Comparison with OKTA Advanced Server Access

This is a datasheet that provides comparison of AuthNull with OKTA Advanced Server Access

Passwordless Privileged Access Management

AuthNull

Passwordless PAM

AuthNull replaces traditional passwordless PAM with a simple Decentralized Identity credentials powered by public key cryptography.

The passwordless authentication mechanism is a gateway to a powerful privileged access management platform that has all the necessary features enterprises need to enable remote server and infrastructure access.

Passwordless authentication

AuthNull enables passwordless authentication by supporting LDAP 1FA or 2FA, Posix account logins with 1FA or 2FA, additionally through protocols such as SSH, VNC, RDP, Telnet and more.

All credentials are stored as a decentralized identity credentials eliminating the need for a vault.

What is the best way to reduce the most critical attack surface of credentials? By removing it of course!

How does AuthNull compare with OKTA?

The biggest credential breach during the pandemic was shared credentials. OKTA does not fully eliminate a central attack surface and still relies on a Certificate authority.

While this can be claimed as "passwordless", and "ephermeral".. the fact is that this requires users to be logged in and allowing their workstations to trust their CA.

This makes the OKTA certificate authority a biggest attack surface. Removing the CA is the best way to secure a system and that is what AuthNull has done,

AuthNull enables organizations to truly deploy Zero trust, passwordless security to access critical infrastructure.

.

Is Zero Trust the answer?

- As the increased remote workforce strained traditional IT perimeter defenses
- And recent attacks exposed further weaknesses, one potential architecture framework emerged: Zero Trust. This is the only model that organizations trust today to protect their IT assets.

Comparison

Please see the following page to see the detailed comparison between OKTA and AuthNull

Contact Us

AuthNull

16668 Winchester Club Dr. Meadow
Vista CA 95722

Feature	OKTA Advanced Server Access	AuthNull	Notes
Authentication protocol – SSH	Yes	Yes	
Authentication protocol – LDAP	No	Yes	
Authentication protocol – RDP	Yes	Yes	
Authentication protocol – Telnet	No	Yes	
Authentication protocol – VNC	No	Yes	
Login clients:	Custom, SSH client	VNC, SSH, RDP – no custom clients	
Passwordless approach	Centralized, ephemeral CA	Decentralized credentials and identity	
Existing passwords and SSH keys supported	No	Supported for legacy reasons	
Windows support	Yes	Yes	
Linux Support	Yes	Yes	
Blockchain based tamper evident credentials	No	Yes	
Blockchain hashes based logging	No	Yes	
Authenticator	OKTA Authenticator App	AuthNull Authenticator App	
FaceID to protect credentials	Yes	Yes	
SSO console depends on passwords	Yes, OKTA SSO	Yes, OKTA SSO	
End user console	Yes	Yes	
Extensive logging	Yes	Yes	
Built in runtime guardrails	No	Yes	
Built in runtime compliance checks	No	Yes	Runtime security powered through LSM – AppArmor and SELinux
Self rotating credentials	No	Yes	
Agent for PAM	Yes	No	
AD authentication	No	Yes	
Passwordless SSH Login	Yes	Yes	