Marketing Resources

E-Book
Conditional Access

Delivering Dynamic Access for all of your infrastructure.

AuthNull

Introduction

In today's digital landscape, where cyber threats are evolving rapidly, traditional perimeter-based security models are no longer sufficient. Organizations need dynamic, identity-centric approaches to protect their resources. Conditional Access (CA) emerges as a critical tool in Identity and Access Management (IAM), allowing administrators to enforce policies that grant or deny access based on specific conditions like user location, device health, risk levels, and more.

This ebook explores Conditional Access in depth, focusing on two prominent solutions: AuthNull's Conditional Access and Microsoft Entra ID (formerly Azure AD) Conditional Access. We'll delve into their features, implementations, and a head-to-head comparison. By the end, you'll understand how these tools can enhance your organization's security posture.

Why Conditional Access? CA aligns with Zero Trust principles: verify explicitly, use least privilege access, and assume breach. It goes beyond simple username-password authentication by incorporating contextual signals to make real-time decisions. For instance, a user accessing sensitive data from an unfamiliar location might be required to complete multifactor authentication (MFA) or be blocked entirely.
The content draws from official documentation and industry insights to provide a balanced view.

As remote work and cloud adoption grow, CA helps mitigate risks like phishing, credential stuffing, and insider threats. AuthNull targets legacy and modern infrastructures, while Entra ID excels in cloud-native environments. This guide will help you decide which fits your needs.

What is conditional access

Conditional Access is a security mechanism that evaluates predefined conditions before granting or denying access to resources. It's essentially an "if-then" policy engine: If certain signals (e.g., user risk, device compliance) meet criteria, then apply controls (e.g., allow access, require MFA, or block).

In IAM, CA integrates with authentication flows to add layers of protection. Unlike static access controls, CA is dynamic and context-aware. For example, a policy might allow full access from a trusted corporate network but limit it from public Wi-Fi.

Key Components of CA:

- Signals: Data points like user identity, location, device state, application, and risk scores.
- Decisions: Outcomes such as grant, block, or require additional verification.
- Enforcement: Applying the decision to the access request.

Benefits include enhanced security, compliance with regulations like GDPR or HIPAA, and improved user experience by reducing unnecessary friction for low-risk scenarios.

Examples from Industry:

- Requiring MFA for administrative roles.
- Blocking access from high-risk countries.
- Enforcing device compliance for sensitive apps.

According to general IAM guides, CA reduces unauthorized access by up to 99% when combined with MFA

CA is not a standalone defense but complements tools like firewalls and endpoint protection. It's particularly vital in hybrid environments where on-premises and cloud resources coexist.

AuthNull’s Conditional Access implementation

AuthNull's Conditional Access provides granular control for diverse IT environments, emphasizing legacy systems like on-premises Active Directory (AD), Linux hosts, Radius devices, Windows local users, and open-source databases. It supports conditions based on location, network, device, user behavior, identity risk, session risk, time-bound access, and just-in-time (JIT) access.

Key Features

Support for Linux. AuthNull supports first class support for conditional access for Linux machines and servers.

On-Prem AD Support. Native integration for domain-joined Windows/Linux machines, controlling access for users, groups, and machines.

Uses User Behavioral Analytics (UBA), user risk, and session risk; dynamically manages sudoers and entitlements.

Radius Devices: Supports Microsoft NPS, FreeRADIUS, Cisco ISE, Clearpass; conditions for specific devices. Windows Local Users: Manages privileged local accounts and group memberships.

.

Active Directory

Azure AD

Windows

Linux

Wireless networks

Databases

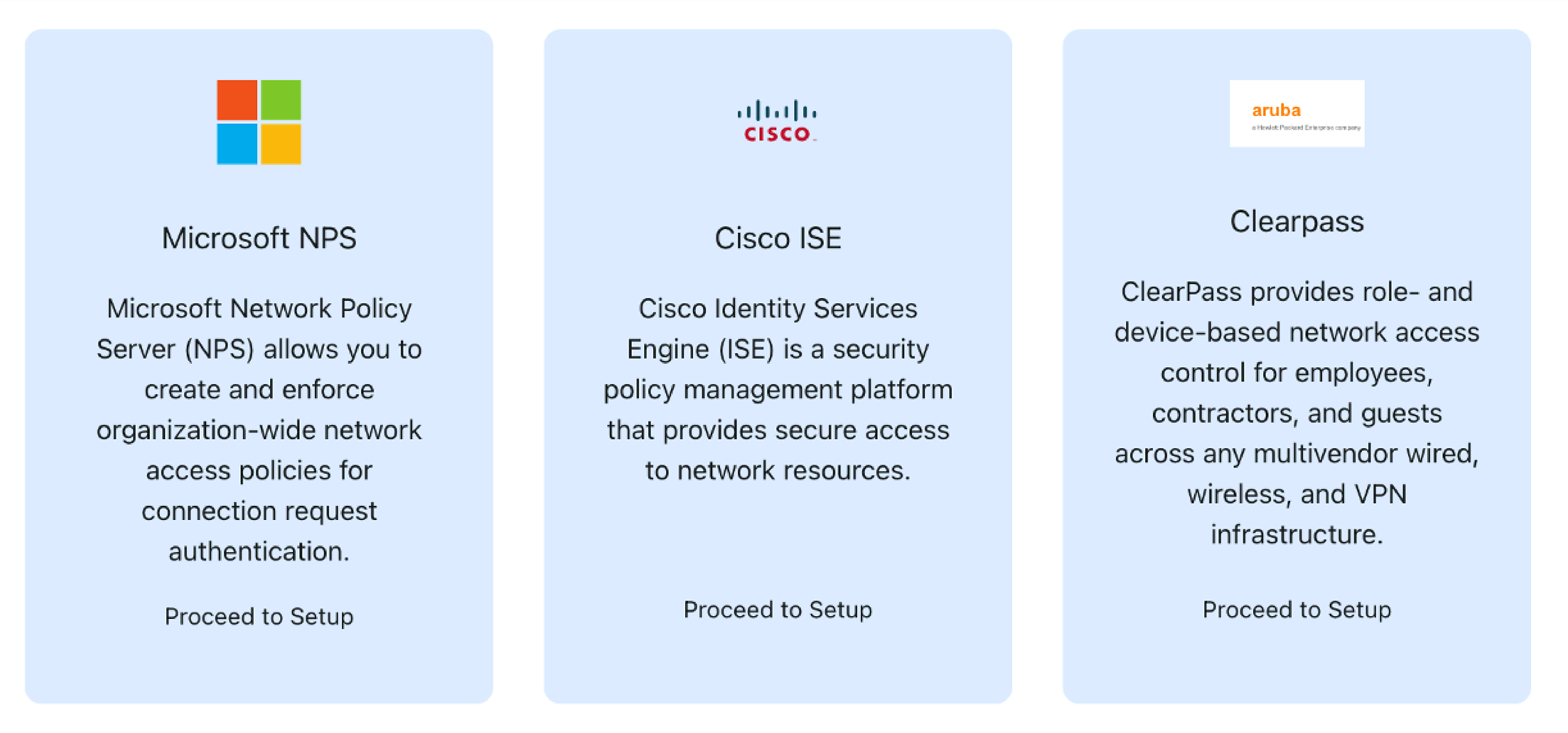
PostgreSQL MariaDB MySQL PERCONA XtraDB Cluster

Open-Source Databases: Full CA for PostgreSQL, MySQL, MariaDB; AI-generated policies for MySQL. Conditions: Continuous tracking of location, network, device; adjustable baselines for UBA and risk scores.

Time-Bound and JIT Access: Policies for specific times or on-demand access, enabling Zero Standing Privileges.

Powered by AI for automated policy improvements: An AI autonomous agent works behind the scenes to measure user risk, session risk, measures trusted devices, locations and networks

Support for RADIUS devices: AuthNull provides full conditional access support for RADIUS devices through Microsoft NPS, Cisco ISE, and Clearpass



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

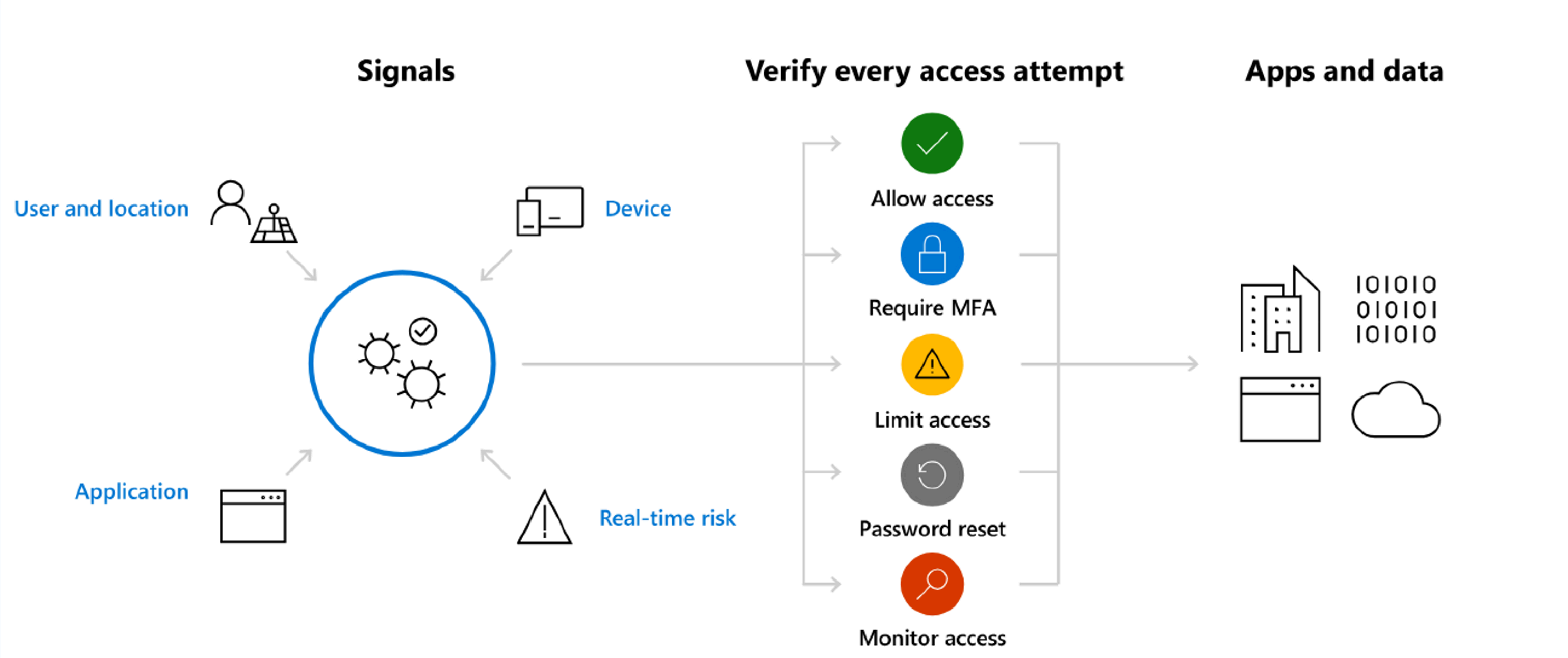
Cisco Identity Services Engine (ISE) is a security policy management platform that provides secure access to network resources.

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

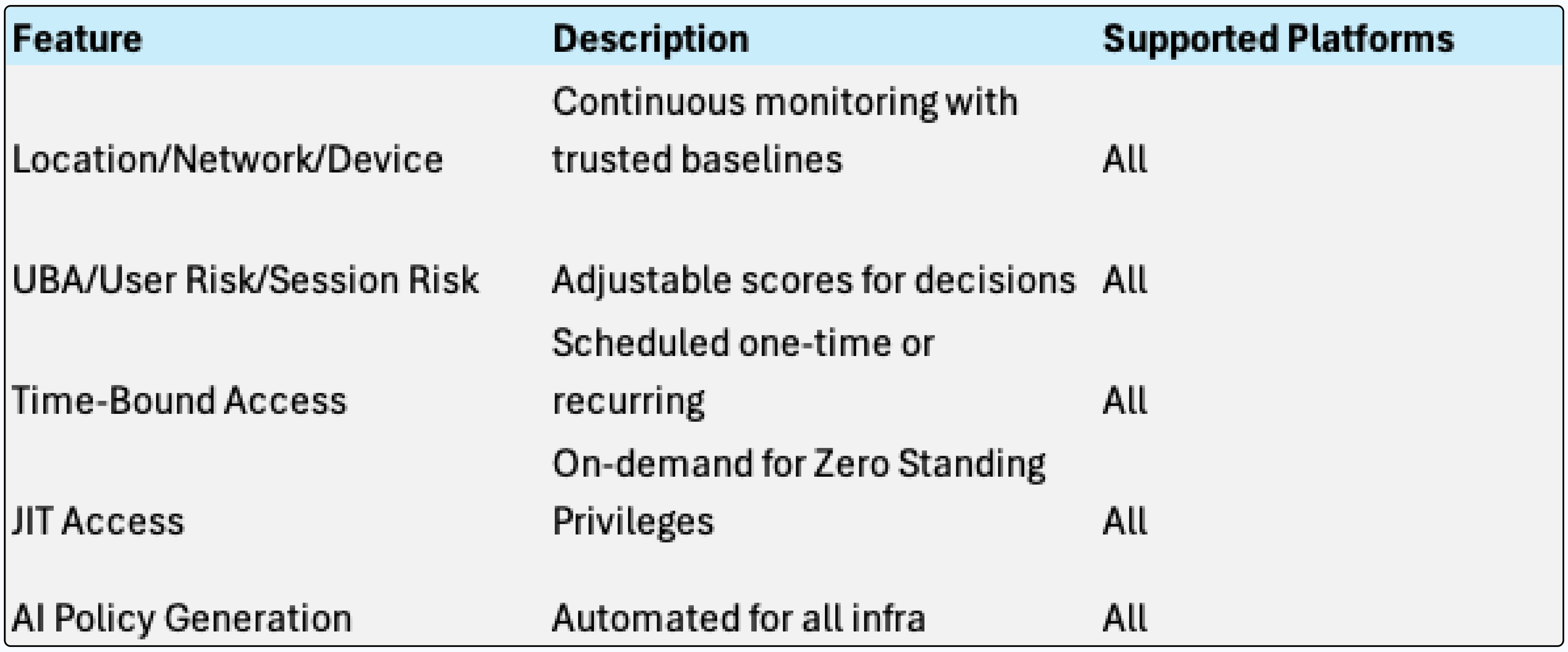


How it works

How It Works: AuthNull tracks attributes in real-time, evaluates against policies, and adjusts access (e.g., add/remove from groups). For databases, it enforces JIT and masking.

Implementation: Deploy via agentless for AD or agents for deeper integration. Customize UBA baselines and integrate with Radius or databases. AI automates policy creation for efficiency.

Use Cases: Securing Linux servers with behavior-based access or time-bound DB queries for audits.

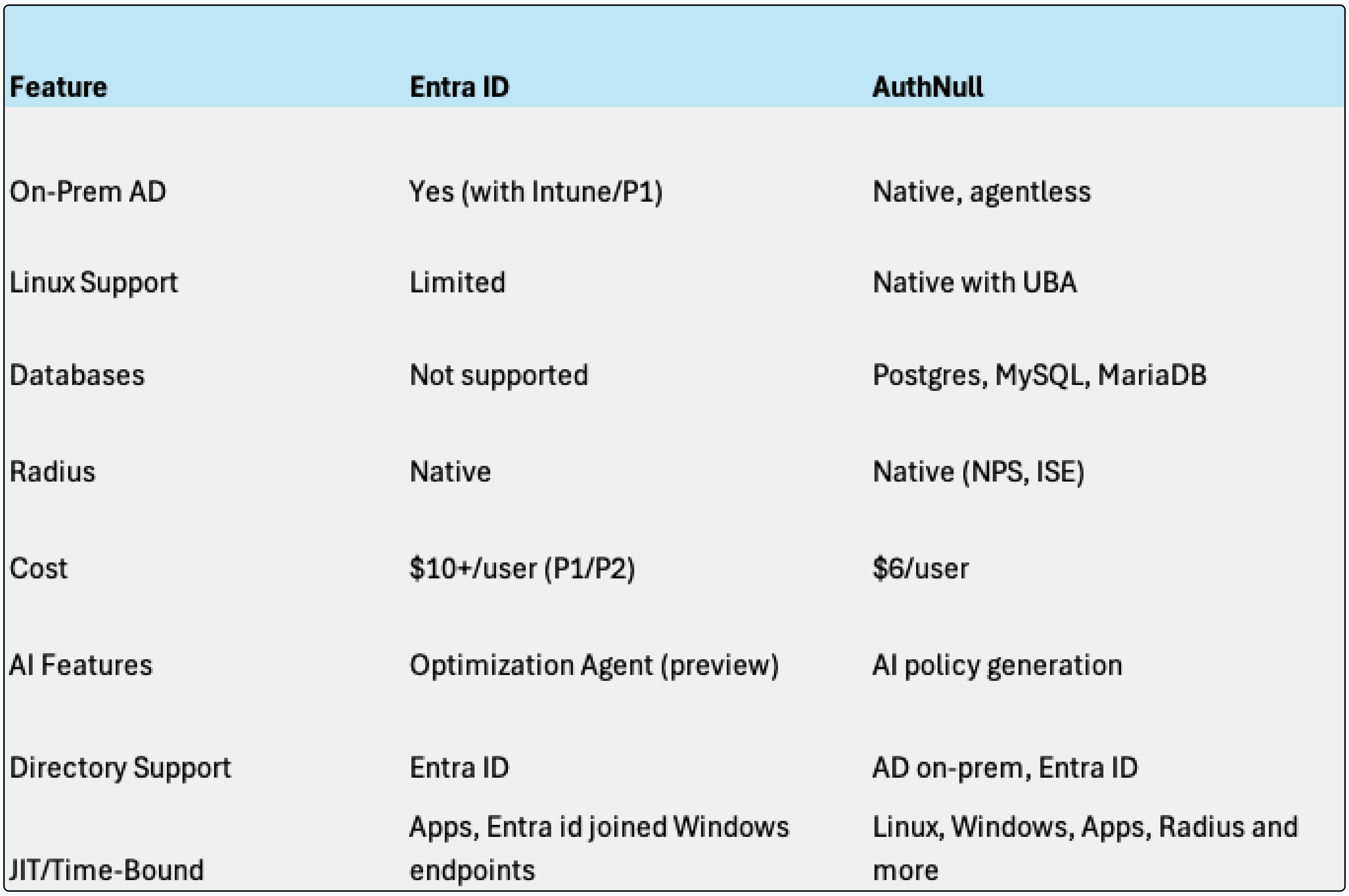


Feature	Description	Supported Platforms
Location/Network/Device	Continuous monitoring with trusted baselines	All
UBA/User Risk/Session Risk	Adjustable scores for decisions	All
Time-Bound Access	Scheduled one-time or recurring	All
JIT Access	On-demand for Zero Standing Privileges	All
AI Policy Generation	Automated for all infra	All

AuthNull

Comparisons with Entra id

AuthNull and Entra ID both offer robust CA but differ in scope. Entra ID focuses on cloud/Entra-connected apps, while AuthNull handles legacy/ modern infra natively.



Feature	Entra ID	AuthNull
On-Prem AD	Yes (with Intune/P1)	Native, agentless
Linux Support	Limited	Native with UBA
Databases	Not supported	Postgres, MySQL, MariaDB
Radius	Native	Native (NPS, ISE)
Cost	$10+/user (P1/P2)	$6/user
AI Features	Optimization Agent (preview)	AI policy generation
Directory Support	Entra ID	AD on-prem, Entra ID
JIT/Time-Bound	Apps, Entra id joined Windows endpoints	Linux, Windows, Apps, Radius and more

AuthNull excels in legacy support and cost, while Entra ID integrates seamlessly with Microsoft ecosystem.
Pros of AuthNull: Broader infra coverage, lower cost. Cons: Less cloud-native focus.

Pros of Entra ID: Deep Microsoft integration, risk-based (P2). Cons: Licensing costs, limited legacy.
Choose AuthNull for hybrid/legacy, Entra for Microsoft-centric.

.

Best Practices and Conclusion

Best Practices:

- Start with templates and monitor impacts.
- Align with Zero Trust: Multi-signal policies.
- Regularly review risks and adjust baselines.
- Combine with MFA and auditing.
- For AuthNull: Leverage AI for policies.
- For Entra: Use P2 for risk detection.

Conclusion:

Conditional Access is essential for modern security. AuthNull offers versatile, cost-effective solutions for diverse infra, while Entra ID provides integrated, cloud-focused protection. Evaluate based on your environment—hybrid for AuthNull, Microsoft-heavy for Entra. Implement CA to fortify your defenses today.

Get in touch

Get in touch with us at https://authnull.com/contact or sales@authnull.com

AuthNull

AuthNull

AuthNull