WORKFORCE IDENTITY TRANSFORMATION

ULTIMATE GUIDE

Ultimate Guide to Workforce Identity Transformation

TABLE OF CONTENTS

03 CHAPTER 1
Managing Digital Transformation Amid a Changing World and Workforce

06 CHAPTER 2
How Legacy IAM Holds You Back

09 CHAPTER 3
How Workforce Identity Transformation Propels You Forward

16 CHAPTER 4
Getting Started on Your Workforce Identity Transformation Journey

19 CHAPTER 5
Making the Business Case for Workforce Transformation

21 CHAPTER 6
Digital Transformation Success Starts with Workforce Transformation

CHAPTER 01

MANAGING DIGITAL TRANSFORMATION AMID A CHANGING WORLD AND WORKFORCE

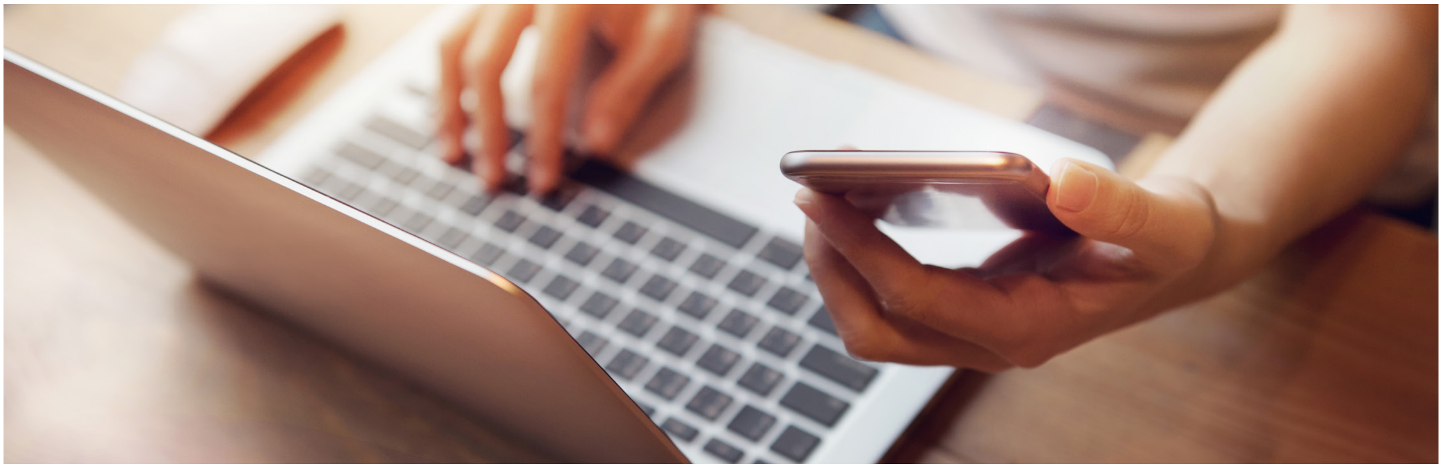
No one could have predicted how our world would change in 2020. The COVID-19 pandemic altered our way of life practically overnight.

For individuals and organizations alike, the changes were swift and significant. As millions of employees around the world were suddenly working from home, the divide between those enterprises that could rapidly adjust and those who couldn't was evident.

While digital transformation has long been recognized as a gateway to new revenue streams and more customers, its impact on workforce productivity is now more pronounced than ever. Whether they're working from home or any other location, your increasingly remote workforce needs frictionless access to resources to maintain any semblance of business as usual.

Many enterprises are fast-tracking digital transformation efforts to provide this access and keep up with today's rapidly evolving business environment. And it's anticipated that this accelerated pace will continue as enterprises charge ahead with the adoption of new technologies that can help them thrive in a changing world.

> “
>
> The more change we see, the harder it is to believe businesses will go back to how things were before this crisis. This 'no going back' attitude is not just coming from the reality that COVID-19 will impact many in-person activities and spaces from open offices, to travel and events. The desire to change is also the result of seeing the positive impact digital transformation has on a business.[1]



Overcoming Typical Digital Transformation Obstacles

The race is on, but the obstacles that hindered digital transformation before haven't gone away. While transitioning to the cloud is often part of a company's digital transformation, not every on-premises application has a suitable SaaS alternative or is able to be migrated. More often than not, a hybrid environment of cloud and on-premises applications is needed at least temporarily if not for the long haul.

But not all identity and access management (IAM) solutions are designed to support hybrid IT. Trying to make do with an inflexible solution often results in additional costs, delays and risks to your cloud strategy. Your workforce productivity is also sure to suffer.

Many are already challenged to provide seamless workforce access while ensuring the security of resources. It's a hard balance to achieve without the right identity foundation in place. Trying to forge ahead without addressing the foundational need for streamlined workforce access could negatively impact your efforts and ultimately thwart your gains. On the other hand, proactively transforming workforce access as part of your digital transformation strategy can effectively double your odds of success. [2]

Learn more about doubling your odds of success in transformation. Read the blog.

Zero Trust Drives Digital Transformation

An authentication authority provides the identity foundation needed to transform workforce access, while providing the solid footing on which to build your digital transformation initiatives. It also helps you transition to an identity-centric Zero Trust approach to security.

A Zero Trust model helps you set the stage for digital transformation success by ensuring:

- Your workforce is able to get work done anywhere, anytime, on any device
- Your enterprise has secure access controls in place to prevent costly data breaches
- Your enterprise architecture is agile and adaptable to new business models and requirements

While digital transformation is needed to remain competitive in an unpredictable world, it must be undertaken wisely. A haphazard or band aid approach will only exacerbate underlying problems and hurt your progress.

Read on to learn:

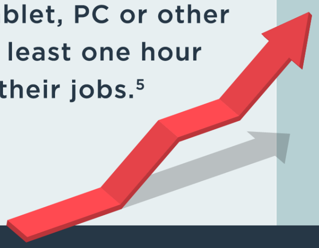
- 3 ways legacy identity and access management tools hurt your progress
- How workforce identity transformation propels digital transformation
- Where to get started with your own transformation and set the foundation for success

THE STATE OF WORKFORCE ACCESS

The global workforce has grown to include

1.25 BILLION KNOWLEDGE WORKERS

defined as those who use a smartphone, tablet, PC or other device for at least one hour a day in their jobs.[5]



64% OF EMPLOYEES

use company-approved personal devices to access company resources, but only 40% are subject to regulations regarding their use.[6]

86% OF EMPLOYEES

use personal devices to check email and 67% use them to access shared documents.[7]

Organizations who invest in digital tools to make information more accessible across their organization are

2.1X MORE LIKELY

to experience digital transformation success.[8]

48% OF EMPLOYEES

will likely work remotely at least part of the time after COVID-19 versus 30% before the pandemic.[9]

> Enable multi-factor authentication (password + one other requirement such as a text message) whenever possible,
>
> **INCLUDING ACCESS TO CRITICAL DATA**
>
> in cloud applications used for data and document sharing.[10]

Improving Digital Transformation Outcomes

While digital transformation can yield big benefits, success isn't guaranteed. A McKinsey Global Survey found that less than two out of 10 organizations (16%) experienced sustainable change and improved performance from their digital transformation efforts.[3]

The same study identified that providing your workforce with access to digital resources and information is often the missing piece of the puzzle. Those organizations that invest in technology to ensure workforce access are 2.1X more likely to experience digital transformation success.[4]

While providing that access may feel like a moving target as workforce dynamics continue to evolve, there are identity solutions built specifically to solve these challenges.

CHAPTER 02

HOW LEGACY IAM HOLDS YOU BACK

There was a time when tools like CA, IBM and Oracle were the de facto standards for access management, promising greater productivity and security. But just like the flip phone was once the pinnacle of mobile phone technology, those days are long gone. And even specialized in-house or custom-built IAM tools grow more obsolete by the day as new digital resources become more diverse and threat vectors expand.

Drains IT Resources

These legacy systems are now a heavy and expensive burden on the IT teams that must continue to manage them. As they approach end-of-life, the original creators have slowed or stopped investment in these tools. Plagued by outages and other issues, they've become unreliable, requiring significant maintenance and dedicated, trained staffing resources just to keep them operational.

For many enterprises, disparate authentication silos—whether as a result of mergers and acquisitions or shadow IT—are also the norm. Legacy IAM tools offer no easy way to scale or consolidate, leaving overburdened IT teams with the unenviable task of maintaining overly rigid and complex infrastructures.

Proprietary and lacking open standards support, these tools aren't able to support cloud, automation or DevOps initiatives. On the contrary, they're slowing the onboarding of new applications and resources. In some cases, business application teams will also resort to deploying their own identity systems and continuing the cycle of shadow IT in the enterprise.

Discover 5 ways workforce transformation helps you boost agility. Read now.

Drags Down Productivity

Increasing workforce productivity is one of the top drivers of digital transformation. But a continued reliance on outdated systems makes productivity improvements challenging if not impossible.

An increasingly remote and mobile workforce means more employees needing access to corporate resources off of the network. At the same time, the workforce is no longer limited to employees. Contractors, partners and vendors are increasingly accessing your resources as well.

To realize the productivity gains your enterprise is seeking, you need to provide quick and convenient access to the apps these diverse users need. But if their access hinges on discrete logins for every resource, you're at a distinct disadvantage. Employees waste nearly 11 hours per year entering and resetting passwords, and your helpdesk will be faced with managing the inevitable password reset requests that ensue. In the end, everyone's productivity suffers.

Learn how workforce transformation supports increased productivity. Read now.

Threatens Security

Giving an increasingly diverse and remote workforce access to corporate resources also presents security challenges. You need to make access consistent and convenient, but you can't do so at the expense of security. Meanwhile, you're also being asked to support access from multiple devices, including personal ones, which introduces new risks.

The traditional enterprise approach would enlist the use of a VPN for remote access. But in today's threat landscape, the use of VPNs can cause more problems than they solve. Because they grant users access to large segments of the corporate network, VPNs can expose an employee to more resources than their role requires or warrants. This makes VPNs an attractive target for bad actors and increases the attack surface they can exploit.

The accelerated adoption of cloud technology is also forcing organizations to re-evaluate how they secure resources that reside on-premises and in the cloud. While legacy IAM solutions provide protection for on-prem resources, most struggle to extend beyond VPN or remote access, leaving them unable to support web and mobile apps, APIs, Linux or Unix servers, Windows login, offline multi-factor authentication (MFA) and other use cases.

Learn more about increasing security through workforce transformation. Read now.

Ping Identity
TOP 10 LEGACY IAM CHALLENGES
HOLDING BACK YOUR ENTERPRISE
WEB ACCESS MANAGEMENT
TROUBLE SECURING RESTFUL SERVICES & APIS
Proprietary tokens aren't compatible with web services
NO PARTNER AND CUSTOMER ACCESS
(Requires bolt-on technologies)
DIFFICULTY PROTECTING RESOURCES IN THE CLOUD
93% OF ORGANIZATIONS are currently using cloud services¹
DIRECTORY
LACKING NATIVE SECURITY FEATURES
The average total cost of a data breach is $3.62M²
MISSING SUPPORT FOR MODERN APPLICATIONS
Limited REST and SCIM support
DIFFICULTY ADDING MORE APPS & USERS
Downtime and latency increase with scale
MULTI-FACTOR AUTHENTICATION
AUTHENTICATION ~~WITHOUT~~ CONTEXT
MISSING USER AND DEVICE INSIGHT

Uncover the top 10 ways legacy IAM is holding you back. See the complete infographic.

You Need New Solutions to Solve New Problems

Because they're working against digital transformation—not to mention introducing unnecessary cost and risk—the once-great access management systems are not enough to meet your new business challenges. But you might not be ready to turn your back on these systems just yet. To move forward, you need to adopt a workforce transformation strategy that allows you to boost your capabilities now while gradually reducing your dependence on legacy systems.

You also need to have reliable and flexible tools that allow you to support your organization's objectives and critical initiatives. While legacy solutions served their purpose at the time, the demands and requirements of today and tomorrow require the flexibility and customization found only in modern solutions.

CHAPTER 03

HOW WORKFORCE IDENTITY TRANSFORMATION PROPELS YOU FORWARD

During this period of rapid change, enterprises are relying on their IT teams to keep employees securely working while enabling the business to meet its overnight digital transformation goals. But legacy solutions make it hard to do either.

When your attention and dollars are swallowed up by managing and maintaining inflexible tools that are nearing obsolescence, you're limited in your ability to be responsive to new and changing priorities. You're also restricted in your ability to enable remote productivity requirements when these same tools weren't designed to meet the demands of supporting an increasingly off-network workforce.

Workforce identity transformation starts with releasing your reliance on legacy systems and implementing modern IAM capabilities. Modern IAM solutions capable of integrating with your existing infrastructure:

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

Reveal the advantages of modernizing identity and access management. Watch the video.

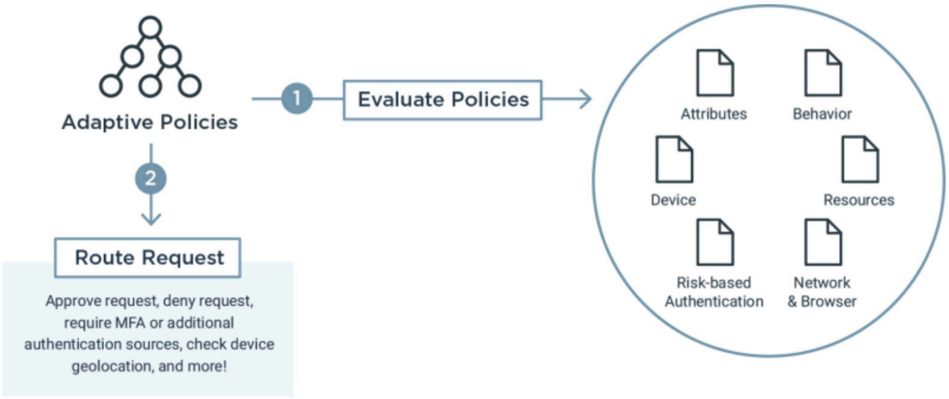
Balance Productivity and Security with Adaptive MFA

There's a balance you need to strike between productivity and security. On the one hand, you don't want to apply so much security that remote employees can't access the resources needed to perform their jobs. On the other, you can't make access to resources so easy that vulnerabilities are introduced and your security posture is sacrificed.

Adaptive MFA gives your team the ability to strengthen security without disrupting employee workflow. You're able to give your users a consistent and convenient experience across all applications and resources.

By leveraging a variety of authentication methods, you're able to provide a frictionless experience. Users can authenticate to applications using a range of convenient methods such as push notifications on smartphones and IoT devices, YubiKey, voice, email and SMS one-time passcodes, desktop applications and more.

Adaptive MFA also lets you use contextual factors and logic-based mechanisms—such as geolocation, time of day, IP address and device identifiers—to match authentication requirements to the risk of the request or action being performed. You can streamline access for low-risk activities—for example, accessing SaaS productivity applications like Office365—or step up security for higher risk transactions—such as requesting access to sensitive data like sales records.


Adaptive Policies
1
Evaluate Policies
Attributes
Behavior
Device
Resources
Risk-based Authentication
Network & Browser
2
Route Request
Approve request, deny request, require MFA or additional authentication sources, check device geolocation, and more!

Ultimately, strengthening security means minimizing your reliance on passwords. Modern MFA helps you move toward passwordless authentication by substituting more secure authentication options, such as biometrics and Yubikeys, in place of passwords. Reducing dependency on passwords is also the basis of Zero Trust. In a Zero Trust environment, users are recognized and authenticated using multiple dynamic factors, including the devices used to access applications and the context in which they're attempting to access them.

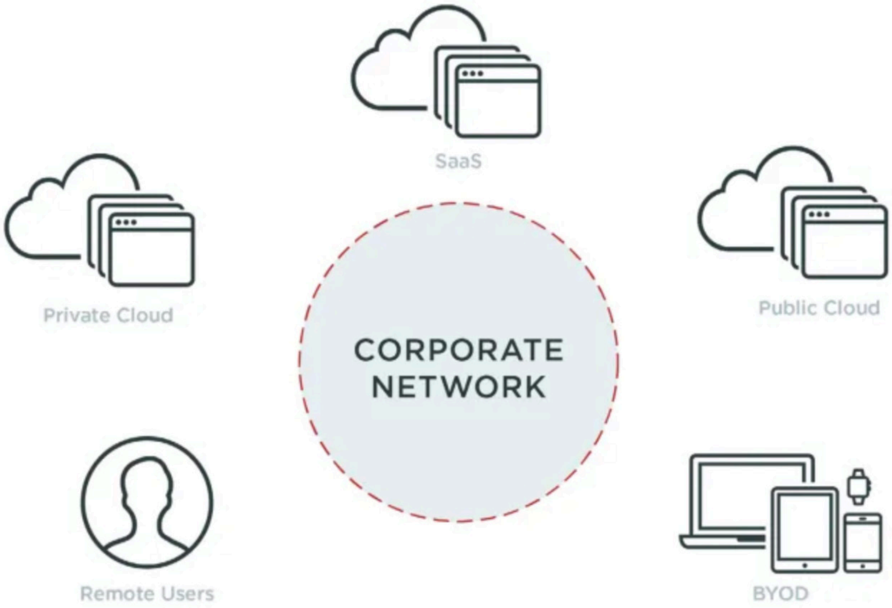
Zero Trust: Establishing a New Perimeter while Minimizing Password Reliance

The concept of Zero Trust is to never trust, always verify. That may sound harsh but when an increasing number of users and resources are located outside the corporate network, you need a more reliable way to protect enterprise resources than passwords.

In a Zero Trust environment, a user's identity in addition to the device they're using to access applications and the real-time context in which they're attempting to access them are all used to verify the person is who they claim to be.

Given the growing number of threats to your enterprise, you need to have confidence that every user is valid and authorized to access the resources they're requesting. Passwords alone aren't enough—and are the most common vulnerability for security breaches. A Zero Trust approach makes workforce identity the new perimeter.

> “
>
> Credential theft, errors and social attacks are the three most common culprits in breaches. Employees working from home could be particularly vulnerable to these attacks. In these uncertain times, it makes sense to focus prevention efforts here.
>
> **2020 DATA BREACH INVESTIGATIONS REPORT, VERIZON**



Given the growing number of threats to your enterprise, you need to have confidence that every user is valid and authorized to access the resources they're requesting. Passwords alone aren't enough—and are the most common vulnerability for security breaches. A Zero Trust approach makes workforce identity the new perimeter.

Effective Zero Trust security requires a central authentication authority. This authentication authority provides a single source of truth about each user, so you're able to continuously and reliably verify a user's identity before granting access to resources.

An identity-centered approach to Zero Trust makes workforce identity the new perimeter, so security can go where your people are. You gain a greater level of assurance that the right people are getting access to the right resources. At the same time, your users benefit from consistent, quick access to the resources they need—without having to create and remember dozens of passwords.

Not only is your workforce able to be more productive, your IT team is, too. By reducing the number of password reset requests, you effectively minimize helpdesk tickets. A centralized administration portal also allows application teams to onboard applications themselves. Your IT team is freed up from low-level tasks to focus on needle-moving transformation initiatives.

Still learning about Zero Trust? Read the blog.

Ready to get started with Zero Trust? Watch the webinar.

Passwordless Authentication: Solving the Password Problem Once and for All

We all know the weaknesses of passwords, but bypassing passwords altogether may seem like a far-off fantasy. Actually, passwordless authentication is more attainable than you may realize.

The FIDO Alliance is on a mission to make passwordless MFA available to all users and the online services they interact with. By defining a common way for browsers and online services to implement MFA, the FIDO2 standard (aka simply FIDO) allows for the removal of knowledge (what you know) factors like passwords, KBA and one-time passcodes, which have proven vulnerable to attacks. Instead, it provides users with passwordless options—such as security keys, biometrics and other mobile-device-based solutions—to improve security.

Zero Trust as discussed previously is the first step. You can start by leveraging modern adaptive MFA policies to step down authentication in low-risk scenarios. For example, you could combine a username only (no password) with a lower friction method of authentication—such as a device-based biometric (a fingerprint) or a swipe—when a user is accessing non-sensitive resources in a typical manner (on a recognizable device and from a trusted network).

You may still require passwords in some situations, but this is where FIDO2 comes in. Instead of passwords, FIDO2 leverages public key cryptography methods that require users to register a device and a domain (a corporate email) from which future access requests will originate.

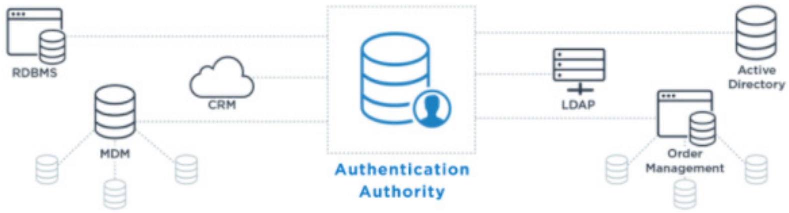
While eliminating passwords may seem out of reach, passwordless authentication is closer—and more achievable—than you may think.

Learn more about passwordless authentication. Get the white paper.

Quickly Onboard New Apps With Augmented Directory Capabilities

It can be difficult to justify to the CEO and other non-IT leaders why you need so much time to onboard a new application, give employees access and drive adoption of valuable information and technology assets. Disparate Microsoft Active Directory (AD) instances, legacy LDAP environments and the multiplication of other identity stores over time are often to blame. These disjointed data stores which contain duplicate and custom identity data create a number of challenges.

But there's a secret to speeding up application onboarding: a workforce authentication authority with modern directory capabilities that augments existing AD user profiles with flexible, custom attributes. In the absence of such an authentication authority with modern features like RESTful APIs and a flexible schema, application teams often resort to shadow identity to launch quickly.



Considering Microsoft Azure Active Directory?

Most organizations with AD are aware of Azure AD's flexible schema and ability to migrate existing AD profiles. But many hold off on moving to Azure AD because it would require shifting identities to the cloud.

This isn't an easy choice for large enterprises in highly regulated industries or for mission-critical use cases where up-time is essential. These organizations can leverage a workforce authentication authority to provide the same modern capabilities. An authentication authority wraps around an existing AD environment, but gives you the choice of on-premises or cloud deployment.

Learn how to consolidate identities with an authentication authority. Get the guide.

A workforce authentication authority gives developer teams the capabilities they need, while giving you the ability to establish a single source of truth. You gain a consolidated workforce user profile that you can leverage across all enterprise applications.

The addition of bi-directional data synchronization capabilities make it possible to consolidate workforce credentials, application data and profiles into a single source of truth. The result is a central credential store that contains any and all on-premises and cloud directories used by your apps, including RDBMS, LDAP, CRM and many more.

Over time you're able to simplify your architecture, gaining a single, scalable and secure user store that all of your applications can access via developer-friendly REST APIs and reducing your dependence on legacy data stores so you can decide whether to retire them at your own pace.

An authentication authority with a powerful, scalable directory that augments your existing AD environments can serve your enterprise needs both today and into the future. The addition of end-to-end security including encryption of data at rest, in transit and during backup and monitoring ensures valuable and highly targeted identity data remains protected—providing even more incentive to shut down insecure legacy identity stores and shrink your attack surface over time.

Learn more about modernizing your directory. Get the guide.

Provide Convenient Access to Every App with Modern Access Management

As part of the increasingly remote and mobile workforce, your employees need access to resources from any location at any time and from any device. Historically, your workforce only needed secure access to applications, but today's employees and partners depend on APIs and data to get their job done. You need to secure all of your most valuable resources and ensure sensitive applications, APIs and data are protected as well.

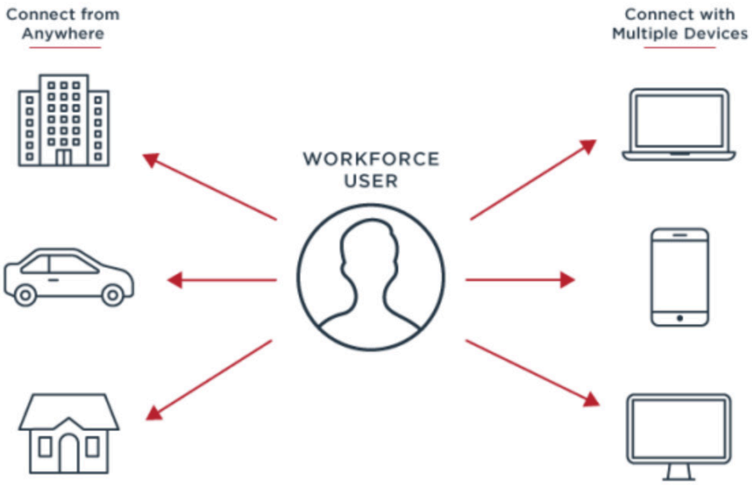
Modern access management starts with an authentication authority to federate identity and streamline access to every application—from on-premises to mobile to SaaS—with convenient single sign-on (SSO). You're able to eliminate password sprawl and unnecessary friction to support increased productivity across your organization.

A comprehensive policy engine ensures that those requesting access have the appropriate permissions, user context and device posture to access applications, down to the URL level. When you combine a centralized, comprehensive policy engine with fine-grained, dynamic authorization, you're able to grant workforce users adaptive, secure access to all of your enterprise's resources regardless of where those resources or users are located.

You can also mitigate risk and improve your security posture by centralizing policy and session management to a single source of truth, ensuring consistency throughout your organization.

When you're able to move away from legacy access management solutions to modern solutions, you're better positioned to support the business and accelerate digital transformation initiatives.

Want to give your workforce secure access? Learn more.



3 Ways You Reap the Benefits of Workforce Identity Transformation

Save Money, Time and Resources

When you're still relying on legacy systems, you must spend an inordinate amount of energy and resources on low-value work. The time spent supporting out-of-date tools, resolving password reset requests and onboarding applications can add up quickly. All of this steals your attention away from the strategic initiatives that can drive your organization forward.

Workforce identity transformation centered on Zero Trust principles frees up money, time and resources by providing features like:

- Centralized authentication services, with an authentication authority for any use case
- Industry standard support, limiting the need for customization
- Self-service options for password resets
- Delegated administration to application teams with a central portal to onboard apps
- Fewer systems for teams to maintain
- Support for DevOps, automation, and flexible deployment options, including cloud

Maximize Productivity

Requiring workforce users to create and remember multiple login credentials to get access is hurting their productivity and yours. When you transform workforce identity and transition to an identity-centric Zero Trust model, you're able to give your workforce users streamlined access to the right digital tools at the right time, regardless of where they're located.

Workforce identity transformation helps your entire organization be more efficient and use time wisely by providing:

- One-click access to every resource, across any application, any cloud and any directory
- Self-service portals so employees can reset their own passwords
- Self-service application integration templates to onboard applications to identity management
- Adaptive authentication using context and intelligence to trigger MFA for only high-risk activities

Strengthen Security

Digital transformation creates new opportunities for your enterprise, but it also creates new threats. A Zero Trust approach to security ensures you're protected while providing convenient access to an increasingly mobile and diverse workforce. It also gives you the solid foundation to keep up with growing demands so you can minimize the incidence of shadow IT and siloed approaches that expose security risks.

Workforce identity transformation helps you strengthen your security posture by providing:

- A foundation for Zero Trust, which reduces risk and shrinks your attack surface
- Adaptive MFA that dynamically assesses risk and responds accordingly
- Secure passwordless login capabilities that reduce your reliance on passwords
- Continuous risk score evaluation and fine-grained dynamic authorization

CHAPTER 04

GETTING STARTED ON YOUR WORKFORCE IDENTITY TRANSFORMATION JOURNEY

With COVID-19 causing an overnight shift in global priorities, enterprises are at a crossroads in determining their strategy for critical workforce identity modernization. They're faced with two options:

A: High-Impact Transformation: Modernize everything in two major phases.
B: Quick Wins: Tackle identity capability modernization one capability at a time.

While ultimately you must decide what's best for your organization, you'll be able to make a better informed decision by having a deeper understanding of what both entail.

OPTION A

- Authentication for Everyone, Everything
- Secure Access to All Resources

OPTION B

- SSO
- MFA
- Access Management
- Directory
- Data Governance
- API Security

Option A: High-Impact Workforce Identity Transformation

Enterprises whose IT organizations are being forced to rationalize projects and therefore are only looking at big impact projects may prefer this option.

But when taking big strides in your transformation, it's important to choose an approach that lets you migrate your current infrastructure to a new system over time. You want to avoid a "rip and replace" effort whenever possible.

We recommend taking two giant leaps as part of a two-phased approach that can ensure you're set up for a smooth migration while also making meaningful forward progress.

Phase I: Provide Authentication for Everyone and Everything

Giving your employees and other workforce users a consistent way to sign-on to the resources they need is a great place to start. When you're able to provide convenient one-click access to on-premises, cloud and SaaS resources, end user productivity will also increase.

You achieve this with a centralized global authentication authority. An authentication authority allows you to secure and control access to resources across all of your domains and platforms, from public and private clouds to legacy on-premises environments. With support for all identity types, user populations, apps and environments, a global authentication authority gives you the ability to identify high-risk behaviors without unnecessary friction so you can strike the perfect balance between security and convenience.

You also want to help your IAM team increase productivity and agility by giving them the ability to quickly onboard applications, automate where possible, delegate administration and gain visibility into all environments. With support for open standards, including OAuth, OIDC and more, an authentication authority lets you automate cloud deployment, rapidly onboard apps and leverage DevOps.

Regardless of where you are in your digital transformation journey, putting an authentication authority in place will get your identity transformation on solid footing and help you increase productivity, agility and security. An authentication authority gives you capabilities including:

- Single-click access (aka single sign-on) for employees, partners and others to all applications
- Centralized authentication services to connect any user to any application
- Contextual and adaptive MFA that can easily extend anywhere and enable passwordless
- Single source of truth working across various on-prem and cloud directories
- Modern directory services such as a flexible schema and REST API access that works within your existing AD environment
- Centralized administration portal with self-service APIs, templates and delegated administration capabilities

Ready to provide authentication for everyone to everything? Learn more.

Phase II: Secure Access to Your Applications, APIs and Data

Giving your workforce secure access to resources is the first step, but it can also create new challenges. You need to support productivity improvement, but you must also ensure only the right people get access to the right things.

To strike this balance, you need the ability to enforce specific access rights for individual employees and other dynamic workforce users, while minimizing the amount of user friction. Adaptive access security helps you boost security without adding friction by balancing security and productivity with fine-grained controls and visibility beyond applications into APIs and data.

Adaptive access security combines centralized session and policy management with fine-grained, dynamic authorization and AI-powered API cybersecurity. You're able to protect sensitive applications, as well as extend that protection to APIs and data, without adding friction.

You're also able to migrate on your terms. An adaptive access security solution capable of integrating with your existing IAM infrastructure and API gateways gives you the flexibility to deploy enterprise IT on-premises, in the cloud of your choice or combine on-premises and cloud deployment in a hybrid environment that fits your enterprise's unique needs.

Adaptive access security helps you support the productivity of an increasingly remote workforce, make smarter security decisions and advance digital transformation initiatives by providing capabilities like:

- Centralized access management for applications, APIs and data
- Dynamic risk score evaluation
- Intelligent API cybersecurity
- Dynamic, fine-grained authorization for data

Support workforce productivity with adaptive access security. Learn more.

Learn more about your advanced workforce solution options. Get the brief.

Option B: Quick Wins for Workforce Identity

Some large enterprises may be unable to implement changes in a two-phased approach. Organizations that are more risk averse may need to take modernization one project at a time to build momentum and prove value. If this is your situation, you can modernize your IAM stack one capability at a time.

You'll want to start with the processes that present the lowest risk, while reaping quick rewards. For many organizations, implementing MFA is a natural place to start, followed by authentication and single sign-on, directory services, access management, data access governance and API security.

Need to take a step-by-step approach to modernizing IAM? Get the guide.

CHAPTER 05

MAKING THE BUSINESS CASE FOR WORKFORCE TRANSFORMATION

While digital transformation is a strategic priority for most organizations, the costs associated with it are often closely monitored. Because of the rapidly changing business environment, you can expect investments to be scrutinized.

To create alignment, you'll want to identify the ways workforce transformation can drive business value. Focusing on how modernizing your IAM will increase productivity, security and agility can help you create support for this transformation.

- **Productivity:** Ensuring a dynamic workforce remains productive with access to every resource to get their job done.
- **Security:** Protecting the enterprise against vulnerabilities and threats by adopting Zero Trust principles grounded in the philosophy of always verifying, never trusting.
- **Agility:** Supporting the quick and efficient onboarding of new applications and technologies to ensure successful digital transformation initiatives.

To make the business case for workforce transformation, you must demonstrate value. To get buy-in from your IAM peers and IT executives, you'll want to home in on the specific capabilities that resonate for each audience.

What IAM and IT Security Professionals Care About

For the IAM and IT security professional, workforce identity transformation enables business continuity through digital transformation efforts that allow the enterprise to adapt to a rapidly changing environment while maintaining productivity and security.

Increasing the Speed of Business

The time and energy involved in maintaining legacy systems can steal your IT teams away from supporting the business. Workforce transformation centered on modern IAM solutions frees your IT teams to drive digital transformation success by:

- Leveraging standards, reducing the need for costly and time-consuming customization
- Accelerating cloud adoption to increase efficiency and reduce costs
- Empowering app teams with self-service capabilities that speed time to market and minimize reliance on IT
- Automating identity into the DevOps tool chain

Maintaining Workforce Productivity

Your IT teams can enable the productivity of increasingly remote employees by:

- Enabling one-click access to resources with SSO
- Using dynamic, adaptive authentication to streamline access and step up authentication requirements only when warranted
- Establishing a central IAM operating portal with delegated administration so users can help themselves
- Being relieved from low-value, manual tasks like password resets and fulfilling application onboarding requests so they can focus on strategic priorities

Securing the Enterprise

As company-wide work from home mandates become the norm, organizations are looking to establish an identity-based perimeter to balance enterprise security with employee productivity. Moving to a Zero Trust approach can empower IT teams to secure the business without adding unnecessary friction to the employee workflow by:

- Putting MFA everywhere, so you can reduce password risk
- Relying on context and risk signals to ensure users are who they claim to be
- Imposing least-access privilege to minimize insider threats and ensure only the right people have access to the right resources
- Consolidating and rationalizing legacy systems to reduce your overall attack surface

Delivering business value with workforce transformation is easy. Learn more.

What IT Executives Care About

As part of any workforce transformation, IT executives are looking to implement Zero Trust security strategies that protect the organization, enable remote employees to remain efficient and support digital transformation efforts.

Architecting for Zero Trust

With more employees accessing resources from outside of the office, the corporate network is no longer a reliable security measure. Using a Zero Trust framework can help increase your enterprise's security posture by:

- Laying the foundation for an identity-centric approach to secure a borderless enterprise
- Leveraging intelligence, context and risk signals for greater confidence in giving access to resources

Enabling Workforce Productivity

Achieving digital transformation success requires supporting your increasingly remote workforce to maintain productivity. Workforce transformation propels digital transformation by:

- Making digital resources more accessible across your business so your workforce is able to work efficiently and effectively
- Empowering IT teams to support transformation efforts rather than handling mundane tasks like password resets and lockouts

Increasing Business Agility

IT executives see IT as an enabler of rapid business model pivots that can keep the enterprise steps ahead of the competition. Workforce transformation increases agility by:

- Utilizing cloud, DevOps, APIs and automation to speed up time to market
- Freeing up teams from supporting legacy systems so they can focus on business improvements that move the needle

Unleash your IT team with a workforce authentication authority. Learn more.

CHAPTER 06

DIGITAL TRANSFORMATION SUCCESS STARTS WITH WORKFORCE TRANSFORMATION

Digital transformation success has been fleeting for some. But workforce transformation done right can greatly improve digital transformation outcomes.

As the shift to remote work and cloud computing is expected to continue and increase, you can expect transformation efforts to become even more mission-critical. To keep pace in our rapidly changing world, high-performing IT teams are essential. Your organization is relying on you to pave the way to go digital, while ensuring workforce productivity and maintaining enterprise security.

By making workforce identity the new security perimeter, you can provide the secure access your workforce needs while building the solid foundation needed for digital transformation success. An identity-centric Zero Trust security approach makes it possible to ensure:

- A productive workforce able to get work done anywhere, anytime
- A secure enterprise with access controls in place to prevent costly data breaches
- An agile enterprise architecture that can easily power new business models and requirements

Quantifying the Value to Your Business

Beyond highlighting the benefits and capabilities workforce transformation provides, you can quantify the value of transforming workforce identity to provide proof of measurable business value.

What value could workforce transformation add to your organization? Calculate now.

Sources

[1] Milanesi, Carolina. "Digital Transformation And Digital Divide Post COVID-19." Forbes. May 11, 2020.
[2] "Unlocking Success in Digital Transformation Survey." McKinsey. Oct 29, 2018.
[3, 4] Ibid.
[5] Gillett, Frank. "The Global Information Worker Population Swells To 1.25 Billion In 2018." Forrester. Oct 2, 2019.
[6] "How Employees Engage With Company Cybersecurity Policies." Clutch. May 15, 2018.
[7] Ibid.
[8] "9 Future of Work Trends Post-COVID-19." Gartner. June 8, 2020.
[9] "Unlocking Success in Digital Transformation Survey." McKinsey. Oct 29, 2018.
[10] "Securing a Remote Workforce." Cyber Readiness Institute. March 2020.

PingIdentity.

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.

#3522 | 01.21 | v03