



# **Infrastructure Protection**

Asif Ali, Founder & CEO | +1 (916) 693-5277 | [a@authnull.com](mailto:a@authnull.com) | [www.authnull.com](http://www.authnull.com)

The Problem:

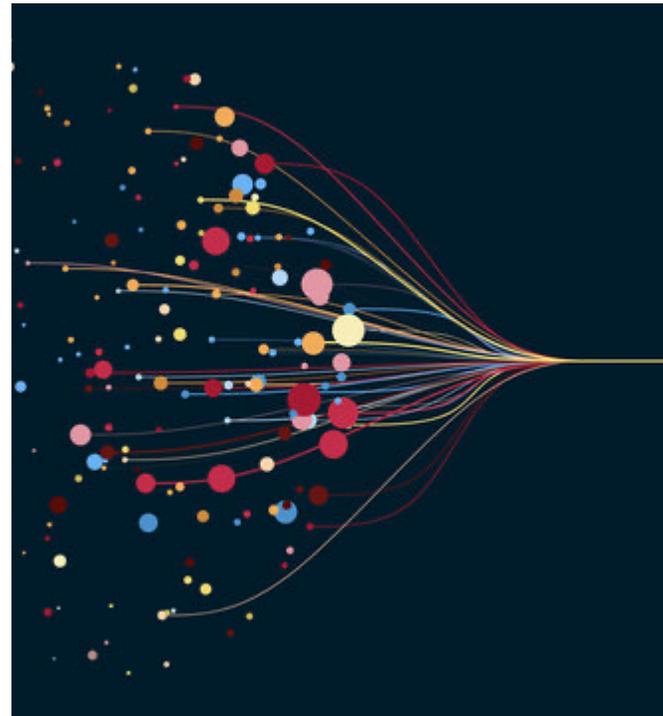
# Protecting Infrastructure is hard, expensive and time consuming

- + Diverse infrastructure within organizations – Workstations, servers, Networks, Databases makes it difficult to uniformly protect
- + Attacks are getting more sophisticated
- + Over-lapping Identity and access security tools is a concern



## What is AuthNull?

- + Unified solution for infrastructure protection
- + Works well with Active Directory, Azure AD, Windows, Linux, Radius and Databases
- + Out of the box MFA, Privileged Access and Conditional Access



# Full featured protection for various infrastructure



Active Directory



Azure AD



Windows



Linux



Wireless networks



Databases

# What does AuthNull do?

- + **Protect access to any resource**

AuthNull protects all resources inside your infrastructure

- + **Secure and verify every identity**

AuthNull verifies identity at every access using biometric MFA and conditional access

- + **Provide only necessary access**

Conditional access policy enables restricted, just in time access of only the resources necessary

- + **Simplify the security experience**



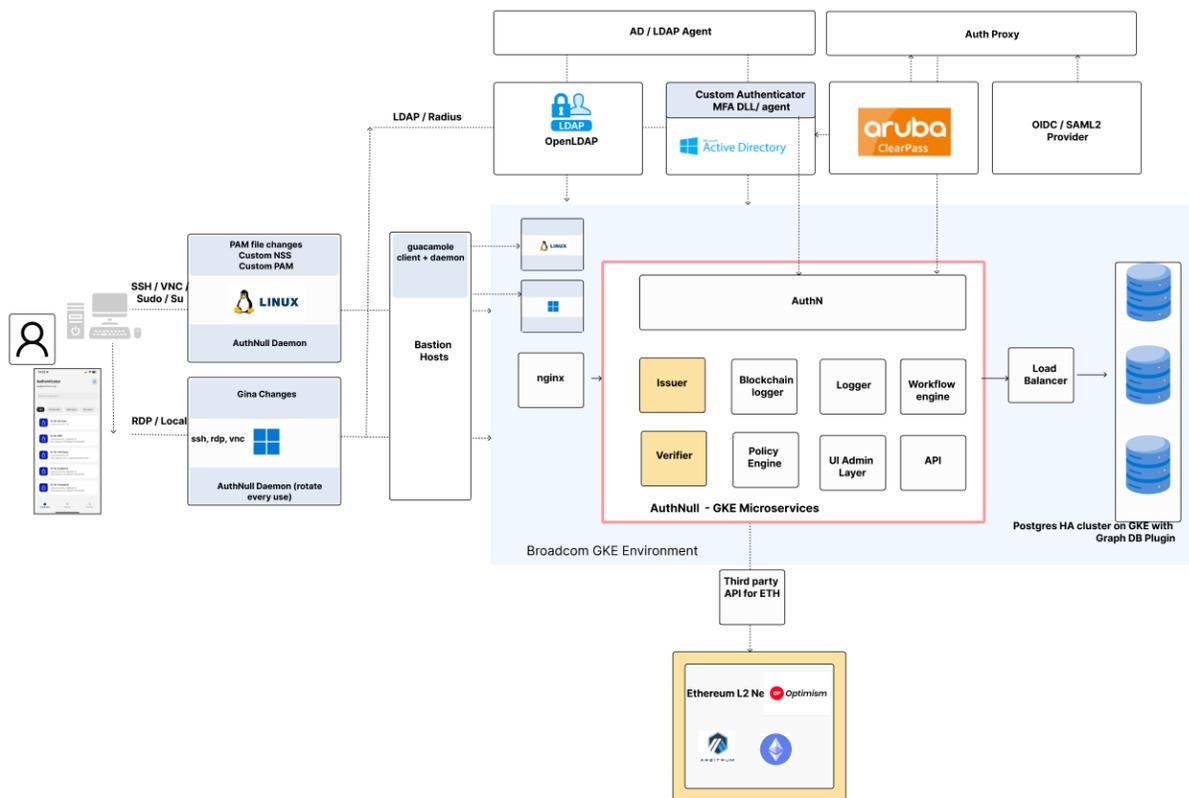
## **Business outcomes with AuthNull**

- + Cut deployment time from Months to days
- + Eliminate needless help desk tickets
- + Achieve faster compliance
- + Lower MFA + PAM cost to as much as 80%

# Identity Protection

- + Risk Score
- + Adaptive MFA
- + Privileged Access Logs
- + Biometric MFA

# Architecture



- High performant architecture with redundancies
- Uses decentralized identity to provide a more secure, robust infrastructure
- Database redundancy (3X) + Regional HA
- Service redundancy with HA, Failover and regional HA
- Data isolation physically for all customer data

# Active Directory, Azure AD and Windows



Active Directory



Azure AD



Windows



Linux

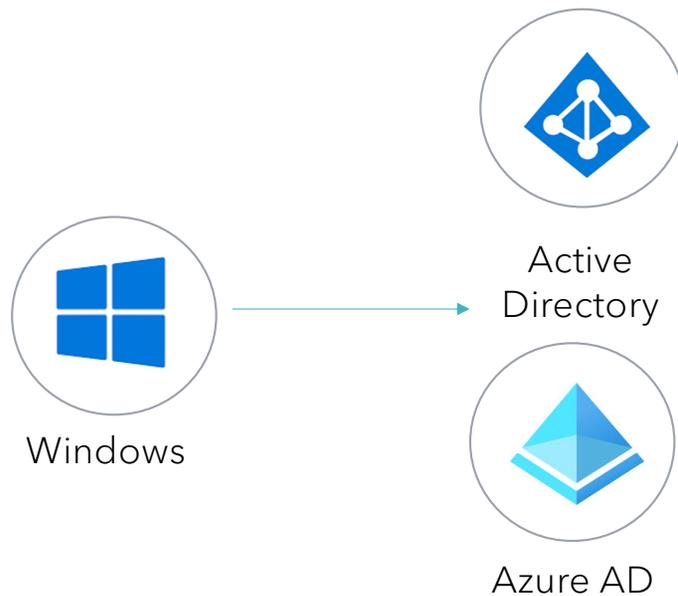


Wireless networks



Databases

# Active Directory, Azure AD and Windows



- + AuthNull plugs into your existing infrastructure
- + AuthNull automatically discovers security policies using artificial intelligence
- + AuthNull then enables
  - MFA
  - Conditional access
  - Recorded sessions
  - Passwordless access
  - Password rotation
  - Local account access
- Across all the infrastructure where AuthNull is plugged in.

# Linux, Wireless Networks and Databases



Active Directory



Azure AD



Windows



Linux



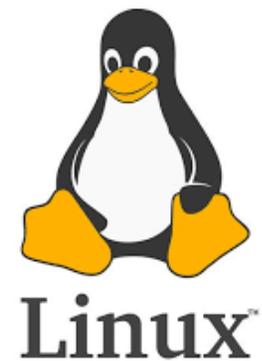
Wireless networks



Databases

# Linux

- Secure all Linux distributions
- Enable AD joined MFA or local user MFA
- Recorded sessions via jump server
- Breakglass features
- Works with SSH / VNC / Local log-on



# Network support

- AuthNull provides MFA and protection for all devices connecting via RADIUS / TACACES+ devices



## Microsoft NPS

Microsoft Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication.

Proceed to Setup



## Cisco ISE

Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources.

Proceed to Setup



## Clearpass

ClearPass provides role- and device-based network access control for employees, contractors, and guests across any multivendor wired, wireless, and VPN infrastructure.

Proceed to Setup

# Database Protection

- Provide MFA to access to database – MySQL, Postgres, Percona, Aurora, Amazon RDS and a variety of open source databases
- Control access to privileged users
- Password rotation
- Data masking of sensitive data
- Database access logs and reports

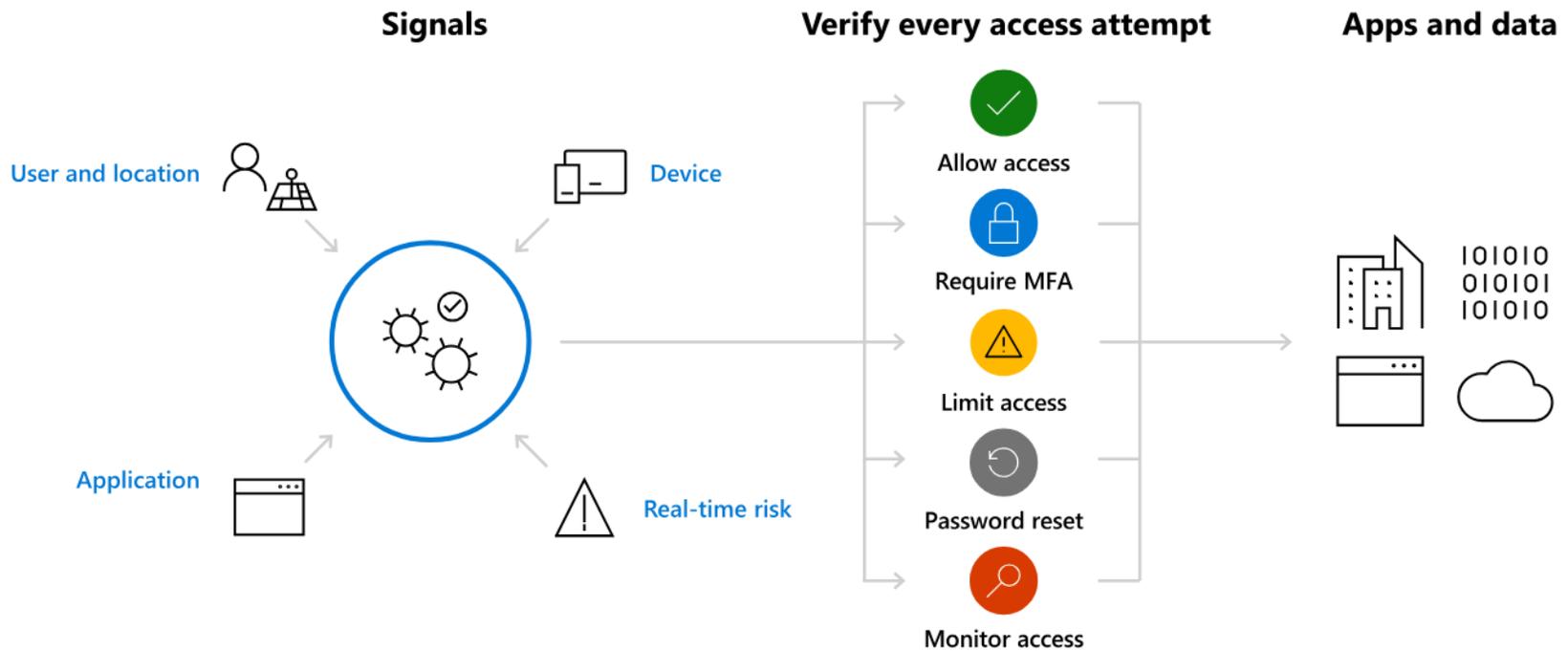


# Privileged Access Features - Matrix

	Discovery with local	AD . Entra ID discovery	Domain joined logon	Password rotation	MFA	Session recoding	Breakglass	Offline access
Windows	X	X	X	X (domain / local)	X	X (via jump server)	X	X
Linux / Firewalls / Switches	X	X	X	X (domain / local)	X	X (via jump server)	X	X
Radius	NA	X	X	X (domain)	X	X (via jump server)	X	X
Databases	X	X	NA	X (database local)	X	X (via jump server)	X	X

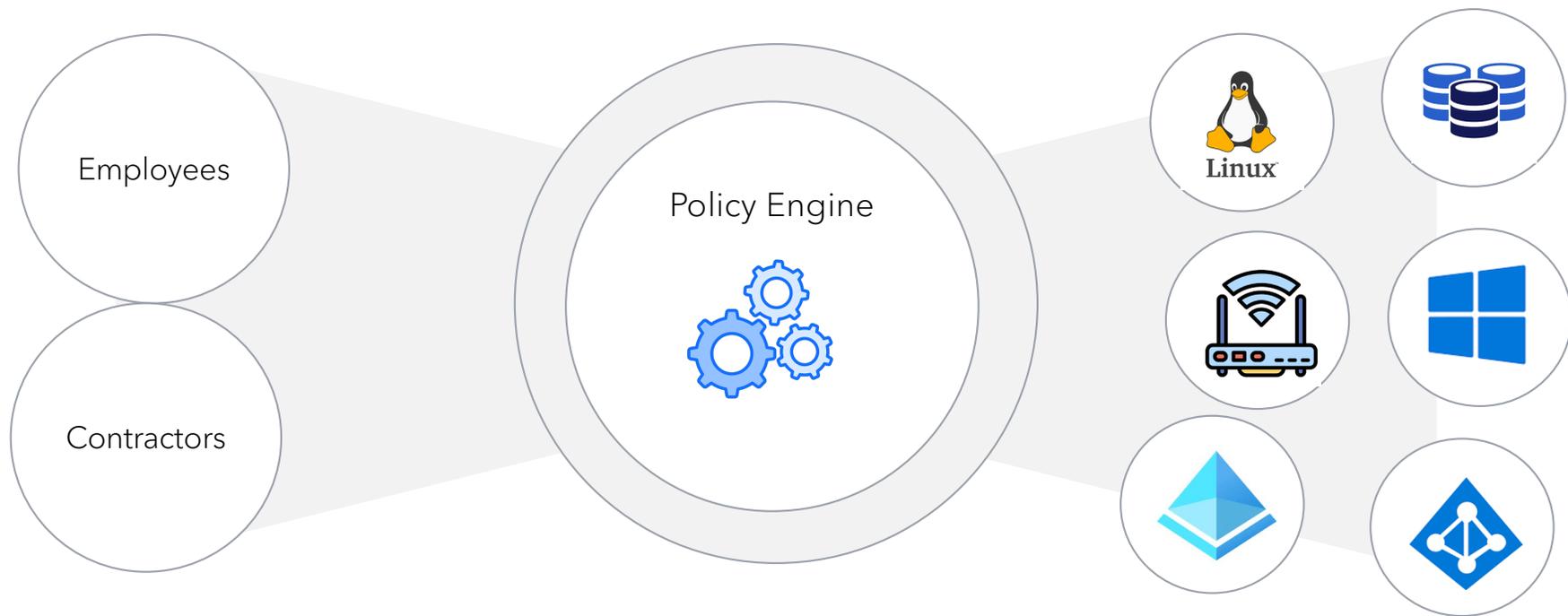
# Conditional Access

Enable zero trust with strong authentication and adaptive policies



# Policy based Access Control

AI agents based policy engine automatically discovers security policies based on user behavior



AI-Copilot to assist In security delivers automated policy discovery, and continuous policy improvements

The screenshot shows a chat window titled "Policy Co-Pilot". The AI assistant's messages are as follows:

- "Hi! I can help you analyze and recommend policies based available authentication patterns." (12:21 PM)
- "I'll analyze your authentication patterns and recommend policies..." (12:21 PM)
- "What type of policies would you like me to show?" (12:21 PM)

The user's response is "Show me recommended policies" (12:21 PM).

The AI assistant provides a "Policy Generation Statistics" table:

Metric	Value
Authlogs Processed	3
Policies Generated	0
Time span since last generation	561 minutes

Below the table, the AI assistant asks "What type of policies would you like me to show?". The user's response is a list of policy types: "Active Directory", "AD Groups", "Endpoints", "RADIUS", "Database", and "End Chat" (12:21 PM).

## How are we different?



No vaults to protect



Automated discovery of security policies



Biometric wallets + identity security



Decentralized = secure design

# Platform Security

## DEPLOYMENT MODELS

- On-prem
- Cloud with multi region redundancy
- Hybrid – fit to your model

## ARCHITECTURE

- Multi-tenant with physical database isolation
- Highly redundant & highly available

ITEM	NOTES
Security	ED25519 Signing scheme for PKI
Trust	Two (2) roots of trust
Authentication	Authentication Assurance levels 2 (AAL 2)
NIST	FIPS 140–2 compliant <a href="https://csrc.nist.gov/pubs/fips/140-2/upd2/final">https://csrc.nist.gov/pubs/fips/140-2/upd2/final</a>
Software design	Decentralized
Wallet	iOS / Android MacOS and Windows App coming soon.

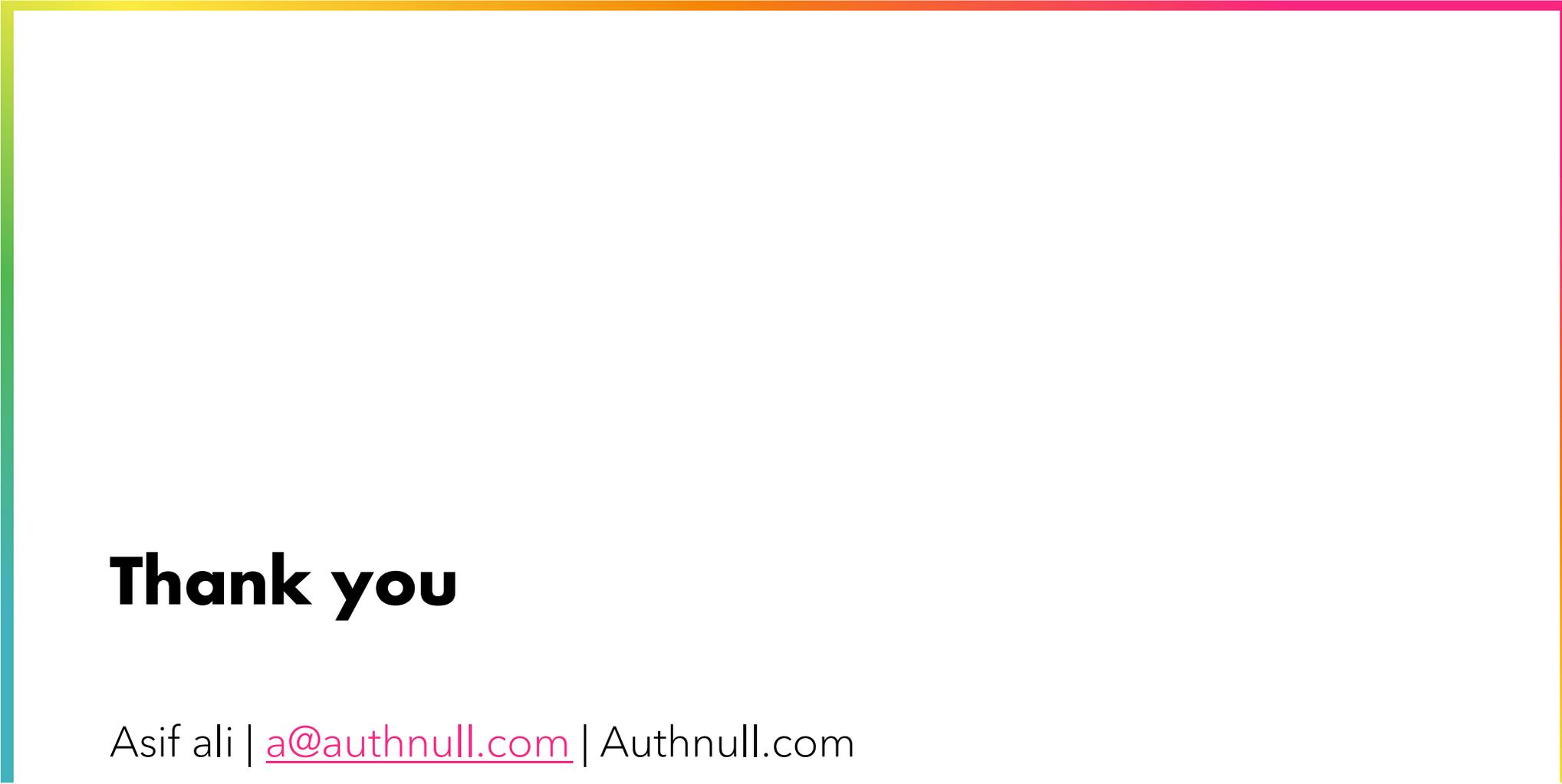


# Demo

GET IN TOUCH WITH US FOR A DEMO

The screenshot displays the 'Endpoints' page in the Passwordless application. The interface includes a sidebar with navigation options like 'Dashboard', 'PAM', 'Endpoints Users', 'Endpoints Groups', 'Endpoints', 'Jump Servers', 'Connections', 'Session Recording', 'Credential Rotation', 'Directory', and 'DID'. The main content area features a table of endpoints with columns for Host Name, OS, User Count, Private IP, Public IP, Group Count, State, Agent Status, and Action. A search bar and a filter dropdown are positioned above the table. An 'Add Endpoints' button is located in the top right corner.

Host Name	OS	User Count	Private IP	Public IP	Group Count	State	Agent Status	Action
windows-11	windows	14		172.190.89.98	25	Active	Offline	
ip-172-31-4-59	linux	36		3.12.123.249	63	Active	Offline	
windows-10	windows	7		172.206.240.126	18	Active	Offline	
ip-172-31-35-99.ec2.internal	linux	159		3.87.38.26	177	Active	Offline	
wint11	windows	7		172.174.164.165	18	Active	Offline	
kloudone01	linux	144		65.109.82.187	210	Active	Offline	
ip-172-31-32-177	linux	149		172.31.32.177	209	Active	Offline	
Ubuntu-2204-jammy-arm64-base	linux	157		195.201.165.12	210	Active	Offline	
windows-jumpser	windows	12		172.174.188.82	18	Active	Offline	



# Thank you

Asif ali | [a@authnull.com](mailto:a@authnull.com) | Authnull.com