NC PROTECT: ADDING VALUE TO MICROSOFT INVESTMENTS

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

archTIS

TABLE OF CONTENTS

Better Together

Nucleus Cyber is a member of the Microsoft Intelligent Security Association (MISA), an ecosystem of ISVs that have integrated with Microsoft's solutions to better defend against a world of increasing data exposure.

Member of
Microsoft Intelligent Security Association
Microsoft

Microsoft Partner

EXECUTIVE SUMMARY

Customers often wonder if they are heavily invested in Microsoft solutions and tools, how do other partner products enhance or provide advantages over Microsoft's core capabilities?

Enterprise platforms, including Microsoft's, deliver a wide range of apps to provide business-critical capabilities and rich functionality to their 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.

It is for this reason Microsoft has developed a large partner ecosystem of complementary third party vendors that fill in any gaps and enhance the capabilities their products provide. While there can be some capability overlap, these third-party products generally enrich and enhance the customer experience and the value of their Microsoft investments. archTIS' advanced information protection and compliance solution, NC Protect, falls into this category.

This Solution Brief highlights the complementary nature of NC Protect, as well as the value and additional capabilities it provides Microsoft customers.

Enhancing Microsoft Information Security Investments

archTIS' solutions are part of the Microsoft ecosystem of validated third party partners and technologies. NC Protect is built on the Microsoft stack, therefore, it allows you to make even better use of your existing investments in Microsoft and further boost your ROI. As a Microsoft Partner, we work closely with Microsoft's security product groups to extend and enhance their out-of-the-box (OOTB) capabilities to provide customers with more tailored information protection in Microsoft apps.

The complementary nature of our solution is why we were invited to become one of the first partners to gain membership into the Microsoft Intelligent Security Association (MISA), an ecosystem of ISVs that have integrated with Microsoft's solutions to better defend against a world of increasing data exposure.

Our membership, which required us to technically validate our integration with Microsoft's products, recognizes NC Protect for the value it provides to customers beyond the OOTB Microsoft solution.

HOW NC PROTECT ENHANCES MICROSOFT INFORMATION SECURITY CAPABILITIES

There are several areas where NC Protect enhances and extends the OOTB functionality of Microsoft's information security capabilities.

Data-Centric Information Protection

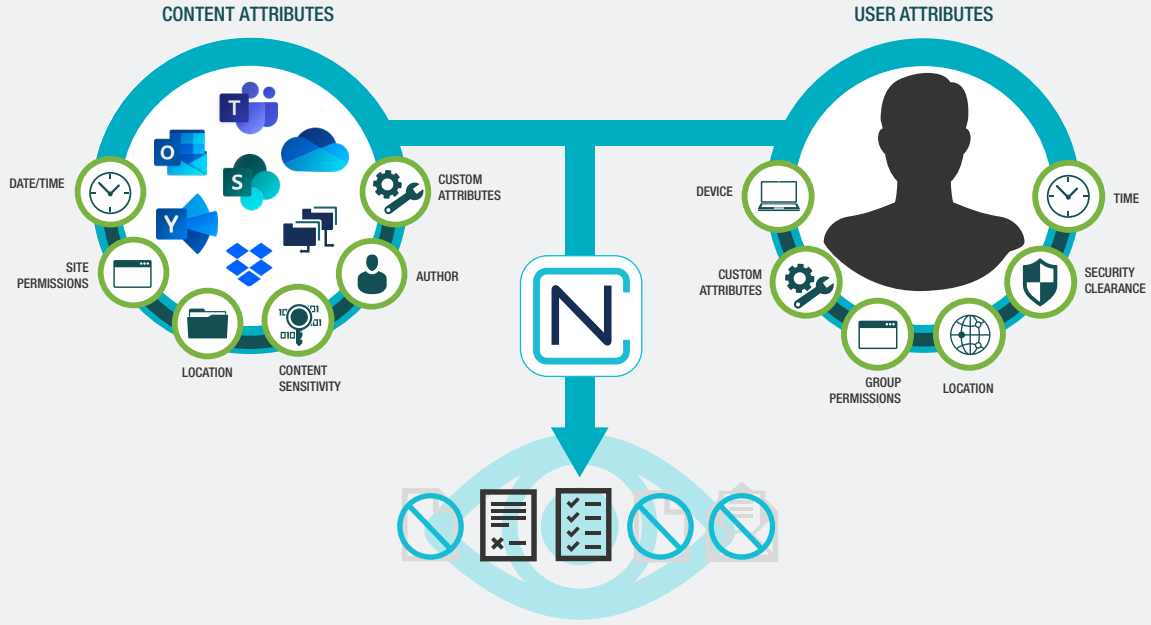
From a technology standpoint, NC Protect was built from the ground up to provide data-centric protection, as opposed to the application layer security that Cloud Access Security Brokers (CASB), which MCAS is categorized as, were originally designed for. Over time CASB solutions in general, MCAS included, 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 MCAS 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.

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

NC Protect approaches security from the 'inside-out' – focusing on all the different attributes at the data layer to achieve more granular protection in a much simpler way. This approach eliminates the complexities of the outside-in approach used by MCAS and other CASBs and provides a simpler way to tailor information protection against insider threats.

NC PROTECT OFFERS DYNAMIC, GRANULAR INFORMATION PROTECTION



NC PROTECT ENHANCES NATIVE SECURITY

Ease of Use

Ease of use is another area where NC Protect's data-centric approach highlights the differences between the two approaches. NC Protect allows you to configure the data, file, and site attributes (Teams, SharePoint, etc.) and the associated protection rules from a single location. In order to get towards similar levels of information protection OOTB requires separate configuration of Active Directory Conditional Access (AD CA) Policies, MIP Label Policies and MCAS 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 conditions to be built into a single Protection Rule to meet the requirements of a given scenario. These can then be stack ranked together which results in far fewer configuration steps and rules. With an MCAS approach separate polices each with associated AD CA and MIP policies are needed and there is 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. This methodology not only eliminates natural rules conflicts but empowers IT and security teams to deploy the solution quickly and easily – protecting your information in a matter of hours, not days or weeks.

Separation of Roles

With other solutions, centrally applying accurate information protection to intellectual property or other sensitive data to meet the evolving business needs of individual Teams would require intensive feedback loops or high volumes of support tickets.

NC Protect can provide separation of roles for configuring or applying rules across SharePoint sites and Teams. NC Protect's User Interface can, if desired, be surfaced directly within an individual Team enabling Team owners to activate or adjust centrally configured rules as appropriate for their Team. This reduces information security risk by giving Team owners a better understanding of the content within their Teams, something that fixed, centrally applied rules can miss.

A completely centralized approach also often results in overly restrictive controls that drive users to seek Shadow IT solutions to work around those restrictions therefore exposing the organization to even greater levels of risk. Giving Team owners the ability to adjust the rules to fit the Team's collaboration and security needs with NC Protect reduces user frustration that drives them to seek out unsanctioned tools to get their jobs done.

Auditing and Reporting

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.

NC Protect integrates into 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 Teams. The auditing includes recording when protection rules are changed or deactivated and when rules have prevented an activity like an unauthorized user accessing a file.

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.

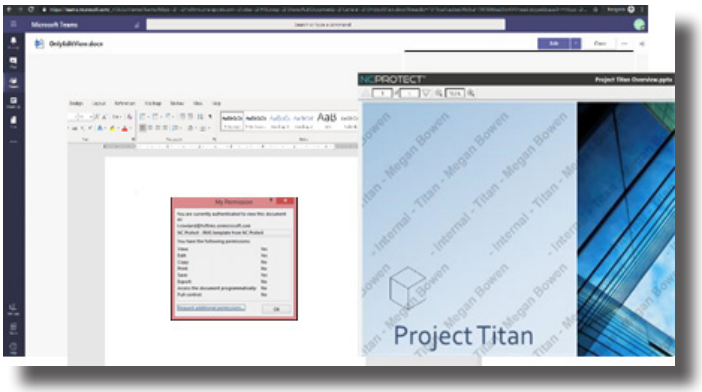
NC PROTECT OFFERS UNIQUE SECURITY FEATURES

In addition to enhancing Microsoft OOTB security, NC Protect offers several unique security capabilities to provide advanced information protection capabilities to further safeguard against data loss, misuse and accidental sharing.

Dynamic Security Watermarks

NC Protect can dynamically add a custom security watermark containing user or file attributes to sensitive and confidential Word, PowerPoint, Excel and PDF for security and auditing purposes. NC Protect watermarks can incorporate attributes such as the user's name or email and the time and date that the file was accessed, as can be seen in the screen shot below.

Dynamic Security Watermarks supplements user education and training relating to the safe handling of sensitive or proprietary information providing users with a very impactful and personalized visual reminder of their responsibilities relating to 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 and sharing in an unauthorized manner or using it for malicious purposes helping reduce data loss and misuse.

File View Augmentation

You can also define rules in NC Protect to prevent the viewing of sensitive information or confidential documents by unauthorized users to minimize the risk of data loss. This differs from other solutions that can encrypt and control access to files but leave them visible to all users regardless of their rights to fully open a view the content. 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. This help prevent data loss and minimize the creation of sites and channels to accommodate different access rights.

Secure Web Reader

Additionally, Users can be forced to view sensitive documents in NC Protect's secure web viewer for read-only access. This prevents users from being able to download, copy or edit sensitive data. Combined with dynamic watermarks it also deters users from taking photos of content, placing a digital thumbprint on the document for tracking and forensics purposes.

ADVANTAGES FOR MICROSOFT TEAMS ADOPTION

For Microsoft Teams users there are some key benefits that NC Protect delivers to enhance the security provided by OOTB capabilities.

First, NC Protect includes features that automatically apply protection policies to existing and newly created Teams and the content within them based on the data and user attributes within Teams. For example for any Team that includes Guest (External) users a set of protection policies can be applied to prevent data breaches by hiding files or chat content from the Guest user or applying encryption and usage rights to files to prevent the Guest user from sharing with unauthorized users.

NC Protect also provides additional capabilities that allow an IT Admin to define and configure policies centrally that are applied to a Team with the option to allow Teams Owners to choose to apply those rules, edit those rules to the specific need of their Team or set the central rules as “Read Only” and allow Owners to create additional rules.

This set of capabilities will allow organizations to avoid the compromises that often have to be made with Teams such as whether to completely block external access or concerns about lack of insight and control of the type of information being shared within a Team. Allowing Team Owners to apply additional rules ensures risks from Insider Threats can be completely cut off as a higher degree of granular control can be achieved than with solutions that only IT Admins have access to configure and apply. This is particularly important for preventing data breaches within chat content.

Advanced Information Barriers

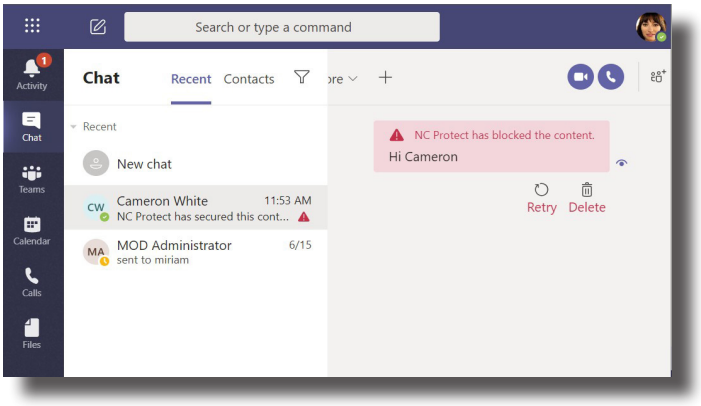
Collaboration tools have quickly expanded the need for restricting collaboration of other types of information between individual or groups of individuals including but not limited to intellectual property (IP), regulated data including personally identifiable information and healthcare information (PHI), and more. The advanced information barriers provide a greater level of simplicity and flexibility than OOTB tools, that only completely cut off communications between these groups.

For example, if you’re using Teams for company wide communications, and barriers are set-up between your traders and marketing teams, then your traders can’t receive the information because the policies say no communication is allowed between these two groups. The context of the communication isn’t considered, it simply creates a wall between these two groups.

The other limitation is that enabling OOTB Information Barriers in O365 requires Microsoft E5, E5 Compliance, or E5 Insider Risk Management subscriptions. And while many companies can benefit from information barriers not every organization may be able to immediately upgrade their current subscription to access this useful, and in some industries mandated, capability.

NC Protect provides capabilities for the configuration and enforcement of information barriers, as well as controlling business data within their Microsoft collaboration environment. It provides the following add-on capabilities using existing Microsoft investments that many organizations have such as Azure Information Protection and Rights Management to:

- Restrict specific types of collaboration between users/groups, but with enough flexibility to allow other types of communication.
- Granularly control of blocking of chat or files within Teams without complex rules.
- 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 e.g. files created by an SVP or higher is restricted to users at that level of the organizational hierarchy or above.
- Provide the data governance needed to control External/Guest access in Teams.



Third Party Sharing

NC Protect eliminates the need to create separate Teams for guests to control access to specific types of content. Instead, NC Protect automatically controls what content guests can see in a Team based on their user attributes, making guest access simpler to manage and more secure. For example, content that is marked “internal use only” can be hidden from guest users in the Team so they only see files they are permitted access to within the Team.

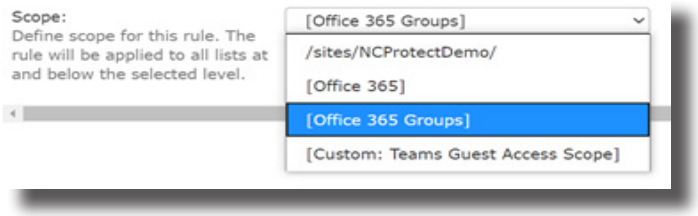
IT Friendly Private Channels

IT Friendly Private Channels provide the ability to simplify the creation and management of private channels that restrict access to specific individuals within a Team. NC Protect restricts private channel access based on user attributes without increasing the number of site collections in SPO to support those channels. It reduces admin overhead over time associated with managing large numbers of site collections and simplifies backup and life cycle tasks.

Security Scopes

Security Scopes are a set of information protection rules in NC Protect that can automatically be applied to Teams based on the team member, chat or file content and context to prevent accidental data leaks.

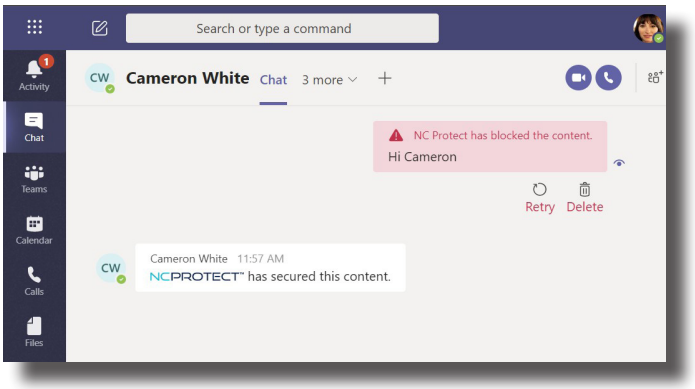
They automatically apply rule sets to multiple Teams or sites as content or member attributes change. For example, if a guest user is added, a Team is automatically moved to a new scope, applying appropriate rules based on the new membership.



Enhanced Chat Blocking

NC Protect can block chat messages in real-time that contain sensitive information, personal information (PII, PHI), payment data, inappropriate content or language, and apply information barriers in Teams to enforce policies for information security and regulatory compliance in chats.

Additionally, if new rules are added to block chat data, any existing conversations with data matching the new rule will retroactively remove the data to ensure the entire chat history is appropriately secured. Other solutions, including OOTB tools, only lock existing chat messages as read-only and block any subsequent messages.



Member of
Microsoft Intelligent Security Association
Microsoft

Microsoft Partner

SUMMARY

As a Microsoft Partner and MISA member, NC Protect leverages and enhances the OOTB security in Microsoft apps to provide integrated, granular, and dynamic information protection, while alleviating the complexity of achieving these results with native tools. For companies needing multifaceted information protection to meet business and regulatory requirements NC Protect provides a complementary solution that adds value to your Microsoft stack making it easier and faster to achieve results, improve information security and ensure compliance.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric 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) 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, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS.com | info@archtis.com

Australia | United States | United Kingdom