

NC PROTECT™

ADVANCED INFORMATION PROTECTION FOR MICROSOFT TEAMS®

Executive Summary

Ensure that your organization's business-critical data is being used and shared according to your business regulations and policies.

NC Protect provides advanced information protection of both chat and file content within Microsoft Teams simpler, faster and cheaper than native tools.

NC Protect provides conditional access control without the overhead of complex user permissions, poorly applied at-rest encryption, and expensive license upgrades to ensure that your information is protected in real-time across all collaboration scenarios. Restrict usage of and hide content based on multiple attributes including data classification, user location, device and access rights, and automatically encrypt files when they leave Teams or other Office 365 applications using NC Protect.

Key Benefits

- Jumpstart security with just a few clicks using built-in rule sets
- Enable private chats and file sharing within teams
- Apply security scopes to teams as they are created or apply to an existing team(s) or site(s) at once
- Identify and protect sensitive information being shared via Teams
- Automatically adjusts protection based on file and user attributes
- Create flexible Information Barriers
- Only encrypt data when the scenario requires as per policy
- Hide sensitive content in the Teams UI from unauthorized users
- Granular information protection at the chat, channel and file level

GREAT FOR COLLABORATION, PROBLEMATIC FOR DATA SECURITY

With over 115M users, the ability to quickly share information via built-in chat and file sharing capabilities has rapidly made Microsoft Teams (Teams) a key collaboration app for organizations. However, the speed and simplicity of creating new teams presents a challenge for IT and security groups tasked with ensuring business-critical information is properly protected.

The impact of not having the right information protection in place can be disastrous when you consider employee collaboration messages are 144% more likely to contain confidential information, 165% more likely to contain identification numbers and 6% more likely to contain passwords.¹

User managed tools like Teams make it even harder to keep track of data and ensure that business sharing and usage policies are being followed.

Advanced Information Protection for Teams

NC Protect offers a simpler, faster and cheaper way to ensure secure collaboration in Teams. NC Protect dynamically adjusts access to and protection of chats, channels and files shared in Teams based on user and file attributes to control what users can see, how they can share information and with whom. Get granular security with less time and effort or the need for upgraded licensing.

NC PROTECT REDUCES COMPLEXITY FOR FASTER RESULTS

Simpler

NC Protect is built on and leverages existing Microsoft security investments to get advanced information protection without the complex and time consuming administration experience of native tools. Benefit from advanced features like dynamic watermarks, secure viewers, and flexible information barriers not available out of the box.

Faster

With NC Protect start securing content in hours, not days or weeks. It requires no additional client-side application simplifying deployment and reducing the time that your content is at risk. Built-in rule sets allow team owners to set security with just a few clicks. Centrally manage access and usage across the suite of Microsoft 365 applications using the same rule sets to reduce admin overhead and resources needed to manage sites and applications.

Scalable

NC Protect enhances and adds value to your existing Microsoft investments. It allows you to get advanced information protection capabilities that are extensible across Microsoft 365 apps, SharePoint on-premises, Windows file shares, Dropbox and Nutanix Files. NC Protect's seamless integration with the Microsoft suite is vetted by the Microsoft Intelligent Security Association.

¹ Dark Reading <https://www.darkreading.com/vulnerabilities---threats/insider-threats/insider-dangers-are-hiding-in-collaboration-tools/d/d-id/1332155>

ENHANCE INFORMATION PROTECTION IN MICROSOFT TEAMS

SET SECURITY WITH JUST A FEW CLICKS

Empower team owners to set team and channel security using built-in rule sets to control internal and guest access to and information protection in teams and channels with just a few clicks from the NC Protect Tab in the Teams UI. Default rules can be customized to match your requirements.

INFORMATION BARRIERS

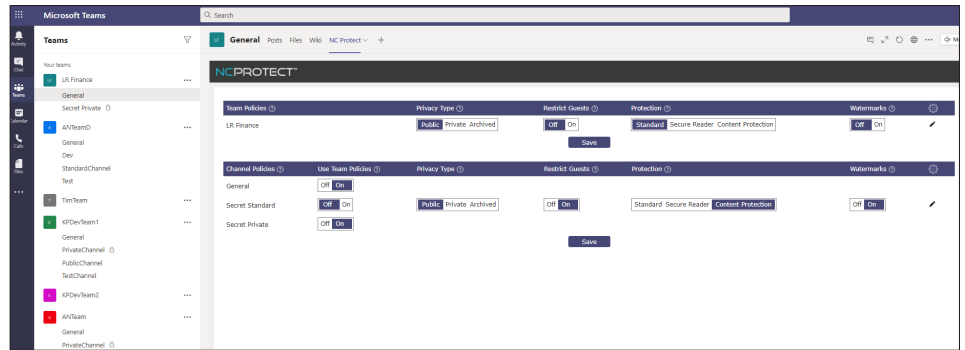
Out of the box Information Barriers completely cut off all communication and collaboration between users or groups of users. NC Protect's flexible Information Barriers allow users to communicate and collaborate on permitted projects or topics, while simultaneously preventing unauthorized or accidental sharing of specific types of information between parties (e.g. insider information).

IT FRIENDLY PRIVATE CHANNELS

Simplify the creation and management of private channels with the ability to toggle privacy settings on and off as required. With no additional site collection needed, it reduces admin resources associated with managing multiple site collections and simplifies backup and life cycle tasks. Preserves eDiscovery in private channels for legal and compliance purposes.

SECURITY SCOPES

Security Scopes are preconfigured information protection rules that can be applied to Teams based on the team member, chat or file content and context to control access and protect data. They automatically apply rule sets to one or multiple teams or sites when they are provisioned, or as content or member attributes of an existing team changes.



Above: The NC Protect Tab in the Teams UI enables a team's owner to easily select and apply default information protection rule sets.

BLOCK CHAT CONTENT

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

SECURE WATERMARKS & VIEWER

NC Protect works natively with Microsoft collaboration and security products to augment native features for enhanced security. Force documents to be opened as read only in a Secure Reader, apply personalized watermarks, and encrypt or restrict attachments sent through Exchange Email.

STOP ACCIDENTAL SHARING

Users can be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of the team based on the document's attributes and sensitivity to prevent accidental sharing and oversharing.

HIDE SENSITIVE FILES

Dynamically hide sensitive or confidential content from unauthorized users in Teams folders, chats and searches—even entire channels and chat conversations, to minimize the risk of data exposure. Only users with access rights will be able to see the content exists.

CONDITIONAL ACCESS & SECURITY

NC Protect leverages dynamic access, usage denial rules and a secure viewer to ensure that only approved users can access and share content – internally and with guests. Apply conditional protection rules centrally or locally, ensuring compliance, while enabling content owners to fine-tune rules.

AUDIT & REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. Report on the number of issues identified by classification level and allows policy officers to review the results and rescan, reclassify or reapply permissions if needed. Integrate user activity and protection logs with SIEM tools like Splunk or Microsoft Sentinel for further analysis and downstream actions.

ADVANTAGES OF DYNAMIC, ATTRIBUTE BASED ACCESS AND CONTROL

archTIS' granular data-centric approach to security enables conditional access control down to the item-level using both data and user attributes. Since access and information protection are applied to individual files, chats and messages, as compared with solutions that secure or encrypt at the app or location level, sensitive content can be safely stored, shared and collaborated in Teams, and other Office 365 apps, regardless of user membership. This approach also controls the proliferation of teams to support individual collaboration scenarios.



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

