

# Solution Brief Multi-Factor Authentication (MFA)

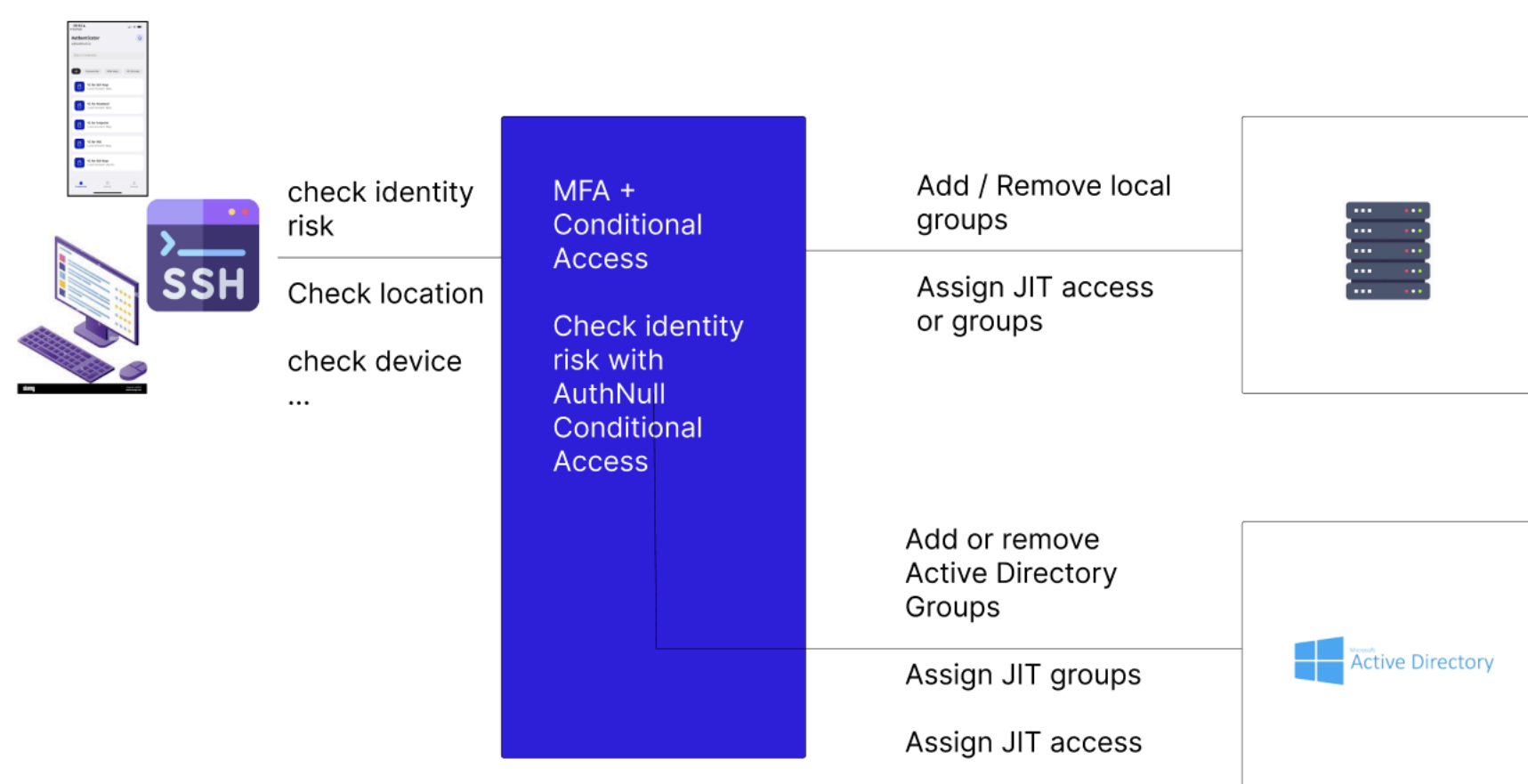
# Multi-Factor Authentication Solution Brief

Passwords alone are no longer enough — and even legacy MFA is easily bypassed via phishing, SIM swap, or token fatigue attacks. CISOs face pressure to implement phishing-resistant MFA for all users, especially those with elevated privileges, while minimizing friction and cost.

## Key challenges with traditional MFA tools

- Don't work well across hybrid infrastructure. With different directories or different kinds of infrastructure example Linux or Windows. Each requires a separate solution
- Fail to enforce step-up authentication at session start
- Can't differentiate between user risk levels or contexts
- Don't support machine identities, and step up to user identities

AuthNull Multi-Factor Authentication (MFA) is much better as it provides a system to detect user identity risk



# AuthNull MFA Features

AuthNull's MFA is purpose-built for privileged and high-risk access scenarios, offering strong phishing-resistant options, contextual enforcement, and passwordless-by-default flows.

- Phishing-Resistant MFA - FIDO2/WebAuthn, passkeys, biometrics, or secure push with cryptographic challenge
- Contextual Access Control - Enforce MFA only when risk, location, or behavior changes
- Passwordless-First - No passwords to steal or phish — use device-bound keys or identity wallets
- Support for Human + Machine Identities - Use verifiable credentials and device attestation for AI agents, CLI users, and service accounts
- Offline MFA + Break-glass support- Resilient MFA even during outages with fallback rules and time-boxed OTP
- Autonomous auto-pilots that enable automated policy discovery and automated policy improvements.

## How it works?

- User initiates access to infrastructure
- AuthNull evaluates context: IP, device trust, risk score, role
- Adaptive enforcement: MFA prompted based on policy
- Session started: All access recorded, credentials brokered securely
- Audit logs sent to SIEM/ITSM tools
- AI Agents discover and continue to improve policies.

## Need more info?

Get in touch with us - [sales@authnull.com](mailto:sales@authnull.com)

# Privileged Access Management must have features

## **Centralized privileged access control**

Enforce and manage privileged account access across humans and machines.

## **Credential vaulting and management**

Secure storage, rotation, and brokering of privileged credentials.

## **Temporary access brokering**

Grant privileged credentials on-demand (just-in-time) to authorized users.



## **Privileged Access Management nice to have features**

These features enhance functionality and support advanced use cases, shaping a mature PAM program:

Privileged session management (monitoring, recording, real-time access control)

Comprehensive auditing (who/when/where privileged access occurred)

Agent-based privilege elevation (e.g., Windows, Linux, macOS)

Just-in-time privilege elevation to minimize exposure

Privileged account discovery across hybrid environments

PAM is a cornerstone for zero-trust and defense-in-depth, beyond compliance alone

A phased rollout is recommended—start with must-haves, then expand to include secrets management, CIEM, automation, analytics, integration with SIEM/ITSM, and resilience features (HA, break-glass

## **Privileged Access Management is a cornerstone**

PAM is a cornerstone for zero-trust and defense-in-depth, beyond compliance alone

A phased rollout is recommended—start with must-haves, then expand to include secrets management, CIEM, automation, analytics, integration with SIEM/ITSM, and resilience features (HA, break-glass



A phased rollout is recommended—start with must-haves, then expand to include secrets management, CIEM, automation, analytics, integration with SIEM/ITSM, and resilience features (HA, break-glass

## **Privileged Access Management is a cornerstone**

PAM is a cornerstone for zero-trust and defense-in-depth, beyond compliance alone

A phased rollout is recommended—start with must-haves, then expand to include secrets management, CIEM, automation, analytics, integration with SIEM/ITSM, and resilience features (HA, break-glass

# AuthNull - Build for the next decade of PAM

## **Credential**

Auto-discovery & rotation of secrets across AD, Linux, databases

## **JIT Access**

Policy- and risk-based elevation with expiration timers

## **Password-less Authentication**

Wallet-based, decentralized credentials for both human and machine identities

## **Privileged Session Recording**

Bastion proxy + keystroke/session video capture

## **Policy Based Access Control + Governance**

AI-generated entitlement maps & dynamic approval workflows

## **Secrets Management without a vault**

Secretless injection for remote access

## **Integration**

SIEM, ITSM, SSO, SCIM, Entra ID, Active Directory, Radius infrastructure and OIDC support

## **Resilience**

HA architecture, offline break-glass, immutable logs

## **Database Protection**

AuthNull protects open source database