OUT OF THE BOX OR THIRD PARTY SECURITY?

10 Questions to Assess Information Security Needs in Microsoft Teams

archTIS

TABLE OF CONTENTS

Executive Summary 3

10 Questions to Assess Your Information Security Needs in Teams. 4

Scoring Your Answers 5

How to Get Advanced Information Protection for Teams Faster, Simpler and Cheaper 5

NC Protect Offers Unique Security Features Not Available Out of the Box . .6

Conclusion 7

EXECUTIVE SUMMARY

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

Microsoft Teams ships with numerous out of the box (OOTB) security features, yet there are a plethora of value added solutions for information security on the market. Understanding whether or not existing Microsoft investments satisfy business, compliance and security needs can be a challenge for many organizations.

If you are confused about whether or not the OOTB information security for Microsoft Teams is adequate, or if you need to add a third party solution to get the data protection capabilities needed to suit your business and regulatory requirements, then this self-assessment is for you.

Based on your answers to the following 10 questions you will get an understanding of your needs, and whether or not they can be satisfied with your existing Microsoft security investments or if you could benefit from a value added partner solution like NC Protect.

INSIDER THREAT FACTS

95%

of cybersecurity breaches are caused by human error

144%

Employee collaboration messages are 144% more likely to contain confidential information

207 DAYS

The average time to identify a breach in 2020

<13% IN 30 DAYS

Only 13% of insider incidents were contained in less than 30 days

10 QUESTIONS TO ASSESS YOUR INFORMATION SECURITY NEEDS IN TEAMS

1. What Teams features are you using?

- ❑ Just calls, meetings and chat.
- ❑ Calls, meetings, chat and collaboration (internal only).
- ❑ Calls, meetings, chat and collaboration (internal and external).

2. Do you collaborate on sensitive or confidential information using Teams (personally identifiable information (PII), protected healthcare information (PHI), intellectual property (IP), company financial information, stock and securities trading, legal information, other regulated information?

- ❑ Yes, we do.
- ❑ No, we do not.
- ❑ I'm not sure.

3. Are you worried about users accidentally sharing any of the information above with unauthorized users or third parties?

- ❑ Yes, I am.
- ❑ Yes, I am required to do so to meet regulatory compliance.
- ❑ No, I am not.
- ❑ I'm not sure.

4. What type of Microsoft License do you currently have?

- ❑ I have Microsoft 365 E3 and do not have any plans to upgrade to Microsoft 365 E5.
- ❑ I have E3 but I would like to upgrade to E5 for to get access to the information protection features but don't have the budget.
- ❑ I have E5 and I am using all the information protection features.
- ❑ I have E5 but I'm not taking advantage of the information features due to their complexity and the time it takes to implement them.

5. Have you enabled Guest Access to Teams?

- ❑ Yes, I am and I'm happy with it.
- ❑ Yes, I am but I'm concerned about guests accessing internal / confidential information.
- ❑ No, I have not because I'm afraid of guests accessing internal / confidential information.

6. Do you need Information Barriers or Ethical Walls that completely cut off communication of any type between individuals or groups?

- ❑ Yes, that's ideal.
- ❑ No, I would like flexibility to block certain types of communication (i.e. regulated information) but allow for other communication such as interaction with our HR team.
- ❑ I do not need this capability.

7. Do you need an easier way to create and manage access and security in new and existing teams as they are created, guests are added or removed?

- ❑ No, I find it easy to manage with OOTB tools.
- ❑ Yes, I do it's time consuming to constantly be provisioning and updating security on teams.
- ❑ Not sure, individual team owners are responsible for team provisioning and governance.

8. Would you like the ability to hide tabs (i.e. wikis, files) and channels in the Teams UI to limit information access?

- ❑ Yes, I would.
- ❑ No, I would not.
- ❑ I'm not sure.

9. Do you need a secure way for users or guests to view information that limits copy, paste, edit, downloading and sharing functions?

- ❑ Yes, I do.
- ❑ No, I don't.

10. How do you think your information protection concerns within Teams is going to change in future?

- ❑ I will become more comfortable with the security of information within Teams.
- ❑ I think my level of concern will remain the same as it is now.
- ❑ I am really concerned about the future implications for information protection with continued use of Teams.

Scoring Your Answers

If you answered NO to most of these questions, then OOTB solutions are likely sufficient to meet your information protection needs.

- If you answered YES to questions 3, 5, and 6, but have concerns, or have E3 but would like to upgrade to E5 to access the additional information protection features, but don't have the budget, you may quickly outgrow security provided by OOTB solutions and benefit from a third party solution.
- If you answered YES to questions 7, 8, and 9, and NO to question 6, or have E3 but would like to upgrade to E5 to access the additional information protection features, then OOTB solutions don't offer what you need to adequately protect your content and you could benefit from the features and cost savings offered by a third-party solution.

Read on to learn how NC Protect can help you achieve your information security objectives, while leveraging your existing Microsoft investments to ensure secure collaboration, empower IT and Teams Owners, and improve ROI.

NC PROTECT FOR MICROSOFT TEAMS

Advanced Information Protection for Teams Faster, Simpler and Cheaper

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 capabilities to provide customers with more tailored information protection in Microsoft apps.

The complementary nature of our solution is why we were one of the first partners invited by Microsoft to apply for membership to 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. We are also Microsoft Co-sell Ready Partner validating the complementary nature of our solutions and value they provide to Microsoft customers.

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.

Microsoft Partner

Member of Microsoft Intelligent Security Association
Microsoft

NC PROTECT OFFERS UNIQUE SECURITY FEATURES NOT AVAILABLE OUT OF THE BOX

Empower Team Owners to Secure Their Own Teams with a Few Clicks

The NC Protect app for Teams enables team owners to activate several NC Protect capabilities with a single click in the Teams UI. The policies and protection come pre-configured out of the box and an intuitive user interface provides team owners with unprecedented control over their information protection needs. Simply apply Dynamic Watermarks, automatic information protection for Guest Users, enable the Secure Reader, convert standard channels to Private channels and vice versa. Many of these features are available for Administrators today but the NC Protect app for Teams extends these capabilities quickly and easily to Teams Owners.

Apply Dynamic Watermarks to Protect Documents

NC Protect can dynamically add a personalized 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 to identify the handler and supplement user training relating to the safe handling of sensitive or proprietary information. Additionally, by having a secure personalized watermark in the body of the document that cannot be removed, the user is deterred from taking a picture with their mobile device, sharing in an unauthorized manner or using it for malicious purposes, helping reduce data loss and misuse.

Hide Files from Unauthorized Users

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.

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

Force Viewing in a Secure Web Reader to Prevent Data Loss

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.

Advanced Information Barriers for Real World Collaboration Needs

Many organizations must restrict communication and collaboration between individual or groups of individuals to enforce regulatory information barriers and ethical walls, as well as protect intellectual property (IP), regulated data including personally identifiable information and healthcare information (PHI). Microsoft's OOTB information barriers completely cut off all communications between these groups regardless of the context. They also require Microsoft E5, E5 Compliance, or E5 Insider Risk Management subscriptions, which can be a budgetary constraint for some organizations.

NC Protect's advanced information barriers provide a greater level of simplicity and flexibility than OOTB options and do not require an upgrade to E5, allowing you to get more value from your existing Microsoft investments. With NC Protect configure and enforce information barriers to restrict specific types of collaboration between users/groups, but with the flexibility to allow non-regulated or restricted communication. It can control access in accordance with business rules for users from different groups, operating companies, or geographical regions beyond sole reliance on permissions.

Guest Access and Sharing Made Easy

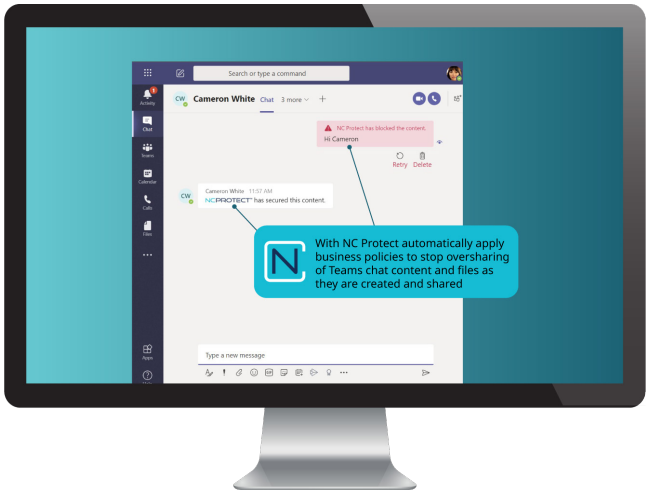
NC Protect eliminates the need to create separate Teams for guests to control access to specific types of content. Instead, NC Protect automatically controls what content guests can see in a Team based on their user attributes, making guest access simpler to manage and more secure. For example, content 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 Reduce Admin Resource Drain

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.

Smart Security Scopes Automatically Adjust Team Security

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 Capabilities for Retroactive Protection

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.

CONCLUSION

Microsoft Teams delivers a wide range of apps and security features to provide business-critical capabilities and rich functionality to their customers. However, it is impossible for Microsoft to successfully provide the full depth and range of capabilities that is often needed to satisfy every customer requirement. 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. An intuitive UI empowers IT and Teams owners to improve information security and ensure compliance simpler, faster and more cost effectively.

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

archTIS.com | info@archtis.com

Australia | United States | United Kingdom