

# PingOne for Workforce



## DATASHEET

Ping's cloud identity solution for the workforce provides central authentication and authorization services to connect employees across any application, any directory and any device. PingOne for Workforce eliminates the authentication silos that plague workforce productivity and security. The result is a centrally managed [authentication hub](#) and access controls to enable seamless, consistent experiences for your workforce and pave the way for Zero Trust.

### Increase Employee Productivity

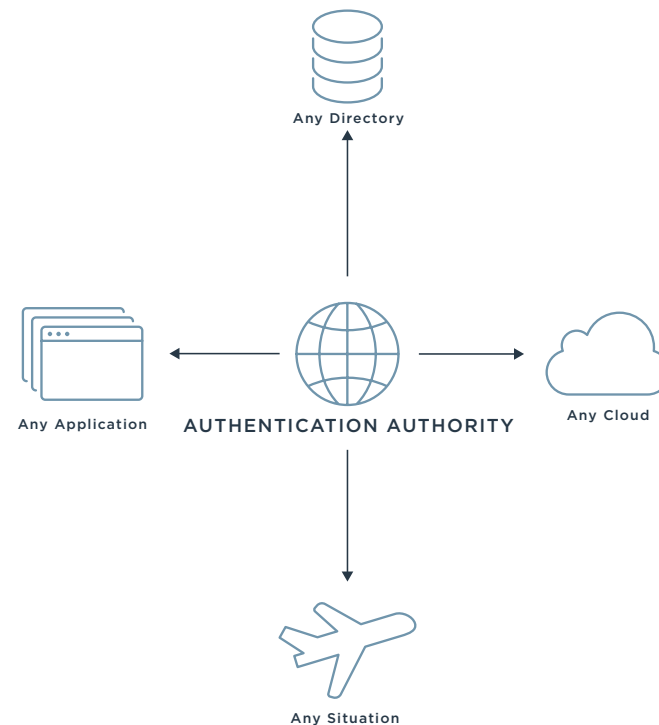
Provide your workforce with [single sign-on \(SSO\)](#) access to all their applications via an employee dock. Deliver frictionless, passwordless and consistent authentication experiences across all app environments.

### Reduce Security Risks

Limit account compromise and stolen credentials with [multi-factor authentication \(MFA\)](#) that can be deployed everywhere. Add adaptive and contextual policies to assess risk in the background to reduce login friction.

### Keep Pace with the Business

Rapidly onboard apps and quickly respond to business needs with centralized management, self-service and delegated administration capabilities. Manage resources in any environment and meet your scaling requirements.



### Key Features

- Workforce authentication authority: centralized authentication services that allow you to connect a user in any directory, accessing any app, hosted in any cloud, in any situation
- SSO and MFA for employees, partners and more
- Centralized management portal with self-service APIs, templates and delegated administration capabilities
- Single source of truth enabled by cloud directory, enterprise integrations and bi-directional data synchronization

# Capabilities & Benefits

## Single Sign-on for All Apps

- Federated authentication authority and single sign-on
- [Integrations](#) with custom, on-premises, SaaS or cloud applications such as Zoom, Slack, ZScaler, SAP, Microsoft Active Directory and more
- Native [support for identity standards](#) including OAuth, OpenID Connect, SAML, SCIM, LDAP, RADIUS, HTTP, WS-Trust, WS-Federation, FIDO and JSON Web Tokens (JWT)
- Connections to all on-premises and cloud-based directories
- Out-of-the-box integrations with legacy systems and extensive server integration kits

## Adaptive Multi-factor Authentication

- MFA that integrates everywhere (MDMs, VPN/RADIUS, AD/FS and apps of all types)
- Adaptive authentication policies (location, IP address, geofencing)
- Intelligent geo-velocity detection (impossible travel times) and IP reputation scoring for malicious activity
- Role-based entitlements and web-based access abilities
- Group and application-level access policies

## Single Source of Truth Directory & Data Source

- Flexible, lightweight directory with SCIM and REST APIs
- Simplified and automated onboarding and offboarding of users
- Popular directory integrations (AD, LDAP and more)
- Extreme scalability—unlimited custom user attributes and fields—with low latency
- Profile synchronization with custom attribute mapping

## Centralized Access Security

- Secure access to applications and APIs down to URL level
- Contextual policies for intelligent authorization decisions
- Session management to reduce man-in-the-middle attacks
- Ability to easily co-exist and eventually migrate off of legacy WAM
- Integration of any application, regardless of architecture or deployment

## Employee Dock

- Customizable one-click access application portal
- User self-service password resets and device management
- Brandable user experience (mobile app, notifications, registration screens, etc.)
- Identifier-first adapter for [passwordless authentication](#)

## Unified Administration

- Authentication via administrator API
- Centralized authentication and SSO operating portal and delegated app administration
- Templates for business users to onboard their own applications to SSO/authentication
- Visibility into lifecycle and promotion of all clients/connections across environments
- Management console that includes dashboards, performance, reporting and audit trails

## Integrations

Unlimited application integrations (legacy, SaaS, mobile, single-page apps, APIs):

- SaaS application catalog
- SAML/OIDC connections
- Legacy standards support
- Agentless kits
- Server kits
- Language kits

Extend strong authentication across your security infrastructure with the following integrations:

- MFA
- VPNs
- MDMs
- Adaptive and contextual policies, including third-party risk scoring
- Unlimited identity provider and datastore integrations (legacy and cloud)

Ecosystem integrations:

- Identity (IGA, PAM)
- [Zero Trust](#) (endpoint, network, services and data security vendors)