WHITE PAPER

Zero Trust for Hybrid Active Directory

Executive Summary

With the proliferation of Microsoft Active Directory (AD) and Azure AD (AAD) in 95 percent of the global Fortune 1000, AD is often the prime target of most cybersecurity attacks. Furthermore, with privileged access becoming an increasingly integrated element of what AD and AAD control, it is paramount that the hybrid environment is secure. Unfortunately, often it is inadequately managed. The result: exploited accounts, exposed assets, costly damage, long-term effects, and difficult remediation and recovery.

It is critical to protect against AD/AAD-targeted threats and provide visibility and control over privileged access – while also satisfying the need to improve hybrid administrative efficiency and reduce errors. The ideal solution will tell you what happened, help you remediate the effects, and help you prevent it from happening again. Establishing zero trust and least privileged access – as recommended by NIST SP 800-207- is key to secure privileged accounts for hybrid AD. It's also an important and effective way to simplify your organization's compliance with industry and governmental regulations.

Security Challenges in the AD landscape

With 95 percent of global Fortune 1000 companies relying on AD and Azure AD for user permissions and access, it is one of first places attackers look to compromise. What makes it worse is that native tools lack adequate management of the AD and AAD admin accounts. Microsoft tells us that 95 million AD accounts are the target of cyberattacks every day.[1]

Forrester estimates 80 percent of all data breaches involve misuse of administrative privileges[2]. This means that managing privileged security in your hybrid AD environment is essential to protecting your users and infrastructure. Additionally, One Identity's global survey[3] of privileged access practices found:

- 88% of survey respondents find managing privileged passwords challenging
- 86% do not change privileged passwords after each use
- 40% do not change default admin passwords on critical systems

All this adds up to making it easier for bad actors to compromise your privileged accounts.

Cloud Complications

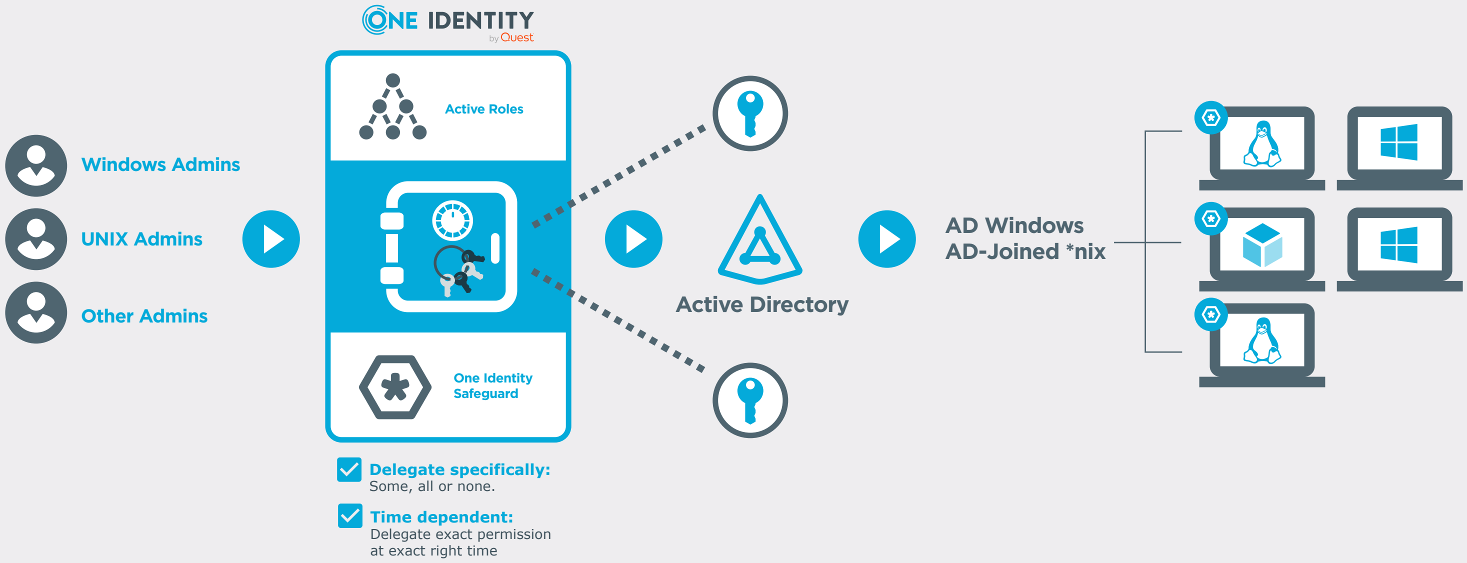
While securing on-premise AD is complex on its own, with Office 365 and Azure AD, the attack surface has increased dramatically. What this means from a security perspective is that any bad actor looking to compromise AD potentially could have a wider effect through Azure AD, unless certain steps are taken.

With cybercriminals honing in on AD and AAD, IT teams must be able to effectively and securely grant administrator access. If they are not successful, they are exposing the organizations to compliance and security risks. With this ever-changing threat landscape, the visibility and control necessary to fight it is lacking without proper tools. Common complications include admins frustrated by all the hoops they have to jump through to work securely and the tremendous amount of overhead it takes to build and maintain compliance.

Admin Accountability

The Active Directory (and Azure AD) admin accounts are all-powerful and must be used every time someone needs to maintain, update, and administer the directories or user accounts they contain. These admin accounts use shared credentials and are therefore anonymous and without individual accountability. So, anyone that needs to do anything on the systems must use the admin credential for on-prem AD and another for cloud-based Azure AD.

Enabling Zero Trust



Zero Trust and Least Privilege Models

However, there is hope. It is possible to secure the AD and AAD privileged accounts with a holistic approach. There are two proven methods for implementing privileged access management (PAM) in hybrid AD environments: Zero Trust and Least Privileged.

- **Enabling Zero Trust** involves eliminating the sharing of Admin passwords. Users are authenticated individually and dynamically for every administrative action. The credential is checked out when needed only after all the right approvals are procured, only for a specified purpose, or a specified time period.
- **Establishing Least Privilege** involves issuing just the permissions an admin requires to do their job – no more and no less. This way, they can get their day-to-day work done without intervention and eliminate the delay and tedium of asking for full admin rights for everything they need to do.

Blending PAM with Access to AD – PAMOps

Privileged Access Management (PAM) has become an integral part of organizational cybersecurity strategies and has been woven into security programs to ensure elevated privileges are controlled and audited. The concept of integrating PAM into business processes is becoming mainstream (now called PAMOps) as the concept of grows. While most organizations see the value of controlling privileged accounts, some have separated AD from the PAMOps strategy. While they may control some privileged accounts that live in AD, but have they fully 'crossed the streams' and blended PAM and AD account management?

Some may have left privileged access to AD out of the PAMOps strategy since AD does provide a basic delegation model. Native tools provide basic delegation however with some significant limitations for most large organizations.

- Assigned permissions are course-grained and static. Assigning permissions natively is simple but there are not many options to meet delegation requirements. This usually results in over-permissioning. Additionally, permissions are statically or permanently assigned, not granted when needed and removed when not being used.
- Permissions are only granted within the OU structure of AD. This also results in over permissions since admins often need access in many locations at different levels. It's much easier to just delegate at the top level or add to the Domain Admins group.

The National Institute of Standards and Technology (NIST) provides SP 800-207, *Zero Trust Architecture* to guide organizations in the concepts to reduce vulnerable permissions. Implementing Zero Trust Architecture in Active Directory presents some challenges since native tools only allow static permissions. The concept of 'Just-In-Time' provisioning allows users to be added to privileged groups when necessary, then removed when not in use. NIST also provides general guidance for managing privileged accounts and many of these recommendations apply directly to AD. NIST recommendations include:

Remove Unnecessary Access

Remove all privileged account access from users who no longer require access to perform their assigned duties. If they don't need it, why have it?

- **Delegation of the AD Admin account** — To do this effectively, your AD management tool should enable a least-privilege access model. This means that permissions for individual employees allows them to access the resources they need to do their job, but no more. This model includes limited management of elevated accounts and groups (such as Domain Admins, Enterprise Admins and Account Operators) without granting individuals unlimited privileges.

- **Temporal group membership (session management)** — This means that privilege elevation is not permanent and doesn't creep as a privileged user changes jobs. Users will only be part of a privileged group during a specified time to accomplish specific tasks. They are added to the group at the start time, then removed when that permission expires or the task is complete. So, if a privileged account is an attack target, the impact of that attack is limited to the user's normal privileges.
- **Integrate PAMOps and Just-In-Time privilege elevation** — This involves automating privileged group memberships when needed and removing when privileged tasks are complete. This ability alone significantly reduces the attack surface and vulnerability of privileged accounts in AD and Azure AD.
- **Controlled administration** — This is an administrative service that acts as a firewall around AD. This provides enhanced access control to privileged accounts by defining administrative roles, associated permissions and allows rules to be strictly enforced. It is the only way to effectively maintain compliance with security policies and regulations.

Remove Unnecessary Accounts

If the account is no longer required, why is it still there? Again, who needs it?

Accounts living in AD that are no longer needed or used are vulnerable to compromise, more so than an account with regular activity. You need a solution that provides the ability to programmatically eliminate this vulnerability through a policy backed up by a process. For example, an effective solution can automatically disable accounts that haven't been used in a certain number of days. Effective solutions should also come with default policies to automate commonly scripted deprovisioning tasks, and permits all provisioning policies to be tailored to an organization's specific needs.

> **Active Roles and Safeguard from One Identity allow enterprises with large hybrid ADs to implement much stronger policies for control and delegation.**

Remove Excessive Access

Do not allow 'role creep' into your AD environment. Commonly, this is where an admin either changes jobs and keeps the permissions from a previous position or is simply elevated to the top-level admin role with access to everything. How can you prevent role creep?

- **Proper delegation in AD** — You should look for a solution that can ensure the admin has just the permissions necessary to do their job. Functions such as dynamic group membership can prevent role creep as it can automatically issue and delete permissions (or roles) when an admin (or even a regular line-of-business user) changes positions.
- **Automated provisioning** — Automates user and group provisioning, including account creation in AD, mailbox creation in Office 365 or on-prem Exchange, group population and resource provisioning in Windows, which helps you save valuable administrative time and ensures accuracy. The solution you select should automate re-provisioning and de-provisioning to achieve an efficient administrative process over the lifetime of a user account or group.
- **Temporary Privileged Groups** — Putting privileged user accounts into permanent privileged groups is a critical vulnerability. You will be best served if your solution can temporarily populate privileged groups so that a user is a member only while performing privileged tasks, then they are removed when the task is complete. If the user account becomes compromised outside of the privileged window, it will not have any elevated privileges so any compromise would be negligible.

Remove Unnecessary Permissions

Remove all unnecessary permissions from privileged accounts. If they don't need access—don't give it. When AD was first released, it was a huge improvement over the directory of Windows NT 4.0 in that it had a delegation model. Not much has changed since then. Delegation needs of large enterprises are significantly more complex than native AD can possibly provide.

- **Provide granular delegation** — Native granular rights delegation in AD (particularly AD admin rights) is difficult, time-consuming and error-prone. Effective solutions provide automation, pre-built workflows and reporting that enables high granularity of access rights provisioning.
- **Look for a solution that enables AD tasks** — or groups of tasks to be easily delegated to any level, and even outside of AD's OU structure. This allows for flexibility in designing your permissions and delegation model, and even allows for overlap of delegation without over-permissioning.

The NIST recommendations are general principals designed to apply to the vast range of information systems. Hopefully, focusing some of those recommendations directly at hybrid AD provides high value. AD, as we know it, is in a state of transition itself. While working to secure the traditional on-premises AD, many enterprise initiatives are examining the feasibility of moving this critical service to the cloud. If your organization is using Office 365 then you're already using AD in the cloud. With most enterprises that have already completed studies on Azure AD feasibility, we see them concluding that hybrid AD is the next inevitable step.

Introducing Active Roles – On-prem or cloud - Hybrid Active Directory, simple and secure

With today's hybrid AD environments and the limited capabilities of native tools, admins struggle to keep up with requests to create, change or remove access. Thankfully, help has arrived. With One Identity Active Roles, you can solve your security issues and meet those never-ending compliance requirements by securing and protecting on-prem and cloud AD resources simply and efficiently. Active Roles:

- Overcomes native-tools limitations
- Manages accounts for Exchange Online, Lync, SharePoint Online and Office 365 and many more
- Provides a single, intuitive security and management tool for hybrid AD environment
- Integrates with One Identity Safeguard for Just-In-Time privileged access to follow NIST ZTA guidelines.

The cloud raises security questions. With Active Roles managing your on-prem AD as well as your Azure AD you will be able to:

- Enforce strong and flexible policies for administration and structure – even attribute control
- Synchronize on-prem AD with AAD through simple, easy-to-control connectors
- Manage on-prem and cloud ADs with a single interface (MMC or Web UI)
- Provide top-level admins with a familiar tool
- Allow fine-grained admin access across your entire hybrid AD environment

Securely store, manage, authenticate, record and analyze privileged access

The critical complementary piece of this Zero Trust and Least Privileged model is the PAM component that integrates seamlessly with your hybrid AD environment. Introducing the One Identity Safeguard family of PAM solutions. They are:

- Self-contained, hardened physical or virtual appliances ready to plug and play either on-premise or on your preferred cloud platform
- Modular, yet integrated, so that you only use what you need
- Easy and affordable to expand to support your growth and increasing needs
- Familiar to users, allowing them to continue to work with the tools and processes they know but with enhanced security and nearly no friction
- Easily updated to ensure that you always have the latest features and capabilities

Summary

Creating well-thought-out practices to secure and manage AD can be a very complex task, but the critical piece of the security pie is how they are implemented. Writing them down and expecting administrators at all levels to abide and enforce is simply not reasonable.

Active Roles and Safeguard from One Identity allow enterprises with hybrid ADs to implement much stronger policies for control and delegation as well as enhance security through automation such as Just-In-Time privilege elevation to follow the NIST Zero Trust Architecture. NIST has armed us with some good technology concepts to make significant strides forward in securing critical information. While they don't specifically address securing on-prem or cloud AD, it is critical that we translate the concepts and apply them to the system that is providing millions of access decisions every day for every organization.

About One Identity

One Identity by Quest, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com

Whitepaper_PrivilegedSecurityforAD_RS_63758