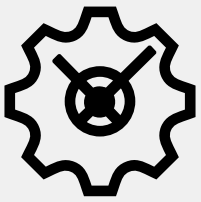
SOLUTION BRIEF

Improve Your Security Posture with FortiGuard Active Directory Security Assessment

Executive Summary

Identity access management (IAM) is a key component of IT operations, and many organizations use Microsoft Active Directory (AD) on-premises to implement their IAM programs. Because of the low requirements and ease of deployment, many AD directory service installations are set up by staff with little or no AD training. There is also often no due-diligence performed to ensure that an implementation is properly managed and fully secure.

With the FortiGuard Active Directory Security Assessment, you can get a top-down review of your AD installation. This service ensures that critical recommendations from Microsoft and various standards bodies have been implemented. Then, once issues have been identified, you can track your progress in addressing any issues and increasing the maturity of your AD environment.



The use of valid credentials was increasingly prevalent among incident response (IR) engagements investigated by the FortiGuard IR team in 2022. They account for about 44% of initial access methods.[1]

Why Is an AD Evaluation Needed?

As your initial AD installation continues to grow with the company, decisions that were made during the early phases may have created new attack surfaces. These will still exist and potentially have expanded. Since AD is a high-value target for threat actors, and they will almost always seek to gain access to it as a core component of an attack, it is critical to make sure all aspects of it are protected.

Further, many issues may exist that are not known or not considered by general system administrators who have the much larger scope of the entire enterprise to contend with. For example, many organizations find that their audit settings did not record critical information needed during an incident response or employee security event. Often, organizations also learn after the fact that monitoring for critical log events could have prevented or mitigated harmful situations.

Assessment Focus Areas

The FortiGuard Active Directory Security Assessment is organized into five areas of focus that each incorporate people, processes, and technology. Each of the areas consists of a number of maturity practices. These are used to assess the AD installation's security and alignment with the larger business mission and current threats, plus the capacity to evolve efficiently over time.

Focus Area	
Policy and Procedures	This area starts with governance and basic procedures that are derived from the goals and objectives of your governance policies. The focus will be to ensure that your AD installation has proper executive backing and resources, as well as basic procedures that ensure the environment is ready for adverse events and incident response.
Account and Authentication Management	This area addresses account management policies, procedures, and security settings that are derived from various standards bodies and Microsoft publications. Many issues addressed in this section are considered to be critical to the security of AD and your IAM program.

Focus Area	
Network and Host Configuration	AD hosts are high-value targets and need to be hardened. In addition, based on its utility and design, AD is frequently deployed redundantly and to multiple locations within the organization. This section addresses both network and host security-configuration issues.
Audit Configuration	To ensure visibility for auditing and investigation, default audit configurations need to be verified and specific audit flags may need to be set. If proper auditing is not enabled, then information will not be collected, and critical questions about access and activities may not be able to be answered. This section covers the most important audit settings based on both Microsoft and standards bodies' recommendations.
Monitoring	Because AD and administrator accounts are high-value targets for threat actors, continuous monitoring of some critical AD events needs to be implemented. This section looks at the most critical events that should be monitored and reviewed for legitimacy and authorization.

While 78% of organizations believe they are "very" or "extremely" prepared to mitigate an attack, 50% still fell victim to ransomware last year.[2]

Half of enterprises fell victim to a ransomware attack in the last 12 months and 46% were targeted by ransomware two or more times.[3]

How the Assessment Works

Document review

Reviewing documents, plans, and settings related to AD security helps make workshops and interviews more efficient and informs future recommendations.

Workshops

This phase includes focused discussions to gauge maturity in the various practices, discover reinforceable or partial strengths, and identify areas most in need of improvement.

Report

The Active Directory Security Assessment Report provides maturity scoring through a proprietary tool (allowing easy visualization at a high level) and a set of prioritized, actionable recommendations designed to return the most value for effort and resources.

Conclusion

Active Directory installations can be simple or complex, with either single or multiple forests and trust relationships. However, all AD environments, large or small, have many of the same security concerns that need to be addressed.

The FortiGuard Active Directory Security Assessment gives managers and system administrators an objective, realistic roadmap to improve right away and continue to improve over years. Our assessment can be adjusted to the architecture of your AD installation and to the needs of your organization, allowing you to focus what is important.

[1] "Global Threat Landscape Report," Fortinet, February 2023.

[2] "The 2023 Global Ransomware Report," Fortinet, April 2023.

[3] Ibid.

FORTINET

www.fortinet.com

August 24, 2023 1:47 PM

2289862-0-0-EN