Mitigating the top 5 modern Active Directory threats

Reduce your attack surface and enhance your identity threat detection and response.

Quest

Introduction

Identity is the new security perimeter — adversaries work relentlessly to compromise user accounts because they provide access to valuable data and critical systems. And one of the top targets of these attacks is Active Directory (AD). The reason is simple: AD is a primary authentication and access provider for the vast majority of organizations today, even those that have embraced cloud technologies like Entra ID and Microsoft 365.

If Active Directory gets compromised, the consequences can be dire. Indeed, when ransomware takes AD offline, the average downtime is 21 days. That's because the forest recovery process is incredibly complex and time consuming if you don't have the right tools and a thorough, well-practiced plan in place. And the cost of that downtime can be astronomical, averaging up to $730,000 per hour. That's $17.5M per day!

Moreover, attackers who compromise Active Directory are not limited to the on-premises environment. They can move laterally into Entra ID and access your cloud resources as well, including critical data in Microsoft 365 workloads. For example, if you have a hybrid Entra ID user account that has administrative rights, an attacker who compromises the on-premises account can take over the Entra ID administrative account, circumventing the modern security controls included in Entra ID.

Clearly, securing Active Directory has to be a top priority for your organization. Discover the key challenges you are likely to face and how to overcome them with a comprehensive solution from Quest.

Key challenges in securing Active Directory

Despite the maturity of Active Directory, organizations still face hurdles in securing their AD environment against threats. The following five challenges top the list:

- Lack of basic security hygiene
- Ever-increasing attack surface
- Failure to use an administrative tiering model
- Alert fatigue
- Neglect of the on-premises environment

Challenge #1. Lack of basic security hygiene

Organizations often assume that adversaries are using super exotic techniques and new research into the inner workings of Active Directory, and sometimes that that is true. But for the most part, the reality is quite different: Most cyberattacks target well-known weaknesses, using well-known techniques and readily available tools. After all, Active Directory is now 25 years old and while Microsoft releases new versions of Windows Server every few years, the basic platform has remained the same for a long time. As a result, the inner workings and common weaknesses of Active Directory are well known by cyber criminals, who eagerly exploit them.

Indeed, the Microsoft Digital Defense Report 2023 reveals that one of the most common exposures found in ransomware response engagements is insecure configuration of the Active Directory platform. That's not surprising, since the previous year's report found that a staggering 88 percent of organizations don't adhere to basic Active Directory security practices.

88%

of organizations don't adhere to basic AD security practices. But basic security hygiene can protect against 99% of attacks!

Examples of insecure AD configurations include:

- Business users with excessive permissions, up to and including having direct or indirect membership in powerful administrative groups
- Highly privileged service accounts whose passwords haven't been changed in ages
- A KRBTGT password that hasn't been changed in a long time
- Orphaned accounts and unneeded security groups
- Unpatched software and outdated systems that no longer receive security updates
- Use of weak protocols like NTLMv1
- Domain controllers (DCs) that have non-essential applications and services installed
- Convoluted Group Policy

The good news is that the Microsoft report also reveals that organizations can protect against over 99 percent of attacks by adhering to fundamental security hygiene practices. When it comes to identity threats, the core set includes the following:

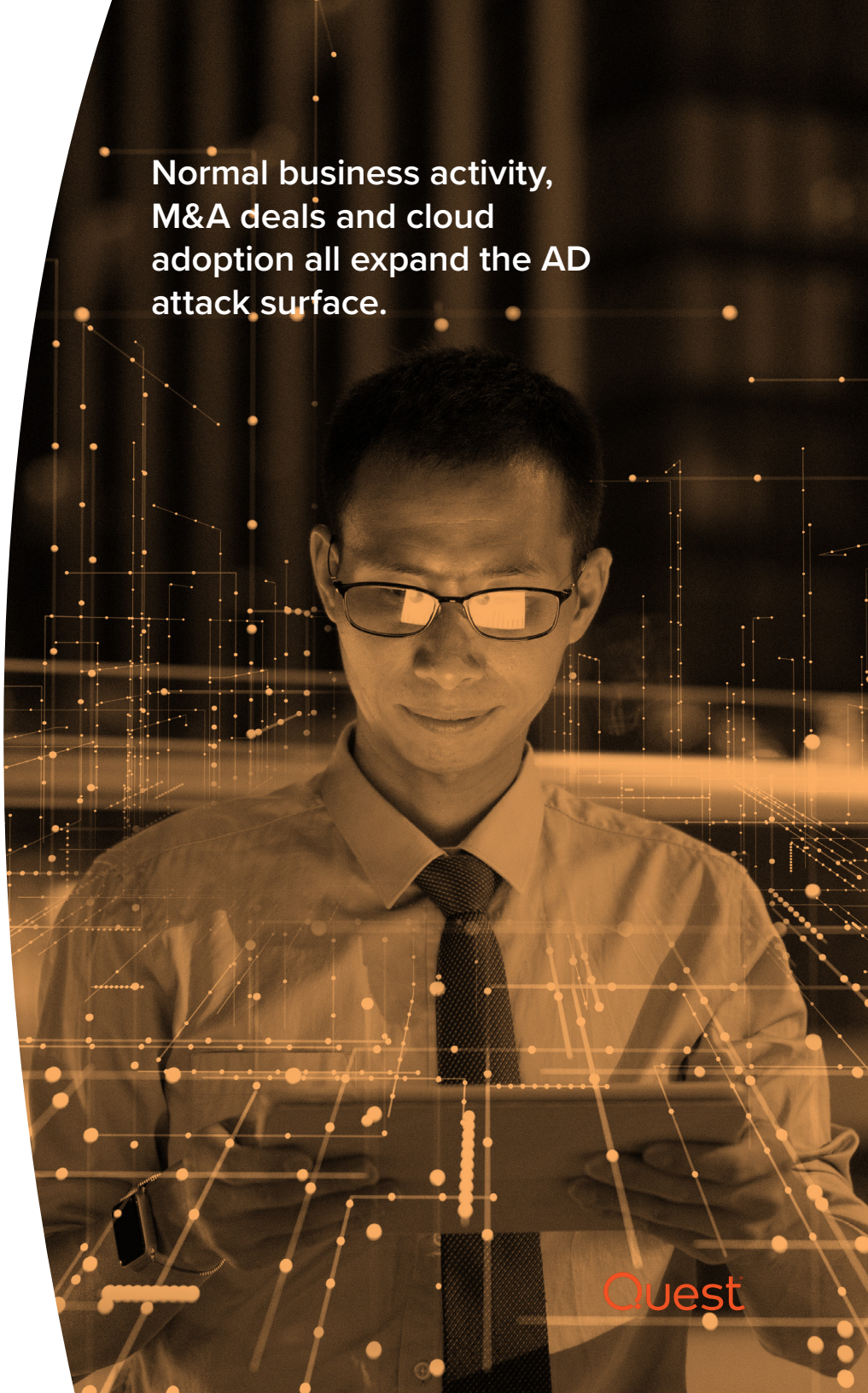
- **Require multifactor authentication (MFA) —** Ensure that stealing or cracking a password won't enable an adversary to gain access. Note that for on-premises AD identities, this control requires a third-party solution.
- **Adopt a Zero Trust model —** Rigorously enforce least privilege and verify entities before allowing access to resources.
- **Implement threat detection and response —** Monitor for suspicious activity, automatically block anticipated threats, and respond quickly and effectively to attacks.
- **Patch and update —** Keep systems up to date, including their firmware, operating systems and applications.

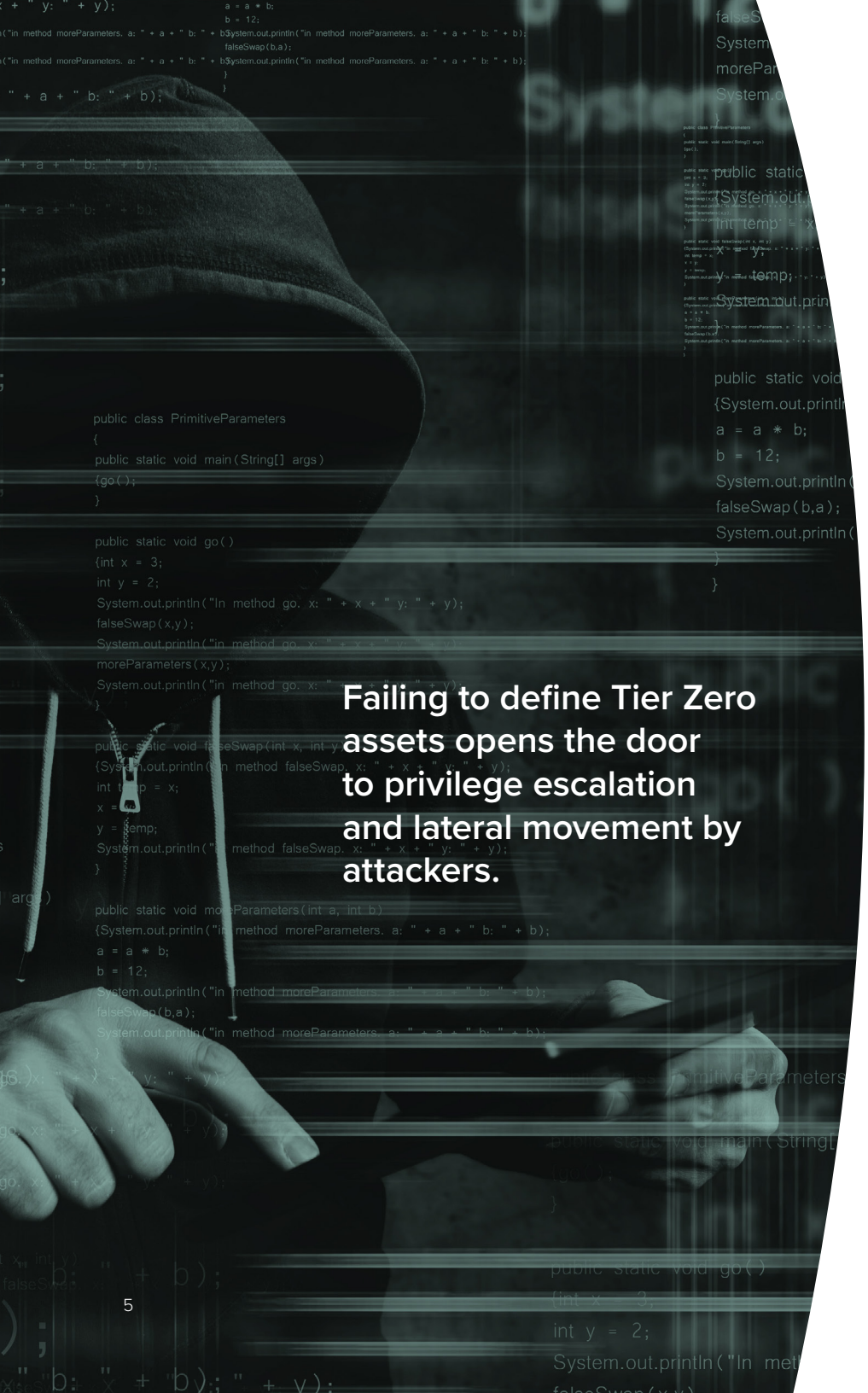
Challenge #2. Ever-increasing attack surface

The attack surface area of Active Directory keeps growing every day. Multiple factors often contribute to this increase. First, Active Directory is a highly dynamic system. In the course of a normal week, new users are onboarded, others change roles within the organization and need reprovisioning, and some accounts need to be removed from the directory as people leave the organization. In addition, new projects are started, others expand or shrink, and some reach completion or are abandoned. Each of those events can require the creation, modification or removal of accounts, roles, security groups and more — which introduces the risks of errors. Indeed, organizations are notoriously lax about deleting users, groups and privileges when they are no longer needed, thereby providing adversaries with opportunities to move through the environment with less chance of being detected. On top of that, applications and systems are constantly being adopted and retired, necessitating additional changes to Active Directory.

What's more, that activity represents just the highlights of a "normal" week. The surface area of Active Directory also grows in response to one-off events. In particular, merger and acquisition (M&A) activity puts AD complexity into overdrive. Each deal usually means incorporating one or more Active Directory environments into the current IT ecosystem, often on a very tight timeline that prevents proper cleanup and rationalization of the source directories. As a result, vulnerabilities like unneeded user and computer accounts, excessive access rights, and misconfigured or conflicting Group Policy objects (GPOs) can explode. Establishing a greenfield Active Directory and migrating everything into it might seem like a solution, but that approach takes a great deal of time and effort, and the resulting environment is subject to the same tendency toward sprawl and chaos.

Another critical source of increased attack surface area is cloud adoption. Most organizations have adopted Entra ID in order to take advantage of core Microsoft 365 applications like Teams, SharePoint and OneDrive for Business. But shifting workloads and data to the cloud rarely means getting rid of the organization's Active Directory. More often than not, organizations have compelling reasons to retain their on-premises identity system, from the reliance of critical business applications on AD to compliance-related requirements regarding data storage and security. Accordingly, migrating data and workloads to the cloud does not solve the problem of an increasing attack surface; it actually compounds it because it adds another directory to manage and secure.





Challenge #3. Failure to use a tiered administrative model

A core best practice of Active Directory security is to implement a tiered administrative model. By organizing user accounts, computers and other IT assets into different tiers, IT teams can better manage those assets and secure them appropriately. All users and computers need to stay in their tier, with no exceptions.

The most important tier to define and secure is Tier Zero, which comprises the organization's most mission-critical IT assets. Tier Zero includes powerful machines like domain controllers (DCs) and privileged access workstations (PAWs), as well as all accounts and groups that have direct or indirect administrative control over the forest, domains or DCs. Examples include highly privileged security groups like Domain Admins, Account Operators and Backup Operators, along with all accounts that are members of those groups, through either direct membership or indirect paths like group nesting. Higher numbered tiers comprise less-sensitive IT assets. For example, Tier 1 could include email servers, file servers, and moderately powerful accounts like application and cloud service, while Tier 2 could include the accounts and devices of business users, which have minimal access rights.

Unfortunately, far too many organizations have failed to adopt this administrative model — or to even define their Tier Zero assets. This failure leads directly to another top problem called out in the Microsoft Digital Defense Report 2023: insufficient privileged access and lateral movement controls. For example, unless the organization has clear insight into its Tier Zero assets, administrators are liable to expose their powerful administrative credentials on vulnerable machines, such as user workstations, where they are ripe for harvesting and misuse by threat actors. Moreover, business user accounts often have unintended administrative rights, making them a lucrative target for takeover by malicious actors intent on gaining access to sensitive data or systems.

Quest

Challenge #4. Alert fatigue

Another core IT security best practice is to take an assume-breach posture. That is, no matter how well secured the IT environment is, organizations need to recognize that a certain percentage of attacks will get through — and that both malicious and negligent users are already inside. Accordingly, it's vital to continually monitor for suspicious activity and alert security teams when threats are detected.

The problem is that IT ecosystems are highly dynamic, and it's hard to spot suspicious behavior in the sea of activity. In modern distributed environments, organizations often collect terabytes of log data per day, most of which represents legitimate activity. Without top-notch data analytics that can weed out the false alarms, security and operations teams are inundated with more alerts than they can possibly investigate, and true threats go uninvestigated and unresolved.

Alert fatigue is a key reason that attackers now roam around undetected in corporate networks for more than two weeks.

In fact, the median number of days an attacker is present in a target's environment before being detected (dwell time) is 16 days — over two weeks. In other words, adversaries still have far too long to roam around freely inside organizational networks, and alert fatigue is a key factor.

Challenge #5. Neglect of the on-premises environment

At The Experts Conference (TEC) 2022, Alex Weinert, VP of identity security at Microsoft, emphasized a key reality of identity security: "On-premises is where we're being attacked." While AD is not inherently insecure, it is more than two decades old, and many installations have built up considerable technical debt over that time. As a result, keeping everything running properly and securely requires an experienced hand.

AD experts are retiring in droves — and Microsoft training in AD is rapidly being retired.

However, expertise in Active Directory is declining. The segment of the population most likely to be well-versed in the technology is Baby Boomers and Gen X — and 10,000 of them are reaching retirement age each day. At the same time, preparing younger IT pros to take their place is getting harder and harder because Microsoft is rapidly phasing out courses and exams related to Active Directory. Multiple training tracks dealing with fundamental skills like Windows Server 2019 administration have already been retired or will be soon. Indeed, Microsoft's current recommended role-based certification path is based entirely on Microsoft cloud technologies.

These realities are leaving organizations with few people experienced in AD. As a result, implementing basic security hygiene practices effectively is more difficult, and knowing how to spot true vulnerabilities and threats and mitigate them effectively can be nearly impossible. For example, inexperienced administrators may not even know what the KGBTRT account is, let alone that it needs to be changed regularly to prevent threats like Golden Ticket attacks and how to update it without impacting business operations.

Solving AD security challenges with Security Guardian

Security Guardian from Quest is designed specifically to help organizations secure Active Directory by:

- Identifying vulnerabilities and misconfigurations
- Detecting suspicious activity and other threats in progress
- Enabling defenders to implement appropriate security controls

Specifically, it can help you overcome all the key challenges detailed above.

Establish — and maintain — a clean and secure Active Directory.

To address challenges #1 and #2, Security Guardian empowers organizations to establish a secure Active Directory environment and keep it that way through both normal daily business activity and special projects like migrations and consolidations required for M&A deals or other business needs. Again, the Microsoft Digital Defense Report reveals that implementing basic security hygiene practices can block 99 percent of cyberattacks. Therefore, it's not surprising that the report finds that remediating insecure Active Directory configurations offers one of the highest return on mitigation (ROM) scores.

The key is to automate the work as much as possible. Security Guardian offers a thorough AD security assessment that will benchmark your current Active Directory configuration against established industry best practices so you can establish a strong security posture and maintain it over time. Moreover, it helps you improve AD hygiene by enabling you to:

- Lock down critical objects, including GPOs, to prevent accidental misconfiguration or deliberate compromise
- Pinpoint indicators of exposure (IOEs) — security weaknesses particular to your unique network that could be exploited by an attacker
- Continually monitor for configuration drift that puts your Active Directory at risk
- Get focused reports on object status and easily revert any unwanted changes to a previous, trusted state

Identify your Tier Zero assets.

The third key AD security challenge organizations face is identifying and protecting their Tier Zero assets. With manual methods, this can be a difficult task. It's easy to see that DCs and PAWs belong in Tier Zero. Similarly, it's clear all highly privileged groups like Domain Admins and Enterprise Admins, along with all members of those groups, should be in Tier Zero.

But most organizations also have assets that belong in Tier Zero that are far harder to spot. For example, some user accounts gain administrative privileges not through direct membership in a group like Domain Admins but through security group nesting. And many organizations overlook critical assets like their Entra ID Connect server and certificate services.

Quest

Protect what matters most with a comprehensive list of your Tier Zero assets.

Security Guardian takes the guesswork and drudgery out of the process: It will thoroughly analyze your environment and automatically produce a list of Tier Zero objects. You can then modify and further categorize that list to ensure it is complete, accurate and maximally useful to your security teams.

Spot true threats and speed response.

Security Guardian also helps organizations overcome the fourth key AD security challenge, alert fatigue, by delivering intelligent identity threat detection and response (ITDR). It provides:

- Continual monitoring for indicators of compromise (IOCs)
- Auditing and analysis of user activity to spot suspicious behavior
- Detailed insight into the who, what, where, how and when of potential threats, with full context

Plus, the ability to forward information to SIEM tools like Microsoft Sentinel and Splunk for additional analysis enables centralized visibility.

Banish alert fatigue with intelligent identity threat detection and response.

As a result, you can reduce noise and reliably surface high-value alerts to ensure swift response to true threats.

Get actionable intelligence.

To address challenge #5, Security Guardian provides a unified AD security workspace with actionable intelligence that reduces the need for increasingly scarce Active Directory expertise. The friendly user interface provides clear visibility into IOEs, IOCs and other security signals across your hybrid identity stack.

For instance, as noted earlier, IT pros with domain-specific knowledge might not even know when it's critical to reset the KRBTGT account password. Security Guardian has their back, proactively alerting them to signals that the password has likely been compromised so they can take the necessary steps to thwart powerful Golden Ticket attacks. Similarly, it automatically correlates and analyzes activity across the IT ecosystem, transforming complexity into clarity.

Let Security Guardian transform complexity into clarity.

Conclusion

Strengthening Active Directory security is critical to improving cyber resilience, controlling costs, meeting compliance requirements and more. Security Guardian can help you overcome all the key challenges that put organizations at risk of data breaches and downtime. Plus, it's a software-as-a-service (SaaS) solution, so you get benefits like simple implementation, easy scalability and cost savings. To learn more, please visit https://www.quest.com/products/security-guardian/.

Quest

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. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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

Quest Software Inc.
Attn: LEGAL Dept
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

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