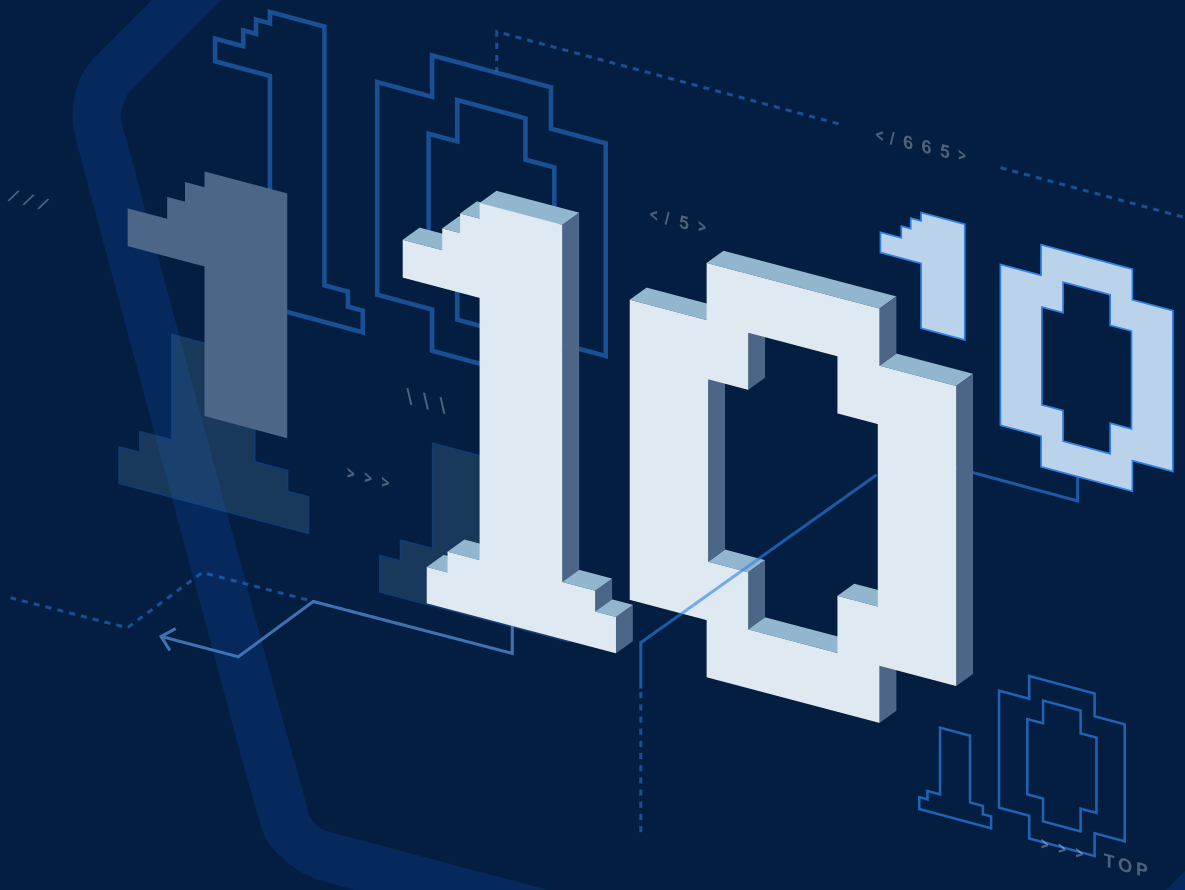
tenable.ad

THE TOP 10 AD SECURITY QUESTIONS CISOs MUST ASK



For more than 20 years, Active Directory (AD) has formed the backbone of organizations worldwide. When fully operational, its purpose goes beyond a tool for governing authentication and passwords to ultimately manage the crucial access control rights for almost every organizational asset.

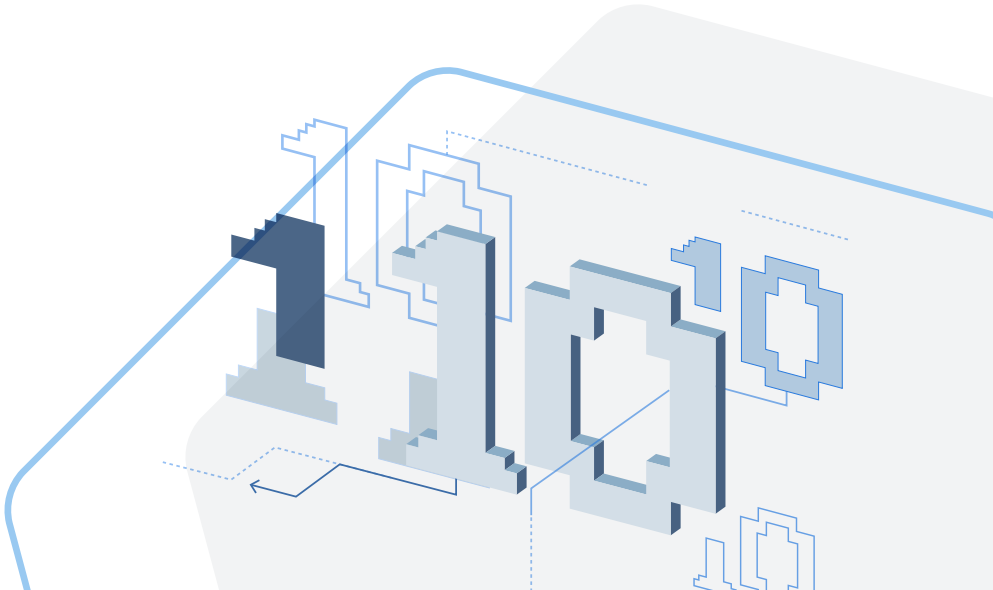
Active Directory is by no means a static software system, and its universal adoption is a testament to its ability to adapt and meet ever-changing business requirements. A modern organization's architecture can change instantly. And AD security hygiene can get ugly fast if not managed or secured properly. So how does management relate to the security of Active Directory?

With inefficient AD management, access control gaps arise where non-privileged users have easy access to data that is not meant for them. That is just the beginning, for AD is now the major target of advanced attackers and ransomware.

Just as one falling domino can start a chain reaction, one change in the AD can snowball into further unexpected consequences. Eventually, this creates a hidden attack pathway in the directory. What if there were multiple attack pathways? How can a single attack pathway be detected before more occur? Are you able to see this happening on your own AD?

AD must scale with your business in resilience and security capability. The reality is that as the demands on AD grow, it will very often deviate to an insecure, non-compliant state where it becomes an organizational risk rather than the trusted platform that facilitates business optimization and growth.

Enforcing AD security in these circumstances is paramount, but only after the most pressing questions are answered. Not all so-called AD security solutions are created equal, so we have assembled some of the most fundamental questions that we believe will help your decision-making process.



1. Does the AD security vendor install agents on the Active Directory, and are privileged rights required?

No security professional wants to give access to a system they spend their days maintaining. The same goes for an AD administrator who manages a complex system like Active Directory. Part of that management is ensuring that AD control is not provided freely to any third party or external source. Control and privileged rights access are usually given through the deployment of agents that act under a "trust-based" jurisdiction. This ultimately gives access to view, modify, or change objects. The installation of an agent should not be a requirement for enabling AD security on the domain controller, or any endpoint for that matter. Knowing the importance of Active Directory within an organization, your administrators should not feel comfortable with vendors requiring mandatory access to the directory. The installation of agents and the surrender of privileged rights imply that access to confidential corporate data is open.

It is imperative to guarantee that privileged rights to the Active Directory are not surrendered and that a platform will be unable to alter or modify objects. Currently, there are only a limited number of auditing solutions for AD, providing little protection and only capable of monitoring and reporting on attacks *after* they have occurred. These auditing solutions may consist of the deployment of agents on domain controllers which lead to partial or full control over the status of AD objects. There is no reason why any third parties require open access to AD objects. Also, some agent-based AD security solutions have strict update requirements to be supported regularly, and sometimes even .net framework must be installed (including on the domain controller).

2. Does the AD security vendor display information in real time?

Picture driving a car. A real-time warning system should alert you when a dangerous, oncoming driver is approaching, not after the driver hits your car. Likewise, you would want to be alerted of brake failure before you start your car, not when they go out. In the world of AD security, real-time alerting is mission critical. A real-time solution must detect and alert you to ongoing configuration changes that affect security measures of the AD, as well as provide recommended steps for remediation. With real-time, you are validating a proactive approach to monitoring and detection. While attackers sit for months within target networks waiting for the right AD attack pathways to appear, constant visibility of your AD security posture is essential.

3. Is the AD security vendor compatible with all Active Directory versions, as well as Azure Active Directory?

Over the past 21 years, Active Directory has released upgraded platform versions. One of the primary changes is the on-prem vs. cloud scenario. A platform should be able to connect with and support both the on-prem and Azure AD components.

In addition, AD has been stuck in the Dark Ages when it comes to directory configuration. Configuration upgrades have taken place periodically or not at all. As such, platforms should incorporate Indicators of Exposure that are used to evaluate how "clean" the on-prem component of Azure AD (aka Azure AD Connect) is. Generally, an AD security platform must be fully compatible with Azure AD Domain Services, which itself is the AD Managed Service by Microsoft.

4. Does the AD security vendor rely on AD Event Logs or AD object changes to provide analysis?

Trying to secure AD continually with AD Event Logs is difficult and cannot provide 100% visibility.

To stay up to date, you need to have dedicated AD security experts constantly surveying the AD security threat intel space, discovering your AD misconfigurations leveraged for attacks, understanding the event logs used to detect attacks, and creating rules to extract the specific AD configuration event log from the full stream of all AD event logs. This is expensive, tough, and inefficient.

There are on average 10 to 20 new toxic AD configurations released or discovered each year.

What's more, attackers are now conducting attacks that do not create event logs, like DCShadow, or they are turning off event logs in the AD via SACL modification so they can make changes in the AD with no event logs being created.

That means event logs can no longer be trusted to give a full view of what is happening in the AD. The only way to do this is at the object level in the AD database, which is precisely what Tenable.ad achieves. Moreover, Tenable.ad includes all new updates when new toxic configurations are released so they can be detected at the AD object level. Simply put, the attacker cannot hide.

5. Does the AD security vendor proactively identify dangerous AD misconfiguration attack pathways out of the box?

Recall the car-and-driver analogy. Similarly, built-in anticipation within an AD security platform provides several benefits that can increase the likelihood of breaking potential attack pathways. Built-in anticipation is focused on delivering a proactive approach to AD security, rather than the reactive method that is used by the vast majority of solutions claiming to cater to AD.

The most common way AD gets hacked today is through misconfigurations in the AD software being used to escalate privilege or propagate ransomware. Therefore, the most effective method to secure AD is to detect continuously and remediate dangerous configurations as soon as possible when they appear on the AD. Tenable.ad provides security teams with this powerful advantage.

AD is constantly evolving, with potentially hundreds of changes occurring in AD every minute. Any of these changes could open your AD to adversaries, such as:

- AD backdooring techniques – i.e. AdminSDProp modification
- AD credential dumping techniques – i.e. Kerberoasting attack

Tenable.ad quickly and simply enables proactive, comprehensive AD security to continuously harden the AD, including GPOs. As attacks on AD are using dangerous AD misconfigurations, the ability to detect and remediate new misconfigurations before they can be weaponized is key. Detecting them after the fact has little value.

With Tenable.ad, you can continue to detect the most complex AD attacks without draining your security team's resources.

6. Can the AD security vendor provide in-context AD security information in real time?

It is not enough to simply display the specific deviance for an AD object, as this view provides limited 'global' information. This data will not reveal where the specific problem is coming from.

An incriminating object needs a detailed, accurate explanation of the security issue and, where relevant, to show how multiple security issues related to each deviant object. You should be allowed to individually select each separate security problem from one specific object and action it independently. Coupled with the detailed information explaining how to fix these complex AD security issues, Tenable.ad clients are empowered to proactively harden their AD.

Tenable.ad enables continuous detection and remediation at an AD object level through:

1. In-depth, real-time explanation of each detected AD security event – what it is and why it is dangerous
2. In-depth, real-time explanation of how to fix each detected AD security event

By detecting the AD attack pathway misconfigurations, attacks like Pass-the-Hash, GoldenTicket, DCShadow, and DCSync can be stopped before they even begin.

7. Does the AD security vendor detect advanced AD attacks in real time—out of the box?

From a detection viewpoint, cyberattacks are becoming more complex. While the types of attacks are diverse and numerous, there are specific attack types that primarily target the Active Directory.

Tenable.ad detects standard attacks like password spraying out of the box, as well as the much more complex and difficult-to-detect attacks like DCShadow. The most advanced attackers will run very stealthy attacks that switch off AD event logs to allow them to establish persistent access to the AD via backdoors. Tenable.ad also detects complex AD backdoors in real time, out of the box.

Remember that real-time detection alone is not enough and should be followed by an easy-to-understand set of remediation steps providing a non-security focused administrator the ability to take the recommended remediation steps.

8. Does the AD security vendor enable AD forensics and threat hunting at the AD object level?

While you should not give access to and control over an AD object, you still want to get accurate information at the object and attribute levels. Organizations need a platform with a built-in trail flow interface that detects and displays in real time with a detailed description of changes at both the object and attribute levels. This advanced, continuous monitoring and alerting should be supported with relevant steps to fix any changes that may create attack pathways.

Recall those 10 to 20 new toxic configurations in AD each year. As Tenable.ad captures and stores every AD object change once connected, this data can be easily accessed for threat hunting in the AD at the object level, including extensive AD object attribute visibility.

Access to real-time, accurate, and relevant security analytics specific to Active Directory is paramount to ensuring AD teams see a realistic picture of their AD security posture. Dashboards should include a security view of the AD, as well as compliance scores, AD attack numbers, and information flow with graphs highlighting the constant evolution of the AD security score. All graphical data should be real time to guarantee continuous, proactive monitoring.

9. Can the AD security vendor visualize AD security attack pathways for easier analysis?

Tenable.ad's founders conducted the advanced AD security research used to develop BloodHound. The Tenable.ad AD topology graph, available within the Tenable.ad platform, provides a unique and intuitive way of exploring AD security attack pathways visually and continuously in real time against existing Tenable.ad-mapped data.

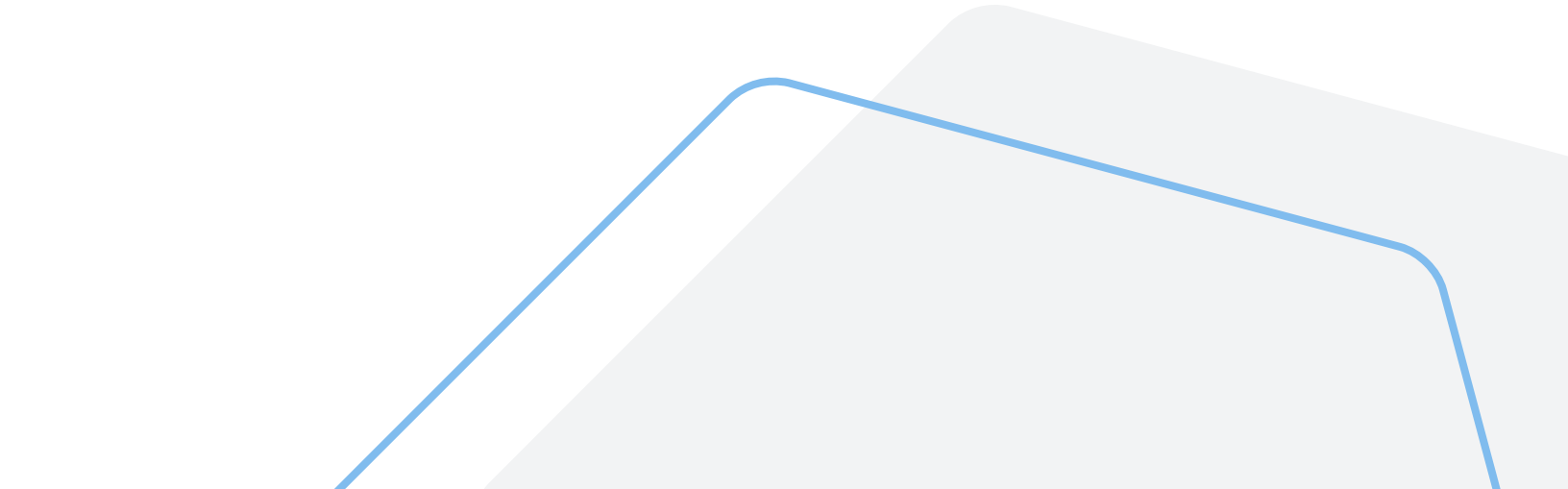
Your security teams can explore trust relationships and interconnections against all existing ones mapped by Tenable.ad. The trust relationships and interconnections highlight the communication that takes place between the various ADs a client may have and are color-coded to highlight the varying degrees of safe and dangerous trust relationships.

10. Can the AD security vendor integrate with other security solutions?

No organization can be 100% secure. However, crucial security steps and technologies at various organization layers need to be implemented to stay a step ahead of attackers. Perimeter and endpoint security solutions are vital instruments as outer-layer security, but do not possess the ability to protect the core of an organization: the Active Directory. Likewise, an application consisting of only access controls could not halt anyone that has deliberately or mistakenly been granted open access to an entire network.

Having the ability to run numerous, integrated security solutions simultaneously is the only way an organization can truly protect its outer and inner core. The ability to integrate via email, Syslog, and API is essential, as is the ability to have alerts correlated with SIEM and even SOAR, which—again—Tenable.ad provides out of the box.

To learn how Tenable.ad can help continually secure and protect your Active Directory, contact an Tenable specialist.



tenable.ad

6100 Merriweather Drive
12th Floo r
Columbia, MD 21044

North America +1 (410) 872-0555

www.tenable.com