ROLE BASED ACCESS CONTROL (RBAC) OR ATTRIBUTE BASED ACCESS CONTROL (ABAC)?

Adopting a Modern Zero Trust Approach to Data Access

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Over the last two years, companies have seen an expedited shift away from using traditional methods to access their data. With more employees working remotely, organizations are finding the security controls they have spent years refining are no longer adequate. It is time for organizations to review their data security practices and decide if a modern approach is required.

Role-based access control (RBAC) has traditionally been the go-to methodology for implementing access control. However, as modern workplaces have shifted from the office to a more dynamic, hybrid-working environment, the role-based security and supporting technologies that we have spent years implementing and maintaining are no longer sufficient to protect business-critical data assets.

As more organizations seek to implement a modern Zero Trust approach to data security, a dynamic approach to access control is required – one that attribute-based access control (ABAC) can deliver.

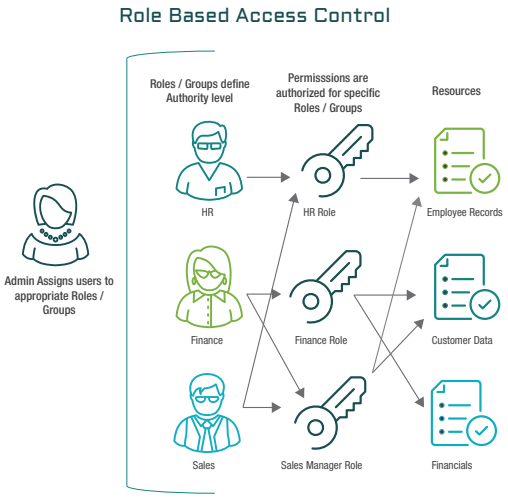
This white paper explores the differences between RBAC and ABAC technologies and their ability to support a modern zero trust approach to data access.

RBAC AND ABAC DEFINED

When it comes to access control, there are two common approaches an organization can deploy: role-based access control (RBAC) and attribute-based access control (ABAC). Understanding the differences between the two and common misconceptions is important to ensure you pick the right technology to match your current needs and can grow with your organization's security goals.

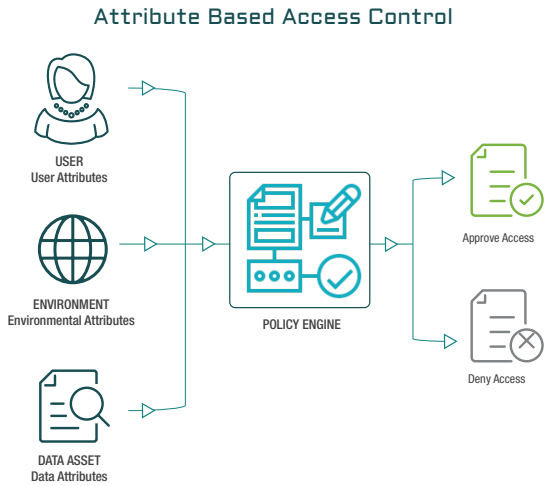
Role-based access control (RBAC)

RBAC grants or rejects an employee's access to data based on the user's role within a company (e.g., department, location, seniority level, work duties). Roles are predefined and apply broad access based on the role. For example, a manager role applies to managers in all departments (e.g., finance, HR, Sales, etc.). To add granularity to RBAC rules, administrators are generally required to add more roles (e.g., Sales manager, Finance manager, etc.).



Attribute-based access control (ABAC)

ABAC is a policy-based approach that considers the attributes of the user (e.g., department, location, seniority level, work duties, nationality, clearance level), the data (e.g., sensitivity, classification, type), and the environment (e.g., device, time of day, network) to deny or grant a user access to the data. With ABAC, rules can be very granular allowing you to give the same user different permissions based on the conditions at the time of access. The permissions and policies are dynamic meaning they adjust to the sensitivity of the content and the context of the access request.



WHAT IS AN ATTRIBUTE?

Attributes are the values or characteristics of a component. Here are some examples:

User

- Name
- Nationality
- Security Clearance
- Organisation
- Group

Location

- Country
- State
- Address

Device

- Name
- MAC Address
- Credentials
- Classification

Network

- Name
- Credential
- Classification

Data

- Document Type
- Sensitivity Level
- Data Classification
- Metadata

For example, a sales employee may be granted access to sales materials. However, sensitive data, such as customer profiles and price lists should only be viewed when the user is using a company-issued device and connected to a secure network. This conditional access is easily achievable using ABAC.

An ABAC policy can also help prevent accidental data exposure and leaks. For example, if an HR user mistakenly dropped a VIP payroll spreadsheet in a sales folder, an ABAC platform, like NC Protect would detect HR data in the document and deny access to non-HR personnel. It could further protect this document by automatically encrypting the content and sending an alert to the appropriate InfoSec team.

The key difference between RBAC and ABAC is how each method grants access. RBAC grants access using roles and static policies. ABAC determines access using attributes and granular dynamic policies.

ADOPTING A MODERN ZERO TRUST APPROACH TO DATA ACCESS

Zero Trust is a newer security approach that assumes that there is no traditional network edge or security perimeter. It simply states that you must verify and validate each action, every time, in context, to the security level needed to maintain the organization's security posture.

These principles not only apply to network and application access, but they must also apply to file access to ensure data is not mishandled or exfiltrated by trusted users. Unfortunately, many technologies that tout zero trust do not address the data layer.

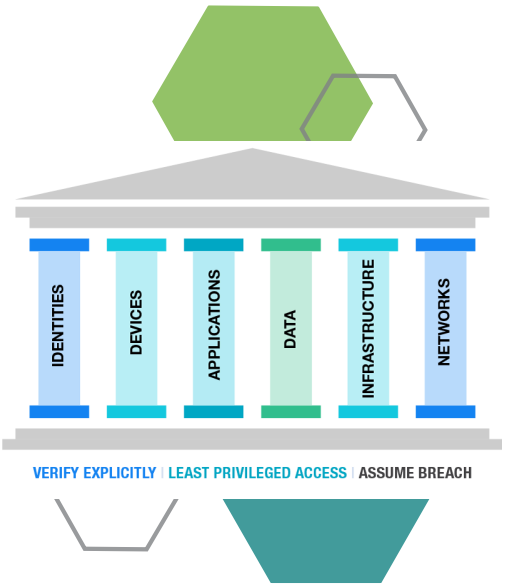
In today's distributed work environment, we not only need to ensure our users are properly authenticated and have appropriate permissions to access our valued data, but we also need to evaluate the sensitivity of the content they are accessing and the suitability of the environment that they are accessing from. Only then, when these variables have been measured, should you authorize the user's access to a sensitive data asset such as customer or employee data, financials, intellectual property, and other audience-restricted information.

RBAC Challenges

Organizations need additional methods to evaluate the context of a user's access request to embrace a zero trust approach. However, with RBAC you can only authenticate the user and their permissions to access the data. It lacks the ability to perform the additional level of validation required for zero trust.

An IT administrator is usually responsible for implementing RBAC to grant users access to the network. Meanwhile, larger IT teams may have several administrators responsible for managing access in separate data stores, such as file servers, SharePoint, CRM systems, email, messaging applications and more. These permissions must be updated when a new user joins a company or an existing user changes departments, and then be revoked when a user leaves the organization.

This can be even more challenging when users have a blended role or are working on joint projects that overlap several departments. Administrators must create additional security groups and/or folders to grant access and allow collaboration between teams. Many of these assignments will be temporary, so access must be monitored and re-evaluated at the end of the project.



THE 6 PILLARS OF ZERO TRUST

1. **Identities** may be users, services or devices
2. **Devices** create a large attack surface as data flows
3. **Application** controls should be applied to ensure appropriate access, monitor for abnormal behavior, and control user actions.
4. **Networks** should be segmented
5. **Infrastructure** whether on-premises or cloud-based, represents a threat vector
6. **Data** should be classified, labeled and encrypted based on its attributes

The adoption of hybrid working environments has created an additional challenge as employees no longer only work from the security of the corporate office. They may work from home occasionally or full-time, or in a shared co-working environment. They may choose to do some work in a coffee shop, or while commuting on public transport.

IT security teams do not have control over these shared environments and will not have visibility of other devices attached to these networks (or if there is any malicious software deployed on devices attached to the same network).

The ABAC Advantage

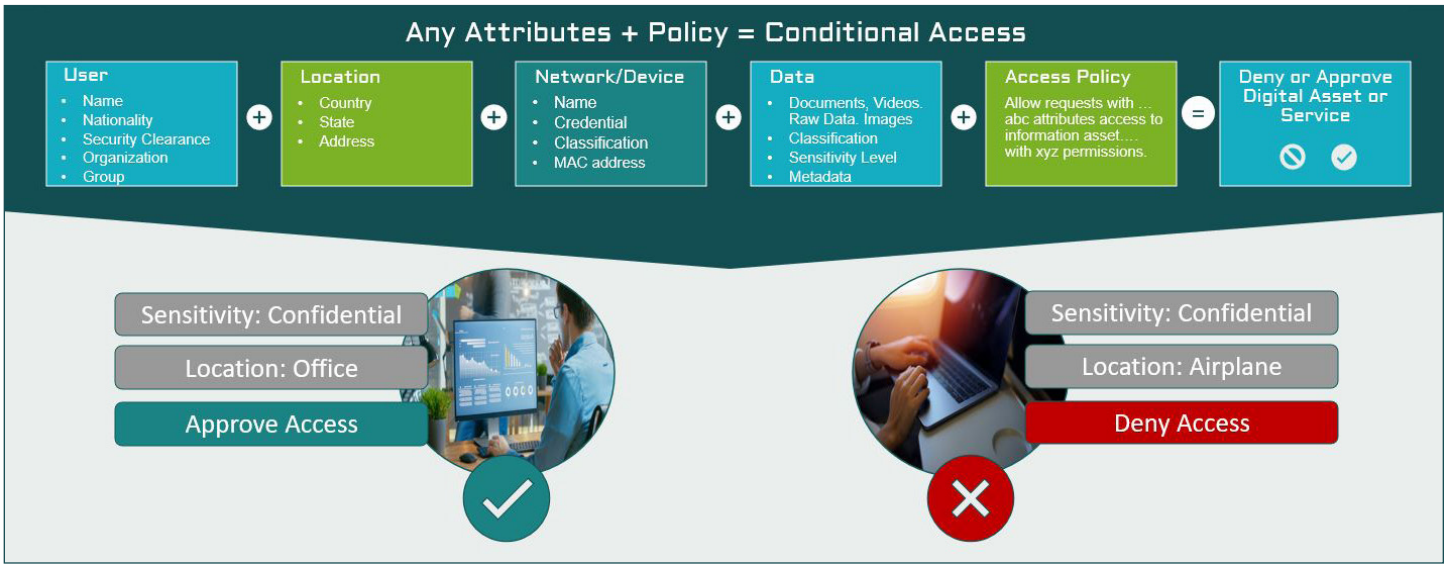
The benefit of ABAC is that it addresses the additional security questions required for a zero trust approach by matching the conditions of the user, environment, and content to grant or deny access to the individual data asset. ABAC policies also verify and validate the access request in context, to the appropriate security level to protect sensitive data.

As an example, an HR user should not be permitted to open an Executive payroll spreadsheet on an airplane, where others could see their screen. How does an ABAC policy do this? The policy is defined with simple statements to review each access attempt and grant or deny access as appropriate:

1. Is the requesting user a member of the HR team?
2. Does the HR user have clearance to access confidential Executive payroll documents?
3. Is the user accessing from a managed company-issued laptop (free from unauthorized software)?
4. Is the user attached to a pre-authorized network or via an encrypted VPN?

The user would **only be granted access if ALL of the above conditions were met.**

ABAC Policies in Action



ADDRESSING COMMON MISCONCEPTIONS ABOUT ABAC

It's hard to overstate the need for dynamic access control in a modern working environment. Data breaches are costing organizations millions of dollars every year. Many of these breaches can be avoided by employing better access and security controls that ABAC affords. Despite this, many businesses today are still using RBAC as their preferred method of permission management.

Role-based access made sense when network access was limited to users inside a secure network perimeter. But as demonstrated above it is too limiting for many modern working environments. Some hesitate to adopt ABAC either because they don't know about it or are basing their viewpoint on some common misconceptions.

MISCONCEPTION 1:

ABAC Takes More Time to Implement

A concern often raised about ABAC is that it appears to be complicated and requires additional time, budget, and resources to manage. While it is true that ABAC offers a much more granular approach to access control, most organizations will only need a few rules to implement an effective data access policy. Mature ABAC solutions, such as NC Protect have rules and policies to address these everyday use cases, out of the box. As ABAC can utilize an organization's established RBAC policy, most of these rules will only require minor modifications to extend existing rule sets.

MISCONCEPTION 2:

ABAC Requires a High Degree of Expertise to Implement

On the contrary, ABAC does not require highly qualified (and expensive) expertise to deploy. Tools like NC Protect offer visual logic-based policy builders that allow admins to create, review and test new policies before they are deployed to the wider company environment.

MISCONCEPTION 3:

ABAC is an IT Resource Drain

Another misconception about ABAC is that it is resource-heavy and requires expensive tools to enforce. Early iterations of ABAC relied on agent-based enforcement with software running on an employee's desktop to enforce policies and protect data. Modern solutions, such as NC Protect are agentless, service-based implementations that allow companies to seamlessly transition their workforce to ABAC. There is no longer any need for additional software to manage that consumes memory and hard-drive space on their endpoints. In fact, in a world where users can access documents on their phones, tablets, and other smart devices, a seamless agentless solution is needed now more than ever.

MISCONCEPTION 4:

ABAC Only Suits Large Organizations

Another key advantage of ABAC is that it is scalable and will grow with your company. Over time, RBAC is prone to 'role explosion' and 'privilege creep', where the role structure becomes more and more complex due to the addition of many users, roles and access strategies to accommodate granular access rules. The end result is hundreds or even thousands of rules to manage. IT teams must constantly evaluate roles and access to clean up stale users and empty groups and ensure that appropriate permissions are always up to date.

ABAC on the other hand easily grows with your company's security needs. The dynamic nature of ABAC policies means you need less rules to handle complex access scenarios. What takes hundreds of rules using RBAC can be handled with just a few ABAC policies. Over time as needs change, additional attributes can also be attached to users and data assets to ensure that appropriate access is managed at all times to protect your data assets no matter where they live or travel within or outside the perimeter.

Today, the terms and conditions of access (often described as rules, policies or controls) need to become adaptable and enforceable to constantly changing access and security conditions.

UPDATE YOUR DATA ACCESS AND PROTECTION WITH NC PROTECT

NC Protect is a dynamic information security solution that offers attribute-based access control and granular information protection without complexity. NC Protect augments traditional data security by acting as an additional layer of security between the user and the data.

The platform does not need to modify existing file properties, classifications, or permissions to enforce ABAC. In fact, these values can be used as attributes to build access and protection policies from.

NC Protect augments the security in your collaboration platforms with unique data protection capabilities you won't find out-of-the-box.

Hide Sensitive Files

When NC Protect enforces access control, the policy can offer different actions, depending on the state of the user , their environment and the data. It has unique capabilities that can not only prevent access but completely hide files from unauthorized users. For example, a user without appropriate access rights will simply not see the protected files as NC Protect will dynamically trim the view for the user. There is no frustrating access denied messages and the user isn't inclined to bypass the security controls in place as a user can't breach what they can't see.

Enforce Read-only Access

In other circumstances, the user may be granted access to the file, however, based on its sensitivity can only be opened in a secure, read-only viewer. The Secure Reader feature presents the original file content as a read-only image, to prevent a user from copy/pasting content, downloading, or saving the file. In addition, NC Protect can apply a dynamic custom watermark that identifies the user, date, location, and other custom variables to inform the user of the sensitive nature of the document and discourage unauthorized redistribution of the content (such as a photograph).

Redact Sensitive Data

Also, NC Protect can redact content from the document, censoring classified information, regulated personal data, intellectual property (IP) and other sensitive content. NC Protect can restrict other file actions within collaboration tools too, such as disabling sharing, printing, and duplication options in the Microsoft application ribbon (Word, Excel, SharePoint, etc.).

Control Overprivileged Access

To manage overprivileged access concerns, administrators can be permitted to manage shared files and folders but can be restricted from opening and viewing their content. Even guests can be managed, and granted temporary, read-only access to content if the data access policy allows.

Apply Data Centric Zero Trust

NC Protect modernizes your data security policies and enforces them completely and transparently for each and every user, for every access attempt, on every device. Using NC Protect to deploy a data-centric zero-trust security approach that is powered by dynamic ABAC policies ensures that appropriate validation is applied and that your security posture is maintained in the context of whatever the access or sharing scenario is.

Audit User Activities for Compliance

In addition to applying dynamic real-time ABAC-powered access protection, NC Protect offers activity audits, permissions reviews, dynamic data discovery and classification and integration with a variety of collaborative data platforms and security solutions including Microsoft Sentinel and Splunk.

NC Protect is simple to deploy and does not need to change the state of your data at rest. It can utilize existing RBAC policies to ensure faster on-boarding and expand to ensure your employees only have access to content that they require. The platform will also consume metadata applied by other security applications, ensuring existing security policies are easily transitioned to a more dynamic access policy.

IT'S TIME FOR DYNAMIC ABAC-POWERED ZERO TRUST DATA ACCESS

The secure perimeter simply no longer exists, and user permissions continue to balloon as the methods of collaboration and the content behind them expand exponentially. Traditional RBAC is not enough to offer the contextual security that is needed to protect data with a distributed workforce. To keep data safe without role explosion and privilege creep - ABAC is the answer.

If you are considering implementing ABAC to enforce zero trust, consider NC Protect. Whether you need to manage sensitive data securely within your Microsoft 365 applications (SharePoint, Teams, OneDrive, Exchange), SharePoint Server or Windows file shares or need managing access and sharing of classified information stored with high levels of assurance – archTIS can assist. archTIS puts you on the path to zero trust access and protection with immediate benefit and return on investment while enabling your big picture goals.

www.archtis.com/contact

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