BUILDING DYNAMIC INFORMATION BARRIERS IN MICROSOFT 365

Creating more effective information barriers using document and user attributes, not just user roles

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Information barriers that were once relegated to financial services and regulatory compliance are quickly becoming a must have to accommodate a variety of business scenarios.

The art of running a business is a forever evolving path of goldmines and hurdles. Trying to map these business processes over current technology, is challenging at best and extremely difficult to achieve for all elements and viewpoints of business workflows.

Just when you believe that you have tamed the digital frontier, by implementing the best user role-based access controls to the various social channels, desktop SOE, financial systems, document repositories, payroll, and HR portals - an urgent request comes in for a “locked down private network” to securely share information to a select few on a need-to-know basis within and external to the business.

This request goes against the grain of your current IT methodology of simplification and consolidation of access controls. However, requests for data separation have become extremely common as business, and its associated communications web, become more global. ‘Information barriers’, also known as information walls, ethical barriers, exclusion/inclusion barriers, or cones of silence, are becoming an essential element of business to prevent the collaboration of material which may lead to conflict of interests or competitive advantage.

This white paper examines the challenge of building information barriers using role based security and how to create more usable separation for more complex use cases using dynamic attribute-based access control (ABAC) policies.

INFORMATION BARRIER USE CASES

1. Financial Services / Trading
2. Legal
3. Compliance
4. Trade secrets
5. Research
6. Departmental / Geographical
7. Defense / Multinational Coalitions

WHEN ARE INFORMATION BARRIERS REQUIRED?

An information barrier might be erected between parties (internal and external) that deal in mergers and acquisition, tendering, investments, and legal representation to name a few.

The act of applying information barriers to actively monitor and separate access to information from individuals or groups is not as simple as applying set and forget viewing (or non-view) rights in your user access management (role-based access control) system.

Traditionally information was held within "documents" therefore, it could be controlled with a simple permissions toggle set on the file. With this permissions model it's difficult to maintain the effectiveness of information barriers, especially:

- If the "information" is held within collaboration tools.
- If you need to provide restrictions based on geolocation or nationality.
- If you need to apply multiple restrictive elements to the information barrier policies.
- If they need to provide "need to know or not" access to certain elements in the same folder / collaboration channel.
- If you information barriers include personnel from outside of the organization (contractors, partners).

7 Use Cases for Information Barriers

Examples of everyday business information barriers are:

1. Ensure users in a trader group do not communicate with other internal business groups.
2. Stop finance personnel working on confidential company information from communicating with certain groups within their organization.
3. Prevent an internal team with trade secret material from calling or chatting in Microsoft Teams with people in certain groups within their organization.
4. Limit a research team's call or chat abilities with a product development team.
5. Restrict collaboration between users in different geographical locations or subsidiaries to meet regulatory guidelines such as GDPR.
6. Ensure files created by, for example, an SVP or higher are restricted to users at that level of the organizational hierarchy or above.
7. Restrict the sharing of files via chat, based on file sensitivity.

Configuring an Information Barriers is not a one size fits all art form. Each and every industry, use case or regulatory requirement will have individual configurations - determined by the individual business circumstances, processes, and compliance requirements.

For example, in the legal world there are a multitude of Information Barriers that need to be enabled. They may require top-down as well as side by side information barriers to ensure client information is segregated and contained on a need-to-know basis between sub entities, legal practices, lawyers and external parties.

Examples where legal information barriers are imperative include:

- When a lawyer moves from one legal practice to another
- A single law firm is acting on behalf of multiple clients in the same (or related) matter.

- When an attorney client relationship ends
- Internal and external parties working on the same matter or internal project.

These information barriers screen individuals within an entity or group of users from any new/conflicting information that may introduce the possibility of confidential information being used inappropriately.

THE CHALLENGE OF CREATING USABLE INFORMATION BARRIERS

While constructing these Information Barriers may seem easy enough to do using out-of-the-box (OOTB) tools, in reality they often completely cut off all communications between these groups regardless of the scenario – hindering other work practices.

For example, if information barriers are set-up between your traders and marketing teams, then your traders can't receive any information from marketing because the information barrier policy specifies no communication is allowed between these two groups. The context of the communication isn't considered, it simply creates a virtual wall between these two groups.

There is also often limits on the number of entities or groups that you can place information barriers between, which can be problematic in today's global economy. The more entities/users adds more complexity to managing information barriers using OOTB tools or role-based security models. Adding to this complexity is the requirement to add and remove internal entities, groups and external guests to these security models.

Another drawback is if a user is removed from a group because they changed jobs within the company, the user can still see old conversations, but won't be able to see or participate in any new conversations with the group. There's no ability to retroactively remove old conversation on the topic.

More effective information barriers consider document and user attributes, not just user roles.

What if you had the choice of creating effective, flexible and content dynamic information barriers for your existing Microsoft investments? Information barriers that enable you to successfully separate your data via granular Attribute Based Access Controls (ABAC) that can dynamically determine if the specific communication should be allowed or restricted.

The trick to successfully implementing dynamic information barriers is leveraging content attributes (e.g. classification, sensitivity, author, site permissions, etc.) and user attributes (e.g. group permissions, security clearance, role, location, time, etc.) as part of the policy to block/allow access. Once the policies are defined, any new data or users that are introduced into the business processes are adopted by these conditions and secured accordingly.

As ABAC is a "do not trust – challenge everything" zero trust methodology, access is based on the attributes of the content (file, chat or message) and the user at that moment in time. When a policy (condition) is modified to included/exclude an attribute, at the next interaction between that user and content the new governing policy will be invoked and applied. The same happens at the content level if the attributes are changed, then a different set of access conditions may instantly apply.

You can see the advantage of using an ABAC-centric solution to create flexible vs finite information barriers that stop all non-compliant communication collaboration.

More effective information barriers consider document and user attributes, not just user roles

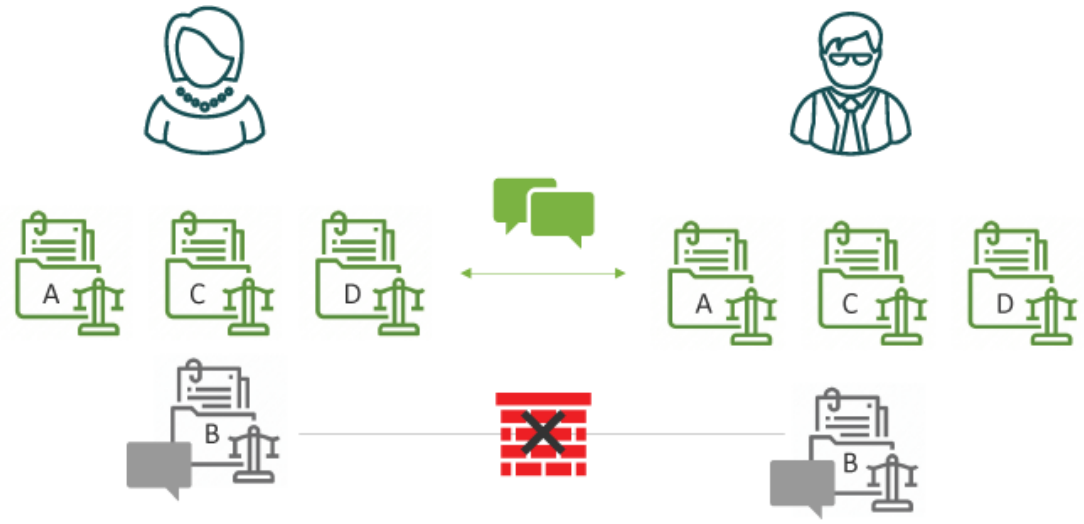
BUILDING DYNAMIC INFORMATION BARRIERS WITH NC PROTECT

NC Protect is an advanced information protection solution built with ABAC controls to empower secure and intelligent security for Microsoft 365 applications (Teams, SharePoint, OneDrive, Office, Exchange) and other file shares.

NC Protect can be easily configured and applied to create dynamic information barriers required to meet your compliance and security requirements, with the following advantages:

- Blocks communication and file sharing on restricted topics, without stopping collaboration on approved topics.
- Can easily apply the same information barrier policies to SharePoint site and files that Teams creates by default.
- Supports information barriers for one to multiple entities or groups, without limitation.
- Segment access to country specific sensitive information in SharePoint and Teams.
- Can delete chat content retroactively if access changes, such as when someone changes jobs.
- Restrict in-application functionality for guest users.

DYNAMIC INFORMATION BARRIERS WITH NC PROTECT



For example, a legal firm is using Microsoft Teams. Two of the firm's attorneys are working on multiple cases that they need to collaborate on, but they are not allowed to communicate on case B, as there is a conflict of interest. NC Protect will allow conversations and file exchange on the other cases, but block any communication or file exchange on Case B.

SUMMARY

If you are looking for a solution that will assist you in creating Information Barriers (cloud or on-premises) to block unauthorized communication but are still flexible enough allow permitted topics within internal groups and external guest users, if required, then reach out to the team at archTIS.

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

Copyright 2021 archTIS Limited. All rights reserved. archTIS, the archTIS logo and NC Protect logo are trademarks of archTIS Limited. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries. All other product names mentioned herein are trademarks of their respective holders.