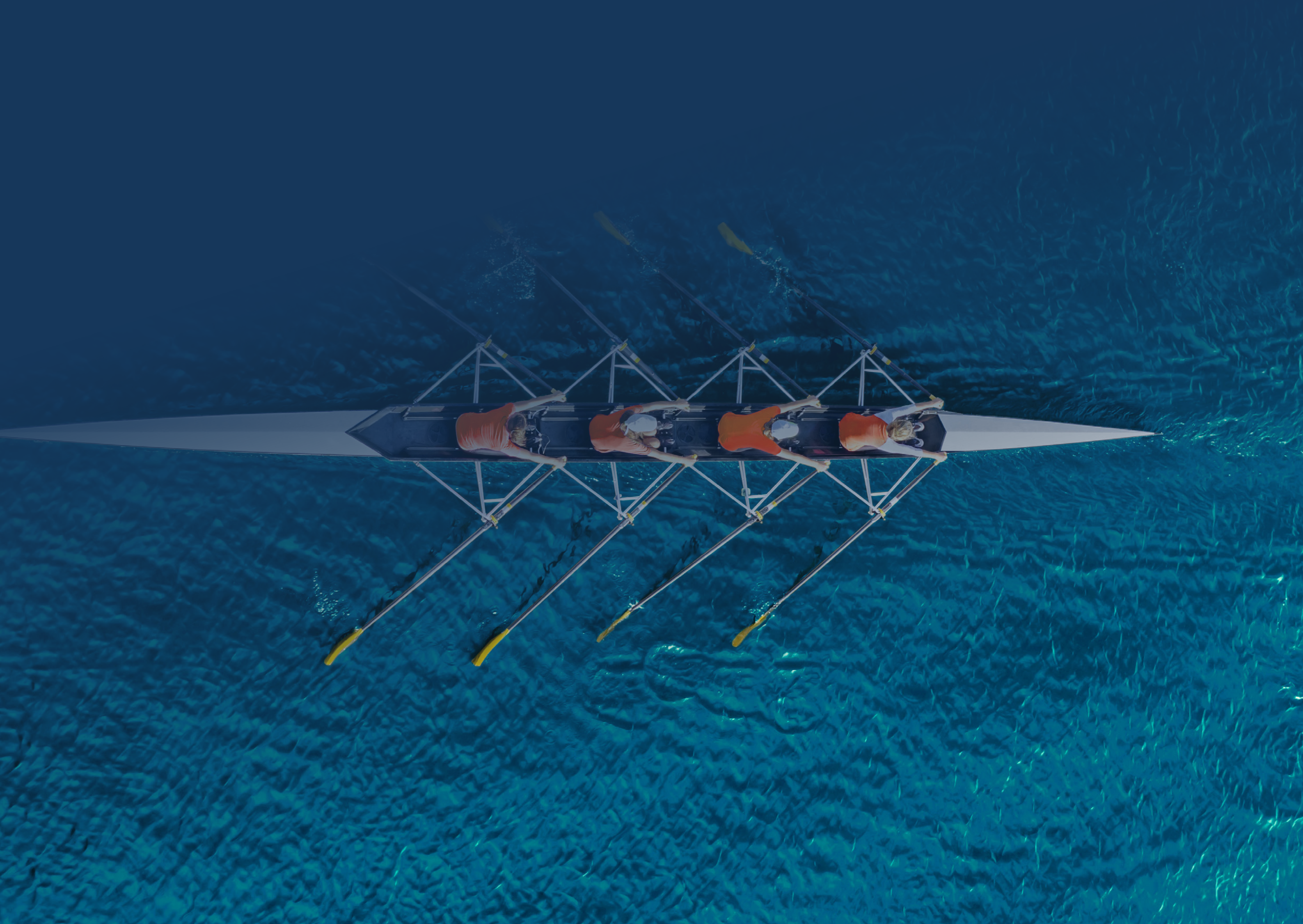
Columbus

WHITEPAPER

Strengthen your digital defences with Microsoft IAM assessment

Protect your organization’s digital assets through IAM assessment – helping you identify vulnerabilities, strengthen access controls, and mitigate security risks.



In this whitepaper, you can read about:

Author Mihai Forlafu, Columbus Security
Editor Gitte Gormsen, Columbus Security
Publisher Columbus Security

Building a secure future

Many companies today continue to rely on Active Directory (AD) for identity and access management (IAM) purposes, especially those with Windows-based IT environments. Active Directory has been a cornerstone of IAM in Windows environments for decades, and it offers robust capabilities for managing user identities, authentication, and access control.

While Active Directory remains a popular choice for IAM in Windows environments, the IAM landscape is evolving. Organizations are increasingly exploring identity and access management solutions that are more cloud-centric and capable of supporting a broader range of devices and platforms.

Azure AD, Microsoft's cloud-based identity service, is gaining traction as a complement to on-premises Active Directory, allowing organizations to bridge the gap between their on-premises and cloud-based resources. However, the continued use of Active Directory remains prevalent in many enterprise settings.

Let’s take a look at some of the challenges with Active Directory:

Legacy solutions

Over time, multiple chief security officers (CSOs) may introduce solutions into their IT security landscape based on their prior familiarity with certain tools or technologies. However, what often goes overlooked is whether the organization already has adequate coverage in that specific area through an existing solution.

For example, if your organization is already safeguarded by Microsoft's suite of security offerings, the addition of another security solution may be redundant and an unnecessary cost. It's imperative for businesses, especially given their already strained security budgets, to allocate funds wisely, ensuring every purchase are both necessary and effective.

There are also many organizations that believe they have sufficient security coverage from Microsoft's suite of products and services, but this perception can lead to a false sense of security. To maintain a robust security stance, organizations should conduct thorough risk assessments and consider investing in specialized security solutions or services to help bridge the gap between perceived and actual security coverage.

Having multiple security solutions not only risks overburdening the IT environment but can also introduce complexities in terms of configuration, management, and compatibility. The integration of legacy solutions with Active Directory, for example, may require additional effort and may not seamlessly align with modern security requirements.

Therefore, organizations must adopt a strategic approach when considering new security solutions, evaluating whether they genuinely address unmet needs in the context of their existing IT infrastructure. It's a critical step toward optimizing security efforts, streamlining operations, and ensuring that every budgetary allocation translates into tangible and meaningful improvements in the overall security landscape.

Overspending on security budgets

Linking from the above point, this issue often arises due to the deployment of redundant security solutions that duplicate the functionalities already available in Azure Active Directory itself.

Redundancy not only drives up costs but also adds complexity to IT environments, increasing the potential for errors and security vulnerabilities. Additionally, overspending can lead to vendor lock-in, making it difficult to switch to more cost-effective solutions in the future and limiting financial flexibility.

To mitigate overspending, organizations should regularly assess their security landscape, identifying and consolidating redundant tools, maximizing the use of built-in Azure Active Directory features, and conducting thorough vendor evaluations.

Budget planning and continuous review are essential to ensure that security investments align with evolving threats and business priorities, helping organizations maintain a strong security posture while optimizing financial resources for other critical needs.

Security gaps

One significant security gap lies in inadequate or misconfigured access controls. When permissions are overly permissive, users may have more access than necessary, increasing the risk of unauthorized access or privilege escalation.

On the other hand, overly restrictive permissions can hinder productivity and lead to workarounds that compromise security. Properly defining and managing access controls is crucial to mitigate this gap.

Another common security gap relates to the management of user accounts and passwords. Weak password policies can result in easily guessable or crackable passwords, making it simpler for attackers to breach AD accounts. Additionally, the lack of multi-factor authentication (MFA) can expose accounts to password-related attacks.

Properly enforcing strong password policies and implementing MFA are key measures to address this gap and enhance AD security. Regular monitoring and auditing of AD changes are also essential for promptly detecting and responding to any suspicious activities or unauthorized modifications.

How can organizations tackle Active Directory challenges?

We've identified three key areas organizations should target to make identity and access management more efficient and secure:

Evaluate your current state against your needs

Clarify if your current IAM solution fulfils your actual needs. It's no secret that almost all hybrid environments are the result of several years of accumulated security decisions made by different people.

This set up is fine if you also have good IAM hygiene and clean up routines. However, the reality is most organizations don't. That's why, now more than ever, it's imperative to gain a comprehensive understanding of your IAM environment and align it with your genuine needs to ensure the success of your business operations.

Develop a remediation plan

After gaining a clear understanding of the vulnerabilities in your IAM infrastructure, the next step is to develop a remediation plan. This plan should be balanced between quick wins, which offer immediate security improvements, and strategic initiatives, which provide long-term security enhancements.

To prioritize effectively, use heat maps to highlight vulnerable areas in your IAM infrastructure, enabling you to allocate resources efficiently and focus on the most critical aspects of your IAM framework.

Ensure you have the necessary technical expertise

The next step is ensuring you have the right technical expertise to fulfil the needs you've identified. Microsoft Entra offers a comprehensive suite of features that can be integrated with other security solutions, helping you maximize your current licenses and cybersecurity investments.

Key questions to address include: How is user provisioning managed, given the diverse user base encompassing employees, partners, and vendors accessing your infrastructure? Consider the specifics of how and when users access applications and data, as inadequate setup may expose you to GDPR, NIS, and other regulatory risks. User governance and administration processes should also be scrutinized, as mitigating "privilege creep" remains a key identity management concern.

Plus, evaluate the interconnectivity of your applications to identify potential vulnerabilities that malicious actors could exploit. Assess your monitoring and reporting mechanisms to ensure robust cybersecurity oversight. Lastly, define your success criteria for identity management, as these aspects are often underestimated yet prove invaluable during cybersecurity incidents.

Case in point: Exploiting conditional access misconfiguration

Imagine the following scenario in which an attacker gained access to sensitive corporate data through a few simple steps, exploiting a misconfiguration in the Conditional Access policy:

1 The attacker got their hands on leaked credentials, although the exact method remains unclear. However, the most common case involves employees using the same password for multiple accounts, including their personal ones for the sake of convenience

2 The attacker impersonated a Windows Phone to access the victim's inbox

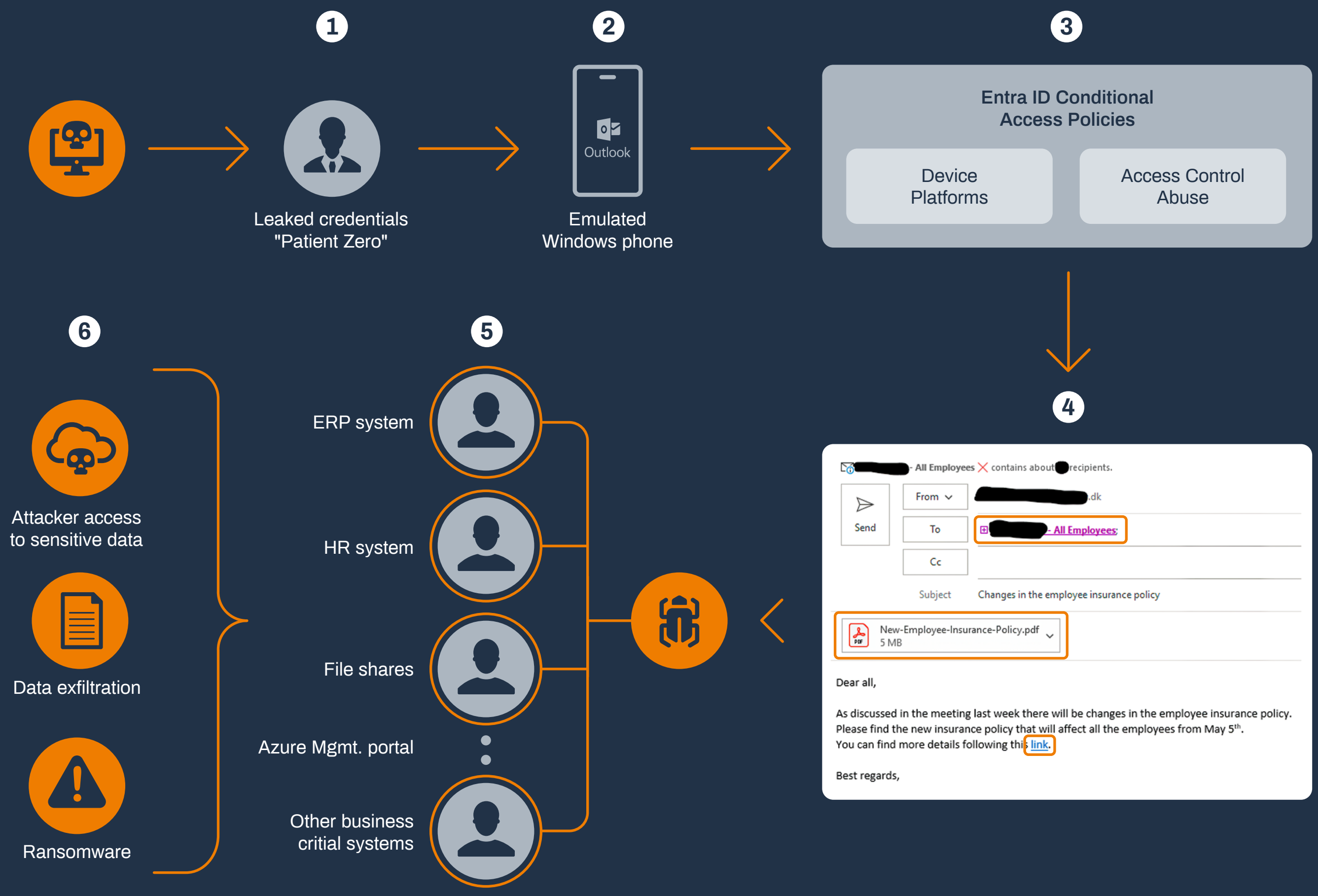
3 Due to a misconfiguration in the Entra ID Conditional Access policy, the attacker was not prompted for multi-factor verification. We'll delve into that later

4 From the victim's inbox, the attacker initiated an internal phishing campaign targeting all company employees

5 Several employees opened the infected attachments or clicked on malicious links, providing the attacker with access to critical business applications and infrastructure

6 The attacker accessed and exfiltrated sensitive data, concluding the attack by deploying ransomware to cover their tracks

Figure 1 Attack Scenario



[redacted] - All Employees contains about [redacted] recipients.

From [redacted].dk

To [redacted] - All Employees;

Subject Changes in the employee insurance policy

Dear all,

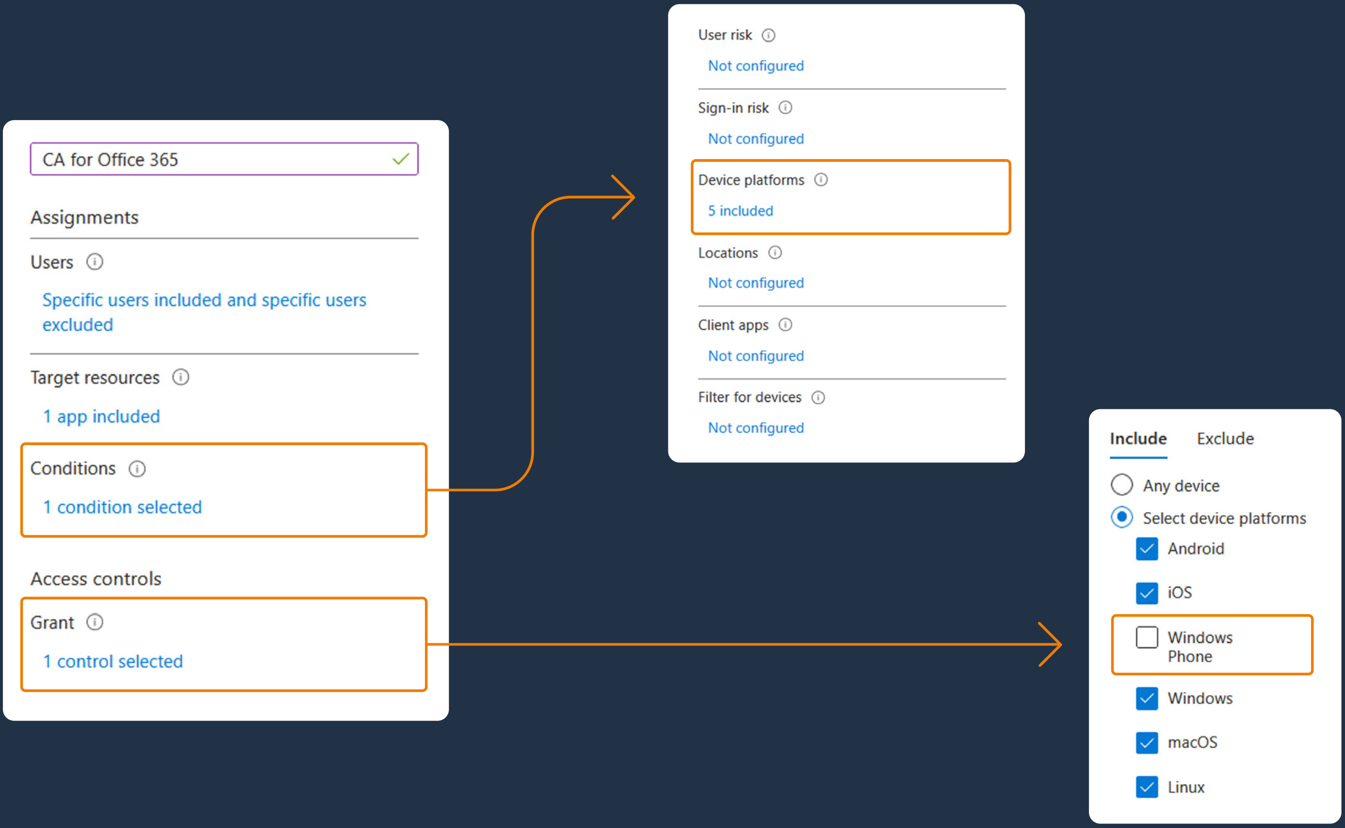
As discussed in the meeting last week there will be changes in the employee insurance policy. Please find the new insurance policy that will affect all the employees from May 5th. You can find more details following this link.

Best regards,

Now, let’s take a look at the misconfiguration of the Conditional Access policy.

It’s not enough to have a Conditional Access policy solely for the supported device platforms allowed to access your corporate data. Many assume that if a device is not on the supported list, it's automatically denied access.

Microsoft recommends you have a second Conditional Access policy for unsupported device platforms. This policy should cover all devices with the "Grant control" set to "Block access", excluding the supported platforms from the previous CA policy, which grants access with the requirement of multi-factor authentication. You can refer to Microsoft's official documentation by clicking here.



CA for Office 365 ✓

Assignments

Users ⓘ
Specific users included and specific users excluded

Target resources ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
1 control selected

User risk ⓘ
Not configured

Sign-in risk ⓘ
Not configured

Device platforms ⓘ
5 included

Locations ⓘ
Not configured

Client apps ⓘ
Not configured

Filter for devices ⓘ
Not configured

Include Exclude

○ Any device
● Select device platforms
☑ Android
☑ iOS
☐ Windows Phone
☑ Windows
☑ macOS
☑ Linux

https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-conditions#device-platforms

What are the benefits of IAM assessment?

Our Microsoft Identity & Access Management Assessment can help you maximize the value of your IAM suite, uncover misconfigurations, and optimize your security landscape. It considers your unique environment and assists your organization in understanding and enhancing your Azure Active Directory (Azure AD) environment through an analysis of your existing cloud and/or hybrid Identity & Access Management implementation.

The assessment covers the following areas:

- Identity provisioning
- Identity management
- Access management
- Security, governance, and identity monitoring

Master your IAM strategy

The evolving needs of modern businesses are driving organizations to explore cloud-centric IAM solutions that provide enhanced flexibility across various devices and platforms. As the IAM landscape continues to evolve, it's crucial for organizations to assess their unique requirements and thoughtfully consider their IAM strategies. Whether they rely on Active Directory, embrace cloud-centric solutions, or adopt a hybrid approach, safeguarding user identities and ensuring access to critical resources is vital in an ever-changing digital landscape where new challenges regularly emerge.

If you require assistance with your IAM strategy, please don't hesitate to contact us below.

Our Microsoft Identity & Access Management Assessment offers several key benefits:

- **Improve security** – pinpoint vulnerabilities and weaknesses in your organization's identity and access management practices, helping strengthen security, reduce the risk of breaches, and enhance data protection

- **Reduce costs** – eliminate redundancy, reduce licensing costs, and streamline operation to make long-term cost savings

- **Enhance efficiency** – identify opportunities to automate processes, simplify user provisioning, and streamline access requests, helping you boost efficiency, reduce administrative overhead, and improve user productivity

- **Improve user experience** – users benefit from easier and more secure access to resources, leading to higher satisfaction and productivity

- **Optimize scalability** – ensure that your IAM strategy is scalable and adaptable to changing business needs as your organization grows

- **Efficient user lifecycle management** – Efficiently manage your organization’s user accounts through-out their lifecycle, from onboarding to offboarding

Determining the appropriate resource allocation for an IAM assessment can be complex, considering factors like an organization's size, complexity, and budget constraints. By partnering with a consultancy, you can address resource allocation challenges more effectively. Consultancies leverage their experience, industry knowledge, and best practices to ensure the assessment is conducted efficiently and cost-effectively while delivering valuable insights and recommendations.

Contact details:

Mihai George Forlafu
mihai.forlafu@columbusglobal.com

Columbus

kontakt.dk@columbusglobal.com