Azure Active Directory and Office 365 Security

Don't let your on-premises Active Directory be your Achilles' heel

Written by Alvaro Vitta

INTRODUCTION

Seventy percent of Fortune 500 companies purchased Office 365 in a recent 12-month window. Microsoft calls Office 365 its fastest-growing commercial product ever.

It's no fad.

However, on-premises Active Directory (AD) still plays the main role in being the authoritative source for authentication and authorization requests to Office 365. System administrators in the vast majority of organizations use one-way Azure AD synchronization in this hybrid directory environment: They synchronize their authoritative, on-premises AD users, groups, attributes and passwords up to the cloud for authentication and authorization to Azure AD and Office 365.

That means that if the on-premises Active Directory is not secure, Azure AD and Office 365 will not be secure.

This paper describes a security methodology for governing a hybrid, on-premises/Azure Active Directory environment. System administrators will find detailed explanations and checklists for improving their security posture and keeping their on-premises AD from becoming the Achilles' heel of their Azure AD and Office 365 security.

THE HYBRID DIRECTORY SITUATION: ON-PREMISES ACTIVE DIRECTORY AND AZURE ACTIVE DIRECTORY

Every organization running Microsoft Office 365 has Azure AD, which is necessary to store user identities and other tenant properties for Office productivity applications, Exchange Online, SharePoint Online, Lync Online and any custom applications in the cloud.

At the same time, more than 90 percent of organizations have run and still run on-premises AD as the main store for the employee authentication, identity management and access

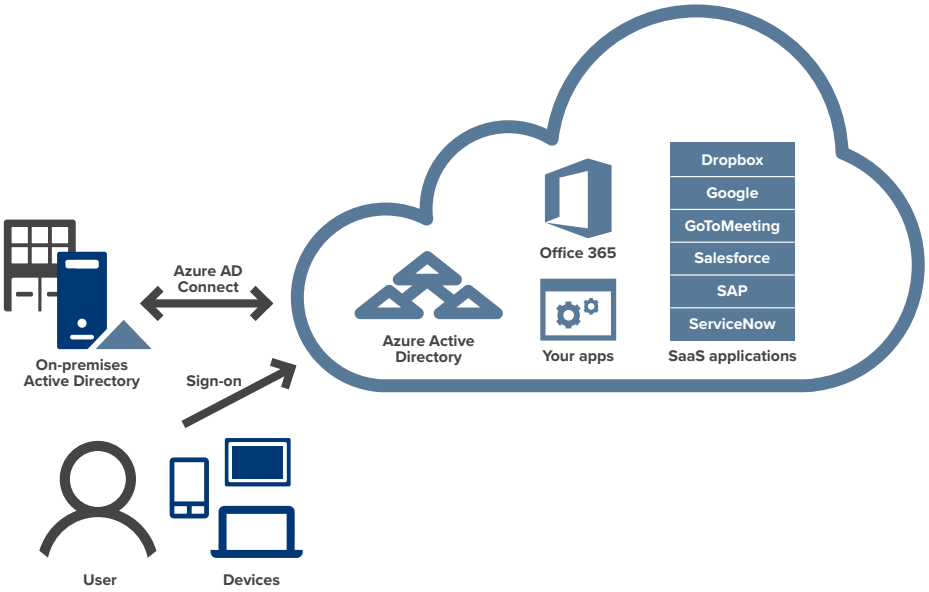

Figure 1: Azure AD Connect Synchronization Workflow Diagram

control polices behind on-premises products like Office, Exchange, SharePoint, Lync and hundreds of custom, line-of-business applications.

To address this hybrid directory situation, Microsoft has provided the Azure AD Connect management tool so that system administrators can synchronize passwords, identities, users, groups and corresponding attributes (potentially including password hashes) from on-premises AD to Azure AD without having to create new ones (see Figure 1).

Currently, Azure AD Connect is Microsoft's one-stop shop for this connection. It replaces the Active Directory management tools DirSync and Azure AD Sync, and allows for upgrading or migrating existing deployments of those tools quickly and easily.

THE HYBRID DIRECTORY ENVIRONMENT IS ONLY AS SECURE AS ITS WEAKEST LINK

When the on-premises Active Directory is the authoritative source, administrators can control and manage user accounts through the Active Directory Users and Computers snap-in. They create and delete user accounts, contacts and groups; modify group memberships; and deactivate accounts on the on-premises AD. The changes are replicated within three hours when using Azure AD Connect 1.0 or 30 minutes if using version 1.1.

Meanwhile, Microsoft's cloud security features, like defense-in-depth security, provides an end-to-end layered approach at the logical, physical and data levels. Unfortunately, on-premises AD does not include the same types of controls.

So, despite the defense-in-depth built into Office 365 security, the access controls in the on-premises Active Directory prevail. That means that all access to Office 365 applications and corresponding data is controlled by the user accounts and their group memberships in the on-premises AD. As a result, the compensating controls (or lack of controls) that govern the on-premises AD will determine whether access to Azure AD and Office 365 is secure or not.

The lack of compensating security controls within the on-premises AD environment is a recipe for data breaches and insider threats in a hybrid directory environment with one-way synchronization from on-premises AD to Azure AD.

All access to Office 365 applications and corresponding data is controlled by the user accounts and their group memberships in the on-premises AD.

ANATOMY OF A DATA BREACH IN A HYBRID DIRECTORY ENVIRONMENT

A report from Ponemon Institute titled "Privileged User Abuse & The Insider Threat" points to three main human-factor risks in privilege user access abuse:

- 73 percent of respondents said privileged users believe they are empowered to access all the information they can view ("I can, therefore I may").
- 65 percent said privileged users access sensitive or confidential data because of curiosity ("I wonder, therefore I may").
- 54 percent said the organization assigns privileged access rights that go beyond the individual's role or responsibility ("Nothing is stopping me, therefore I may").

Consider this scenario, in which those risk factors lead to a weakened security posture, a data breach and insider trading in a hybrid directory environment.

Sam is an IT contractor and domain administrator working at a midsized financial organization. The company uses on-premises AD groups to grant access to on-premises applications and uses one-way synchronization of groups and memberships to its Azure AD tenant for access to Office 365.

1. Mary, Sam's new colleague, forgets the service account password used to run a financial application across several Windows servers. She asks Sam to delegate her rights to reset passwords.
2. Sam uses the built-in Active Directory Users and Computers snap-in delegation wizard to delegate access to Mary to reset passwords on the organizational unit (OU) containing the service account. It does not occur to Sam that the OU also contains other service accounts and administrative accounts (members of the domain admins groups). Nor does it occur to him that he is granting Mary much more access than she needs to accomplish the immediate task.
3. Mary resets the password on the finance application service account.
4. Mary realizes that she can also reset the passwords to other elevated admin accounts. She resets a privileged admin account password.
5. She logs on with the admin account and grants her secondary account permissions to be able to make group membership changes across any group in AD.
6. She uses her delegated rights to add her secondary account to the finance operations group within the company's on-premises AD.
7. Like many other groups, the finance operations group membership in the on-premises AD is synchronized to Azure Active Directory to grant access to the company's Office 365 applications. In this case, the group membership provides access to Sarbanes-Oxley (SOX) financial data in Office 365 SharePoint Online documents.
8. Mary becomes curious. She discovers that she has access to confidential financial information on the company's Office 365 SharePoint Online.
9. She opens folders, finds a file named AcquisitionsPending.docx, opens it and takes screenshots. This file contains information about the proposed acquisition of a publicly traded competitor.
10. Mary uses this insider knowledge to purchase 10,000 shares of the acquisition target company. Three months later, the acquisition goes through. Mary sells her shares and makes a 30 percent gain.
11. An SEC investigation ensues, embroiling the company's legal, finance and compliance teams for months. Mary is eventually prosecuted for insider trading, but the damage to the company's reputation lingers.

That is an example of how a lack of compensating security controls on the authoritative source for access policies — here, on-premises Active Directory — can affect the applications and data that users can access on Office 365.

AN APPROACH TO STRENGTHENING THE WEAKEST LINK IN THE HYBRID DIRECTORY ENVIRONMENT

Quest recommends an approach to security in the hybrid directory environment that protects access to on-premises AD and consequently enhances Azure AD and Office 365 security. The result is a greater overall hybrid directory security posture.

Mary becomes curious and discovers that she has access to confidential financial information on the company's Office 365 SharePoint Online.

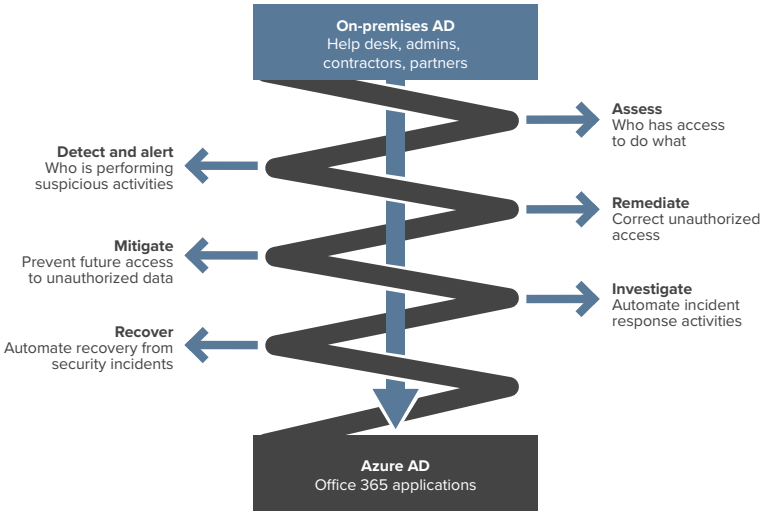

Figure 2: Hybrid directory security methodology

Hybrid directory security starts by continually assessing privileges and access, then establishing security configuration baselines.

As shown in Figure 2, the approach covers six areas of inquiry.

Assess

Where does hybrid directory security start? It begins in continually assessing privileges and access, then establishing security configuration baselines. This includes periodically reporting which users have access to perform which tasks, either directly through their account or indirectly through group membership.

Assessments should include details about all users with the most sensitive types of access:

- Permissions to back up and restore AD
- Permissions to reset user passwords on any objects
- Elevated privileged groups, such as built-in administrators, domain admins, schema admins and enterprise admins
- Sensitive business groups, such as finance, executive staff and R&D
- Sensitive data, such as personally identifiable information (PII), Payment Card Industry (PCI) details and information required for compliance with SOX and HIPAA
- Nested groups that are indirectly part of an elevated privileged group or a sensitive business group
- Permissions on the AdminSDHolder object
- Inactive accounts (last logon more than 90 days ago, expired accounts, last password reset exceeding password policy)
- Permissions to log on locally to domain controllers
- Permissions to install software on domain controllers

Detect and alert

What happens in case of security changes that deviate from the assessment baselines? The system must detect them as soon as they occur and automatically alert administrators.

Changes of greatest interest include the most common suspicious activities:

- User passwords changed by non-owners
- Direct and indirect (nested group) membership changes on elevated privileged groups
- Changes to security permissions on the AdminSDHolder object
- Changes to sensitive Group Policy Object (GPO) settings, such as “Deny logon locally,” NT LAN Manager (NTLM) level and AppLocker policies
- Mass deletions of accounts
- Assignment of sensitive AD permissions, such as delegation of user password resets across sensitive OUs
- Multiple failed logons followed by successful logons to domain controllers

- Logons to domain controllers during non-business hours
- Mass deletions or modifications of AD objects and attributes
- Addition of a user to the administrators group, followed by successful logon and removal from the group

Remediate

How do administrators continually remediate unauthorized access and security changes to stick to the assessment baselines? To bring about a self-healing environment that does not require human intervention, they should automate remediation in as many ways as possible:

- Reverting changes to unauthorized groups based on whitelists of users authorized to make membership changes. Changes made by users not in the list will be undone automatically.
- Reverting mass changes or deletions to AD objects such as group memberships, users and attributes in the on-premises AD automatically.
- Automating workflow to detect when user accounts are inactive (for example, no logon for 120 days).
- Moving inactive accounts to a disabled user container and automatically deleting them if not used within three days.
- For accounts created by users not in the whitelist, disabling both the initiating account and the created account.

Mitigate

What keeps unauthorized access from recurring after remediation? The principle of least privilege is an access model that further restricts the permission typically available for AD tasks and GPO permissions, mitigating the risk of recurrence.

Mitigation techniques focus on automated controls at the most conspicuous points of exploitation:

- Externalize AD permissions and control them in a proxy model. The model restricts not only who can do what in AD but also which objects given users can even see. For example, delegating rights in AD for a user to move accounts from one OU to another OU would also mean delegating the additional rights to delete any user object from the source OU and to write to the target OU. Similar to the scenario of the finance company above, those additional rights are unnecessary and excessive for the move operation. A proxy-based model of least-privileged access should allow only the move, without the unnecessary rights to delete and write.
- Next, enforce a real-time whitelisting permission model across AD objects and GPOs. Whitelisting ensures that only service accounts in a least-privileged-access proxy model may make changes to sensitive objects like the domain admins groups and domain controller GPOs. This will ensure that native privilege permissions (such as members of the domain admins group) are not abused or exploited.
- Use temporal group memberships coupled with approval workflows to mitigate risk arising from permanent memberships in sensitive and privileged groups. This also shrinks the window of opportunity for unauthorized access.
- Employ password vaulting to protect the powerful service accounts that control the least-privileged-access proxy model. The password vaulting product should automatically manage privileged accounts and sensitive business user accounts as well.

Investigate

How does the organization identify and contain security incidents? It performs quick investigations of the access lifecycle of users and groups in on-premises AD.

Effective investigations rely on 360-degree forensics and full-text search to correlate events, access activities and security configuration across multiple indexed repositories. Searches should reveal the most likely paths to any potential data breach:

- Any activity in AD, GPOs, files and computers by a given user during a given period
- Any activity in OUs, groups, files, computers, users and attributes containing a given word, such as "finance" or "salary"

> Automating remediation of unauthorized security changes helps admins stick to the assessment baselines without human intervention.

Effective investigations rely on 360-degree forensics to correlate events, access activities and security configuration across multiple indexed repositories.

- Security configuration and changes for a given user, including status of the user account in AD, department, last logon time, account expiration, accessible files, group memberships, changes to this object and activities initiated by the user
- Membership information for any given group, including recent changes to membership

Most important, investigations depend on contextual information around an incident. If, for example, a search on "NTLM" reveals a change to a GPO, the next step is to find the GPO name, the settings containing "NTLM," before and after values for the setting, where the changes originated and the domain controller on which the change was made.

Recover

How does the organization adjust to the continuous state of potential data breach and insider threat? It assumes breach and prepares itself to recover from unauthorized changes to on-premises AD, Azure AD and Office 365.

Every contingency plan must cover the basics, with as much automation as practical:

- Daily backup of AD database information, including attributes, GPO security and settings, cross-domain group memberships and all user attributes, including passwords
- Tight control and auditing of delegation of the rights to back up and restore Active Directory objects
- Encryption of AD backups on disk (encryption at rest) to prevent exposure of the NTDS.dit database
- Daily backup and automated recovery of the Active Directory schema forest metadata; since native AD backup does not protect this, it requires a third-party product to ensure quick, automated recovery of complete AD forests or of the domain
- Establishment of a recovery time objective for a full Active Directory recovery
- Documentation and testing of partial and full disaster recovery (DR) plans at least once a year
- Cross-training for IT staff on activating and executing the AD DR plan

CONCLUSION

In organizations that synchronize on-premises Active Directory with Azure Active Directory, automating the compensating controls for on-premises Active Directory is the best way to reduce the risk of data breach and insider attack.

The end-to-end approach outlined in this paper strengthens the organization's security posture in a hybrid directory environment. It promotes better management of access to on-premises AD and to all AD-dependent applications, resources and data. The approach also keeps on-premises AD from becoming the Achilles' heel of Azure AD and Office 365 security.

ABOUT THE AUTHOR

Alvaro Vitta is a principal solutions consultant specializing in security for Quest. He has been assessing, designing, testing and deploying security solutions at large enterprises for on-premises and cloud-based platforms in the private and public sectors for more than 15 years in the areas of identity and access management, Active Directory, and governance, risk and compliance. Alvaro holds industry certifications, including CISSP, CISSO, MCSE and ITIL.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (www.quest.com) for regional and international office information.