NCPROTECT™

DYNAMIC DATA DISCOVERY, CLASSIFICATION & SECURITY FOR NETAPP® ONTAP®

NetApp®

Executive Summary

NC Protect™ for NetApp® ONTAP® 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 regulations and policies.

NC Protect with ONTAP addresses the protection of information, dynamically at the data layer at the time of access. The combined solution provides a multi-faceted, 360-degree layered approach to protecting a customer's most important asset, data, that is accessed on Windows File Shares in ONTAP.

Key Benefits

Augments built-in ONTAP security functionality with the ability to:

- Automatically discover, classify, and restrict access to or encrypt files based on the presence of sensitive data.
- Control who can access files and how they can be used, copied and shared with dynamic fine-grain policies.
- Dynamically add custom security watermarks containing user or file attributes to sensitive or confidential Office docs and PDFs.
- Dynamically obfuscate/hide files from unauthorized users.
- Automatically encrypts sensitive files at rest and in motion.
- Enforce secure read-only viewing of sensitive/classified information with a built-in Secure Reader.
- Audits and tracks access to and usage of sensitive data to ensure transparency and compliance.

DATA PROTECTION IS CRITICAL

Organizations rely on data management platforms to store and collaborate on sensitive data. However, 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. It's time for a proactive data-centric approach to access and security.

DYNAMIC DATA DISCOVERY, CLASSIFICATION & SECURITY FOR ONTAP

archTIS NC Protect adds data-centric, dynamic policy-based access and security controls to NetApp ONTAP Windows File Share content. NC Protect enhances ONTAP Windows File Share data security with unmatched information protection capabilities to prevent accidental sharing, misuse and loss, while maintaining a simple and intuitive user experience that empowers customers to collaborate securely.

Discover and Classify Data

Automatically discover and classify files based on the presence of sensitive data including PII, PHI, IP and other factors. NC Protect's policy manager features predefined discovery rules for global privacy regulations. Easily define and configure custom checkpoints to match your organization's unique privacy, confidentiality and security policies.

Control Access and Sharing

The NC Protect solution dynamically controls access to business-critical content and restricts how authorized users can share it and with whom, based on real-time comparison of user context and file content to enforce data governance and security policies. NC Protect applies fine grain data security capabilities as the user accesses files, including dynamic watermarking, secure viewing and redaction and can automatically encrypt data if and when required. It audits access to and usage of sensitive data, and can initiate workflows and notifications in SIEM applications (Microsoft Sentinel and Splunk) to mitigate risk.

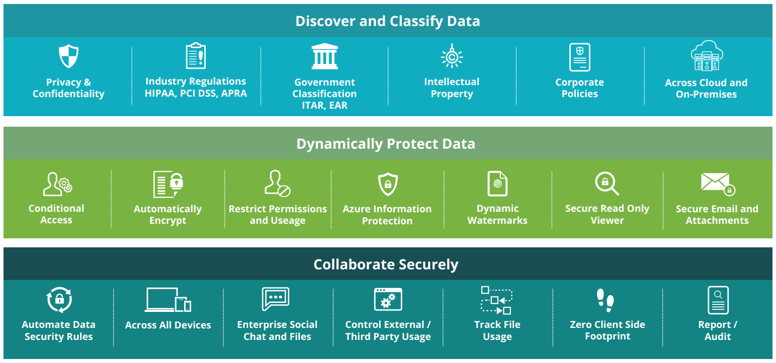
Reduces Complexity for Faster Results

A NetApp Technology Alliance Program Preferred Partner, NC Protect's NetApp field validated integration is transparent to end users when accessing their file data on Microsoft Windows shares running on an ONTAP system. It adds dynamic granular access and protection controls to the end user when reading or writing files with no impact on ONTAP data storage. NC Protect requires no client-side application, simplifying deployment and removing complexity.

KEY CAPABILITIES

NC Protect uses metadata-driven, file level security to restrict access to, encrypt, track and prevent unauthorized sharing of content based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection (DLP) capabilities for ONTAP Windows File Shares.

Organizations using ONTAP in addition to Microsoft 365 or SharePoint on-premises for file storage and collaboration can leverage the same NC Protect's rules across all of these platforms to centrally manage policies, classifications and access controls.



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 & CLASSIFY

NC Protect scans and inspects files for sensitive or regulated data (PII, PHI, HR, IP, etc.) according to defined policies. When detected, it can automatically classify the file and apply access controls and information protection based on its sensitivity and your policies.

Define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

RESTRICT ACCESS

NC Protect's attribute-based access control (ABAC) policies use data and user attributes (e.g., classification, geolocation, device, time of day), not data location, to determine access rights in real time. Access to a file can be restricted to a specific individual or group, even if a wider audience has access to the site or folder.

Granular security policies automatically restrict access to, sharing of and protection of content based on the policies and the context of the user at the time of access.

ENCRYPT

If a sensitive document that requires encryption is identified, NC Protect can encrypt the content immediately and limit the audience to only credentialed users. The contents of an email and any attachments sent through Exchange can also be encrypted automatically. Additionally, the optional NC Encrypt module offers key management and BYOK support.

PREVENT

Define rules in NC Protect to prevent the sharing of sensitive information or confidential documents within or outside of ONTAP to minimize accidental or malicious data loss and exposure.

HIDE SENSITIVE FILES

Dynamically obfuscate data to hide sensitive or confidential documents from unauthorized users in folders, chats and searches. Only users with access rights will be able to see that the content exists to minimize data exposure and the need to create multiple sites and channels to accommodate different access rights.

SECURE READER

Forced users to view sensitive documents in NC Protect's Secure Reader for read-only access. It prevents users from being able to download, copy, edit or print sensitive data.

DYNAMIC WATERMARKS

Dynamically add security watermarks and CUI markings customized with user and/or file attributes to sensitive and confidential Word, PowerPoint, Excel, PDF and image files for security and auditing purposes. Watermarks can incorporate attributes such as user name, email, time and date that the file was accessed. They deter users from taking photos and create a digital thumbprint for tracking and forensics purposes.

REDACTION

Remove/redact sensitive or confidential information, such as keywords or phrases, in a document when viewed in its native application (Word, Excel, PowerPoint and PDF) or when the file is presented in the Secure Reader for legal or security purposes.

AUDIT & REPORT

Provides centralized reporting on classified data and user activity logs. Report on the number of issues identified by classification level, review scan results and rescan, reclassify or reapply permissions if needed. Integrate user activity and protection logs with Splunk and Microsoft Sentinel for further analysis and downstream actions.

ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED POLICIES

archTIS' granular data-centric approach to security enforces a zero trust methodology through conditional, attribute-based access control (ABAC) and data protection at the item-level. Since access and protection policies are applied to individual files 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 any ONTAP Volume. NC Protect ensures access to the file is restricted to only those who have permissions to it and applies real-time file protection as defined by the policy.

archTIS

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