AuthNull

Data Sheet

AuthNull – A Zero trust, decentralized approach to server access

Remote infrastructure access and privileged access management (PAM) is never easy. IT administrators find it hard to implement, and users find it painful to deal with forced SSH Key and password rotations.

This leads to entropy in systems leading to credential compromise attacks. AuthNull addresses these issues by simplifying the implementation with a decentralized, passwordless credential that requires no user effort to remember.

An Identity aware, next generation privileged access management solution – AuthNull delivers value by simplifying infrastructure access with 1FA or 2FA Passwordless.

AuthNull solution brief

AuthNull replaces passwords and SSH keys with Decentralized credentials managed by users on the wallet. With two roots of trust (organization, and user).

AuthNull (https://authnull.com) is a next generation Privileged Access Management solution that has been tailor built from ground up to **eliminate passwords and SSH Keys** while complying to stringent federal government standards including FTC safeguards rule, NIST Secure Software Development Framework (NIST SP 800-218) and (2) the NIST Software Supply Chain Security Guidance.

AuthNull:
* Enables Passwordless1FA Authentication
* Removes the need for a centralized Vault, removing a major attack vector.
* Provides All features of a traditional PAM – endpoint management, session recordings and more.

How it works? – Security by Obscurity

How AuthNull Works

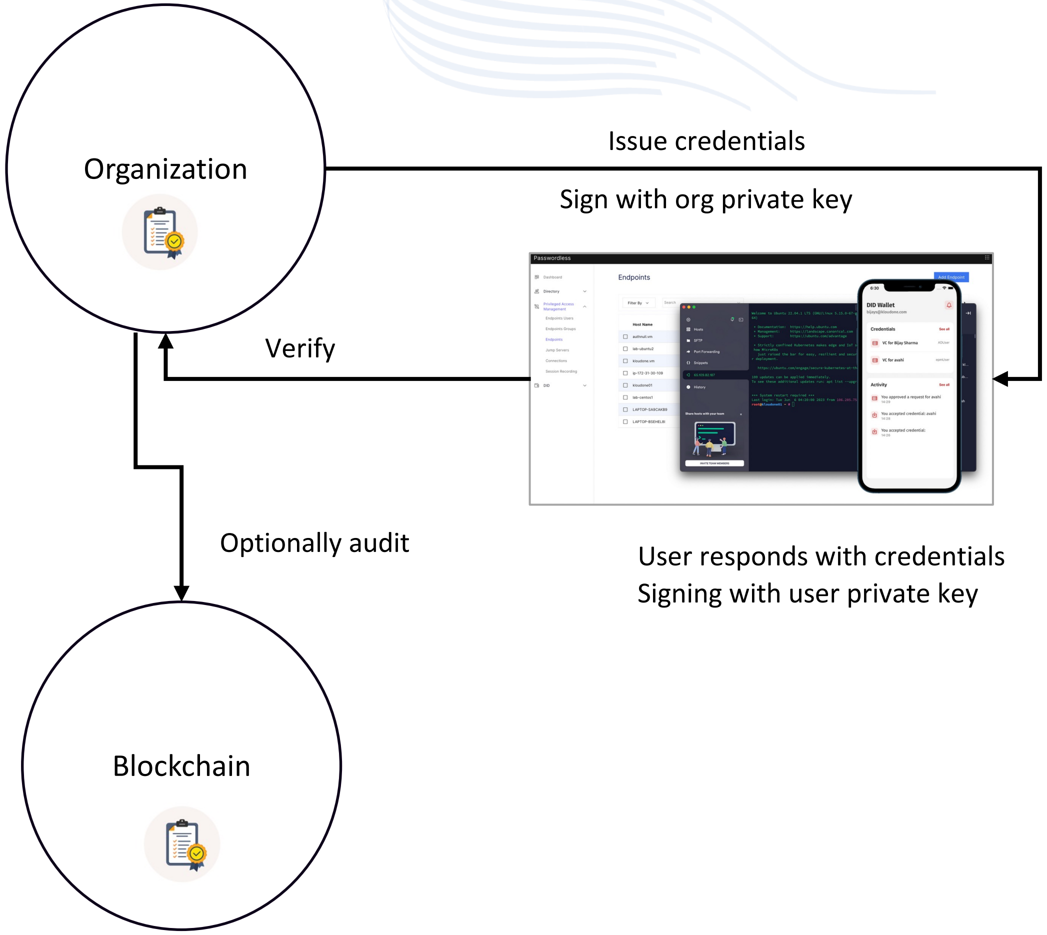
1. **User signs into any remote infrastructure**
2. **Wallet is pinged. User is verified on wallet using Biometrics.**
3. **User logs in**

Behind the scenes:

- Both users and organizations are issued private / public keys
- Using public key cryptography – organization signs credentials and assigns to a given user.
- These decentralized credentials are stored on the user's wallet identified by the user's identity.
- When user attempts to login, the wallet is pinged.
- The wallet user signs credentials with their private key
- Organization
- All of this happens with minimal user interaction except for FaceID / Biometric validation..

Blockchain features

- Identities and credentials can be optionally be written, and verified additionally using blockchain



Organization

Issue credentials

Sign with org private key

Verify

Optionally audit

User responds with credentials
Signing with user private key

Blockchain

Immutable records and verification on any private/ public blockchain

Security / Compliance of AuthNull

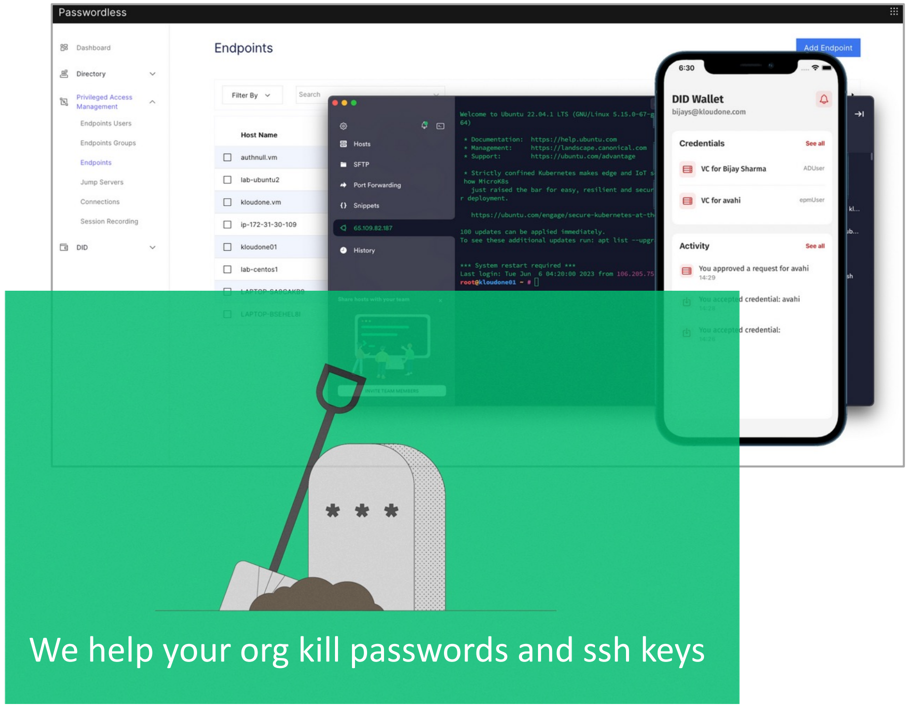
- FTC safeguards rule
- NIST Secure Software Development Framework (NIST SP 800-218) and
- (2) the NIST Software Supply Chain Security Guidance.
- MITRE
- CIS Benchmarks
- SOC 2 Type 2 certification
- PCI-DSS
- NIST SP 800-53
- NIST SP 800-171

Deployment model

Due to the extensive security requirements of accessing secure infrastructure, AuthNull is preferred to be deployed on Airgapped on prem.

We provision AuthNull using K8s infrastructure which can be deployed in your environment in a few days.

AuthNull Features



Host Name
authnull.vm
lab-ubuntu2
kloudone.vm
ip-172-31-30-109
kloudone01
lab-centos1
LAPTOP-SA9CAKB9
LAPTOP-BSEHEL8I

```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-67-g
64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT s
 how MicroK8s
   just raised the bar for easy, resilient and secur
r deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-th

100 updates can be applied immediately.
To see these additional updates run: apt list --upgr


*** System restart required ***
Last login: Tue Jun  6 04:20:00 2023 from 106.205.75
root@kloudone01 ~ #
```

DID Wallet
bijays@kloudone.com

Credentials

- VC for Bijay Sharma ADUser
- VC for avahi epmUser

Activity

- You approved a request for avahi 14:29
- You accepted credential: avahi 14:28
- You accepted credential: 14:26

We help your org kill passwords and ssh keys

Passwordless Authentication

- Simple Passwordless authentication for local posix, or LDAP users
- Connect with SSH, RDP, Telnet, VNC and against K8s

PAM

- Self-service admin and end user console
- SSO with SAML2
- End point management
- Session management, Session recording and play back (video and text)

• Decentralized Identity

- User credentials fully decentralized using Decentralized Identity standards
- Legacy support for SSH Keys and Passwords where needed

Vault / Wallet App

- AuthNull does not use vault as it uses decentralized wallet for credential storage.
- Wallet provides 1FA / 2FA authentication.

Tamper Evident Credentials

- Extensive logging, Merkle hash and Ethereum (or other blockchain) write of transactions leading to immutable and tamper evident credentials.

How do we compare?

AuthNull Vs Okta Advanced Server Access vs Cyberark

Feature	OKTA Advanced Server Access	AuthNull	CyberArk
Login	SSO Password / Passwordless login	SSO Password / Passwordless login	SSO Password / Passwordless login
Credential storage design	Centralized with Centrally controlled CA	Decentralized Using Decentralized Identity Standard.	Centrally controlled with Conjur Vault
Session management	Text recording only	Text and Video recording	Text and Video recording
Authentication protocols	SSH and RDP only	SSH, VNC, RDP, Telnet, and K8s accounts	SSH, VNC, RDP and Telnet,
SSH Tunnelling	Not available	Yes	Yes
What is used for authentication	Ephemeral SSH Certificates	Decentralized ID Credentials, SSH Keys and Passwords	SSH Keys, Passwords + Ephemeral SSH certificates
Credential Storage	Ephemeral SSH Certificates with no storage.	Wallet	Vault
Authentication trust sources	Single Trust source (CA)	Two trust Sources (Org Issuer, User)	Single Trust Source (CA) or Vault

AuthNull Vs Okta Advanced Server Access vs CyberArk continued

Feature	OKTA Advanced Server Access	AuthNull	Cyberark
Login client	Custom, SSH client	VNC, SSH, RDP – no custom clients	VNC, SSH, RDP – no custom clients
Passwordless approach	Centralized, ephemeral CA	Decentralized credentials and identity	Centralized + Ephemeral CA
Existing passwords and SSH keys supported	No	Supported for legacy reasons	Supported
Windows support	Yes	Yes	Yes
Linux Support	Yes	Yes	Yes
Blockchain based tamper evident credentials	No	Yes	Yes
Blockchain hash logging	No	Yes	No
Authenticator	OKTA Authenticator App	AuthNull Authenticator App	Cyberark authenticator app
FaceID to protect credentials	Yes	Yes	Yes
SSO console depends on passwords	Yes, OKTA SSO	Yes, OKTA SSO	Yes, OKTA SSO
End user console	Yes	Yes	Yes
Extensive logging	Yes	Yes	Yes
Built in runtime guardrails	No	Yes	No
Built in runtime compliance checks	No	Yes	Yes
Self rotating credentials	No	Yes	Yes
Agent for PAM	Yes	Yes	Yes
AD authentication	No	Yes	Yes
Passwordless SSH Login	Yes	Yes	Yes

Thank you

Asif Ali
+1 408-368-3404
a@authnull.com

Let's chat?

Here's our calendar link to setup a quick discussion.