AuthNull

Identity Aware, Passwordless Privileged Access Management

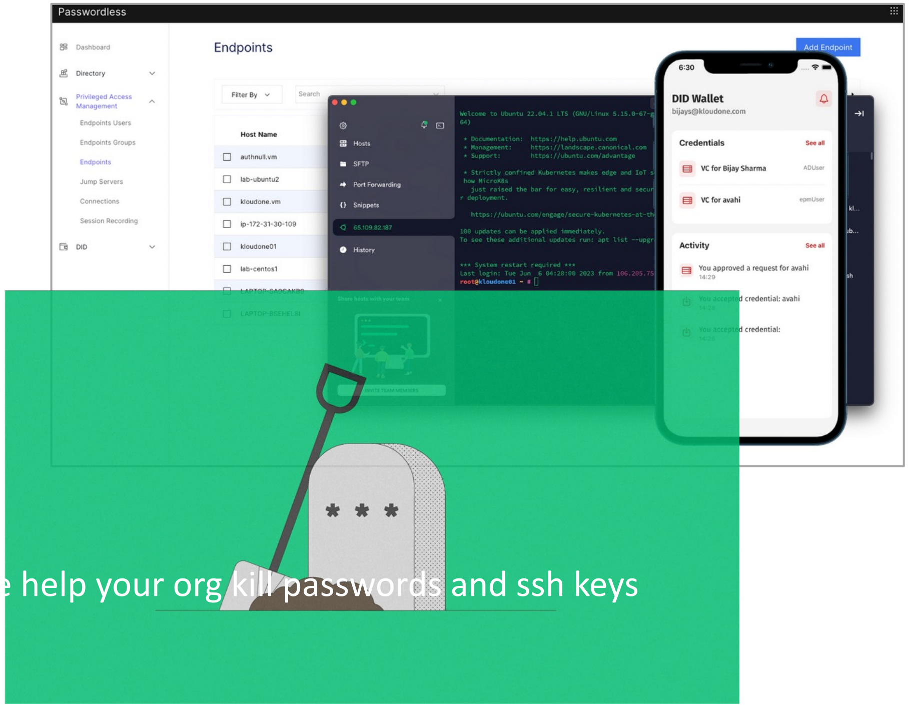
Passwords & SSH Keys are a bane to enterprise authentication

- Passwords and SSH Keys are commonly compromised through phishing attacks, credential thefts, password re-use, and credential stuffing.
- Credential loss and and attacks on critical infrastructure are about 24-50% of all attacks.

Our value proposition / approach

- Eliminate SSH Keys and Passwords, rotation and distribution and introduce Passwordless 1FA.
- Support for Passwords / SSH Keys with Passwordless 2FA where backward compatibility is required
- Remove the need for a Centralized Vault, a major attack vector.

AuthNull – Next Generation Infrastructure Access Solution



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

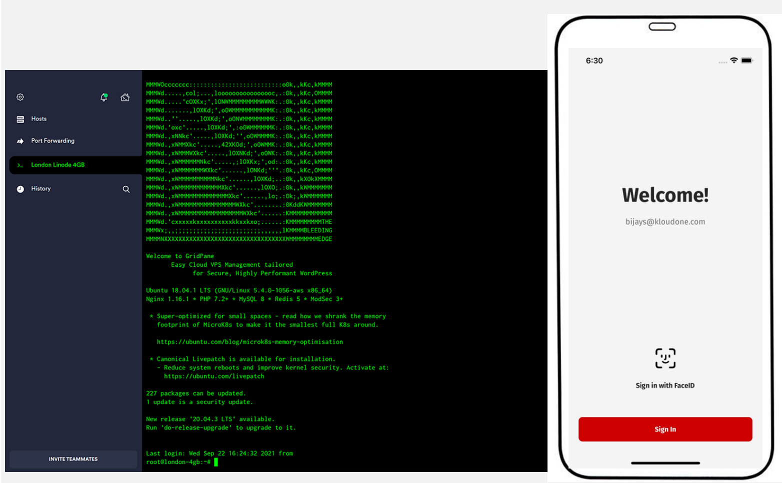
Activity

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

e help your org kill passwords and ssh keys

- Secure, Passwordless Infrastructure access at Scale.
- Available as On-prem, your private cloud or as a SAAS solution.
- Full PAM feature set including session recording, endpoint management
- 1FA or 2FA Passwordless authentication
- Powered by Decentralized Identities, and introducing two roots of trust. Optional Blockchain integration identities and claims
- Tamper evident credentials; extensive logging for compliance

How does it work?

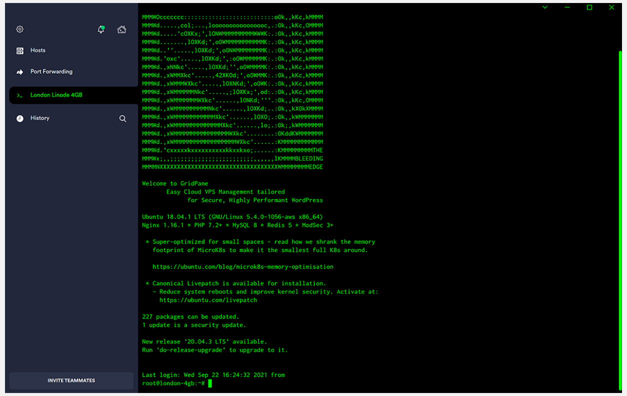


```
MMMWOccccccc::::::::::::::::::::::::::o0k,,kKc,kMMMM
MMMWd.....,col;...,loooooooooooooooc,.:0k,,kKc,OMMMM
MMMWd.....'cOXKx;',lONWMMMMMMMMWWWK:.:0k,,kKc,kMMMM
MMMWd.......,lOXKd;',o0WMMMMMMMMMMK:.:0k,,kKc,kMMMM
MMMWd..''.....,lOXKd;',o0NWMMMMMMMK:.:0k,,kKc,kMMMM
MMMWd.'oxc'.....,lOXKd;',:o0WMMMMMK:.:0k,,kKc,kMMMM
MMMWd.,xNNkc'.....,lOXKd;'',o0WMMMMK:.:0k,,kKc,kMMMM
MMMWd.,xWMMXkc'.....,42XKOd;',o0WMMK:.:0k,,kKc,kMMMM
MMMWd.,xWMMMWXkc'.....,lOXNKd;',o0WK:.:0k,,kKc,kMMMM
MMMWd.,xWMMMMMMNkc'.....,;lOXKx;',od:.:0k,,kKc,kMMMM
MMMWd.,xWMMMMMMMWXkc'......,lONKd;'''.:0k,,kKc,OMMMM
MMMWd.,xWMMMMMMMMMMNkc'......,lOXKd;..:0k,,kX0kXMMMM
MMMWd.,xWMMMMMMMMMMMMXkc'......,lOXO;.:0k,,kWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMXkc'......,lo;.:0k;,kWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMMMWXkc'........:0KddKWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMMMMMWXkc'......:KMMMMMMMMMMMM
MMMWd.'cxxxxxkxxxxxxxxxxkkxxkxo;......:KMMMMMMMMTHE
MMMWx;,,;;;;;;;;;;;;;;;;;;;;;;;;,,,,,,lKMMMMBLEEDING
MMMMNXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXWMMMMMMMMEDGE

Welcome to GridPane
       Easy Cloud VPS Management tailored
             for Secure, Highly Performant WordPress

Ubuntu 18.04.1 LTS (GNU/Linux 5.4.0-1056-aws x86_64)
Nginx 1.16.1 * PHP 7.2+ * MySQL 8 * Redis 5 * ModSec 3+

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

227 packages can be updated.
1 update is a security update.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Sep 22 16:24:32 2021 from
root@london-4gb:~#
```

#1

While authenticating to server, simply login using biometrics to the wallet.

Wallet gets pinged and Wallet based credentials are picked up.



```
MMMWOccccccc::::::::::::::::::::::::::o0k,,kKc,kMMMM
MMMWd.....,col;...,loooooooooooooooc,.:0k,,kKc,OMMMM
MMMWd.....'cOXKx;',lONWMMMMMMMMWWWK:.:0k,,kKc,kMMMM
MMMWd.......,lOXKd;',o0WMMMMMMMMMMK:.:0k,,kKc,kMMMM
MMMWd..''.....,lOXKd;',o0NWMMMMMMMK:.:0k,,kKc,kMMMM
MMMWd.'oxc'.....,lOXKd;',:o0WMMMMMK:.:0k,,kKc,kMMMM
MMMWd.,xNNkc'.....,lOXKd;'',o0WMMMMK:.:0k,,kKc,kMMMM
MMMWd.,xWMMXkc'.....,42XKOd;',o0WMMK:.:0k,,kKc,kMMMM
MMMWd.,xWMMMWXkc'.....,lOXNKd;',o0WK:.:0k,,kKc,kMMMM
MMMWd.,xWMMMMMMNkc'.....,;lOXKx;',od:.:0k,,kKc,kMMMM
MMMWd.,xWMMMMMMMWXkc'......,lONKd;'''.:0k,,kKc,OMMMM
MMMWd.,xWMMMMMMMMMMNkc'......,lOXKd;..:0k,,kX0kXMMMM
MMMWd.,xWMMMMMMMMMMMMXkc'......,lOXO;.:0k,,kWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMXkc'......,lo;.:0k;,kWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMMMWXkc'........:0KddKWMMMMMMM
MMMWd.,xWMMMMMMMMMMMMMMMMMMWXkc'......:KMMMMMMMMMMMM
MMMWd.'cxxxxxkxxxxxxxxxxkkxxkxo;......:KMMMMMMMMTHE
MMMWx;,,;;;;;;;;;;;;;;;;;;;;;;;;,,,,,,lKMMMMBLEEDING
MMMMNXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXWMMMMMMMMEDGE

Welcome to GridPane
       Easy Cloud VPS Management tailored
             for Secure, Highly Performant WordPress

Ubuntu 18.04.1 LTS (GNU/Linux 5.4.0-1056-aws x86_64)
Nginx 1.16.1 * PHP 7.2+ * MySQL 8 * Redis 5 * ModSec 3+

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

227 packages can be updated.
1 update is a security update.

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Sep 22 16:24:32 2021 from
root@london-4gb:~#
```

#2

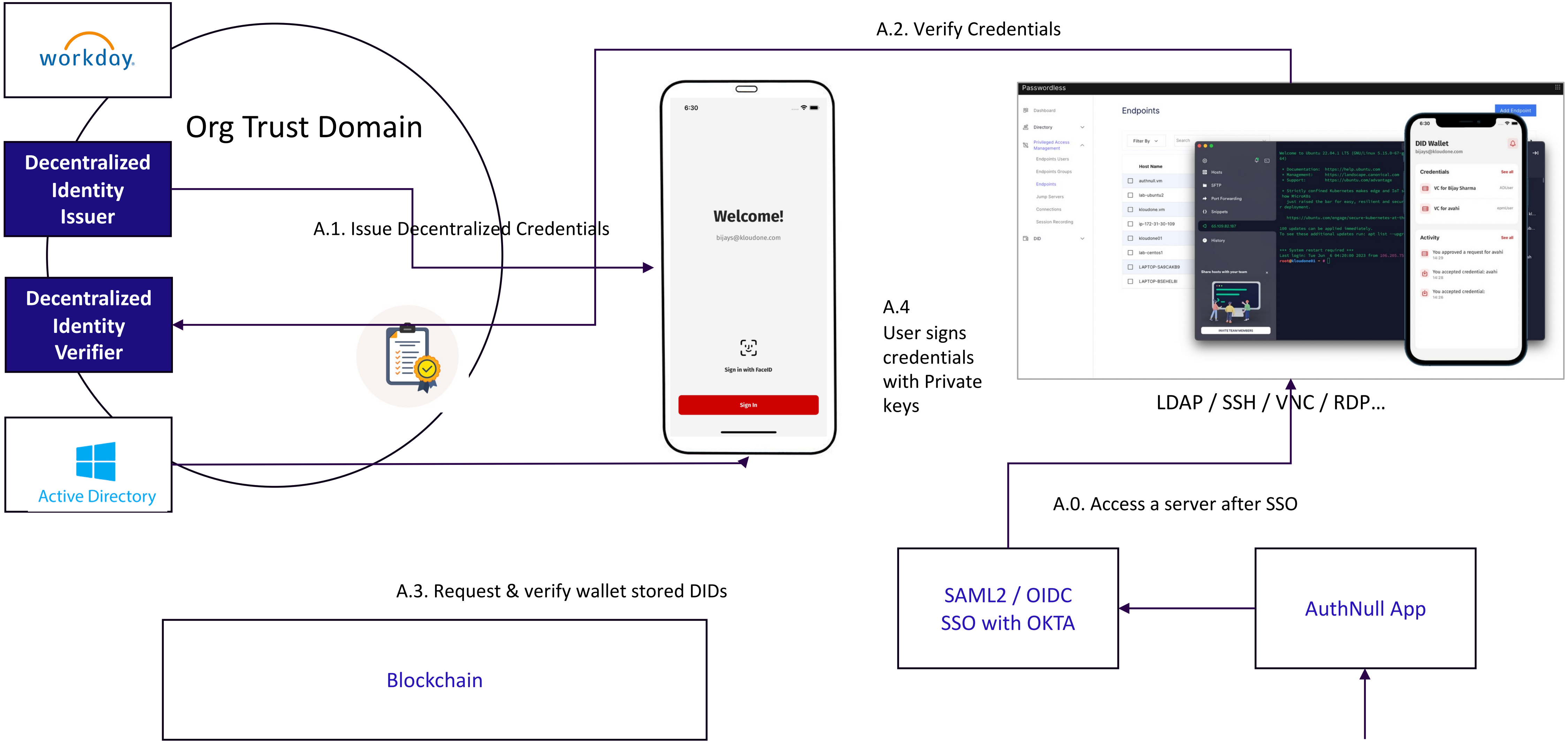
Once credentials are verified

User is authenticated and logged in.

AuthNull’s Security Model

Two (2) roots of trust (User Wallet and the Organization)

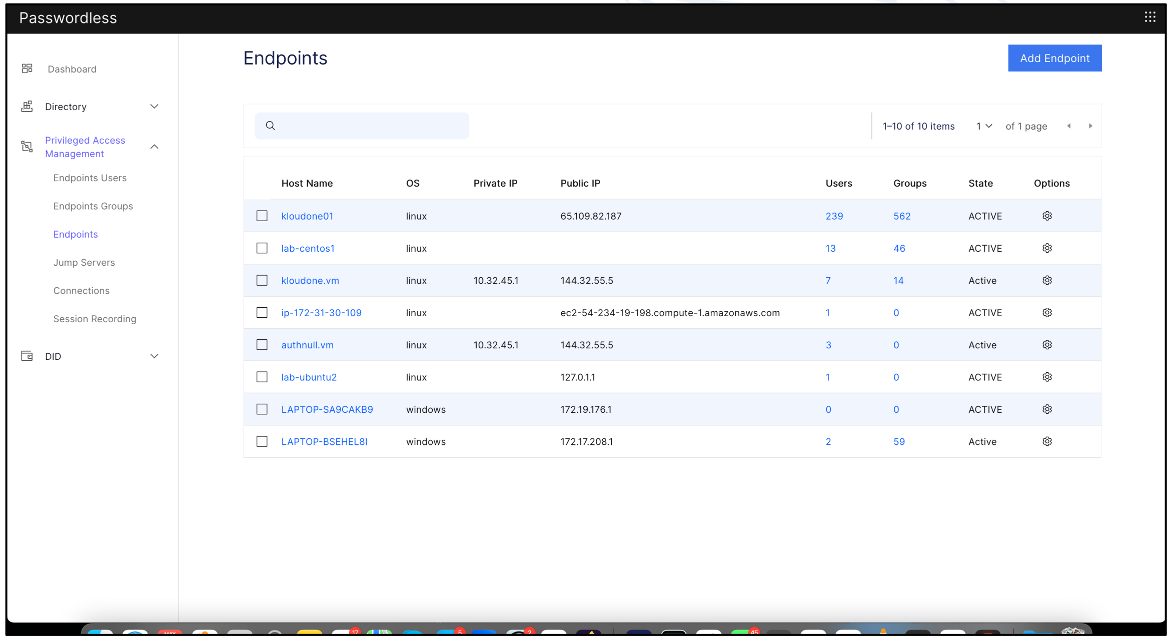
Trusted components Issue, and Verify Credentials stored which are saved, signed by users private key and presented on Authentication requests.



```
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 ~ #
```

PAM Features

- Discover / synchronize privileged users and groups
- 1FA or 2FA LDAP authentication or local privileged authentication
- Password rotations, ssh key rotations with automated distribution to wallets.
- Session Video and Text recording
- LDAP, SSH, RDP and VNC Authentication with 2FA support with 2FA
- Support for Linux, PiOS (windows coming soon)

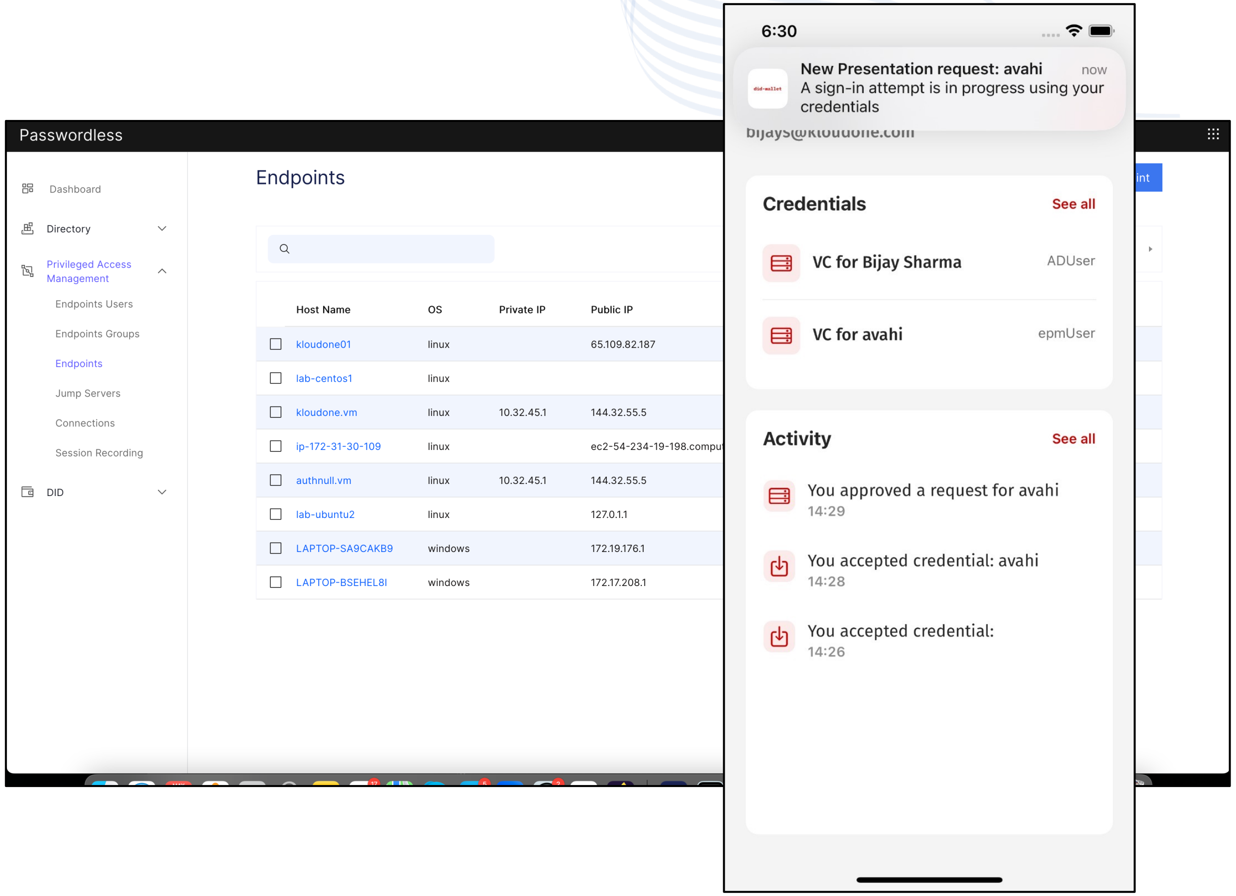


Endpoints

	Host Name	OS	Private IP	Public IP	Users	Groups	State	Options
□	kloudone01	linux		65.109.82.187	239	562	ACTIVE	⚙
□	lab-centos1	linux			13	46	ACTIVE	⚙
□	kloudone.vm	linux	10.32.45.1	144.32.55.5	7	14	Active	⚙
□	ip-172-31-30-109	linux		ec2-54-234-19-198.compute-1.amazonaws.com	1	0	ACTIVE	⚙
□	authnull.vm	linux	10.32.45.1	144.32.55.5	3	0	Active	⚙
□	lab-ubuntu2	linux		127.0.1.1	1	0	ACTIVE	⚙
□	LAPTOP-SA9CAKB9	windows		172.19.176.1	0	0	ACTIVE	⚙
□	LAPTOP-BSEHEL8I	windows		172.17.208.1	2	59	Active	⚙

Credential Management without a Vault or an Ephemeral CA

- Support for Credential rotations, credential policies **<u>without needing a centralized vault.</u>**
- AuthNull enables effortless SSH Key and Password rotations where credentials are converted to Decentralized credentials and directly shipped to the user.



Endpoints

	Host Name	OS	Private IP	Public IP
□	kloudone01	linux		65.109.82.187
□	lab-centos1	linux		
□	kloudone.vm	linux	10.32.45.1	144.32.55.5
□	ip-172-31-30-109	linux		ec2-54-234-19-198.comput
□	authnull.vm	linux	10.32.45.1	144.32.55.5
□	lab-ubuntu2	linux		127.0.1.1
□	LAPTOP-SA9CAKB9	windows		172.19.176.1
□	LAPTOP-BSEHEL8I	windows		172.17.208.1

New Presentation request: avahi — now
A sign-in attempt is in progress using your credentials

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

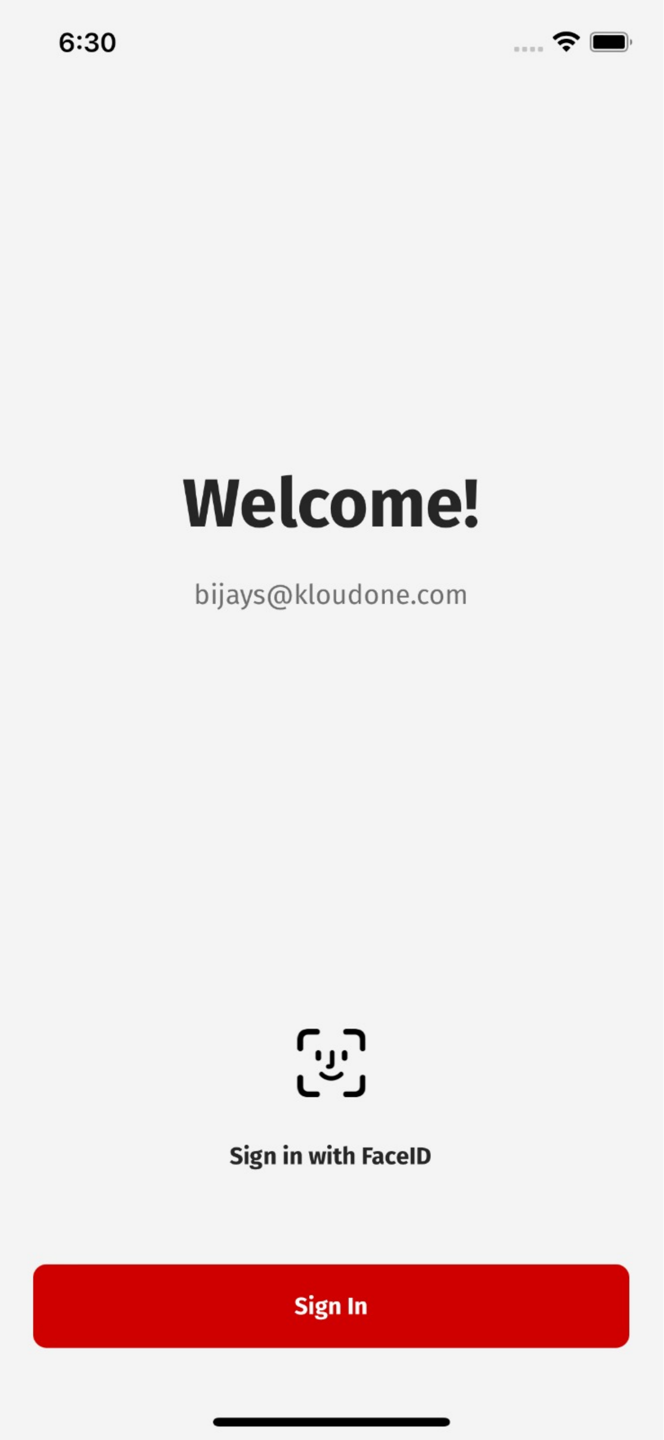
You accepted credential:
14:26

Authenticator Wallet

- Authnull provides a wallet (white label, or otherwise) that stores credentials and enables authentication,.

- Repeat authentication for the same servers can be cached (~30 mins)

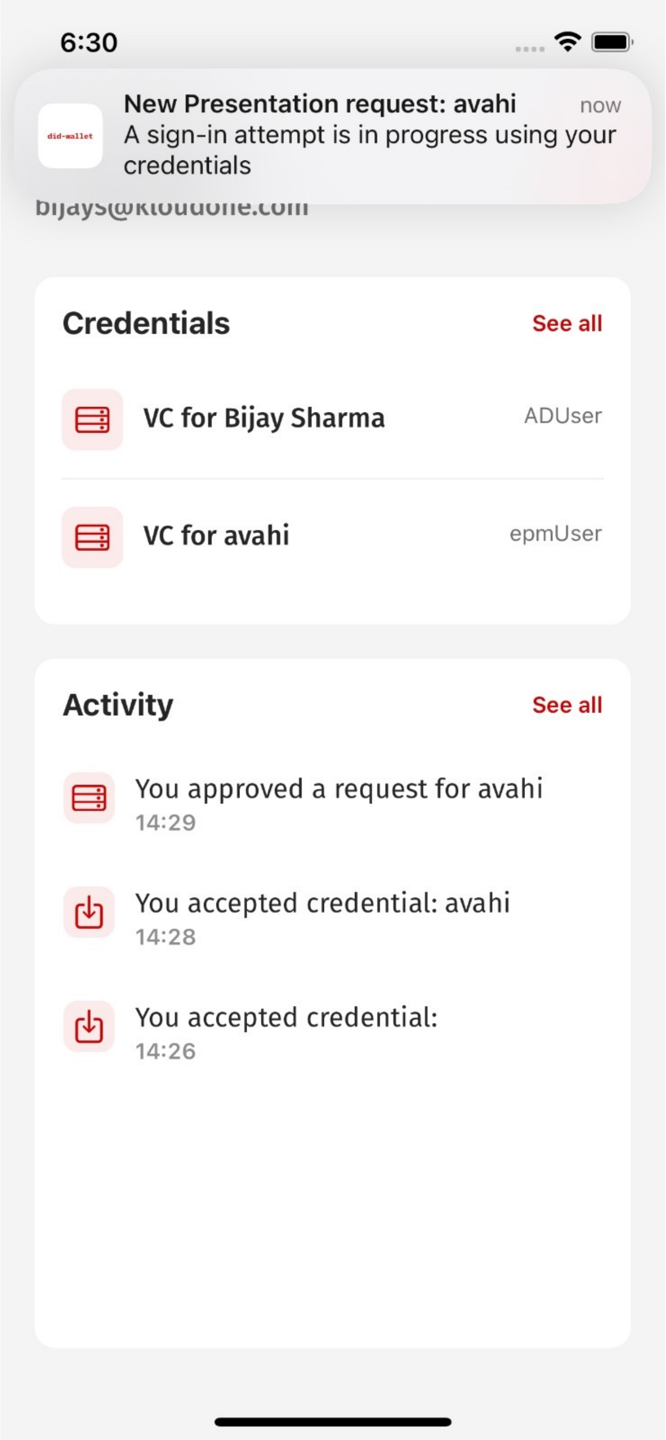
- SSO Login can also be used to eliminate Authentication notifications on the wallet entirely. i.e the Authorization Header can be used as a proxy for authentication when the user simply providing the biometric authentication.



6:30

Welcome!

bijays@kloudone.com



6:30

New Presentation request: avahi now
A sign-in attempt is in progress using your credentials

bijays@kloudone.com

Credentials See all

VC for Bijay Sharma	ADUser
VC for avahi	epmUser

Activity See all

You approved a request for avahi
14:29

You accepted credential: avahi
14:28

You accepted credential:
14:26

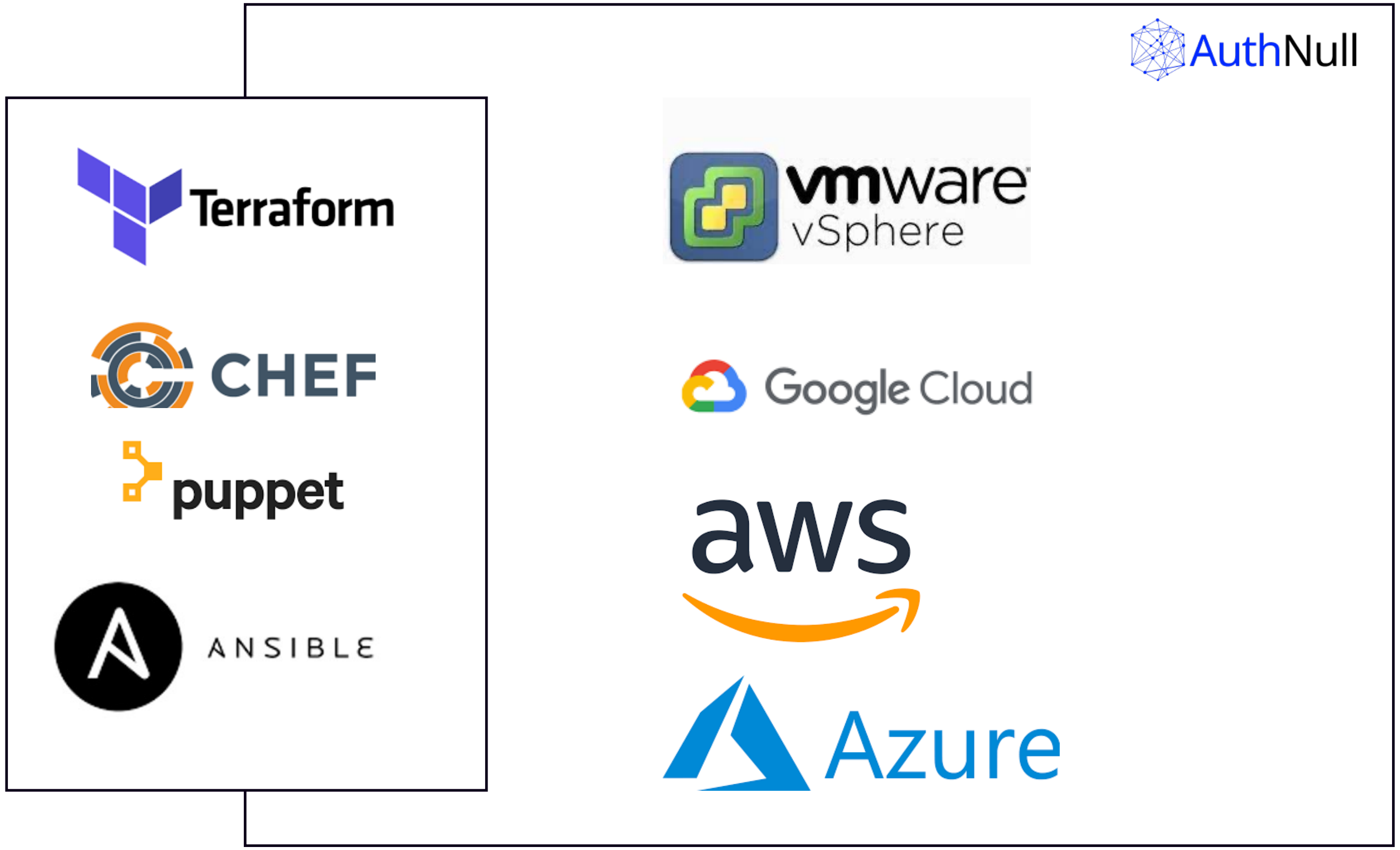
Active Directory Integration
Enabling Join / Manage and Leave cycle of employees

- Automated onboarding / offboarding based on employee Join-Manage-Leave Cycle with
  - Active Directory Sync Agent
  - CSV based onboarding / offboarding
  - OKTA Sync
  - Workday Sync

- All active directory users are automatically issued the relevant credentials

- Credentials can be rotated, issued or re-issued for new, lost device and more really easily and quickly.

Adoption through DevOps tools and APIs



- API first Design

- Extensive and easy integration with existing Devops tools such as Chef, Terraform, Puppet and Ansible

- Support for Major clouds, on prem data centres, private clouds and VMWare Vsphere

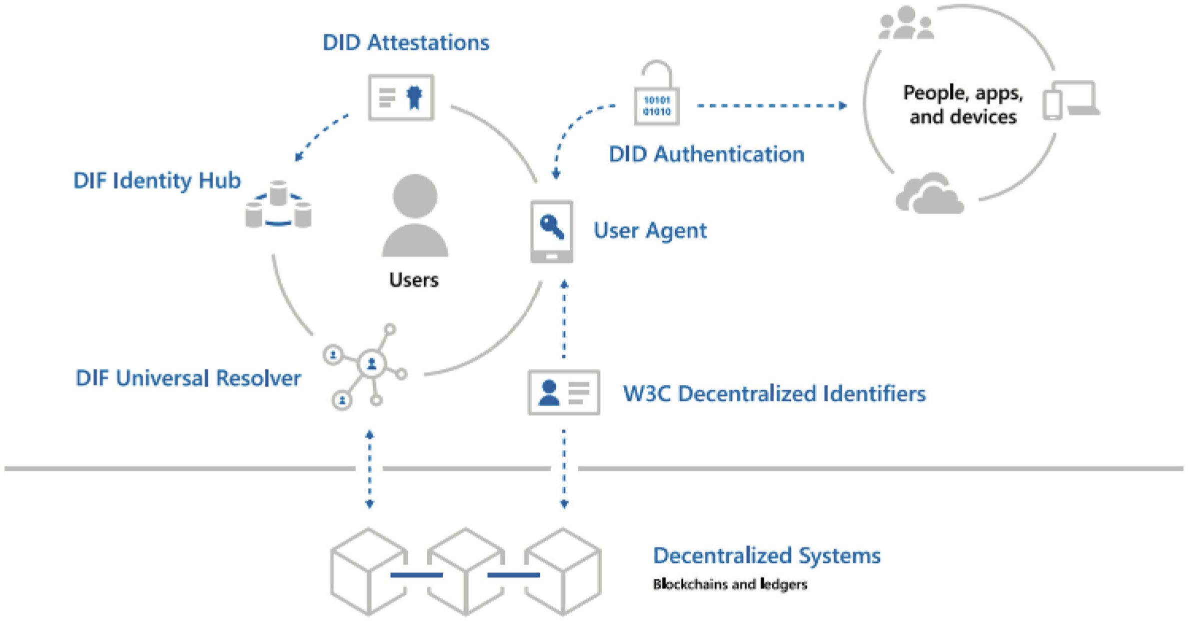
Better compliance through logging, built in runtime security

- AuthNull agents come with Run-time guardrails using SELinux and AppArmor restricting it to only perform certain functions
- AuthNull platform is shipped with runtime controls for its application software including policy templates for PCI-DSS, SOC2, MITRE, NIST, and CIS.
- AuthNull platform provides extensive logging:
    - All transactions via database & wallet
    - All transactions on ELK stack
    - All API calls on ELK stack
    - All Agent actions on Agent, and ELK Stack
    - All Authentication logs from OS shipped to ELK Stack.

Decentralized Identity – The core of our Identity Solution

- **AuthNull uses the W3C Decentralized Identity (W3C DID) standards and W3C Verified Credentials (W3C VC) to implement Decentralized Identity**

- Every organization / user is used a unique DID., identifiers that are generated using EDSA / ED25519 signature scheme.
- Additionally, organizations which manage decentralized credentials **issue Verified Credentials (VCS)** – objects with claims including attestation signed by the issuer.



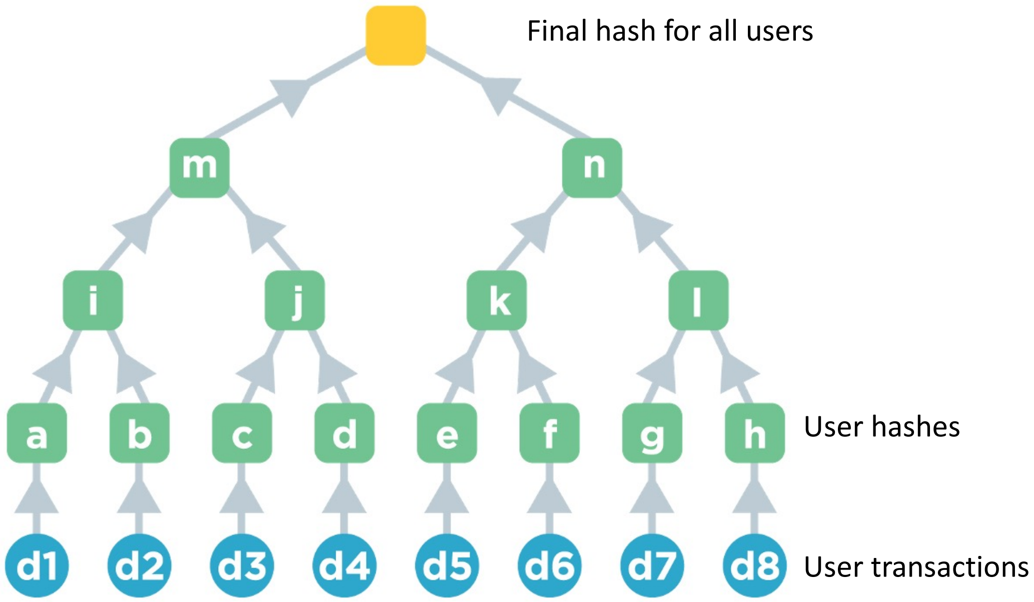
Open standards:

- W3C Decentralized Identifiers
- W3C Verifiable Credentials
- DIF Sidetree
- DIF Well Known DID Configuration
- DIF DID-SIOP
- DIF Presentation Exchange

AuthNull improves your security & compliance through

Tamper proof credentials, and blockchain powered immutability

- <u>On AuthNull - All credentials are tamper proof.</u>
- A blockchain is an immutable data store that enables us to store a non tamperable record of transaction history.
- To enable tamper proof transaction history and credentials, Authnull does the following:
  - All authentication and transactions issued by the platform are issued a cryptographic [Merkle hashes that form a part of a Merkle tree]()
  - Merkle root hashes are written to an Ethereum address (or any private blockchain).
  - Suspicious transactions or tampering can be identified with the merkle hashes + Ethereum data.
  - All data stored on Ethereum is encrypted using the Organization's private key
- Any suspicious transaction will mark the given users transaction history as "tampered" as a new hash that was generated does not tally with existing hash.



AuthNull Features

Active directory + LDAP Auth

- Support for AD as the primary Identity store + Active directory or other LDAP Authentication 2FA
- Support for Integration with LDAP for synchronization of users

OS support

- Support for a wide variety of *NIX OS
- Support for Windows coming soon
- Support for Raspberry PiOS as well as other IOT OS coming soon.

Protocol / OS support

- SSH, LDAP, VNC, RDP, Telnet, K8s
- Support for *NIX operating systems including PiOS
- Support for other IOT systems coming soon

Raspberry Pi OS

Red Hat Enterprise Linux

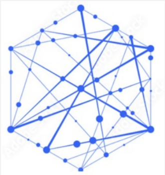
ubuntu

ORACLE LINUX

CentOS

aws BOTTLEROCKET LINUX DISTRIBUTION FROM AMAZON

Why AuthNull? – Only Passwordless multi-factor PAM focused at legacy infrastructure

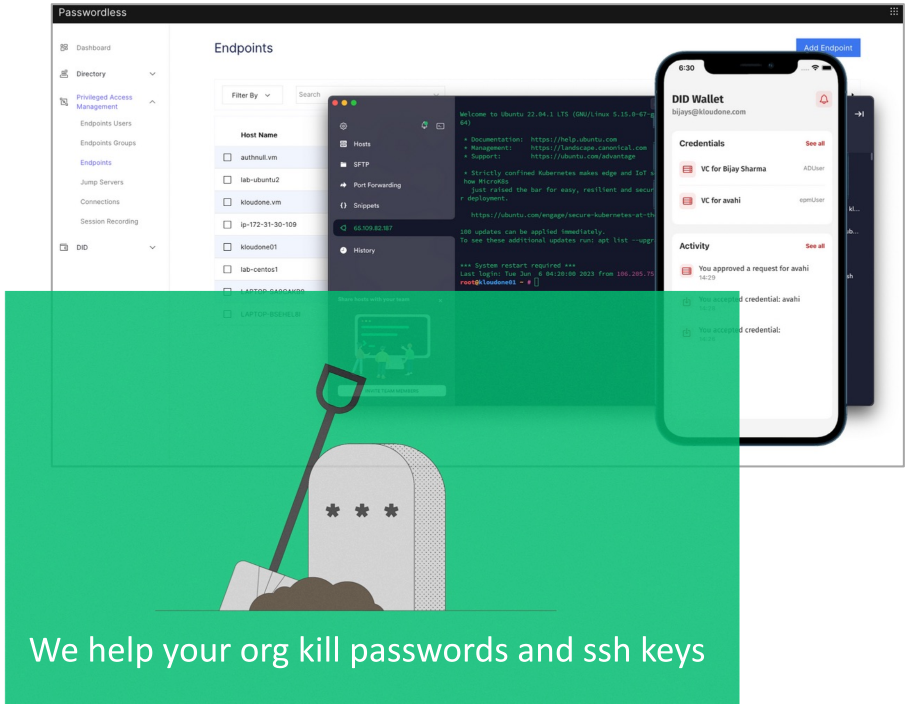


- Decentralized Identity for legacy use cases
- No single central attack vector
- Deployed on prem inside a walled garden

- Lower cost;
- Self managed infrastructure

- Highly secure with two factors of trust. 1FA or 2FA passwordless
- Improves security compliance through immutable audit logs and public keys
- Privacy preserving technology with Blockchain based hash storage.

AuthNull – Next Generation Infrastructure Access Solution



```
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 secu
 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 ~ #
```

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.

Appendix – 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.