Active Directory Holds the Keys to Your Kingdom, But Is It Secure?

Swetha Krishnamoorthi, *Industry Analyst, Cybersecurity,*
and Jarad Carleton, *Global Program Leader, Cybersecurity*

A Frost & Sullivan White Paper

Powering clients to a future shaped by growth

FROST & SULLIVAN

CONTENTS

Enterprises globally use Microsoft's Active Directory (AD) to connect and manage individual endpoints inside corporate networks. AD, which the Windows server operating system incorporates, stores information about users, passwords, devices, applications, services, and operations across the information technology (IT) infrastructure. It also controls access to Windows networks, programs, and data.

Microsoft AD enables policy and data management with add-on modules, such as AD Users and Computers and Group Policy Management Console, which help enterprises maintain visibility, security, and user experience for networked enterprise assets.

Today, Microsoft AD is the dominant mode of managing Windows domain networks, with approximately 90% of the Global Fortune 1000 companies using it as a primary method to provide seamless authentication and authorization.

Consequently, AD has become a primary target for cyberadversaries to access confidential company data. Once inside AD, cyberadversaries can move across systems and access myriad proprietary and essential data across systems that AD manages, and with the widespread adoption of Office 365, which uses AD to authenticate users, the attack surface has extended from on-premises to cloud environments.

The Business Challenge

An Expanding Digital Ecosystem

Enterprises' IT infrastructure is expanding in volume and complexity. Diversity in endpoints, applications, and operations characterizes the IT architecture of today's enterprises. Even workplaces are no longer solely on physical campuses. The COVID-19 pandemic accelerated the shift to remote and hybrid work models, placing additional demand on enterprises to provide remote network login capabilities for employees.

Unfortunately, many businesses are unable to extend their AD architectures to support modern digital workplace requirements. As a result, security teams are often faced with the choice of providing a relatively smooth user experience for remote workers accessing corporate assets or heightened security, which puts more restrictions on remote workers than for those inside a traditional office. Also, an IT team must manage issues such as privileged access for different user profiles and systems integration requirements —password- or X.509 smart card-based authentication systems—that are not adequate for modern workplace practices.

Moreover, businesses saw mass employee exits and hiring during the Great Resignation in 2021. For IT teams, this implied high volumes of user account provisioning and deprovisioning and frequent changes in access privileges.

External cyberadversaries are not the only security risk—indications of insider threats also require monitoring in the AD environment.

AD requires continuous monitoring and analysis to track changes to environments and group policies. Increasing the complexity of a constantly changing AD environment, Windows event logs from AD are technical and require manual searching or advanced PowerShell scripting skills.

Collecting and aggregating Windows event logs centrally at scale is also impossible. For example, if a systems administrator adds a user into a group in AD, they generate 1 event log each to remove and re-add every group member. Depending on the group's size, the event log can run into thousands of entries for a single event. Therefore, for a large enterprise, aggregating event logs of all AD operations is time- and resource-intensive.

While it is essential to track in real time every change in the AD environment, 80% of changes are benign. However, the high volume of AD event logs increases the challenge of pinpointing errors that could unintentionally increase the cyberrisk for the organization and allow cyberadversaries to slip in without detection.

Cyberdwell time is the duration an adversary resides inside an organization's network before detection. Cyberadversaries' average cyberdwell time is 287 days.[1]

The cyberattack on the International Committee of the Red Cross (ICRC) in January 2022 demonstrates the adverse impact of an AD attack on organizations.[2] The ICRC attack began in November 2021 with the cyberadversary exploiting an unpatched crucial vulnerability to access the network. Once inside, the cyberadversary deployed web shells that enabled it to compromise administrator credentials, move laterally, and exfiltrate registry hives and AD files.

In this case, the cyberdwell time was more than 70 days. By then, the adversary had accessed the personal data of more than 500,000 people seeking to reconnect with their families.

Even for organizations with staff skilled in using PowerShell scripts to detect threats in Windows event logs, it is an inefficient and time-consuming process.

Operationalizing AD Security

Enterprise security budgets have increased during the past few years in response to the never-ending evolution of the cyberthreat landscape. Although organizations have implemented numerous point solutions to gain visibility across systems and detect and remediate threats, AD security has not kept pace with the increasing complexity of the modern digital ecosystem. Three common reasons explain a poor AD security posture.

1. Many Highly Skilled AD System Administrators Are Not Security Literate

AD system administrators or managers focus on maintaining system uptime and frequently lack an understanding of the security implications of their actions. For instance, when enterprises do not follow a policy-based approach to assigning user and administrative rights, some staff may get privileged access to restricted system-modifying features meant for specific administrators and users.

Access to domain controllers (DCs)—servers that respond to security authentication requests within a Windows Server domain— require restricting and securing. A cyberadversary with privileged access to DCs can modify, corrupt, or destroy the AD and all systems and accounts it manages. For instance, in a DCSync attack, the cyberadversary simulates a DC's behavior and retrieves user credentials from other DCs. The adversary now has privileged access to a DC and complete control over other user accounts on the domain. The adversary then uses the privileged access to replicate the user credentials of all DCs in the AD and steals data, which the organization does not detect.

Similarly, a cyberadversary with privileged credentials can register a rogue DC to amend a domain by replication. This type of attack is a DCShadow attack.

The challenge is that large enterprises with multiple branches and disparate information systems have many DCs to manage, and the problem can worsen following mergers and acquisitions.

Often, little difference exists between the privileges for different administration accounts, such as workstation, server, exchange, help desk, or local. However, such a situation can contribute to a lack of visibility on any changes or privilege misuse in DCs, which can lead to a potential attack. With a haphazard privilege management policy and lack of clarity on individual user and domain privileges, the AD environment can be an easy target for cyberadversaries.

2. AD Security Is Not a Priority

Although an improperly configured AD can allow cyberadversaries to access vital information, securing AD is not a top security concern for many enterprises. During the pandemic, security concentrated spending around safeguarding the human factor and endpoints and optimizing or automating security operations. Across various surveys that research organizations conducted, AD security did not feature in the top 10 security priorities for 2022. Only 26% of survey respondents to a study that Dark Reading conducted indicated privileged access management (an essential ingredient of AD security) as a priority for their organizations in 2022.[3]

Cyberadversaries begin their efforts to access the AD of an organization using simple methods such as a web search, exploiting virtual private network (VPN) access, or even a phishing mail. For instance, in May 2021, Colonial Pipeline, a major US-based oil pipeline firm, suffered a ransomware attack that forced it to halt operations for almost a week and pay a $4.4 million ransom. The adversaries used a VPN to enter the company's system, gained privileged access to its AD, and leveraged the integrated group policy to automate the ransomware deployment.[4]

Local administrators have simplified the task for cyberadversaries by using the same credentials across branches, reflecting improper security hygiene. Despite increasing password fatigue among workers, the use of simple and easy-to-guess passwords is increasing the cyberrisk for organizations globally. Reusing passwords enables cyberadversaries to leverage them in password spraying, an attack where cyberadversaries use a few common passwords against multiple accounts to identify administrator credentials. As of August 2021, Microsoft reported more than 50 million password-based attacks daily on Azure AD.[5]

The reuse of passwords was so rife in 2019 that Microsoft found more than 44 million Azure AD and Microsoft services accounts with compromised credentials that required a forced password reset.[6]So, in March 2021, Microsoft released a passwordless authentication feature for all Microsoft applications through its Microsoft Authenticator app.[7]

Ideally, all administrator account credentials need regular updates. However, this seldom occurs because it is cumbersome to update all the local and global administrative accounts and their policies. Thus, anyone who may have received temporary access, including a cyberadversary, is likely to become a permanent member of the AD.

3. AD Security Specialist Shortage

IT teams and AD engineers have traditionally lacked the knowledge to incorporate security best practices and fully understand the scope of cyberrisk from AD misconfigurations. The cost of managing in-house AD security can be high, with many potential limitations. The average cost of a security specialist with Microsoft AD skills in the United States is about $68,000 and can go up to $123,000.[8] For large enterprises, changes in the AD environment happen frequently, making it essential to closely monitor such changes to detect any potential risks or threats. However, the longstanding shortage of experienced cybersecurity professionals is worsening, and for AD security specialists, the situation is dire. An AD security specialist must execute 900 PowerShell commands to manage the AD environment proactively. Consequently, a security analyst can monitor changes in the AD only once or twice a week instead of in real time. While robust scripts can help administrators gain control of the environment, the resulting complexity increases cyberrisk because it is hard to manage. A common observation among enterprises is that only 1 person in the IT team has the competence to manage PowerShell scripts. Therefore, it is easy to miss a scripting misconfiguration, thereby significantly increasing the risk of cyberattacks from advanced persistent threats.

The Business Impact of AD Attacks

In March 2021, CNA Financial, a leading cybersecurity insurance provider, suffered a ransomware attack.[9] Cyberadversaries disrupted the network, caused an outage to the company's corporate email system, and demanded $40 million as ransom.

They also injected a malware that encrypted data on more than 15,000 devices on CNA's network. The company could not resume business operations for more than 2 weeks, resulting in severe financial losses and reputational damage.

Ransomware attacks have become so rampant that even law enforcement departments experience them. In May 2021, cyberadversaries took control of 250 GB of highly confidential data from the Washington DC Police Department and demanded a $4 million ransom.[10]

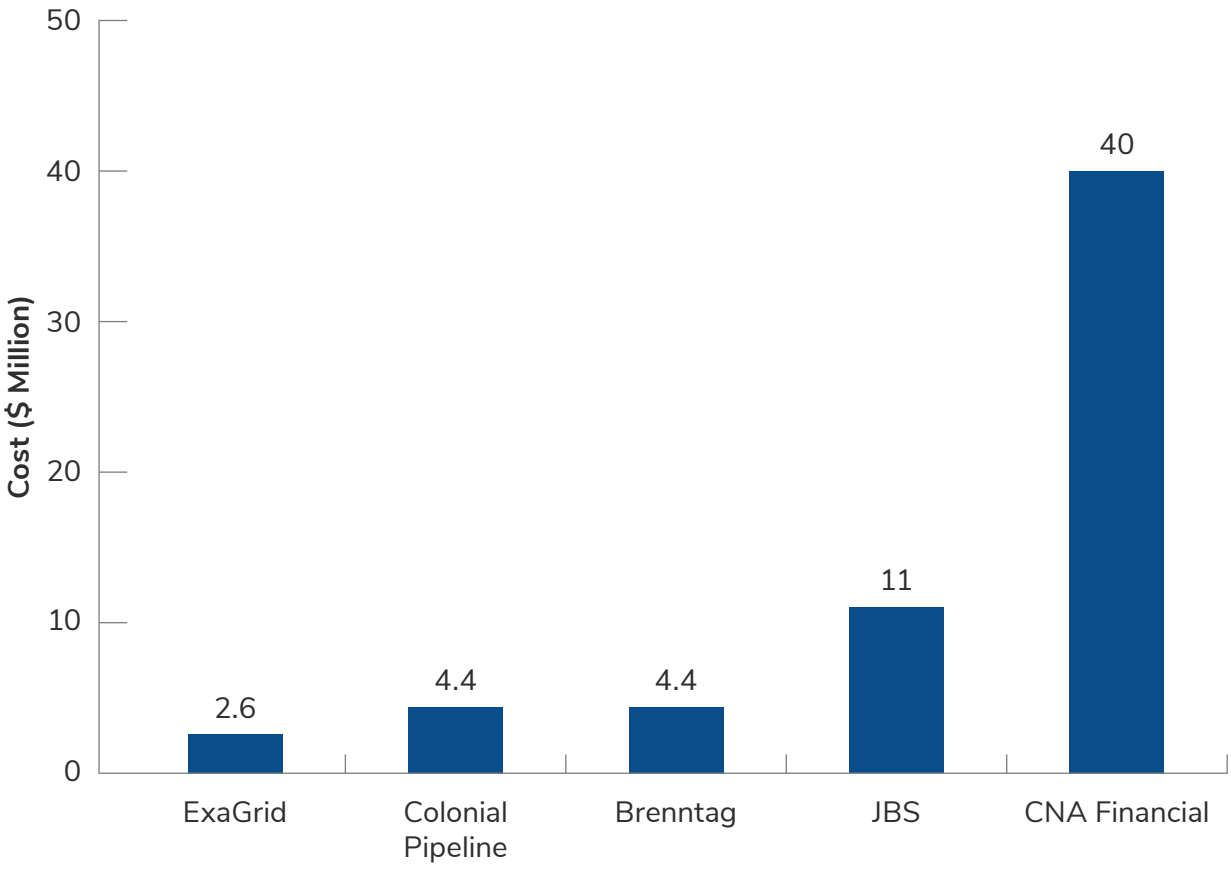
In 2021, there was an unprecedented surge in ransomware attacks, with 105% more than in the previous year, according to SonicWall's report.[11]

A common thread across many ransomware attacks is the exploitation of AD vulnerabilities. Through a targeted phishing attack, cyberadversaries access the network and leverage commonly available toolkits, such as Mimikatz, Metasploit, or Cobalt Strike, to access privileged user accounts. After finding domain administrator credentials, cyberadversaries access AD and plant ransomware. With privileged access, these cyberextortionists disable any company cyberdefense mechanisms and move laterally across the network.

When a poorly managed AD environment enables the lateral movement of malicious software, the fiscal impact on enterprises can be significant. Figure 1 displays the costs of a ransomware attack that 5 companies publicly reported.

Thus, cyberattacks do not solely involve data theft. Most targeted ransomware attacks focus on extortion, business disruption, or physical damage to equipment. Moreover, the fiscal impact is severe and includes disruption; information and revenue loss; damaged equipment; legal fees; and the cost of production, post-attack communication to end users, and compliance. Alongside tangible costs, cyberattacks damage brand reputation. Frost & Sullivan's statistical research, the Global State of Online Digital Trust, has shown that cyberattacks have led to a measurable loss of trust among customers, with a long-term moderate to strong negative impact on top-line revenues for almost 60% of companies.

FIGURE 1: Publicly Reported Costs of Ransomware Attacks



Technology to Address the Business and Security Challenge

Administrators have wide-reaching access to confidential information. Hence, it is essential to keep a well-curated list of these accounts and their permissions to continuously monitor them for any suspicious changes. However, the AD does not include tools to identify security risks and system failures quickly and easily. Behavioral analysis technologies can help to develop standard behavior profiles for individual users and flag abnormal behaviors for closer examination.

Attacks on AD typically start by exploiting a vulnerability on the surface. Once inside the network, the cyberadversary identifies more vulnerabilities that it can exploit to access a specific asset or move within the network. The cyberadversary connects the dots between multiple vulnerabilities to identify an attack path targeting a specific asset. Individual analysis of the attack vectors or vulnerabilities will only give a localized view of the risk level. Attack path analysis will help organizations understand the risk in the context of the attack path leading to a vital asset. Tools that provide a visual representation of the attack paths will help organizations prevent attacks on AD.

Detecting threats and vulnerabilities requires knowledge of the threat landscape, which is continuously in flux. Understanding how the threat landscape is evolving is possible with threat intelligence feeds, but operationalizing that information is a common challenge, even to large enterprises with substantial resources.

Weak password policies and leaked credentials cause AD security compromises too often. Requiring the use of unique complex passwords and regular password updates will limit an attack's impact, although these changes could necessitate the use of a password vault to help both administrators and end users.

Detecting threats and vulnerabilities requires knowledge of the threat landscape, which is continuously in flux.

Monitoring account lockouts, individual user and group permissions, or any suspicious or noteworthy changes in the AD environment through command line-based queries is daunting, even for experienced security professionals. Furthermore, malware begins a lateral movement through the network as soon as it detects a bad configuration. Often, within 4 to 5 hours, the malware can spread across the enterprise's network, so any change in the AD environment needs real-time detection. PowerShell scripts can help to an extent but are inefficient and lack the capability to monitor and detect changes in real time. Often, IT or security teams do not have the expertise, resources, or time to manually maintain and monitor AD environments, which increases cyberrisk for organizations. Unfortunately, the AD security challenge remains because the expanding digital footprint of modern enterprises also requires continuous monitoring of cloud environments.

To establish a proactive AD security plan, organizations should take the following steps.

Step 1: Find and fix AD vulnerabilities before attacks happen

A real-time assessment of existing vulnerabilities in AD is an essential first step in AD security. Scoring vulnerabilities by risk level can help organizations prioritize remediation actions.

Step 2: Uncover new attack paths

Thorough attack path analysis in real time will help organizations uncover and dismantle new attack paths and reduce threat exposure.

Step 3: Detect and respond to AD attacks in real time

It is imperative to reduce adversaries' cyberdwell time within the network to detect and respond to AD attacks and changes in real time. Integrating AD and security information and event management (SIEM) can address this by generating accurate AD-specific alerts with no false positives that enrich the security operations center's activity.

Step 4: Investigate incidents and hunt for threats

Finally, security teams must be able to identify and correlate any object- or attribute-level changes in the AD environment. This will help security teams detect any backdoors and trigger response playbooks to prevent an adverse impact.

Many point solutions in the market only address specific aspects of AD security. For instance, some products conduct a gap analysis of AD security, while others monitor changes in the environment or abnormal activity that require administrator analysis. However, deploying or leveraging point solutions for each of these functions can be complicated, inefficient, and hard to manage. A holistic solution that addresses all AD security requirements would be best for IT teams and security departments to achieve security maturity in AD environments.

Intelligent, real-time AD security tools, such as Tenable.ad, enable enterprises to monitor and detect threats based on indicators of exposure (IoEs) and integrate with SIEM or security orchestration, automation, and response (SOAR) tools to support highly focused remediation plans in context.

The use of intelligent real-time AD security tools helps enterprises understand where and how to strengthen AD security, detect insider threats, and prevent external attacks before they inflict costly damage on a business. Also, intelligent, real-time security solutions directly address challenges arising from the ongoing shortage of experienced AD security professionals.

Intelligent, Real-time AD Security is a Business Enabler

The impact of a compromised AD environment on a business is high. In addition to brand damage, production stoppages, lost revenue, remediation expenses, potential fines, regulatory scrutiny, and a medium-to long-term impact on top-line revenue, a successful attack on an AD environment will significantly impact bottom-line revenue.

Acknowledging that enterprises must increase security, government regulations and some industry self-regulation require enterprises to ensure confidentiality, integrity, and availability of sensitive data. Some of the most wide-reaching regulations and standards, such as the EU General Data Protection Regulation (GDPR), Sarbanes Oxley Act (SOX), California Consumer Privacy Act (CCPA), Healthcare Insurance Portability and Accountability Act (HIPAA), and Brazilian General Data Protection Law (LGPD), show that enterprises conducting business in major global economies or processing payment card transactions must be more proactive in closing security gaps.

Each regulation requires enterprises to have infrastructure, policies, and processes in place to protect from destruction, loss, or unauthorized alteration. That includes aspects such as access control, auditing capabilities, and change management processes, which are essential to these regulations. Failure to meet the minimum requirements of data protection mandates can result in significant fines and enhanced scrutiny by regulatory bodies.

Investing in an intelligent, real-time, managed AD security solution is a business enabler for enterprises. Chaos in enterprise AD environments can unintentionally weaken an organization's security posture. Administrators can gain control over their network and prevent attacks without AD security specialists. Using Tenable.ad, even skilled AD administrators lacking security literacy can monitor AD for suspicious changes; detect risks, threats, and misconfigurations; and harden Group Policy Objects. With a platform like Tenable.ad, chief information security officers (CISOs) or security teams may only need to spend about 30 minutes reviewing a vulnerabilities report to understand the reasons behind the changes.

Achieving Measurable AD Security Improvements with Tenable.ad

With headquarters in Columbia, MD, Tenable® is a cybersecurity vendor that offers real-time active protection for AD infrastructure. The company's AD security platform, Tenable.ad differentiates itself with an automated intelligent detection approach based on changes in the AD infrastructure, rather than based on Windows event logs.

	PILLAR			
	1	2	3	4
Features	Find and fix AD vulnerabilities before attacks happen	Uncover new attack paths	Detect and respond to AD attacks in real time	Investigate incidents and hunt for threats
IoEs	✓			✓
AD Topology Graph	✓	✓		
Dashboard	✓			
Attack Path	✓	✓		✓
	✓	✓	✓	✓
Alerts Panel		✓	✓	
IoAs			✓	
Trail flow			✓	✓

Tenable.ad differentiates itself with an automated intelligent detection approach based on changes in the AD infrastructure, rather than based on Windows event logs.

The Tenable.ad platform has 4 pillars:

1. Find and fix AD vulnerabilities before attacks happen
2. Uncover new attack paths
3. Detect and respond to AD attacks in real time
4. Investigate incidents and hunt for threats

The Tenable.ad platform helps security teams identify and remediate AD vulnerabilities using the following features:

Indicators of Exposure (IoEs)

IoEs are potentially exploitable attack vectors, such as misconfigurations or vulnerabilities, that cyberadversaries can use to enter the network. Tenable.ad scans the AD environment to expose the list of attack paths and AD-opened backdoors. For each IoE, the platform lists the deviant objects and highlights the technical reason, dangerous attributes, and accurate values.

Trail Flow

Tenable.ad provides a simple interface for security teams to query information in AD, such as access privilege changes or security backdoors. The trail flow structure catches all the changes made in the Ntds.dit database and system volume folder.

AD Topology Graph

The platform provides an interactive graph visualization of the entire AD infrastructure and helps companies see trust relationships to investigate dangerous ones.

Indicators of Attack (IoAs)

The IoA module helps security teams detect attacks on AD by analyzing event logs and monitoring changes in the environment. The module can detect advanced attack types, such as DCSHadow, DCSync, and Golden Ticket.

Attack Path Visualization

The attack path visualization module helps provide a real-time visual representation of attack paths for assets and enables security teams to tackle all the escalation paths. The module captures the implication of a change in AD on the attack path in real time, and the asset exposure module can help security teams check the exposure level of a specific vital asset. Also, the blast radius tool helps evaluate potential lateral movements in the network from an exposed asset. Using trust relationships, the attack path feature can help security teams anticipate privilege escalation techniques that an adversary can use to access an essential asset.

Alerts, Notifications, and Dashboards

Tenable.ad enables security teams to create and distribute meaningful reports for different user groups, such as top management, business heads, information security managers, AD administrators, and security analysts. Security teams can also configure alerts and notification criteria for specific changes, such as access privilege changes or abnormal activity.

Achieving Measurable AD Security Improvements With Tenable.ad

Tenable®'s team of AD security experts continuously improve the platform by adding new attack techniques and security-based best practices. The Tenable.ad platform provides enterprise customers with advanced detection capabilities before they need it. With its application programming interface (API)-based integration to third-party security tools, such as SIEM and SOAR, Tenable.ad ensures that enterprise customers can secure AD environments with 1 tool.

Tenable.ad connects with the DCs of enterprise AD infrastructure and employs agentless installation to connect to the DC. Using a nonprivileged account, Tenable.ad scans and analyzes every object in the AD and rapidly pinpoints IoE. In just 1 hour, an organization can view the weaknesses in its AD environment and understand where the most serious issues are. Following the initial baseline analysis, Tenable.ad then shifts into monitoring mode to detect any exploits and alerts the administrator, who can then use a playbook or other industry best practices to remediate potential threats.

A Tenable.ad Customer Case Study

A European travel company with operations in 40 countries had a significant challenge in managing 20 different information systems across its organization. The absence of a unifying platform to centralize the management of information systems had created an essential lack of visibility of end user and administrative rights in the AD environment, posing severe security risks. Without a unifying system in place to detect AD misconfigurations, the CISO's team had to rely on open-source tools to paint an incomplete picture of AD infrastructure and potential security issues. However, even when an issue surfaced, the CISO struggled to find available resources to manage incident response and resolution.

Understanding that AD security is a crucial business enabler, the CISO implemented Tenable.ad as part of his strategy to rapidly improve the security maturity of his AD environments. Deployment of Tenable.ad took less than a day thanks to its agentless, non-intrusive approach to connect to the customer's AD DC instance in the cloud. Preliminary results of a thorough AD infrastructure scan were available within 24 hours. Tenable.ad accurately identified existing misconfigurations and vulnerabilities that could have exposed the company to attacks similar to those that Norsk Hydro, Maersk, FedEx, Target, and the Democratic National Committee (US Democratic Party) experienced.

Deployment of Tenable.ad took less than a day thanks to its agentless, non-intrusive approach to connect to the customer's AD DC instance in the cloud.

Post implementation, the CISO was able to monitor system activity and, with the help of Tenable.ad's dynamic reports, get an evolving and real-time overview of his organization's AD infrastructure. Tenable.ad's recommended action plans to remediate potential threats and misconfigurations measurably helped to decrease significant cyberrisk factors that were present in the infrastructure but previously out of sight.

Tenable.ad's recommended action plans to remediate potential threats and misconfigurations measurably helped to decrease significant cyberrisk factors that were present in the infrastructure but previously out of sight.

Conclusion

AD is an essential component of modern IT infrastructures for both private and public organizations globally. Cybersecurity best practices suggest that business and government agencies using AD should have real-time visibility of the security hygiene for their AD environments, including user and administrator accounts, policies and privileges, policy violations, abnormal behavior, and unintentional misconfigurations.

While the use of PowerShell scripts is prevalent, it is also a tedious, expensive, and error-prone approach to detecting misconfigurations, vulnerabilities, and threats in real time. Leveraging an intelligent and automated AD security solution, such as Tenable.ad, can springboard enterprises toward AD security maturity. It offers full visibility and control over networked IT infrastructure and can help decrease cyberrisk before it impacts business operations and revenue.

Points of Consideration

Consider the following questions when evaluating vendors for AD security:

- Does the platform offer risk and security assessment of AD forests, domains, and objects?
- Does the platform enable tracking changes in an AD environment, including account logons, lockouts, and access privilege changes?
- Does the platform provide attack path visualization?
- Does the platform enable role-based access control?
- Does the platform integrate with existing SIEM and SOAR tools in the organization?
- Does the platform offer and prioritize alerts and notifications of crucial changes?
- Does the vendor offer both cloud and on-premises deployments?
- Does the vendor offer managed service support?

AD is an essential component of modern IT infrastructures for both private and public organizations globally.

About Tenable®

Tenable® is the Cyber Exposure company. Approximately 40,000 organizations around the globe rely on Tenable® to understand and reduce cyber risk. As the creator of Nessus®, Tenable® extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable® customers include approximately 60% of the Fortune 500, approximately 40% of the Global 2000, and large government agencies. Learn more at tenable.com.

Next Steps

Would you like to learn more about how Tenable® can assist in your AD Security journey? See these white papers and webinars from the Tenable® website to gain valuable insights on implementing AD security.

Endnotes

1. Cost of a Data Breach Report 2021 | IBM
2. Red Cross Hack Linked to Iranian Influence Operation? – Krebs on Security
3. When IT Spending Plans Don't Reflect Security Priorities (darkreading.com)
4. Colonial Pipeline ransomware attack - Wikipedia, The Paramount Defenses Blog: At the HEART of the Colonial Pipeline Hack - Admin Access in Active Directory
5. Secure your Azure AD identity infrastructure - Azure Active Directory | Microsoft Docs
6. https://www.microsoft.com/securityinsights/Identity
7. Microsoft Expands Passwordless Sign-on to All Accounts | eSecurityPlanet
8. Active Directory Salary | PayScale
9. Insurer CNA Paid Hackers $40M for Ransomware Decryption - MSSP Alert
10. DC Police victim of massive data leak by ransomware gang | AP News
11. Ransomware cyberattacks surged in 2021 according to a new report | Fortune

FROST & SULLIVAN

Growth is a journey. We are your guide.

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion