NCPROTECT™

SIMPLE. FAST. DYNAMIC. DATA PROTECTION

TRADITIONAL SECURITY IS NO LONGER ENOUGH

In today's workplace, users can access data from a wide range of sources, including cloud collaboration platforms, on-premises repositories, and email. Consequently, data breaches caused by both negligent and malicious insiders are increasing and security incidents caused by insiders are hard to detect – often taking months.

The issue with many security technologies, including zero-trust tools, is that once you're inside the perimeter and have access to an application and file, you can freely share, copy, or download it. A reactive security approach is no longer sufficient, as simple user mistakes can be just as damaging to your bottom line if sensitive data is involved.

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. Fine-grained attribute-based policies ensure only the right people – access the right information – at the right time – enforcing zero trust principles at the data layer.

DYNAMIC, DATA-CENTRIC SECURITY FOR SECURE COLLABORATION

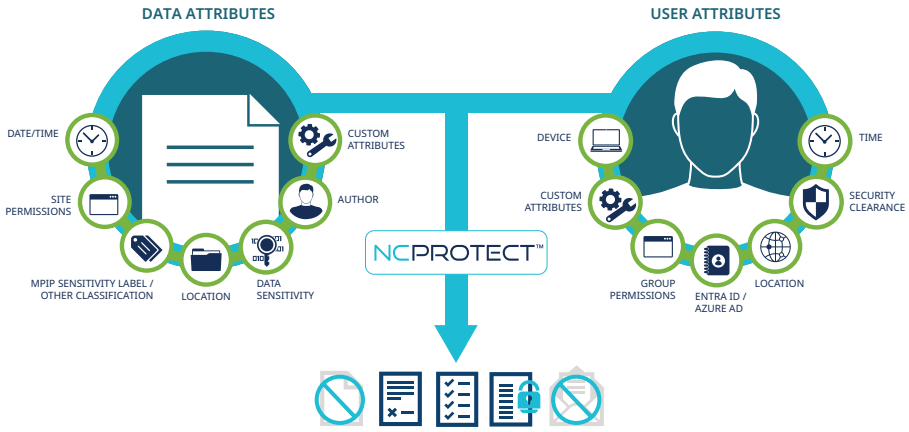
NC Protect classifies and secures unstructured data, including files and email. It dynamically adjusts access and security based on a real-time comparison of user and file context to ensure that internal and guest users access, use and share information according to your organization's policies.

Real-time attribute-based access and data protection policies evaluate the user's current context, blending traditional user permissions with 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.

It enforces your data access and security policies for each and every user, every time access to a file is requested and is completely transparent to the end user.

NC Protect integrates seamlessly into your Microsoft 365 and GCC High applications, including SharePoint Online, Office and Exchange, and on-premises applications, including SharePoint Server and Windows File Shares. It also supports other cloud storage tools, including Nutanix Files and NetApp ONTAP.

CONDITIONAL ATTRIBUTE-BASED ACCESS AND DATA PROTECTION



Real Time, Contextual Access and Protection Policies Determine:

If access to a file is approved or denied based on the policy and attributes	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

DYNAMIC, DATA-CENTRIC ACCESS, PROTECTION AND COMPLIANCE

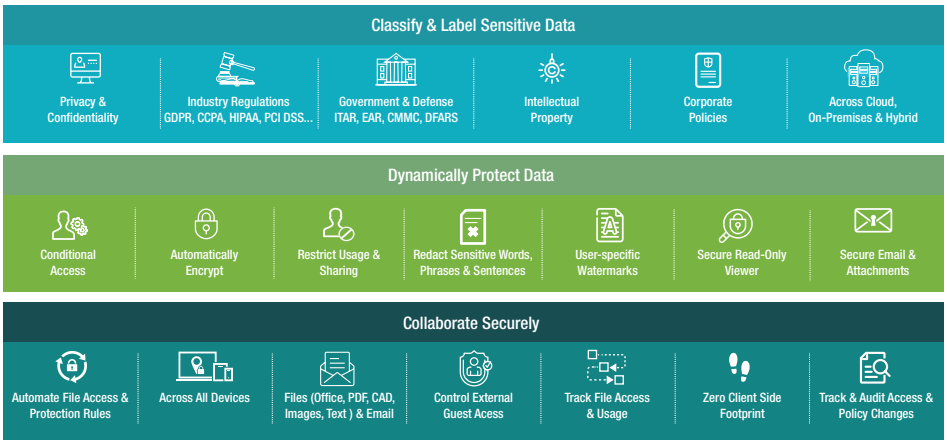
NC Protect ABAC policies dynamically adjust access and protection based on real-time analysis of file content/ sensitivity and user context to ensure that users view, use and share files according to your organization's regulations and policies.

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 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
- Hide files from unauthorized users
- Redact sensitive information
- Apply persistent user-specific digital security watermarks
- Manage your own encryption keys (BYOK)



CLASSIFY & TRACK DATA

Classify and protect sensitive data using one or multiple labels to meet complex taxonomies. NC Protect polices can also use and augment MPIP sensitivity labels or classification data from other tools. Use a single set of rules for your on-premises, cloud or hybrid environments. Define who can classify or reclassify data, unlike standard metadata that can be modified by anyone with file access. Track access to and actions taken with sensitive data, as well as policy changes.

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, apply dynamic user-specific security watermarks and automatically encrypt or restrict attachments sent through Exchange Email.

Dynamically Encrypt When Required

Automatically apply encryption with NC Protect policies using MPIP or NC Encrypt when needed. Read/write privileges are automatically adjusted, so users can concentrate on collaboration rather than the policies governing it. For added security and flexibility, the optional NC Encrypt module provides BYOK capabilities and connectors to third party key management platforms so customers can maintain control of their keys.

REDUCES COMPLEXITY FOR FASTER RESULTS

Get granular security without the complexity of native tools and 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. It seamlessly integrates with Microsoft 365 and GCC High (SharePoint Online, Office, Exchange), SharePoint Server, NetApp ONTAP, Nutanix Files and Windows files shares to safeguard all your data.

Member of Microsoft Intelligent Security Association

Microsoft Security Excellence Awards 2024 FINALIST archTIS Compliance & Privacy Trailblazer

archTIS

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