ACTIVE DIRECTORY AGENTLESS MFA + PAM

SOLUTION BRIEF

Agentless Active Directory MFA and Privileged Access management provides agentless access to privileged infrastructure as well as multi-factor authentication.

The Problem:

Traditional MFA solutions require installing agents on domain controllers or modifying applications, leading to costly and complex deployments. This is a problem where privileged infrastructure cannot have agents, and also problematic to install / configure and maintain agents everywhere.

Organizations additionally face increasing risks from compromised credentials, particularly in environments relying on Active Directory for authentication. Moreover, legacy systems and tools like Kerberos or NTLM lack support for modern MFA protections, leaving them vulnerable to attacks.

Solution – AuthNull's agentless MFA and privileged access for Active Directory Infrastructure.

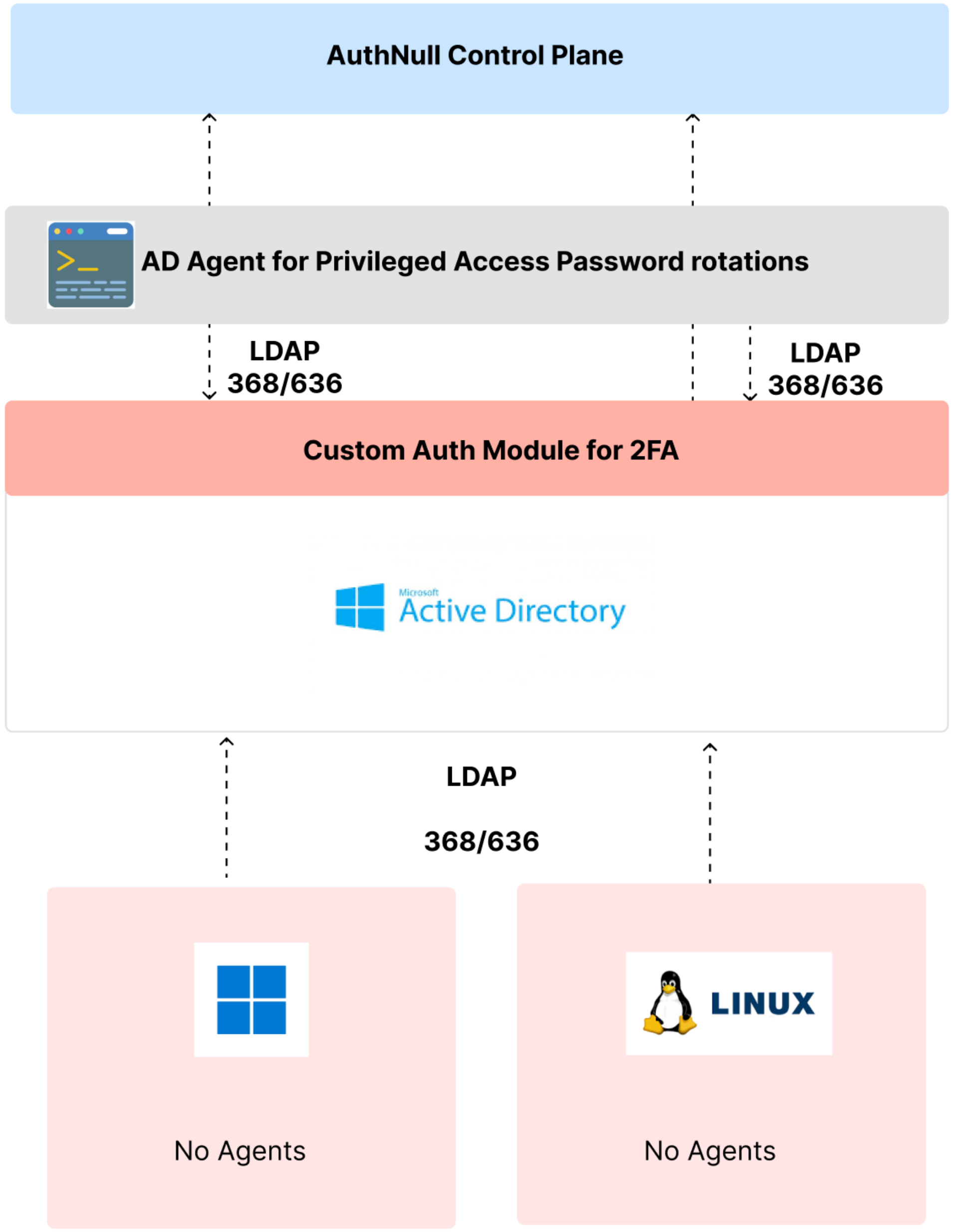
Our agentless MFA solution delivers complete protection for all AD authentications, leveraging existing protocols like LDAP, NTLM, and Kerberos. By integrating directly into the authentication flow, it enforces MFA across legacy systems, cloud resources, and on-prem applications—all without the need for installing software agents or proxies. This non-intrusive solution offers full MFA coverage, detecting risky logins and enforcing adaptive authentication without compromising user experience.

Key benefits

- **Low Overhead**: No need to install agents on servers or modify applications, ensuring faster, cost-effective deployment.
- **Comprehensive Coverage**: Protects all resources, including legacy systems, file shares, and command-line access.
- MFA:
- **Simplified Management**: Unified platform to manage all MFA policies, monitoring all AD authentications in real-time.
- **Seamless Integration**: Works with Active Directory Domain Services (on-prem) and OKTA infrastructure to extend Active Directory

Technical Specifications and solution deployment

- **Architecture**: Agentless integration with Active Directory, requiring no modifications to the underlying system or applications. This requires a deployment of an Active Directory bridge that sits close to the domain controller communicating, discovering users and policies.



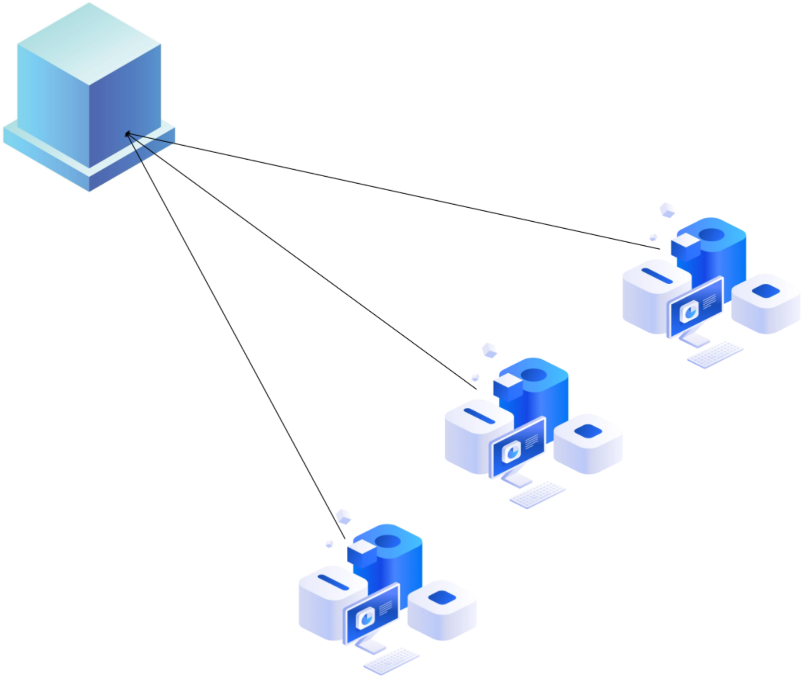
In a typical deployment, you will have some changes to the active directory domain services (to control 2FA and enable privileged access) as well as an AD agent for privileged access. Please note that while this solution is agentless – what this means is that client machines will not need any changes whereas the domain controllers will need an agent / bridge sitting next to it to deliver password rotation, user discovery, policy discovery and more, The connecting machines do not need any agents or changes to configuration in order to enable MFA and privileged access.

Use cases:

1. **Protect Active Directory service accounts**: Agentless MFA can be used to seamlessly protect Active Directory service accounts without additional overhead.
2. **Protect Active Directory interactive user accounts:** Agentless MFA can bne used to protect all existing Active Directory interactive user accounts.
3. **Provide privileged access management use cases against Active Directory:** Discover all privileged users, rotate passwords based on password policy, enable MFA and more.

Value Proposition:

AuthNull enables agentless MFA and privileged access for Active Directory helping eliminate friction, bringing ease of use and more to your privileged infrastructure



Contact Us to Learn More

Get in touch with us to learn more at sales@authnull.com or visit https://authnull.com/agentless.