ConversationalGeek

Improve SECURITY, MANAGEMENT, *and* PRODUCTIVITY *through* Active Directory Modernization

Sponsored by Quest

www.conversationalgeek.com

Today, Active Directory (AD) environments continue to remain in use worldwide, spanning from small businesses to massive enterprises. However, most of these environments are far from optimized. They are often weighed down by years of incremental changes, outdated security configurations, and a sprawling number of domains and trusts. While AD has served as a reliable backbone for many organizations, the time has come for *modernization*—a thorough review, consolidation, and securing of AD environments to ensure they are not just functional but also resilient against today's evolving cyber threats.

Organizations with on-premises Active Directory should be (or hopefully, are) taking a hard look at their current environment and recognizing the need to simplify, secure, and modernize it for a number of reasons:

Security: Decades of AD configurations, permissions, and group policies left unchecked create a fertile ground for cyber threats. An outdated AD environment can inadvertently provide multiple access points for cybercriminals.

Years of Mismanagement: Active Directory sprawl—multiple domains, trusts, groups, and permission sets—leads to a significant management burden. IT teams spend more time managing and troubleshooting than strategically improving the environment.

Anything but Simplicity: Environments with multiple AD domains create unnecessary complexity, creating undocumented dependencies and making everything from domain management to user authentication difficult.

Productivity: The current state of these kinds of AD environments impacts the productivity of users, but also (and more to the point) IT teams as well. Increasing AD management overheads means IT teams have to place their focus on reactive problem solving rather than strategic initiatives.

The answer to these challenges is *Active Directory modernization*—a structured approach that involves consolidating and securing AD environments, reducing the attack surface, and aligning the organization's directory services with current security standards and business needs.

The goal of this eBook is to provide you with an understanding of the necessity for AD modernization, highlight real-world use cases, and guide you on how to best approach modernizing your Active Directory environment.

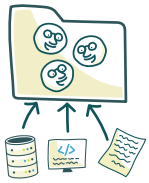
Why Modernizing AD isn't a Simple Task

Historically, managing an Active Directory environment was a straightforward process: set up domains, create users, manage permissions, and keep things running. However, as organizations have expanded, merged, and adapted to new technological landscapes over the decades, these environments have evolved into highly complex ecosystems. Modernizing an AD environment today is not just about moving to a new domain; it is about securing, consolidating, and configuring the entire environment to mitigate risks, enhance manageability, and support future growth.

Several key factors make AD modernization complex:

Security Risks: Over the years, Active Directory environments often become riddled with security vulnerabilities that need to be identified and remediated. These vulnerabilities can come from a variety of sources, including misconfigured permissions, excessive access rights, orphaned accounts, and legacy trusts between domains. Attackers exploit these vulnerabilities to gain initial access, escalate privileges, and move laterally within the network. AD modernization provides a vital opportunity to address these risks by re-evaluating every aspect of the directory's configuration and consolidating domains to reduce the attack surface.

Over-Permissioned Users and Groups: One of the most significant challenges in managing an AD environment is ensuring that user accounts and groups have the appropriate level of access. Over time, user accounts accumulate permissions as roles change, temporary access is granted, or policies are implemented without proper documentation. This "permission creep" results in over-permissioned users and groups, which can significantly increase the risk of insider threats or unauthorized access during a cyberattack. Proper modernization involves not just auditing current permissions but also implementing least-privilege principles and automated controls to prevent permission creep from occurring again.



Configuration Sprawl: Active Directory environments can suffer from "configuration sprawl," where Group Policy Objects (GPOs), domain trusts, and other settings are created and then forgotten. These configurations can contradict one another, create security holes, or simply clutter the environment, making it difficult to manage and understand. For example, outdated GPOs might conflict with new security policies, leading to unintended access or misconfigured devices. AD modernization should include a comprehensive review and cleanup of these configurations to ensure they align with current security and business requirements.

Ongoing Management Needs: The journey to a secure and modern AD environment does not end after the initial modernization process. Continuous management and monitoring are crucial to maintaining a secure posture. New vulnerabilities, policy changes, and user additions can all introduce new risks. A robust AD modernization strategy includes implementing tools and practices for ongoing monitoring, alerting, and auditing to quickly identify and address any deviations from the desired state.

Addressing these concerns requires a comprehensive strategy that goes beyond simple migrations or configurations. It involves rethinking the architecture of AD environments, establishing a clear roadmap for security and consolidation, and leveraging advanced tools to automate and streamline the process.

Below are the four primary Use Cases for AD modernization. Each use case will cover the specific challenges organizations face, outline the risks of not addressing these issues, and then take a look at what your options are to modernize AD.

USE CASE 1

IDENTIFY AND PROTECT "TIER 0" ASSETS

At the heart of every organization's IT infrastructure lies a set of core services, systems, and accounts referred to as "Tier 0" assets. These are the most critical components, such as domain controllers, DNS servers, and administrative accounts, that, if compromised, could result in catastrophic damage to the entire environment. Over the years, as organizations grow and their environments evolve, visibility into these Tier 0 assets and who has access to them can diminish, resulting in an expansive attack surface ripe for exploitation by cybercriminals. Protecting Tier 0 assets is not just about knowing what they are but also consolidating and securing them to ensure they are well-managed, and their access is tightly controlled.

Why It Matters to AD Security

Tier 0 assets form the backbone of an organization's IT environment and serve as the foundation upon which all other systems and services are built. If these critical assets are compromised, the attacker potentially may gain control over the entire environment. This makes Tier 0 assets a high-value target for cybercriminals. Effective AD modernization involves not just identifying these assets but also implementing strict access controls, auditing capabilities, and protective measures to ensure a limited number of trusted individuals have access, minimizing risk.

What's the Challenge?

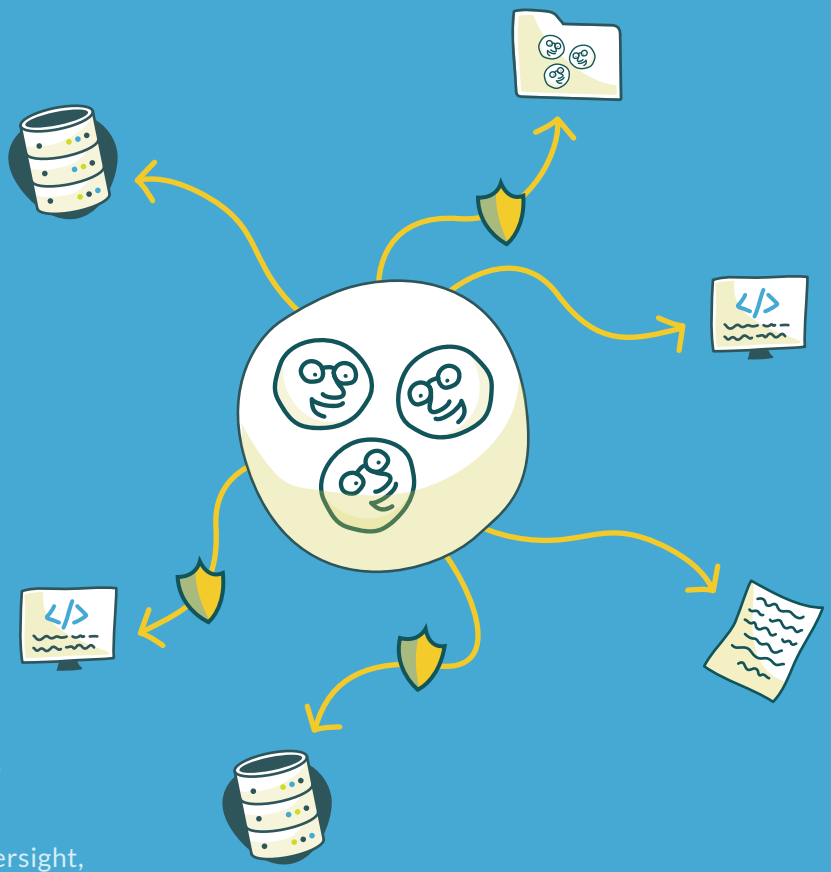
Over time, the clarity of which systems and accounts qualify as Tier 0 assets tends to blur. This issue is exacerbated by mergers, acquisitions, and organic growth, leading to a situation where *too many users or accounts have privileged access.* This over-permissioning creates multiple potential points of failure that threat actors can exploit. Organizations may struggle to accurately map out all Tier 0 assets due to years of incremental changes, poor documentation, or turnover within IT teams.

And If You *Don't* Address It?

Failure to secure Tier 0 assets is akin to leaving the keys to the kingdom under the doormat. Attackers who gain access to these critical assets can launch devastating attacks, such as stealing sensitive data, encrypting it as part of a ransomware attack, or shutting down essential services. Without clear visibility and control over Tier 0 assets, an organization is left vulnerable, with no real understanding of how exposed they are to a potential breach.

USE CASE 2

IDENTIFY & MANAGE ELEVATED ACCESS



Elevated access is a double-edged sword within any Active Directory environment. On the one hand, it is essential for certain users (e.g., IT admins) to have elevated privileges to perform their tasks. On the other hand, without strict management, these elevated privileges can become widespread and uncontrolled, leading to a phenomenon known as "elevated access sprawl." Over time, accounts may be granted excessive permissions without proper documentation or oversight, leaving the organization vulnerable to insider threats or external attacks.

Why It Matters to AD Security

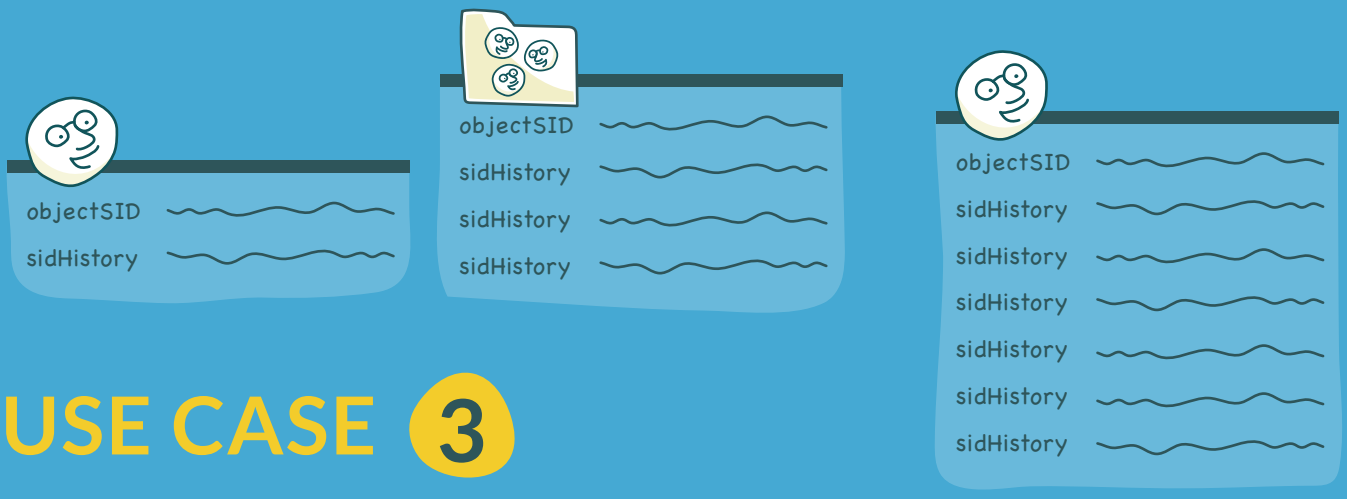
Elevated access permissions, such as those granted to Domain Admins or Enterprise Admins, provide the keys to the kingdom within an AD environment. When these permissions are spread too broadly or managed poorly, they create significant security vulnerabilities. Effective management of elevated access is critical because it helps reduce the risk of a compromised account being used to gain widespread access to sensitive systems and data. By minimizing the number of accounts with elevated access and implementing least-privilege principles, organizations can significantly strengthen their overall security posture.

What's the Challenge?

The challenge with elevated access is twofold: first, accurately identifying where all elevated permissions exist across the AD environment, and second, managing and minimizing these permissions without disrupting business operations. Over the years, elevated permissions may have been granted temporarily, but have remained in place long after they were needed or become intertwined with other permissions and roles. Additionally, without centralized control and documentation, it is nearly impossible to know which accounts genuinely need elevated access versus those that have accumulated unnecessary permissions over time.

And If You *Don't* Address It?

Leaving elevated access unchecked can be catastrophic. If an attacker compromises an account with elevated privileges, they can quickly escalate their privileges, access sensitive data, disable security controls, or even bring down critical systems. In essence, the more points of elevated access that exist, the easier it becomes for attackers to move laterally across the environment. Organizations serious about cybersecurity cannot afford to ignore the risks associated with poorly managed elevated access.



USE CASE 3

MANAGE THE RISKS OF SID HISTORY

Security Identifier (SID) History is a feature within Active Directory that was initially designed to ensure continuity of access during domain migrations. However, while useful for maintaining productivity, SID History can create significant security vulnerabilities. This is because it allows old SIDs to remain associated with user accounts long after the old SIDs are needed, potentially granting users unauthorized access to resources across domains. Modernizing AD involves carefully managing SID History to eliminate these risks, ensuring that access is tightly controlled and that old SIDs no longer pose a threat.

Why It Matters to AD Security

SID History was a helpful feature during past AD migrations, allowing for a smoother transition by preserving access rights associated with old user accounts. However, while this capability is beneficial for productivity, as more domains are added and old ones are decommissioned or merged, SID History can become a hidden security liability. If not managed correctly, SID History can grant users unintended access to resources long after a migration is complete, creating opportunities for unauthorized access and data breaches. Modernizing AD involves eliminating these risks by carefully managing SID History and ensuring that only necessary access remains.

What's the Challenge?

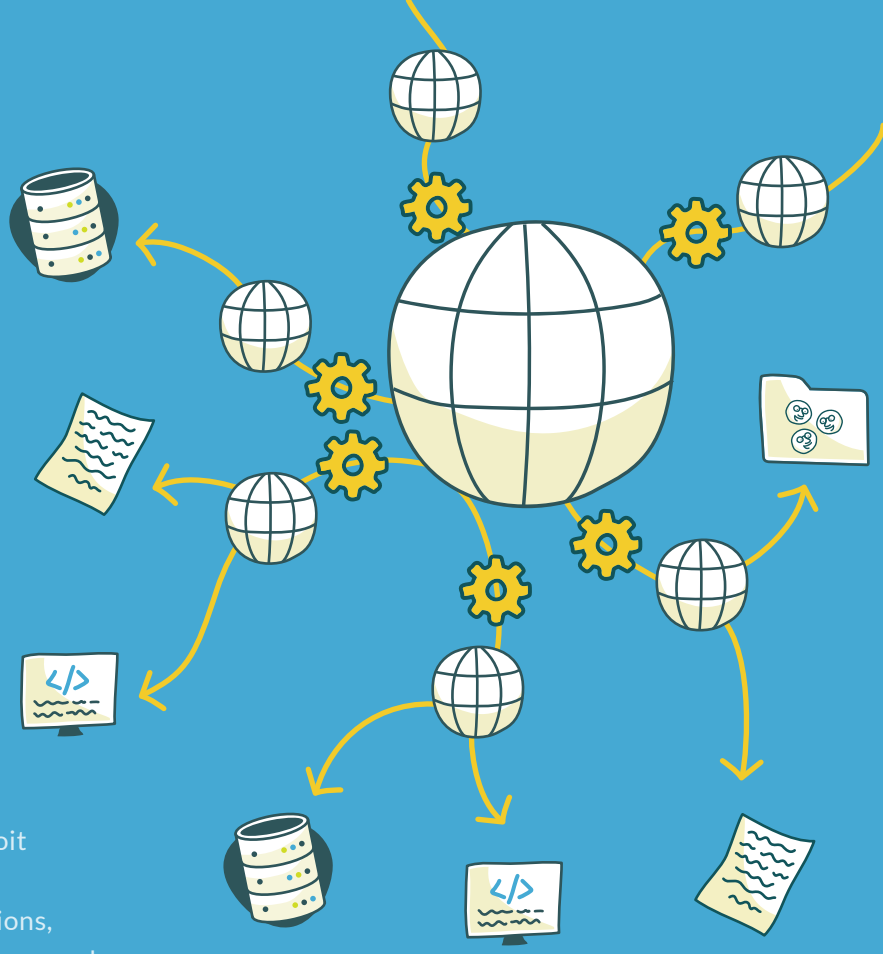
The challenge of managing SID History lies in understanding which SIDs are still relevant, and which are no longer needed. It is a meticulous process that requires a comprehensive review of all existing SIDs and their associated permissions. In environments with multiple domains, this task becomes even more complicated as legacy SIDs can cross domain boundaries and provide backdoor access to sensitive resources. Additionally, the successful removal of SID History without breaking necessary access or disrupting business operations requires a well-planned approach and the right tools to ensure a smooth transition.

And If You *Don't* Address It?

Retaining SID History indefinitely is like leaving multiple unlocked doors in a secure facility. Over time, these doors multiply as more migrations occur, increasing the complexity and risk. Attackers can leverage these old SIDs to gain access to sensitive resources across different domains, making the environment vulnerable to data breaches and insider threats. For organizations aiming to secure their AD environment, managing and eventually removing SID History is non-negotiable.

USE CASE 4

ADDRESS AD CONFIGURATION SPRAWL



Over the lifetime of an Active Directory environment, configurations such as Group Policy Objects (GPOs) and domain trusts accumulate, often with little to no ongoing review or documentation. This "configuration sprawl" can create a labyrinth of settings and policies that, if not properly managed, may provide ample opportunities for attackers to exploit weaknesses. Modernizing AD requires a thorough evaluation and rationalization of these configurations, ensuring that the environment is streamlined, secure, and easier to manage moving forward.

Why It Matters to AD Security

Changes to AD configurations are often set and forgotten, leading to security vulnerabilities, conflicts, and inconsistencies. For example, conflicting GPOs could inadvertently grant users access to systems they shouldn't have or apply outdated security settings that compromise the environment's integrity. AD configuration sprawl can also make managing the environment increasingly complex, leading to conflicting policies, misconfigurations, and security gaps. Addressing configuration sprawl is essential to create a streamlined and secure AD environment that is easier to manage and less prone to attacks.

What's the Challenge?

The primary challenge in addressing configuration sprawl is the sheer complexity of auditing, rationalizing, and managing every GPO, trust relationship, and configuration setting across multiple domains. Many of these configurations were created years ago and may no longer be documented or relevant, yet they continue to impact the environment. Misconfigurations or overly permissive trusts can open doors for attackers, allowing them to move laterally or escalate privileges. Cleaning up this sprawl requires a detailed understanding of each configuration's purpose, its current impact, and the potential risks it introduces.

And If You *Don't* Address It?

Ignoring AD configuration sprawl is a significant security risk. Misconfigurations can easily be exploited by cybercriminals to gain unauthorized access, disrupt services, or launch ransomware attacks. Furthermore, managing a sprawling and inconsistent AD environment becomes increasingly difficult for IT teams, leading to inefficiencies, increased costs, and a higher likelihood of security incidents. For organizations looking to future-proof their AD environment, addressing configuration sprawl is a critical component of any modernization effort.

The Path to Seamless AD Modernization:
What Are Your Options?

To address these challenges, IT departments have several options, each with its own advantages and drawbacks. Choosing the right approach depends on the size and complexity of the environment, as well as the organization's specific goals and resource availability:

1 Manual Review and Remediation

This traditional approach involves manually reviewing and remediating AD environments, which is labor-intensive and prone to human error. IT teams will need to map out every domain, trust, user account, group policy, and permission manually, identify redundancies, and decide what to consolidate or eliminate. This process can take months or even years to complete, depending on the size of the organization.

Pros	Cons
• A manual review allows for complete control over the process, ideal for organizations with specific needs.	• Manual remediation is highly time-consuming, making it impractical for large environments.
• This approach enables highly tailored configurations that can address unique requirements.	• It is prone to human error, increasing the risk of overlooked security gaps or misconfigurations.
	• This method does not scale well and requires significant resource investment.
	• Legacy configurations can easily be missed, leaving security vulnerabilities unaddressed.

2 Using Microsoft Native Tools

Microsoft provides several native tools to help with modernizing your AD environment, such as Active Directory Migration Tool (ADMT), Security Compliance Manager, and Group Policy Management Console (GPMC). These tools can be used to create basic levels of visibility into current configurations (necessary for identification and rationalization of configuration or access sprawl). They also address basic migration tasks (needed for addressing SID History), manage GPOs, and perform security baselines, but they often lack the capabilities needed to comprehensively address the security risks outlined in this eBook.

Pros	Cons
• Microsoft's native tools are familiar to many IT teams, reducing the learning curve.	• Native tools lack robust automation, making them unsuitable for complex environments.
• These free tools work well with existing Microsoft infrastructure, making them a cost-effective option.	• They do not cover all aspects of AD modernization, especially around security and legacy issues.
	• Customization and additional scripting may be required, adding complexity and time to the process.
	• They are less effective for managing cross-domain permissions and complex configurations.

3 Third-Party Automation Solutions

Comprehensive solutions like the Quest Active Directory Modernization Suite offer enhanced security features, centralized management for AD modernization, and – in some cases - end-to-end automation. These solutions go beyond what native tools provide, offering a more streamlined and efficient approach to consolidating domains, managing permissions, and securing AD environments.

Pros	Cons
• Third-party tools provide full automation, significantly reducing manual effort and improving efficiency.	• Third-party solutions require an upfront investment and additional training for IT teams.
• They preserve user configurations during migration, minimizing disruption to end users.	• There may be a learning curve as IT teams become familiar with the tool's capabilities.
• These solutions offer centralized management and visibility, ideal for large-scale environments.	• Highly customized environments may need additional services to fully configure the solution.
• Enhanced security features ensure that vulnerabilities are addressed throughout the modernization process.	

CHOOSING THE RIGHT MODERNIZATION PATH

For most organizations, the decision on how to modernize Active Directory involves balancing control, effort, cost, and security. While manual methods and native tools may suffice for smaller or less complex environments, comprehensive solutions like Quest's offer the automation and security enhancements needed for larger, more complex AD environments.

By choosing the right strategy, IT can ensure a secure, efficient, and well-managed Active Directory environment that aligns with both current and future organizational goals. Organizations that invest in a thoughtful, comprehensive AD modernization strategy today will find themselves better positioned to protect their assets, streamline management, and support future growth.

Quest®

You're not alone if you're evaluating your AD environment and feeling overwhelmed by the complexity. But you'll realize the benefits of modernizing AD are worth the effort. Quest has been helping IT professionals consolidate AD since its inception and protecting against the next threat with identity-centered cyber resilience. Our solutions for Active Directory modernization include a broad range of consolidation, security and management solutions.

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.

For more information, visit: www.quest.com/solutions/active-directory