SentinelOne White Paper

SentinelOne®

Achieving Effective Active Directory Protection Through Security and IT Team Collaboration

June 2023

Table of Contents

01

Introduction

With greater frequency and severity than ever before, enterprises are seeing an increase in ransomware and other advanced threats, and Active Directory (AD) is the primary attack target to gain access. Mandiant research consultants estimate that about 90% of the attacks their team investigates involve AD, and for good reason. Since AD is used by 90% of enterprises as a primary method for authentication and authorization, it contains a myriad of valuable company and employee data. Targeting AD provides attackers with the information they require to perform reconnaissance, obtain sensitive user and system data, deploy ransomware, and execute a multitude of other nefarious activities.

90%

Of enterprises use Active Directory as a primary method for authentication and authorization, it contains a myriad of valuable company and employee data.

Regardless of the tools and tactics used in these attacks, nearly all adversaries target Active Directory (AD) due to its role in storing credentials and identity-related information. In addition, protecting Active Directory has become increasingly complex due to distributed organizations, pervasive access, hybrid cloud authentication systems, and many objects with varying privilege and domain control levels. Monitoring and securing an environment is an ongoing challenge, and when that control is lost to an attacker it can result in dire consequences.

Adding complexity to these challenges is the organizational structure in many enterprises, with siloed security and IT teams. These groups have different goals and objectives which can cause unintentional gaps in the protectiof of enterprise AD infrastructure.

This paper explores why organizations have difficulty battening hardening their Active Directory deployments. It includes best practices for achieving proactive AD security, using insights from tools that offer continuous visibility of domain exposures and the risks they create. Additionally, the paper will detail methods attackers are using to enumerate Active Directory and how to detect live attack activities. When used in a collaboration between teams, it can close security gaps, mitigate risk, and more efficiently derail attacks earlier in its lifecycle.

02

Challenges Protecting Active Directory

Modern enterprises face increased challenges when it comes to protecting Active Directory. Most businesses have distributed organizations, with the added challenge of remote workers becoming the status quo. It takes a great deal of expertise and time to identify all known vulnerabilities, determining the minimal permissions required for each role and app, and the maintenance in keeping newly identified issues from taking root. Most organizations do not have the expertise and time to properly address their Active Directory security.

You may consider:

- Should Active Directory permissions be granted to a centrally based team, or should there be members worldwide?
- How do you delegate permissions to support operations without doling out excessive access? (You may allow pervasive access into your Active Directory for contractors or external entities.)
- If you've rolled out ADFS or utilized guest accounts, do you know who's using those accounts?
- Active Directory can contain a vast collection of objects, each with different levels of privilege and control over the forest or domain. How do you ensure proper hygiene over these objects?
- Is your AD optimized to serve your organization but with the appropriate safeguards to prevent an attacker from gaining access to your AD environment or making a return visit?
- Are you monitoring your Active Directory to catch suspicious activity and secure it early in the process?
- How are you reviewing events and acting on alerts?
- Most importantly, how are you securing your Active Directory before it's compromised and an attacker does something nefarious?

03

IT or Not IT – That is the (Security) Question

The challenges listed above require administrative access to objects within Active Directory. Many organizations face the dilemma of where the ownership lines are drawn to determine how these permissions are assigned. IT and security teams play distinct roles in managing AD and have specific agendas they must follow. IT traditionally provides operational oversight, deploying and managing computers and systems, software deployments, and user provisioning. Security teams typically focus on securing the endpoint, server and workload environments – locking them down and restricting access. These agendas can frequently conflict with one another, and IT will often take precedence whenbusiness service could be impacted, leaving an inadvertent gap in your Active Directory's defense.

04

Proactively Protect Your Active Directory

IT and Security teams face challenges in achieving security effectiveness without supporting tools. Both teams need information to help them take appropriate, timely actions. Various specialized tools can automatically report vulnerabilities and detect attacks early or even in real-time. These tools will be critical to the teams' success in protecting your identity environments.

05

How SentinelOne Protects Your Active Directory

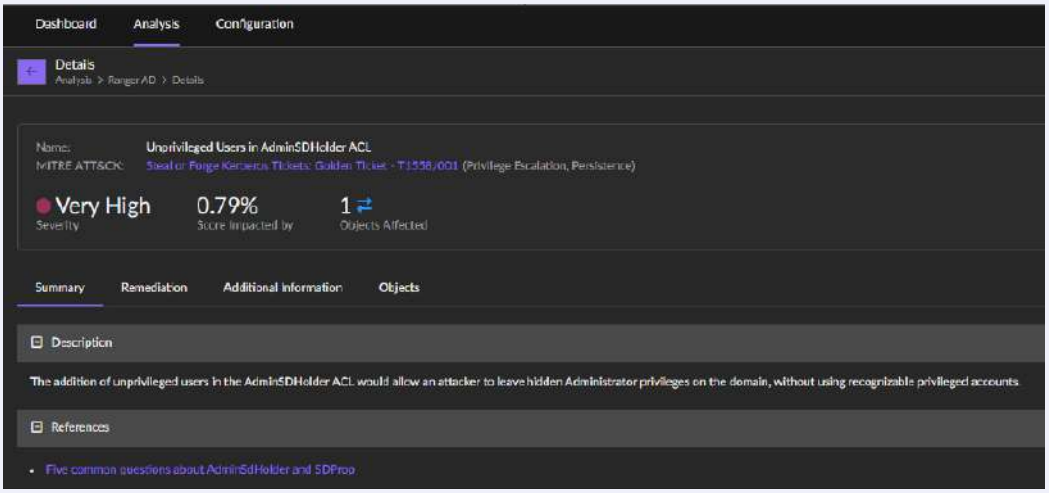
SentinelOne offers two effective tools that provide proven protection for your Active Directory infrastructure to address the above concerns: Singularity Ranger AD and Singularity Identity. Let's see how they work.

Using a standard (non-administrative) user account running on a client machine to query Active Directory, Ranger AD can examine your identity stores in both on-premises and Azure AD and highlight which, if any vulnerabilities you have and the level of risk for each. The vulnerabilities are rated by their MITRE severity and include mitigation steps to remediate them so that you can reduce the attack surface, thus improving your Active Directory's security posture.

Mitigate your way through all the findings to improve your overall health score to 100%, and your AD will be hardened against attackers who manage to slip past your endpoint protection into your network. Every quarter, additional exposure checks are added to stay on top of newly discovered risks, vulnerabilities in other Directory Services areas, such as Certificate Services and ADFS, and cloud vulnerabilities found in Azure or AWS.

This continuous scanning and assessment is performed on a weekly basis as new or modified user accounts can easily become mismanaged, opening the organization up to compromise through vulnerable accounts.

Active Directory Exposure Details

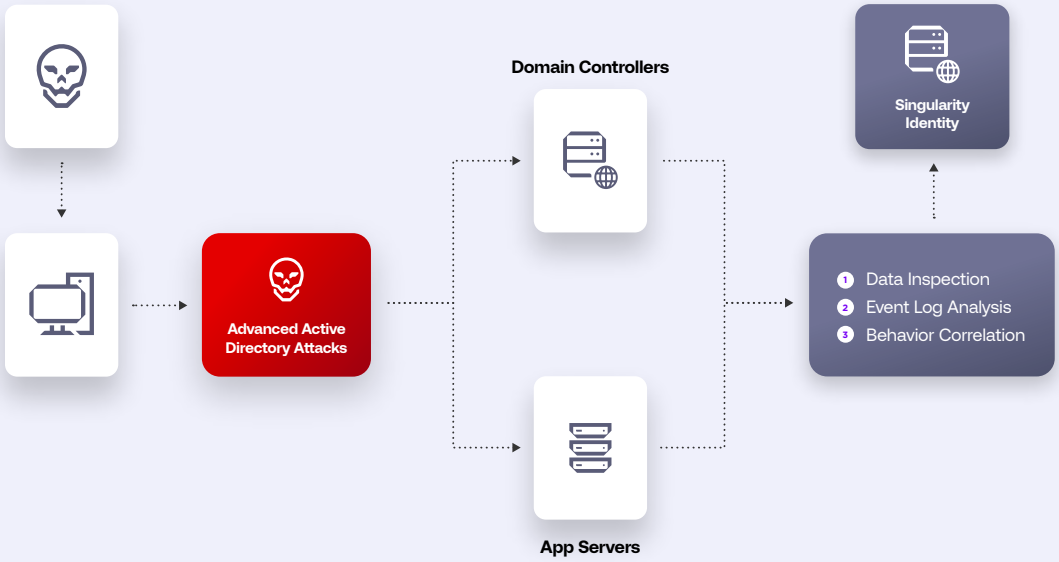


By having your on-prem machine's agent subscribe to directory changes, Ranger AD also provides real-time alerts on attacks to your Active Directory. It will detect password spray, lockout, suspicious password changes, DC service installation attacks, etc. Having these alerts as soon as there is a determination of potential risk can mean the difference between losing or keeping control of your Active Directory.

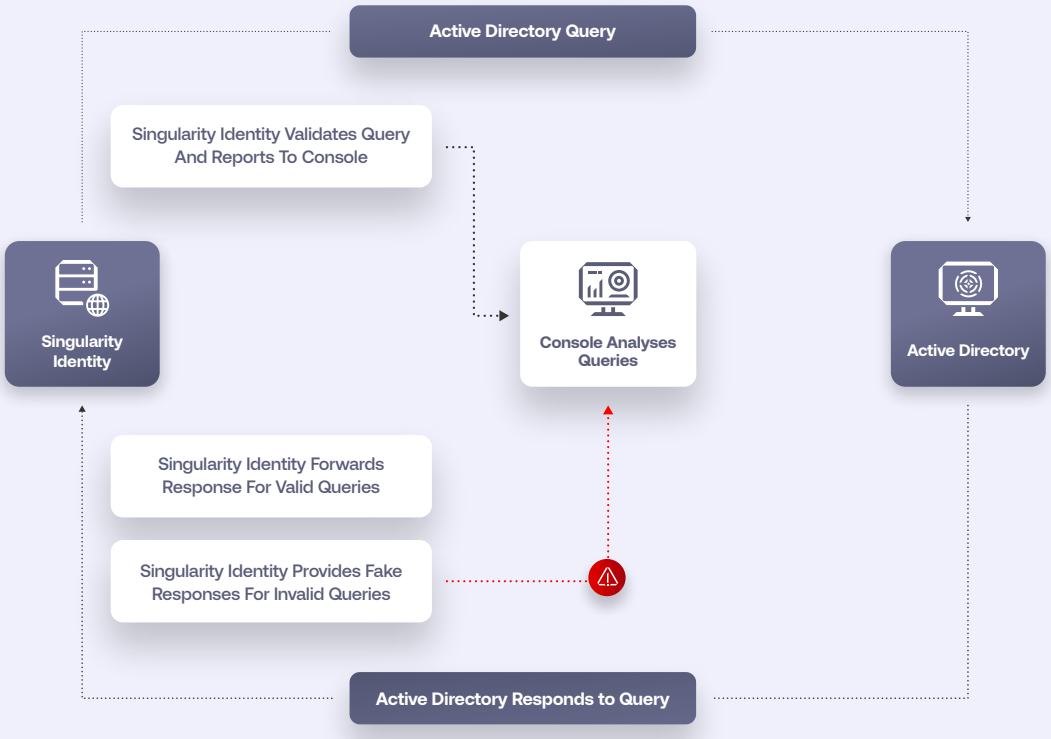
Singularity Identity offers complementary Active Directory protection to Ranger AD by intercepting queries to AD intended to perform reconnaissance through object enumeration and returns false answers. This makes it impossible for an attacker to glean anything of value to stage a successful attack. Furthermore, Singularity Identity can send e-mail alerts to your security and IT teams, notifying them of the suspicious activity. The machine can be contained and the user account can have its password reset.

Singularity Identity is available to install on either a domain controller or endpoint, respectively.

Active Directory Domain Controller Protection



Active Directory Protection from Endpoints



This flexibility allows you to either deploy to a relatively small number of domain controllers or if you'd rather not add additional software to DCs, deploy on all your endpoints instead.

06

Security – Now a Team Sport

While Ranger AD and Singularity Identity are both incredible defensive and informative tools, you still need the organization in place to operate them. Since both tools are security-oriented, they can run under the ownership of a security team. Security teams are responsible for taking exposures discovered from Ranger AD and bringing them to the change advisory board (CAB) meetings. The IT team will be aware of such changes and can raise concerns if they believe a business system could be impacted, a check to ensure the Security team's implementation can be performed safely. If Security doesn't have the authority to make the changes in Active Directory, then the IT team can implement the changes with oversight and assistance from them. Should Ranger AD detect any attacks, Security can work with IT to determine whether an actual attack is occurring and take immediate action if needed. This will be similar with Singularity Identity: the Security team is responsible for configuring the false information which will be presented to attackers. They will grant themselves and the IT team access to receive legitimate AD queries. If an alert is received, the Security team will respond by coordinating with the IT team to determine if the attack is genuine and leverage all available methods such as EDR to contain the machine where the attacks are sourced, disable the user account, and notify the employee who was compromised.

07

Conclusion

The expertise and time required to handle the constant flow of vulnerabilities, changing permissions, and maintenance exceeds what the typical organization performs on their Active Directory. This leaves most organizations wide open to attacks. Active Directory security can be managed cooperatively by delegating the implementation and business safety check to the IT team while monitoring and response is performed by your Security team.

SentinelOne's identity security solutions automatically gather information on vulnerabilities and attacks so that both teams can focus on addressing problems rather than testing and searching for them. Having the right teams and tools in place can prevent attacks on your Active Directory and your organization's infrastructure.

SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com