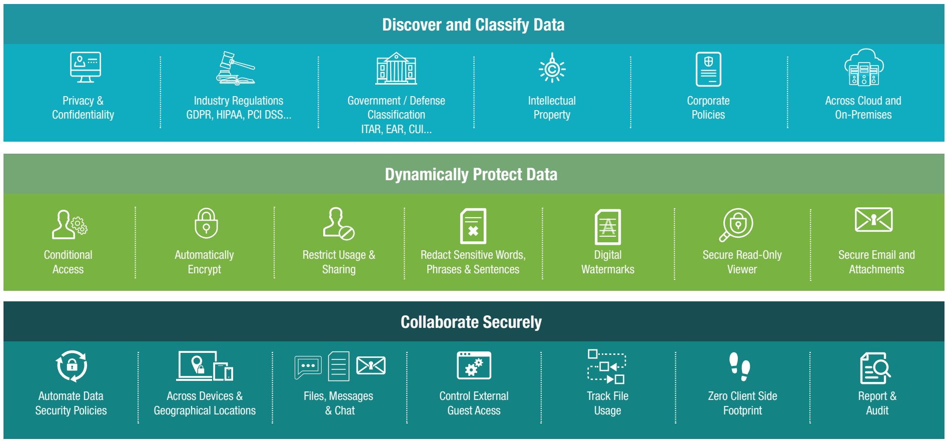
NC Protect also restricts usage and visualization of data based on the file's classification and the user's current location, device and access rights. It can automatically encrypt files when the data leaves the safety of corporate information and collaboration systems.

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 automatically adjusts 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
- Redact sensitive information
- Apply persistent digital security watermarks
- Manage your own encryption keys

Member of
Microsoft Intelligent Security Association
Microsoft Security

Microsoft Security
Excellence Awards 2023
Microsoft Intelligent Security Association
FINALIST
archTIS
Compliance & Privacy Trailblazer



Discover and Classify Data

Privacy & Confidentiality | Industry Regulations GDPR, HIPAA, PCI DSS... | Government / Defense Classification ITAR, EAR, CUI... | Intellectual Property | Corporate Policies | Across Cloud and On-Premises

Dynamically Protect Data

Conditional Access | Automatically Encrypt | Restrict Usage & Sharing | Redact Sensitive Words, Phrases & Sentences | Digital Watermarks | Secure Read-Only Viewer | Secure Email and Attachments

Collaborate Securely

Automate Data Security Policies | Across Devices & Geographical Locations | Files, Messages & Chat | Control External Guest Acess | 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 on 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. Alternatively, use MPIP sensitivity labels or classification data from other tools and add dynamic access and protection policies.

DYNAMICALLY PROTECT DATA

Secure Data At Rest and In Motion

NC Protect leverages dynamic access and protection policies to ensure that only approved users can access and share your business content - at rest or in motion. Keep control of your sensitive information as it's accessed, used and shared across on-premises, in hybrid environments or in the cloud. Apply protection rules centrally or locally, ensuring compliance, while enabling IT to easily fine-tune rules.

Get Unique Data Protection Capabilities

NC Protect works natively with Microsoft collaboration and security products to enhance security with unique capabilities: enforce secure read-only access, hide sensitive files from unauthorized users, redact sensitive or classified information, trim the application ribbon, apply dynamic security watermarks, and automatically encrypt or restrict attachments sent through Exchange Email.

Encrypt When Required

Microsoft or NC Protect's proprietary encryption can be automatically applied when needed, and read/write privileges are automatically adjusted, so users can concentrate on the content rather than the policies governing collaboration. For added key management security and flexibility, the optional NC Encrypt module provides connectors to third party key management platforms so customers can easily leverage existing encryption investments.

REDUCES COMPLEXITY FOR FASTER RESULTS

Get granular security without the complexity of native tools to start securing content in hours, not days or weeks. NC Protect is agentless so there is no endpoint management, reducing IT overhead and the risks involved in implementing new cloud services or BYOD policies. The solution seamlessly integrates with Microsoft 365 (SharePoint Online, OneDrive, Office, and Exchange), SharePoint on-premises, NetApp ONTAP, Nutanix Files and Windows files shares to centrally manage data protection across all of your collaboration tools.

archTIS

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