DATASHEET

NUCLEUS CYBER

NCPROTECT™

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. It can restrict usage and even hide content based on multiple attributes including data classification, user location, device and access rights, and automatically apply encryption when it leaves the safety of Teams and other Office 365 applications.

KEY BENEFITS

- 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 Information Security

With over 75M users, the ability to quickly share information via built-in chat and file sharing capabilities has rapidly made Microsoft 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. NC Protect requires no additional client-side application simplifying deployment and reducing the time that your content is at risk. Centrally manage access and usage across the suite of Microsoft Office 365 applications using the same rule sets to reduces admin overhead and resources associated with managing sites and applications.

CHEAPER

NC Protect is a complementary solution that leverages and adds value to your existing Microsoft investments. It allows you to get advanced information protection capabilities without the cost of upgrading to E5 licensing. 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

KEY CAPABILITIES

ADVANCED 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. trade secrets, insider information, etc.).

IT FRIENDLY PRIVATE CHANNELS

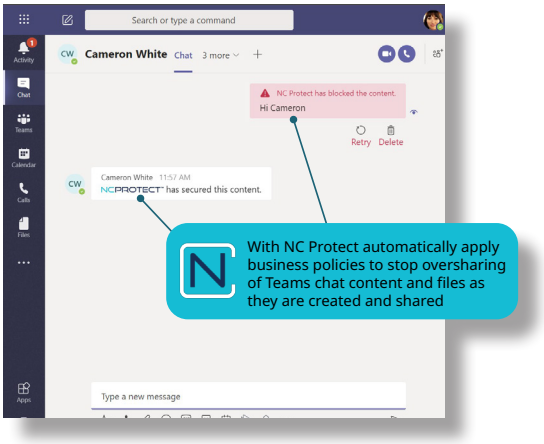
Simplify the creation and management of private channels to restrict access to specific individuals within a Team. Reduces admin overhead over time associated with managing large numbers of site collections and simplifies backup and life cycle tasks.

SECURITY SCOPES

Security Scopes can automatically be applied to Teams based on the team member, chat or file content and context to prevent accidental data leaks. Rules can be applied to multiple Teams or sites at once. Attributes are used to define Scope membership e.g. If a guest user is added a Team can be automatically moved to a new scope and rules applied.

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.



DYNAMIC WATERMARKS & VIEWS

NC Protect works natively with Microsoft collaboration and security products to augment native features such as methods for viewing files, applying dynamic watermarks and encryption or restriction of attachments sent through Exchange Email.

For example, if a file is added to a Team and member does not have proper access to that category of document, then the file can be hidden from the view of the unauthorized individual.

PREVENT 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.

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 your business content – internally and with third parties. 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, ITEM-LEVEL SECURITY

Nucleus Cyber's granular data-centric approach to security enables conditional access control down to the item-level using secure metadata and user attributes. Since access and information protection can be 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 on from any Team or Office 365 app regardless of user membership. This approach also controls the proliferation of Teams to support individual collaboration scenarios.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com

Member of Microsoft Intelligent Security Association

Microsoft