ENZOIC

E-BOOK

KEEPING ACTIVE DIRECTORY OUT OF HACKERS' CROSS-HAIRS

I. Active Directory

Active Directory (AD) is an authentication and directory service launched in 2000 that has been widely adopted by large enterprises, small businesses, and government agencies. The solution is now ubiquitous, with an **estimated 90% of enterprises and 100% of Fortune 500 companies** relying on it or its cloud-based version, Azure Active Directory, for seamless authentication and authorization. AD provides users with a single login to access systems, applications and resources. And administrators have an efficient way to manage and control access in order to keep the network organized and secure.

However, AD security has not kept pace with the growing complexity of the modern digital ecosystem. And given that AD is an entry point to valuable assets such as customer data, financial records, and other corporate information, it's not surprising that hackers continually target the service.

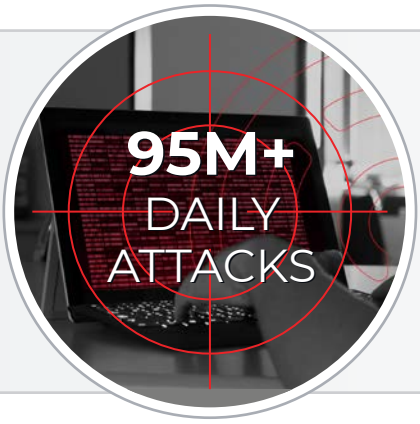
CREDENTIAL SECURITY

Exploiting compromised credentials and other password-related vulnerabilities is a chief avenue threat actors use to attack AD. Microsoft offers some basic capabilities in on-premise AD to address this issue, including password length and complexity requirements and enforcing password history. Azure Active Directory takes this a step further, with a Password Protection feature that uses a banned-list algorithm to vet password strength and block those that don't make the cut.

However, as we'll discuss, these capabilities leave many credential security gaps that fail to eliminate passwords as a threat vector. As the size of the credential problem continues to escalate, organizations must take action or risk falling victim.

A PRIME TARGET

Five years ago, Microsoft estimated that there were 95 million daily attacks against AD, but with today's increased attack surface due to hybrid work environments and cloud applications, it is likely far more than that. Research from Enterprise Management Associates (EMA) found that 50% of organizations experienced an attack on AD in the last 1-2 years, and 40% stated that the attack was successful.



The skyrocketing number of publicized attacks is shining a spotlight on AD as an attack vector and the need to take steps to reduce the risks.

II. Active Directory Snapshot

Before exploring the security concerns with AD it's important to understand more about the technology and its purpose.

WINDOWS PLATFORM

AD is Microsoft's directory service that runs on Windows Server, enabling administrators to efficiently manage permissions and access to network resources.

DYNAMIC

It's a dynamic directory that stores account login data and information on other resources within the network.

HIERARCHICAL

Unlike other solutions, it uses a hierarchical structure to organize information and IT administrators can manage every item within the database to ensure it's correctly grouped.

EASE OF MANAGEMENT WITH ADDS

Active Directory Domain Services (ADDS) is a directory service that stores and manages information about network resources and handles user interactions with the domain. ADDS employs a hierarchical structure composed of domains, domain trees, and forests to manage networked components. Administrators can locate directory information in any domain. They can also implement security policies based on users' roles and responsibilities, and they can layer these policies to refine or enhance access. For instance, administrators can create privileged accounts and groups, granting users extensive rights, privileges, and permissions to perform almost any action in AD and on domain-joined systems.

REPLICATION

Within the AD environment, data is replicated across a network so that every controller in a domain has a copy of all the information, regardless of whether it is on-premises or in the cloud. This makes it easy for administrators to manage; **however, it also presents a significant security risk.**

Once access is established, the entire company network and all data become vulnerable. As a result, AD is an attractive target for hackers since once they get inside a network, they have access to the entire system, including sensitive information such as password hashes.

HYBRID CONFIGURATIONS

AD is frequently deployed in a hybrid configuration with Azure Active Directory to extend an enterprise's on-premises infrastructure to the cloud while maintaining a centralized identity and access management system. This approach enables organizations to take advantage of both environments while preserving security and compliance. However, it may introduce additional security risks if the integration is not appropriately secured or if there are misconfigurations that weaken the security posture.

What Does AD Provide?

Provisioning - a flexible and scalable way to manage security and access to network resources based on groups and locations. Administrators can fine-tune access and security policies to AD resources while maintaining a secure environment.

Ease of Use - only one account is necessary for a new employee to access networked resources such as printers and shared files. Adding and deleting accounts is straightforward, as well as adding resources.

Organization of Network Hierarchy - quick and easy to organize the network hierarchy. For example, determine which computers and printers should be on the network.

Permissions - administrators create security groups and set permissions for users to access different resources, including applications and systems.

Passwords - management is easy; once a credential is reset, it automatically updates across the network. However, this is not sufficient when it comes to password management, as it fails to determine if a credential has already been exposed. This is a critical AD flaw that organizations must address to prevent compromised credentials from being used to gain network access.

III. Keys to the Kingdom

AD has been so pervasive as it is an efficient way to manage access and authentication. Administrators no longer have the tedious task of manually updating every change; instead, they do it once and it automatically updates across the entire network.

However, the centralized system has a fatal flaw: if a bad actor gains privileged access, they theoretically have a golden ticket to everything. The cybercriminal can move around and gain access to a myriad of proprietary and business-critical data across systems managed by AD.

For example, the NTDS.DIT file in Active Directory is replicated across domain controllers and can contain various types of personal information about users and other objects within a domain, such as user account details, contact information, and password hashes.

In addition, with the wide scale adoption of Microsoft Office 365, which uses AD to authenticate users, the attack surface extends from on-premises to cloud environments. And this makes AD an alluring target for hackers.

Once AD is compromised, hackers can modify the directory database and security settings and prevent legitimate users from accessing resources. Another tactic is to set up backdoors to access the network in order to distribute ransomware.

WORKING FROM HOME

The rapid shift to the cloud during the pandemic expanded the attack surface and, coupled with the staggering and growing volume of identity-based attacks, it's clear that enterprises must prioritize AD security. In 2022 Microsoft Security blocked more than 70 billion email and identity threats. ***Therefore, securing user identities should be mission-critical for every entity that uses AD .***

IV. Keeping Hackers Out of AD

Understanding how hackers are able to obtain AD access is a critical step in bolstering AD security. Some of the vulnerabilities can be addressed through better account auditing and management. For example:

ENSURING PROPER ACCESS PERMISSIONS

As mentioned, one of AD's chief benefits is its ability to efficiently grant access to numerous accounts and systems via a single login. However, if companies fail to frequently review the access governed by AD and confirm it's still relevant, this can easily become a vulnerability for threat actors to exploit. System upgrades, legacy security structures, outdated policies and workforce evolutions are among the factors that can unintentionally give users unnecessary privileges. This creates a situation where compromised accounts pose an even greater risk to system security.

PERIODICALLY REMOVING STALE ACCOUNTS

According to Microsoft, more than 10% of user accounts in Active Directory are considered stale based upon the user's last login timestamp or when the password was last changed. Former employees or hackers could use these stale accounts to attack the organization, so it's critical that companies frequently check for and remove all stale AD accounts.

Keeping a close eye on access permissions and inactive accounts is not enough to keep hackers out of AD. Microsoft offers guidance for hardening AD as well as frequent patches and updates.

However, the burden for adhering to and installing updates falls to IT teams—many of whom are already overburdened and grappling with an ever-increasing workload.

Another challenge is that hackers can often gain access to the network and inflict lasting damage before companies are even alerted to the threat. Verizon's DBIR found that 85% of Active Directory breaches took weeks or longer to detect. It's clear that this reactive security posture simply fails to meet the requirements of today's heightened threat landscape.

Closing the Password Loop

Many of the recent high-profile breaches resulted from attackers using compromised credentials.

According to Verizon, stolen passwords were responsible for 37% of breaches in 2017 and by the end of 2022, this had grown to 49%.

And with the ubiquity of deployment, most of these attacks are happening within AD. To underscore the magnitude of the problem, a study from Microsoft found that 90% of organizations have an insecure AD configuration reducing their cyber resiliency. It also found that 80% of security incidents could be fixed by adopting modern security practices.

THREATS TO ACTIVE DIRECTORY *FROM COMPROMISED CREDENTIALS*

1. Privilege Escalation
Once a hacker has access to an AD user account, they can escalate privileges in order to access other resources and systems and potentially compromise sensitive information or databases. Such access can be achieved by exploiting compromised credentials found on the Dark Web, including those leaked in third-party breaches.

2. Ransomware/Malware
Again, once inside the network, a bad actor can deploy ransomware or malware to compromise other systems within the organization.

3. Lateral Movement
By deploying techniques like pass-the-hash or pass-the-ticket, the threat actor can move laterally across the network and access additional resources. If the compromised password is for an AD administrator, hackers can create new user accounts or change permissions to gain access to anything they want.

4. Insider Threats
Legitimate AD users can also be a source of security breaches. This can be intentional, such as abusing privileges to steal sensitive data, or they can inadvertently misconfigure permissions or settings that bad actors then exploit.

Microsoft's Approach to Password Security

As mentioned, AD has some native capabilities to address credential security including:

COMPLEXITY REQUIREMENTS:
Enabled by default, this feature mandates that passwords meet complexity requirements such as being a minimum of six characters, and including both upper and lower-case letters and non-alphabetic symbols. As we'll highlight in subsequent sections, research has documented that this practice actually results in weaker passwords, making this an insufficient strategy for securing AD.

ENFORCE PASSWORD HISTORY:
The goal is to prevent password reuse by determining the number of unique passwords a user must cycle through before being allowed to deploy a previously-used password. However, there is no policy governing the use of the same root phrase with small character substitutions–for example, changing "Password1!" to "Password2!"

MIINIMUM PASSWORD AGE:
This determines the amount of time a password must remain valid before it can be changed again, and prevents non-compliant users from circumventing the above feature by immediately changing a password numerous times before returning to the original one.

While these and other built-in AD security features are certainly better than nothing, they fail to adequately protect the password layer.

Azure AD Enhances Credential Security–*But Gaps Remain*

Microsoft Azure AD provides more robust credential security through its free Password Protection feature. The solution evaluates a new password for both strength and complexity against the combined list of terms from Microsoft's Global Banned Password list and custom banned lists curated by the individual organization. The former is the result of Microsoft's Azure AD security telemetry data, providing a list of "base terms" discovered in weak passwords. Benefits include:

- The rejection of matches using leetspeak substitutions–for example, if "blank" is banned then "bl@nk" is also banned.
- If the proposed password adds, removes, or swaps the last character of an entry in the banned list, it won't pass.
- Users are prevented from including their name in a proposed password.

> *These enhanced features offer a basic level of protection but are no match for today's security landscape for numerous reasons detailed on the next page...*

PASSWORD SECURITY DEFICIENCIES *IN MICROSOFT'S AZURE AD*

LACK OF DARK WEB MONITORING

The solution does not actively monitor the Dark Web for compromised credentials, which means it cannot automatically ban passwords that have been exposed in breaches. This oversight creates a security risk, as attackers can potentially exploit such compromised passwords to gain unauthorized access to systems and sensitive information.

ALGORITHM LIMITATIONS

Microsoft also employs a confusing score calculation to evaluate "bad" passwords. Whenever a user changes or resets their password, the feature assesses its weakness and assigns a score based on specific criteria. However, it's possible for passwords containing entries from Microsoft's own Global Banned Password List to receive a passing score if the rest of the credential is determined to be strong enough. This means that users can employ passwords or portions of passwords that appear in cracking dictionaries—a situation that hackers can readily exploit.

FAILS TO CONTINUALLY MONITOR CREDENTIAL SECURITY

Another challenge is that the tool only checks password integrity when it is created. With breaches occurring constantly, it's highly likely that a credential that is secure at its creation will become compromised down the road.

Q: What should companies do to keep bad passwords out of AD and ensure network security?

A: One of the best ways to address AD security challenges is through tightening authentication. For example, employing multi-factor authentication (MFA) and hardening to prevent compromised and vulnerable passwords.

TIGHTENING AUTHENTICATION

MULTI-FACTOR AUTHENTICATION

Strong MFA relies on at least two factors from separate categories to verify users' identities— for example, a password (something you know) followed by a one-time code on a local device (something you have). Requiring this additional authentication layer when accessing AD is a critical component of keeping hackers out. However, while adding new authentication layers is beneficial from a security standpoint, it doesn't eliminate the need to harden each layer.

In addition, while Azure AD supports MFA, Microsoft does not offer it for on-premise AD, meaning that companies need to deploy third-party options. This requires additional costs and resources to set up, manage and maintain, all of which could lead to security gaps.

PASSWORD HARDENING

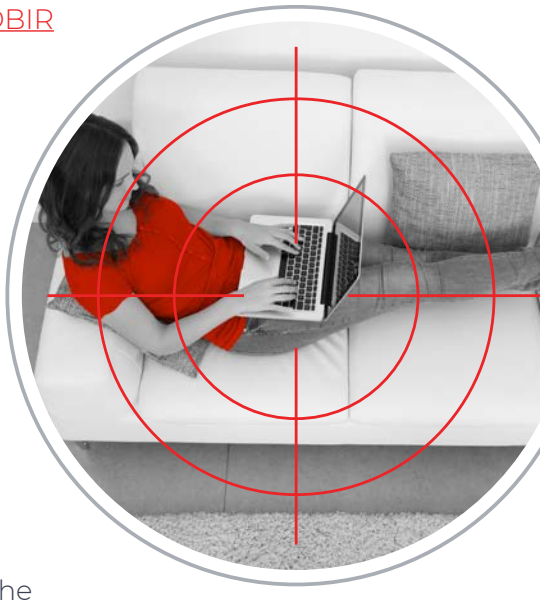
Password hardening refers to various methods of strengthening passwords to make it more difficult for bad actors to guess or crack them. This involves implementing more stringent password requirements and enforcing better password management practices such as:

Lockout Policy: Locking a user's account after a certain number of failed login attempts to prevent a successful brute-force attack.

Continuous Screening: Continuously screening for compromised passwords is an important component of password hardening. However, given the staggering rate at which new breach data is exposed, it's critical to ensure that credential screening reflects the latest threat intelligence. Vetting credentials both at their creation and on an ongoing basis against a continuously updated list of breached credentials found on the Dark Web is the single most important step a company can take to strengthen user passwords.

V. Protecting the Password Layer

Ultimately, AD security starts at the password layer. To provide insight into the scope of the problem, over 80% of breaches studied in the Verizon DBIR were attributed to stolen credentials. While implementing MFA and hardening passwords can help combat this vulnerability, ***it's important to understand why credential security has historically been so problematic.***



Unpacking the Password Problem

People are to blame for many password security issues:

POOR PASSWORD PRACTICES

In theory, users understand the importance of creating strong, unique passwords for every online account. In practice, however, these considerations are often outweighed by demands for convenience, efficiency and the inability to remember numerous complex passwords. This leads to poor password behavior, like using the same basic root phrase with minor changes for different accounts—for example, "Password1!" or "Password2!"

It's worth noting that, as mentioned, this substitution would pass muster with AD's native password security capabilities.

PASSWORD REUSE

Equally troubling behavior is the pervasive issue of password reuse. Ninety-one percent of respondents in one survey acknowledge the inherent risks of using the same password across multiple accounts, but 59% admit to doing it anyway. What's more, 62% of employees are reusing the same password or an easily guessable variant of the same password for both work and personal accounts—including signing into Active Directory. If just one of these accounts has been breached, then every other site or service associated with the exposed password is also at risk.

In the case of AD, an exposed credential gives hackers easy access into the network, enabling them to avoid detection and move laterally to conduct a range of nefarious activities.

When a targeted attack is occurring, hackers will oftentimes start by perusing readily available breach corpuses, with billions of previously compromised credentials, looking for a match with a target's personal or corporate email. Once one or more matches are found, these passwords will become sources used to attempt to guess the target's current AD password, which quite often will be a variant of a previously used password.

According to research from the UK's National Cyber Security Center (NCSC), 75% of organizations use credentials that were found in the top 10,000 most common passwords in their Active Directory.

Legacy Password Management Approaches Leave Gaping Holes

Companies have historically tried to address password vulnerabilities through policies like time-based forced resets, but this exacerbates the issue.

REAL-TIME THREATS: One reason is that, with new breach data available on a real-time basis, no scheduled period is short enough to eliminate the vulnerability.

PREDICTABLE PATTERNS: Another issue is that when a user knows they must reset their password every quarter, they follow a predictable pattern such as the one outlined above, in which just one or two characters on a reused password are changed.

COMPLEXITY IS NOT SECURITY: Another archaic password management practice is equating complexity with security. Again, the challenge here comes back to human behavior. Users want an easy-to-remember password and are likely to select basic phrases such as "P@ssword1!". This might check all the boxes from a compliance perspective but it's clearly a weak password guaranteed to exist on a list of stolen credentials.

Focus on Exposure—Not Expiration or Complexity

As mentioned, research has documented that these and other legacy password management approaches encourage more predictable behavior patterns that hackers can exploit. In fact, Microsoft itself has come out against password complexity and expiration, calling the latter ***"...an ancient and obsolete mitigation of very low value."*** That's why companies should forget about complexity and expiration, and rather ensure that credentials used in AD have not been exposed.

The National Institute for Standards and Technology (NIST) recommends that companies screen new passwords against those known to be commonly used, expected, or compromised.

> *Given the vast and ever-growing amount of newly exposed credentials available to hackers, organizations must continuously check password integrity to keep these credentials out of AD.*

VI. Enzoic for Active Directory

ENZOIC

The only way to do this effectively is by continuously screening credentials against a database that reflects the latest breach intelligence. Enzoic for Active Directory vets password and username combinations against its proprietary database of billions of exposed credentials. Enzoic maintains the latter using a combination of proprietary automated processes, submitted contributions and research from its threat intelligence team. In addition, the database is updated multiple times per day, ensuring that companies' AD password security mirrors the most current breach data.

Enzoic for Active Directory works by plugging into a company's AD environment and screening passwords both at their creation and on an ongoing basis to eliminate credentials as a threat vector.

The solution is the only AD product to provide this level of continuous, comprehensive protection against compromised credentials.

CREDENTIAL PROTECTION	Microsoft Azure AD Protection	ENZOIC for Active Directory
Uses Dark Web Data	✗	✓
Continuous Monitoring for Account Compromise	✗	✓
Full Compliance With NIST 800-63b Digital Identity Guidelines	✗	✓
Allows Values Found in Cracking Dictionaries to be Used in Passwords	✓	✗
Proprietary Scoring Algorithm	✓	✗
Leetspeak substitutions	*Limited number of Leetspeak substitutions*	*Includes all common substitutions, such as 1 for L or $ for S*

"After deploying Enzoic we were able to follow NIST standards, and eliminate all compromised passwords from our Active Directory environment. The installation process took only one hour across our eight domain controllers. The project allowed us to improve enterprise security and reduce helpdesk resources dedicated to passwords by 90%."

~ Ramon Diaz, director of IT, Hylan

Automatic Active Directory Peace of Mind

In addition to enhancing AD password security, Enzoic ensures that it comes without adding any additional burden on IT. The solution is easy to deploy, with some customers having Enzoic for Active Directory fully implemented in just 15 minutes. By facilitating NIST compliance the solution allows organizations to adopt modern guidance to forgo routine password resets, which in turn helps to cut down on helpdesk calls and lessen operational interruptions tied to these resets. Because the screening happens automatically, IT resources can be deployed to other strategic areas with the knowledge that AD security is addressed.

Should a compromise be detected, organizations can automatically activate a remediation plan. These offer a range of actions based upon the threat's severity, up to and including the immediate disabling of the compromised account. In addition, Enzoic for Active Directory enables companies to set specific password rules and remediation actions by Container, Group, Organizational Unit, or account. This allows them to have a more aggressive monitoring and response for sensitive accounts—for example, those related to finance or IT.

Enhanced Security without User Friction

Another benefit of Enzoic for Active Directory is that it offers a friction-free user experience, unlike other approaches to password security that have historically frustrated employees. Users with uncompromised credentials gain access without additional steps or device requirements. Employees only become aware that the screening has occurred in the event of a compromise, at which point companies can automate the process of facilitating safe access to the account or system.

With the pace of credential-based attacks showing no sign of slowing, it's clear that protecting the password layer is a critical component of a modern AD security strategy. Every organization must take steps to shore up its defenses and reduce the threat of attacks and data breaches occurring.

Enzoic for Active Directory is a cost-effective, efficient solution that complies with NIST recommendations to protect account and system access without adding an additional IT burden or introducing friction into the user experience.

With Enzoic for Active Directory, companies can check password integrity at creation and on an ongoing basis—ensuring that the IT environment is free of unsafe passwords. It's an easy-to-install plugin that provides a frictionless way to identify, monitor, and remediate unsafe passwords. Click here to try Enzoic for Active Directory.