The Workforce Identity Buyer's Guide

What to Prioritize in a Workforce Identity and Access Management Solution to Make the Best Decision for Your Needs

BUYER'S GUIDE

INTRODUCTION

Digital transformation is accelerating in every industry as organizations of all sizes fight for market share. Yet many digital transformation initiatives fail to deliver the intended results. Why? Because most existing identity and access management (IAM) systems aren't able to support the requirements of a digital-first enterprise.

Take moving to the cloud, for example. Not every on-premises application has a suitable SaaS alternative or is able to be migrated. Most enterprises find they need to maintain a hybrid IT environment of both cloud and on-premises applications. But their legacy IAM systems can't support this hybrid architecture without significant costs, delays and risks.

Legacy IAM also exposes challenges when it comes to granting workforce access to resources. Over time, you've likely amassed identity silos that are disparate and disconnected. Lacking a modern identity foundation, you'll be hard-pressed to provide the seamless access an increasingly remote workforce needs, while also maintaining the security of resources and data.

> "The vision for AM has always been remote-work-centric, or at least remote-work-agnostic, to ensure that 'any user, can work anywhere, on any application, from any device.' However, the global health crisis and the subsequent shutdowns across the world has brought this approach to reality far more quickly, and more definitively than any conventional technology or business driver could have."
>
> Gartner 2020 Magic Quadrant for Access Management

To enable digital transformation, you need greater flexibility than legacy solutions can provide. You need to keep your dynamic, mobile workforce productive by providing access to the resources they need from anywhere on any device. You need to ensure security against growing threats and increase agility to be responsive to shifting priorities and requirements.

In short, you need a workforce authentication authority. An authentication authority gives you the power to strike the just-right balance of secure and convenient access for your workforce users. And you'll find it in an intelligent workforce identity solution.

The success of digital transformation isn't a foregone conclusion. You need an intelligent identity foundation upon which to build digital transformation success. Read on to learn:

- The must-have capabilities needed to build your workforce identity foundation
- How to quantify the business value of a workforce identity investment
- The step-by-step process to make the best decision for your needs

THE BENEFITS OF WORKFORCE IDENTITY TRANSFORMATION

When you continue to rely on legacy and siloed identity, you set yourself up for a host of problems like complex layers of multi-generational IT, fragile systems resulting from patchwork maintenance, lack of self-service capabilities for developers—which causes delays in application onboarding—and the emergence of shadow IT solutions as business units grow frustrated by IT rigidity.

In contrast, a future-proof identity foundation provides a host of benefits needed for digital transformation success. When you free yourself from relying on legacy systems and implement modern IAM capabilities instead, you gain critical capabilities that:

- Save time, money and resources
- Boost productivity across the enterprise
- Strengthen security

Centralized Administration

A workforce identity solution with centralized administration gives you a consolidated view of your identity infrastructure. You're able to significantly streamline administration by managing your entire enterprise through a single administrative portal.

Strong Authentication

You need to deliver a seamless and secure user experience, while defending against evolving security threats and vulnerabilities. An identity solution that supports strong authentication enables this. When you're able to rely on authentication policies that utilize a number of factors—including user behavior, AI/ML, risk scoring, biometrics and more—you can match authentication requirements to the risk of the action being performed, without adding unnecessary friction.

Developer-friendly Capabilities

Application developers need to rapidly deliver new projects, but security can't be sacrificed in the process. You can support their need for speed AND ensure identity is securely embedded in their applications when your workforce identity solution provides self-service capabilities and APIs, and supports open standards.

Integrations Support

A modern identity solution must support work across all application types and directories, including Microsoft Active Directory (AD). It should also provide synchronization capabilities that allow you to make use of existing investments.

Flexible Cloud Deployment

Whether you're deploying to the cloud or the data center, you need options and independence to meet your organization's goals. A modern identity solution allows identity to be consumed or deployed anywhere.

Better Experience

A modern identity solution should dramatically improve your users' experience. When you reduce friction and login prompts through intelligent, advanced authentication, you deliver the kind of experiences that keep your employees happy and secure.

QUANTIFYING THE BUSINESS VALUE OF WORKFORCE IDENTITY

When determining your identity needs, you can start by evaluating your total cost of ownership (TCO) savings. But don't stop there. You'll also want to examine the broader impact on the business. Workforce identity drives quantifiable improvements in productivity, security and agility. The following questions will help you calculate just how much value you can create.

Productivity

- How much time do employees waste switching between applications?
- How much time could they save if they could single sign-on (SSO) to all of their applications?
- How many hours are spent each week or month resetting passwords?
- How much time is spent resolving helpdesk tickets and fielding support calls?
- What are some of the other hidden costs of not having an end-to-end identity solution in place?

Security

- How many passwords does the average employee have to manage?
- How are passwords and multiple authentication silos affecting your risk of a security breach?
- How many critical assets are protected by multi-factor authentication (MFA) currently?
- How much exposure do your critical assets have to unauthorized users within your own company?
- How are workforce users being offboarded when they leave the company?

Agility

- How much time is wasted on maintaining your existing identity solution?
- How does the lack of identity features slow down the business and application onboarding? If so, how many hours are spent working through these problems?
- What IT operations can be streamlined with a new identity platform?

You can also use this business value calculator to build a solid business case for the value of a workforce identity investment. You'll see the exact value you can create by making employees more productive, keeping your company's critical assets more secure and making your business more agile. Calculate now.

DEFINING YOUR BUSINESS OBJECTIVES

Investing in identity is often a strategic project that requires buy-in from multiple stakeholders and business units. When you tie workforce identity to existing initiatives, you create alignment with broader organizational goals and make it easier to gain traction. Below are some of the most common objectives workforce identity investments support.

Cloud Migration

Organizations are increasingly operating in a hybrid, multi-cloud world and they need identity solutions that can adapt with them. Modern identity is deployable in a public, private or managed cloud environment.

Digital Transformation

An explicit digital transformation project or roadmap provides a clear starting place. Identity provides the foundation needed for rapid application onboarding, better user experience and streamlined integration.

Zero Trust & CARTA

Remote work initiatives accelerated rapidly in 2020. In response to evolving threats and more resources living outside of the corporate network, organizations are abandoning the concept of perimeters and adopting Zero Trust and CARTA. A modern identity solution makes it possible to authenticate any user, on any device, in any situation—and do so using adaptive policies to ensure an optimal user experience.

DevOps

Speed provides a competitive advantage, which is why DevOps is the preferred method for software development. Ensuring that your organization is reaping the full benefits of DevOps requires leveraging identity that can be easily consumed in a DevOps environment.

Passwordless Login

In order to keep your employees secure and productive, you need to mitigate risks and eliminate friction from their day-to-day tasks. Passwordless login lets you provide seamless access, while also providing greater assurance that your users are who they say they are.

WHAT TO LOOK FOR IN A WORKFORCE IDENTITY SOLUTION

Once you've clarified your business objectives and gained buy-in to move forward, you need to identify vendors to consider. When evaluating a vendor, consider the following:

- How long has the vendor been in business?
- Is the vendor a recognized leader within the industry?
- Does the vendor have demonstrated expertise in the form of customer success stories and testimonials?
- Does the vendor engage in continual R&D to improve and enhance products and meet evolving industry and customer demands?
- Does the vendor offer robust training, support and an active user community?

To build the future-proof identity foundation you need for digital transformation success, you also need a core set of critical capabilities. In fact, the absence of these capabilities is frequently the so-called straw that breaks the camel's back and what ultimately drives enterprises to begin the search for a modern identity solution.

Here are the capabilities you'll want to prioritize to help you create a shortlist of vendors. Of course, each organization has its own unique needs, so you may want to adjust or add to these to address your specific use cases and requirements.

SINGLE SIGN-ON	REQUIREMENTS
Scalability	Does the vendor support scalability across all application types (on premises, homegrown, SaaS)?
Federation	Does the vendor provide federated authentication and standards-based assertion with unlimited, flexible policies?
Single Source of Truth	Does the vendor handle attribute aggregations from multiple on-prem and cloud-based directories on the fly?
Simplified Architecture	Does the vendor support cloud, on-prem and hybrid deployments that can be pre-configured with Docker and Kubernetes?
Migration	Does the vendor support migration paths and co-existence with legacy WAM vendors with out-of-the-box tools?

SINGLE SIGN-ON	REQUIREMENTS
Integrations	Does the vendor offer extensive server integration kits, adapters and support for your legacy applications?
Centralized Management	Does the vendor provide visibility into all clients and connections through a centralized management portal?

INTELLIGENT AUTHENTICATION	REQUIREMENTS
Diverse Authentication Methods	Does the vendor provide a range of authentication options to support your use cases? • Mobile app with swipe, tap, OTP • Pin-protected desktop app • Push notifications for iOS and Android • Fingerprint and facial recognition • Apple watch tap notifications • FIDO-certified passwordless • Third-party authenticators • Security keys • Offline authentication
Adaptive Authentication Policies	Does the vendor provide adaptive policies based on contextual factors like location, IP address and geofencing to support risk-based authentication?
Device Posture	Does the vendor allow you to identify device attributes such as security settings? Can you tell if a device has been rooted/jailbroken?
Passwordless Login	Does the vendor provide options that limit or eliminate passwords via time-based policies, FIDO, Zero Trust architectures, etc?
Integration	Does the vendor support integrations with VPNs, MDMs and other MFAs?
Ease of Management	Does the vendor provide dashboards, detailed event reporting, audit trails and management via an admin UI and APIs?

DIRECTORY & DATA STORE	REQUIREMENTS
Security	Does the vendor provide data encryption at every state, modern password hashing, admin alerts and record and attribute controls to data?
Single Source of Truth	Does the vendor provide unlimited user attributes and fields that can sync across multiple directories?
Flexibility	Does the vendor provide scalability with low latency across millions of identities and billions of attributes?
Simplified Architecture	Does the vendor support cloud, on-prem and hybrid deployments that can be pre-configured with Docker and Kubernetes?
Integration	Does the vendor integrate with multiple directories (on-prem and cloud) by offering real-time, bi-directional data synchronization?
Delegated Administration	Does the vendor provide a management console for performance and infrastructure monitoring along with delegated admin of user profiles?

EMPLOYEE EXPERIENCE	REQUIREMENTS
User Experience	Does the vendor provide a consistent experience across all devices and application types?
One-click Access	Does the vendor provide a comprehensive employee dock that provides access to all apps?
Self-service	Does the vendor provide options for users to reset passwords and perform similar actions without having to call the help desk?
Easy Authentication Methods	Does the vendor provide convenient authentication methods such as device biometrics?

Use this workforce solution checklist to evaluate vendors. Blank rows have been provided at the bottom if you have additional requirements to add.

Requirements	Ping Identity.	Vendor 2	Vendor 3
Single Sign On			
Scalability			
Federation			
Single Source of Truth			
Simplified Architecture			
Migration			
Integrations			
Centralized Management			
Intelligent Authentication			
Diverse Authentication Methods			
Adaptive Authentication Methods			
Device Posture			
Passwordless Login			
Integration			
Ease of Management			
Directory & Data Store			
Security			
Single Source of Truth			
Flexibility			
Simplified Architecture			
Integration			
Ease of Management			
Employee Experience			
User Experience			
One-click Access			
Self-service			
Easy Authentication Methods			
Additional Considerations			

MAKING THE BEST WORKFORCE IDENTITY DECISION FOR YOUR NEEDS

Choosing identity solutions for your workforce use cases is an important decision. The right solution will provide the foundation you need to ensure digital transformation success, not to mention making your job significantly easier.

The Ping Intelligent Identity platform increases operational efficiency so you're able to quickly respond to changing business needs. More than 60 of the Fortune100 trust Ping for centralized and flexible identity services. Supported by powerful capabilities like dynamic authentication and adaptive access, they're providing the right people secure and seamless access to the right resources—and you can, too.

To learn more about Ping's capabilities and how we rate against other IAM vendors, read the 2020 Gartner Magic Quadrant for Access Management.

To get more specific insights into Ping's workforce identity capabilities, check out the 2020 Gartner Critical Capabilities Report.

ABOUT PING IDENTITY: Ping Identity is pioneering Intelligent Identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity™ platform provides customers, employees, partners and, increasingly, IoT, with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale. Over half of the Fortune 100 choose us for our identity expertise, open standards leadership, and partnership with companies including Microsoft and Amazon. We provide flexible options to extend hybrid IT environments and accelerate digital business initiatives with multi-factor authentication, single sign-on, access management, intelligent API security, directory and data governance capabilities. Visit www.pingidentity.com.

#3552 | 16.20 | v03