DATASHEET

NUCLEUS CYBER

NCPROTECT™

INTELLIGENT DATA-CENTRIC SECURITY FOR MICROSOFT TEAMS®

EXECUTIVE SUMMARY

The number and variety of collaboration channels and tools have increased dramatically. NC Protect dynamically adjusts access and protection of both chat and file content within Microsoft Teams to ensure that your organization's sensitive business data is being used and shared according to your business regulations and policies.

NC Protect provides conditional access control without the overhead of complex user permissions and poorly applied at-rest encryption, ensuring that your information is protected at the right time across all collaboration scenarios. It can restrict usage and even hide data based on multiple attributes including data classification, user location, device and access rights, and automatically apply encryption when the data leaves the safety of your collaboration systems.

KEY BENEFITS

- Enable private chats and file sharing within Teams
- Automatically apply business policies to Teams chat content and files as they are created and shared
- Identify and protect sensitive information being shared via Teams
- Adjust protection based on file content and user context
- Only encrypt data when the scenario requires as per policy
- Hide sensitive content from unauthorized users
- Granular approach to security and protection mitigates risk down to the item level

Great for Collaboration, Problematic for Data Security

There is little doubt that Microsoft Teams growth is changing how people collaborate with colleagues and external parties. With almost 500,000 organizations now using Teams the ability to quickly share information through the built-in chat and file sharing capabilities it is rapidly becoming a key collaboration tool for organizations.

However, the speed and simplicity for which users can create Teams presents a new challenge for those tasked with ensuring intellectual property, regulated and sensitive data is properly protected. Consider this; 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 collaboration tools like Teams make it problematic to keep track of the nature of data being shared and to ensure that sharing and usage policies are being followed.

Data-Centric Security and Compliance for Teams

NC Protect offers centralized, cost-effective policy compliance management and data loss prevention (DLP) for Teams. It ensures data compliance and security by continuously monitoring and auditing chat messages and files against regulatory and corporate policies to protect against data breaches, unauthorized access and sharing, and misuse.

Policies for encryption and usage rights can be automatically enforced based on the content and context of the collaboration scenario. It provides an unmatched level of data-centric protections without impacting productivity to facilitate secure collaboration and reduce the risk of Shadow IT.

Protect Teams Chat and Files with Conditional Access and Security

LEVERAGE INTELLIGENT RULES

NC Protect's policy manager features hundreds of pre-defined polices for US and international data regulations (PII, FINSEC, HIPPA, and more) as well as the ability to define contextual enforcement rules to match collaboration needs.

Easily define and configure custom rules to match your organization's unique intellectual property, confidentiality and security policies.

AUTOMATE DISCOVERY & COMPLIANCE

Scan files for policy violations and confidential content, once detected the file is automatically classified based on the sensitivity of the content and your pre-defined governance policies.

SECURE INDIVIDUAL MESSAGES & FILES

Enable secure, private chat and file sharing within a Team by applying business security rules in NC Protect to automatically restrict access to chat or file data, apply encryption, and prevent it from leaving the organization.

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

NC Protect Delivers Conditional Access Control at the Document Level

NC Protect uses metadata-driven, item level security to restrict access to, encrypt, track and prevent the sharing of content based upon the presence of sensitive and/or non-compliant information, offering content-aware data loss protection capabilities for Teams chat messages and files. Organizations using Teams in addition to SharePoint and Exchange for storage and collaboration can leverage NC Protect's rules across all platforms to centrally manage policies, classifications and controls.

DISCOVER

Locate all sensitive and confidential data (PII, PHI, HR, IP, etc.) to create an 'information footprint' of your sensitive data using a single set of rules for one or multiple on-premises and cloud environments.

CLASSIFY

Once sensitive information is detected the file can be automatically classified based on the sensitivity of the content and pre-defined governance policies. You can also define which users can classify or reclassify data, unlike standard metadata that can be modified by anyone that has document access.

RESTRICT

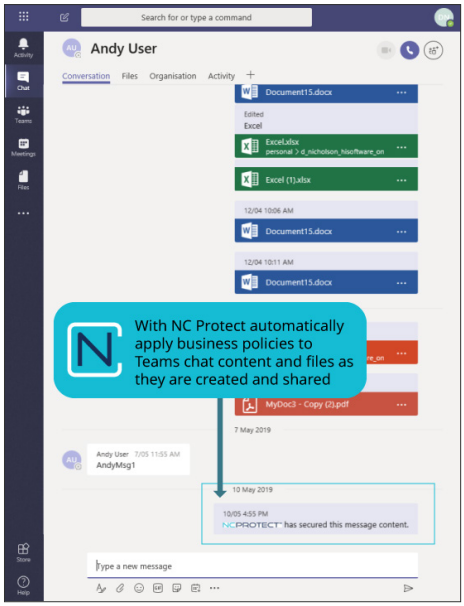
Based upon the business rules associated with its classification, access to a chat message or file within a Team can be restricted to a specific individual or group within the Team, even if a wider audience has access to the rest of the Team where the item physically resides. With file level controls, users and administrators can reduce the number of Teams needed to enable secure collaboration with a subset of Teams members. Managing access down to the file level is made possible by leveraging the data and user attributes rather than the data location.

ENCRYPT

Data loss prevention is a critical issue for many organizations. In addition to securing a document based on its classification (metadata), NC Protect can further secure Teams content by encrypting it to ensure only properly authorized and credentialed users will be able to access the content even if they have Team owner privileges. This additional security makes it safe to store confidential documents such as internal only, Board or HR documents. It also ensures access can be controlled for any data shared with external parties, even when it is removed from the Team.

PREVENT

To further extend the tracking process you can also define rules in NC Protect to prevent the distribution of sensitive information or confidential documents to minimize the risk of data loss. 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. Users can also be prevented from printing, emailing via Exchange, saving or copying the contents of Microsoft Office documents and PDFs outside of the Team.



CONTROL

Using workflows, NC Protect can trigger access approval requests for policy officers or managers or to request justifications from users. Complete business rules can be developed so that you can remediate compliance issues and task the proper individual(s) in the organization to review and potentially classify, alter the classification of, or encrypt the content.

REPORT

A dynamic Results Viewer provides centralized reporting and management of classified data. It reports 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. The list can be filtered based on flexible search conditions and exported to various formats for reporting or archiving purposes.

ADVANTAGES OF INTELLIGENT, 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 usage rights can be applied to specific content or individual files (using classification), 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 regardless of user membership. In addition to better protecting your organization from an accidental breach, this approach also controls the proliferation of Teams to support individual collaboration scenarios.

NUCLEUS CYBER

info@nucleuscyber.com | www.nucleuscyber.com