ManageEngine
Identity Access

DATASHEET

Smarter security at every sign-in

What organizations are up against

- Phishing and credential theft
- Exposed RDP, SSH, and VPN logins
- High-risk actions with no extra checks
- Zero sign-in visibility
- Password fatigue across dozens of apps

What a modern access layer must do

- Leave no login unprotected
- Make context-aware access decisions
- Resist phishing by design
- Authenticate reliably, with or without connectivity
- Define and enforce access policies consistently
- Prove who accessed what

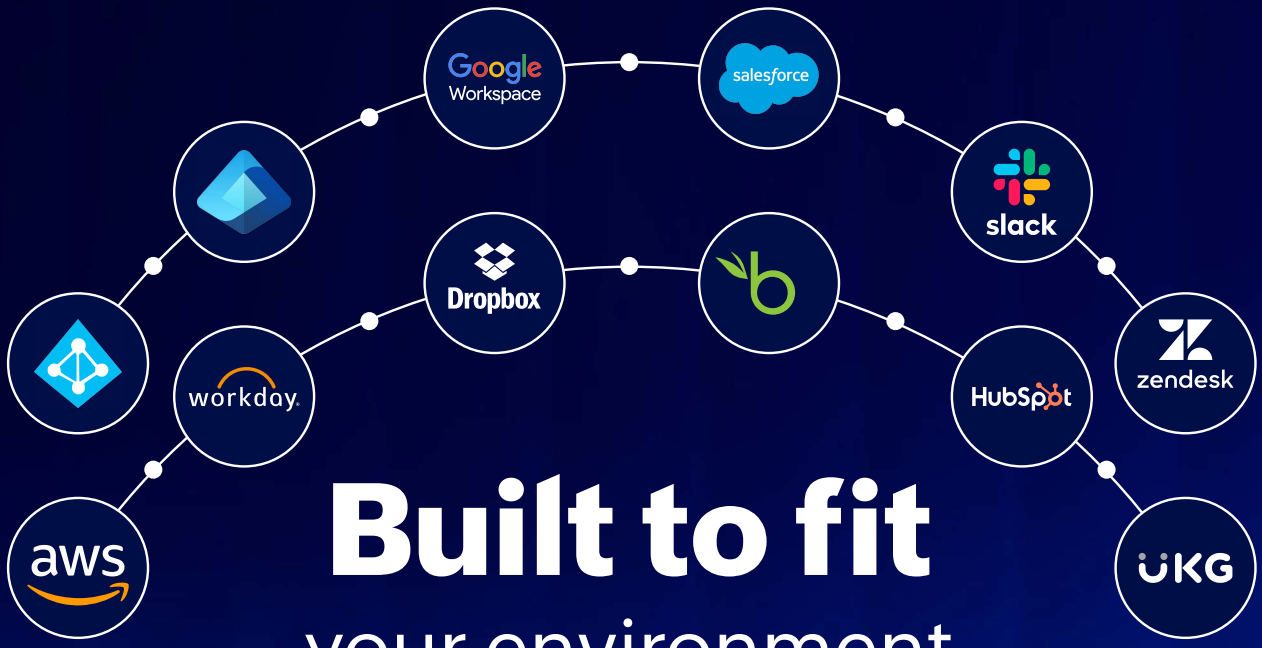
INTRODUCING IDENTITY ACCESS

ManageEngine Identity Access is a cloud-native workforce access management platform that replaces fragmented authentication tools with a single, consistently enforced policy layer. Each attempt is evaluated in context, allowing trusted users to proceed without interruption while high-risk sign-ins encounter additional verification. Your workforce moves through fewer checkpoints while every application, endpoint, and high-risk action stays protected.

Identity Access at a glance

DATASHEET

THE CHALLENGE	HOW IDENTITY ACCESS SOLVES IT	VALUE DELIVERED
Password fatigue	**Single sign-on** gives users one-click access to over 500 preintegrated applications with support for SAML, OAuth, and OIDC	One login for everything, with fewer passwords to forget, reset, or keep track of
Context-blind access decisions	**Adaptive MFA** evaluates every authentication attempt against IP address, geolocation, business hours, and device OS	Sensitive resources stay open to trusted users and closed to risky sign-ins
Unsecured device access	**Device authentication** enrolls devices directly into Identity Access and secures Windows, macOS, and Linux logins with MFA	Strong device security without added infrastructure or complexity
Network access points exposure	**MFA for endpoints** adds stronger verification to RDP, VPN, Wi-Fi, and other RADIUS-supported endpoints	Only verified users are granted critical network access
Blanket MFA enforcement	**Step-up authentication** adds stronger verification when users access critical applications	Right-sized security, with stronger checks reserved for critical apps
Unchecked privilege elevation	**MFA for privilege sessions** safeguards UAC, SSH, CLI, and sudo session access	Privilege escalation and lateral movement both blocked at the point of access
Phishing-prone passwords	**Passwordless authentication** enables sign-in with phishing-resistant FIDO2 passkeys and smart cards (PIV/CAC) across product, device, cloud app, and VPN logins	Phishing campaigns fail even when users are tricked
Network-bound authentication	**Offline MFA** secures disconnected devices through the IDSecurity Agent, with Emergency Access Codes as backup	Continuous protection with no silent bypass and no lockouts



Built to fit your environment

1
Console for application and device access

11
Strong, context-aware authenticators

500+
Enterprise applications protected

Pricing and licensing

$5

per user / per year*

*Pricing based on a contract for 1,500 users

We'll shape a plan around your team.
Receive a custom quote.

Specifications

Supported device platforms: Windows Server 2016 and above, Windows 8.1 and above, macOS 14 (Sonoma) and above, and Ubuntu 22 and above

Supported browsers: Internet Explorer 11, Mozilla Firefox, Google Chrome, Microsoft Edge, and Safari

www.manageengine.com/identity-360/access-management/

identityaccess-support@manageengine.com | +1-844-293-1074

$ Get Quote

Sign up