NC PROTECT: ADDING VALUE TO MICROSOFT SECURITY INVESTMENTS

Enhancing Microsoft Security with One of a Kind Features for Simple, Fast and Dynamic Information Protection

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Customers heavily invested in Microsoft solutions often wonder how other partner products can enhance or provide advantages over Microsoft's security capabilities.

Enterprise platforms, including Microsoft's, deliver a wide range of applications to provide business-critical capabilities and rich functionality to customers. However, it is impossible for one vendor to successfully provide the full depth and range of capabilities that is often needed to satisfy every customer requirement. For this reason, value-added resellers and independent software vendors (ISVs) have long played a prominent role in the information technology (IT) industry, providing additional capabilities to augment core product functionality.

Microsoft has developed a large partner ecosystem of complementary third-party vendors to enhance the capabilities of their products and fill in any gaps. While there can be some overlap in capabilities, these third-party products generally enrich and enhance the customer experience, thereby increasing the value of their Microsoft investments. One such solution is archTIS' advanced information protection and compliance solution, NC Protect.

This brief highlights the complementary nature of NC Protect and the additional value and capabilities it provides Microsoft customers with.

Enhancing Microsoft Security Investments Through Partners

archTIS is part of the Microsoft ecosystem of validated ISV partner technologies. NC Protect is built on the Microsoft stack, which enables customers to improve their existing Microsoft security investments with minimal impact and further increase ROI. As a Microsoft Partner, we closely work with Microsoft's product groups to extend and enhance their out-of-the-box (OOTB) capabilities. Our aim is to provide customers with more specialized, integrated information protection in Microsoft collaboration applications.

The complementary nature of our solution is why we were honored to be among the first partners invited to join the Microsoft Intelligent Security Association (MISA). MISA is a select group of Microsoft premier security partners—independent software vendors (ISVs) and managed security service providers (MSSPs) that have integrated their solutions with Microsoft Security products.

Our membership, which required us to technically validate our integration with Microsoft's products, underscores the credibility and value of our solution, NC Protect.

Better Together

archTIS is a member of the Microsoft Intelligent Security Association (MISA), an ecosystem of premier Microsoft partners that have integrated with Microsoft security products to better defend customers against cyber threats.

Member of
Microsoft Intelligent Security Association
Microsoft Security

Microsoft Partner

HOW NC PROTECT ENHANCES MICROSOFT SECURITY

NC Protect is a powerful product that can improve and expand the existing information security capabilities of Microsoft. With its advanced features, NC Protect can enhance the out-of-the-box functionality of Microsoft's security tools, enabling businesses to better protect their sensitive information and prevent data breaches.

From a technology standpoint, NC Protect is built from the ground up to provide data-centric protection, instead of the application layer security that Cloud Access Security Brokers (CASB), which Microsoft Defender for Cloud Apps is categorized as, were originally designed for.

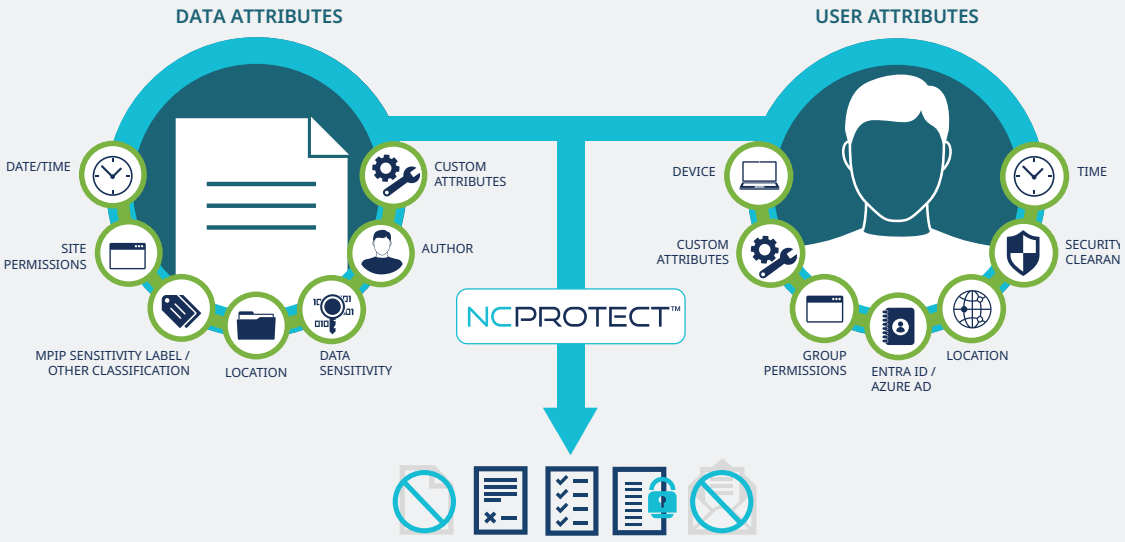
Over time, CASB solutions, Defender for Cloud Apps included, started to add some data-centric features, often through technology acquisitions. The additions were needed because application layer security capabilities do very little to protect against insider threats, the security issues stemming from negligent or malicious trusted users, that data-centric solutions are designed for.

These enhancements, however, can make information protection considerably more complex to manage. This is because CASBs and Defender for Cloud Apps use a multi-layered 'outside-in' security approach, applying protection from the application layer down to the data. This frequently requires one process for evaluating user attributes at the data container or application layer and a separate process or technology for consideration of data attributes, both of which must be carefully coordinated to apply protection correctly.

For example, Microsoft Defender for Cloud Apps can use Microsoft Purview Information Protection (MPIP) to apply sensitivity labels to files as a file policy governance action. Depending on the label configuration, it can also apply encryption for additional protection.

It is easy to understand why, when you look at the high-level capabilities of NC Protect and the Microsoft solution set, particularly Defender for Cloud Apps combined with MPIP, the solutions seem similar. However, when you start to see the two products in action the differences become apparent.

NC PROTECT OFFERS DYNAMIC, GRANULAR INFORMATION PROTECTION



Data-Centric, Attribute-based Access and Data Protection

archTIS has developed a unique solution for adding fine-grain policy-based attribute-based access control (ABAC) and protection to Microsoft 365 and GCC High content, as well as SharePoint Server and Windows File Shares. Access and protection policies are based on data and user attributes to achieve more granular protection in a much simpler way.

Classify your data with NC Protect or use your existing sensitivity labels along with any combination of attributes to control access and apply protection policies. NC Protect ingests Microsoft Entra ID (formerly Azure Active Directory) user attributes, environment attributes (e.g. device, location, connection), Microsoft Purview Information Protection (MPIP) sensitivity labels, other classification labels/metadata and custom attributes to apply conditional attribute-based access and data protection policies. Policies are run in real-time at the time of access each and every time a file is accessed, extending zero trust principles to the data layer.

NC Protect extends Microsoft access and protection capabilities, offering customers a more robust solution for tackling sensitive data handling requirements to meet government, defense and enterprise needs.

Centralized Policy Management

NC Protect also simplifies information security management in Microsoft with centralized policy management. With NC Protect's policy engine, you can centrally configure the attributes of data, files, and sites (such as SharePoint, OneDrive, and Exchange emails), and the corresponding access and protection rules. This helps you to easily manage and consistently apply your organization's security policies.

To get similar levels of information protection OOTB requires separate configuration of Entra ID Conditional Access policies, MPIP label policies and Defender for Cloud Apps policies, in disparate administration interfaces. Care must also be taken to ensure that the separate policies work together without causing conflicts.

NC Protect allows multiple factors to be built into a single rule to meet the requirements of a given scenario using dynamic attribute-based policies that automatically adjust access and security based on the conditions. These conditional rules can then be stack ranked together, resulting in far fewer configuration steps and rules.

With Defender for Cloud Apps, separate policies, each with associated AD CA and MPIP policies, are needed. There is also no concept of stack ranking for them to work in concert. This means that every condition for a scenario must be addressed separately, resulting in many more rule configurations and associated ongoing administration overhead.

NC Protect's dynamic, attribute-based methodology not only eliminates natural rule conflicts but empowers IT and security teams to deploy policies quickly and easily.

Control Access by Geolocation or Nationality

Data sovereignty and Defense regulations often require data segmentation based on geography or nationality, which can be challenging using native Microsoft tools. They often require restricting access to and collaboration of specific types of information between individuals or groups of individuals, including but not limited to intellectual property (IP), regulated data including personally identifiable information and healthcare information (PHI), defense information and more.

NC Protect's ABAC-based policies can control access to individual files and apply different file-level protections based on the user's location and/or nationality as well as the file's sensitivity. It can also hide files in the application user interface (UI) so users only see files that they are authorized to access. NC Protect makes it safe to store data in a single site by dynamically enforcing information barriers.

Extend File Protection to Non-Microsoft Documents

Today's unstructured data comes in many forms and Microsoft security tools are limited to Office documents (Word, Excel, PowerPoint) and PDFs. NC Protect can protect a wide range of file types to ensure all of your files, including Office, PDF, CAD, text, html and image files, and SharePoint list items are protected using the same dynamic protection policies and controls.

Multi-label Support and Unlimited Security Labels

Companies with an Office 365 Enterprise E3 or Office 365 Enterprise E5 license can apply Microsoft Purview Information Protection sensitivity labels to their Office files and emails. While sensitivity labels are incredibly versatile, there are some limitations:

- If your taxonomy requires more than a single label or your organization works with government and defense. Defense contractors must often augment out-of-the-box labeling and protection capabilities to satisfy their internal requirements and those for Controlled Unclassified Information (CUI), ITAR and other complex government and defense data protection mandates.
- If files have been digitally signed (for example, by DocuSign), applying an MPIP label will break the integrity of the file, and it will no longer be considered "signed."
- If files need different protections for at-rest, managed devices, BYOD, and guest users.
- If data sovereignty or ownership is critical to an organization. Microsoft must comply with the rules of the U.S. jurisdiction and release information to the U.S. government when requested.

NC Protect enhances your existing Microsoft sensitivity labels with additional capabilities to:

- **Create Unlimited labels.** Although Microsoft Purview technically allows for the creation of unlimited sensitivity labels, if the label applies encryption that specifies the users and permissions, there is a maximum of 500 labels per tenant. This is problematic for organizations in Defense and other regulated industries, which often quickly exceed this limit. NC Protect allows you to add unlimited additional labels to meet your classification needs while still allowing you to use your existing MPIP labels.
- **Use multi-label classification.** MPIP supports one label per document, which can be problematic if the data is associated with two or more categories. With NC Protect, you can tag documents with unlimited multi-labels to support complex taxonomies.
- **Apply ABAC using sensitivity labels.** NC Protect uses attribute-based access control to control access and apply file and email protection in real time. Your existing sensitivity labels can be incorporated along with any combination of attributes to control access and apply protection with NC Protect policies.

Auditing and Threat Management

Auditing and reporting are key requirements for information security and compliance, particularly for customers that leverage some of the decentralized capabilities. NC Protect includes full auditing capabilities of user activity in supported Microsoft 365 apps that can be consumed in several ways. It also records when protection rules are changed or deactivated and when rules have prevented an activity like an unauthorized user from accessing a file.

Logs can be integrated with SIEM tools, including Microsoft Sentinel and Splunk, to trigger alerts and take further action as needed to better assist IT with the overall security and management of Microsoft applications.

NC Protect also includes a comprehensive permission scanning capability to show the at-rest permissions overlaid with the additional protection provided by NC Protect. The combination of these auditing and reporting capabilities provides everything that auditors would need for compliance, and helps IT troubleshoot user file access issues.

NC Protect can also change at-rest permissions to automatically correct any security gaps with permissions. In other words, its protection policies can both prevent data leaks from incorrectly configured permissions and subsequently correct the permissions issue in a single step. While Microsoft certainly has auditing capabilities, the combined permissions reporting, auditing and automatic permissions correction of NC Protect greatly simplifies these administration tasks compared to OOTB tools.

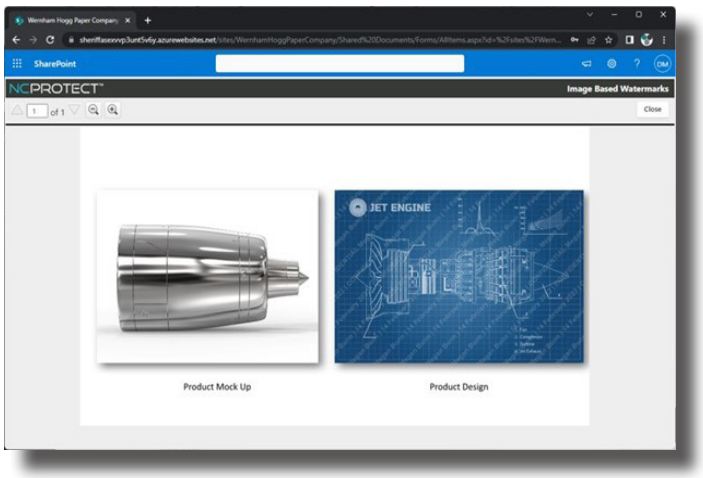
NC PROTECT'S UNIQUE DATA-CENTRIC SECURITY FEATURES

NC Protect offers several unique security capabilities to further safeguard against data loss, misuse and accidental sharing. NC Protect not only controls who can access information, but what users can do with it and who it can be shared with once access is granted.

Dynamic User-based Security Watermarks

While Microsoft offers watermarking capabilities, it is limited to the document creator's information. NC Protect can dynamically add user-based security watermarks containing the user's information and other attributes to sensitive and confidential Word, PowerPoint, Excel and PDF files at the time of access for security and auditing purposes.

When an employee views or downloads a document, NC Protect will automatically watermark the document and/or sensitive images within it with the employee's name, date,



time, client name, and any other data required by your organization as can be seen in the screen shot below.

Watermarks are automatically applied in the native application (e.g., Word, PowerPoint, Excel) or in the Secure Reader when enforcing policies for read-only access. For security and auditing purposes, users can share and edit watermarked document contents but not the watermark itself.

User-based watermarks offer several advantages. They supplement user education and training on the safe handling of sensitive or proprietary information, providing a visual reminder of their responsibilities regarding the protection of the data.

Additionally, by having a personalized security watermark in the body of the document, the user is deterred from taking a picture with their mobile device, sharing it in an unauthorized manner or using it for malicious purposes. This helps reduce data loss and misuse and aids in forensic investigation in the event of a data leak.

File Obfuscation

Define rules in NC Protect to hide files from unauthorized users. While other solutions can encrypt and control access to files, they remain visible to all users regardless of their access rights. Obfuscating files minimizes the risk of data exposure and loss.

For example, if a file is added to a site and a member does not have proper access rights to that category of document, then the file is hidden from the view of the unauthorized individual. Only authorized users will be able to see the document. That means two users can have competently different views of the same site based on their permissions. In addition to preventing data loss, it also minimizes the need to create multiple sites and channels to accommodate different access rights.

Secure Reader for Web-based Read-only Access

For additional security, users can be forced to view sensitive documents in NC Protect's Secure Reader. The web-based viewer enforces read-only access and prevents users from being able to download, copy or edit sensitive data. When combined with NC Protect's dynamic watermarks it also deters users from taking photos of content to circumvent security. In the event of data loss, the personalized watermarks act as a digital thumbprint for tracking and forensics purposes.

Encrypt Files and SharePoint Columns Dynamically

When paired with MPIP or NC Encrypt, NC Protect policies can automatically encrypt:

- Sensitive documents to limit the audience to only authorized users with proper credentials.
- The contents of an email and attachments sent through Exchange based on the policy, content or file sensitivity.
- SharePoint list columns values based on predefined policies and data sensitivity; a capability not offered in Microsoft natively.

NC Protect helps extend your MPIP investment and encryption options.

Key Management and BYOK for M365

Pairing NC Protect with the NC Encrypt add-on module offers dynamic encryption capabilities and Bring Your Own Key (BYOK) for M365. It's the perfect solution for organizations that prefer to maintain control of their encryption keys in the Cloud to maintain data sovereignty.

It provides exclusive, customer-only control of encryption keys for M365 (a Microsoft-controlled environment) and enables keys to be stored in specific geographical locations for data sovereignty and compliance.

Use NC Encrypt's dynamically created keys or supply and manage your own keys. NC Encrypt has the option to integrate with third-party key management platforms using Thales CipherTrust Manager, which provides connectivity to VSMs and HSMs. Linking CipherTrust Manager to NC Encrypt provides an innovative solution that allows you to manage your encryption key processes independently in CipherTrust Manager while managing your dynamic encryption and access control policies in NC Protect.

Information Barriers

NC Protect provides capabilities for the configuration and enforcement of information barriers, as well as controlling data access within their Microsoft collaboration environment. It provides the following add-on capabilities using existing Microsoft investments that many organizations have, such as MPIP and Entra ID to:

- Restrict specific types of collaboration between users/groups, but with enough flexibility to allow other types of communication.
- Control access in line with business rules for users from different operating companies or geographical regions beyond sole reliance on permissions.
- Automatically secure access to content based on the creator of that content. For example, files created by an SVP or higher are restricted to users at that level of the organizational hierarchy or above.
- Provide the data governance needed to control External/Guest access.

Redaction

NC Protect can dynamically redact sensitive or confidential information when viewed in its native application (Microsoft Office and PDF) or when a file is presented in the NC Protect Secure Reader.

Redact sensitive document content such as words, phrases and values from Word, Excel, PowerPoint and PDF documents based on defined policies. For example, a user needs to access a specific document, however it contains a credit card number they are not authorized to see. NC Protect can redact the credit card number and only show the portions of the document that the user has permission to view.

NC Protect's redaction capabilities safeguard your company's confidential and regulated data, help manage governance and meet compliance requirements.

Visual Markings for Defense Documents

Several defense regulations, including CMMC, ITAR, and DFARS, govern the secure collaboration of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) and require the application of visual markings. NC Protect can embed the required CUI Designation Indicator markings, including Owner Name, Controlled By, Category, Distribution/Limited Dissemination Control and POC, as well as headers/footers into documents as a persistent watermark to meet compliance.

BETTER TOGETHER: MICROSOFT SECURITY & NC PROTECT

NC Protect enhances the security capabilities across your Microsoft collaboration tools to deliver comprehensive, data-centric access control and protection. It has been recognized as a finalist for the Microsoft Security Compliance and Privacy Trailblazer Award in 20023 and 2024. The awards are a testament to archTIS' continued commitment as a Microsoft Partner to integrate our ABAC policy-based approach with Microsoft security products to provide unparalleled solutions to safeguard sensitive data in Microsoft applications. With NC Protect and Microsoft, you can rest assured that your data is secure and protected at all times.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9, OTCQB:ARHLF) is a global provider of data-centric software solutions for the secure collaboration of sensitive information. The company's award-winning information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute-based access and control (ABAC) and data protection policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, SharePoint on-premises, NetApp ONTAP, Nutanix Files and Windows file shares. For more information visit archtis.com.

archTIS.com | info@archtis.com

Australia | United States | United Kingdom