1KOSMOS

Overcoming Resistance to Change on the Journey to Passwordless MFA

How to ease users into their new non-phishable login experience and control the roll out of passwordless MFA

WHITEPAPER

Executive Summary

Passwords and legacy two-factor authentication (2FA) have well-known vulnerabilities, but changing the way workers and customers authenticate into digital services has significant implications in terms of user adoption, information security and overall project management.

For most the move to passwordless represents a much bigger change management initiative, and the risks of failure for hastily planned passwordless deployments are high.

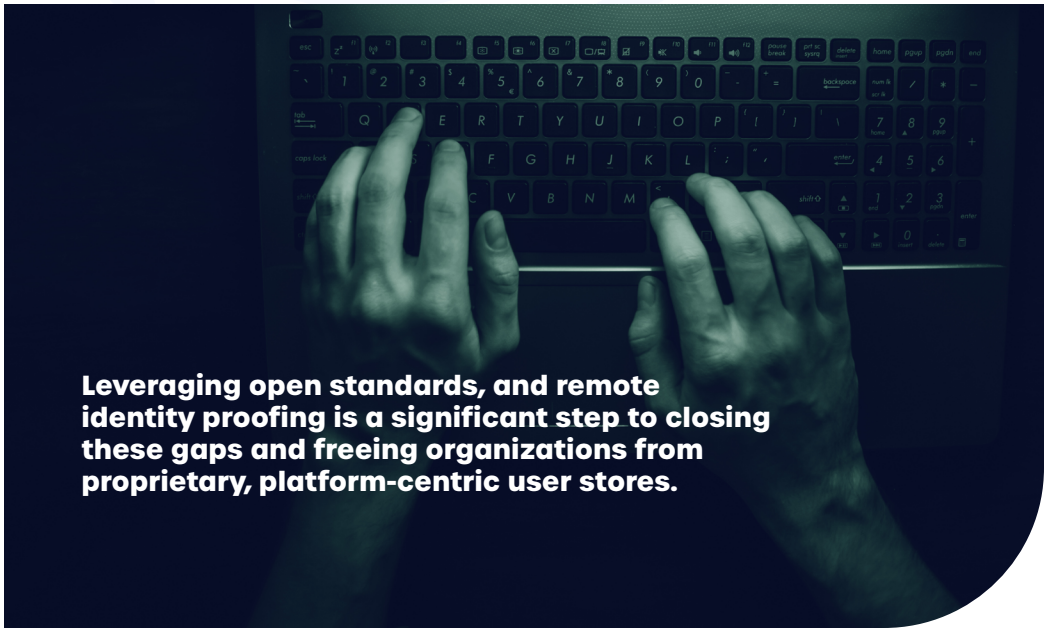
The penalty for failure is much higher if workers get alienated or customers lose confidence and the business misses an opportunity to fundamentally streamline operations, reduce administration costs and launch innovative online services at scale… all equating to a missed opportunity to break from the pack and win market share.

This is particularly true for a broad-scale move to passwordless without sufficiently crafting a vision for how the key challenges and use cases will be addressed. Success requires comprehensive planning and calls for equipping the team with the right tools and expertise for the implementation and to manage performance across the many edge cases spanning endpoints, VPN, countless web and mobile applications, disparate operating systems, and, of course, single sign-on (SSO) technologies.

Central to all of this is how organizations onboard and manage users. There are two fundamental challenges with onboarding new users into organizations. First, it is difficult to prove the identity of remote users. New forms of fraud include "proxy interviewing" and "contractor jacking" where the person doing the work is not who was interviewed or hired.

Second, large gaps can exist between the users accessing digital services and who IT believes those users to be. When going password-less with biometrics, access to critical services and sensitive IP hinges on a fingerprint, facial scan, voice match, or some other biometric. But whose biometric is it? Has it been verified? Has it been stolen or spoofed? How much trust is the business willing to assert in the identity behind the authentication?

Leveraging open standards, and remote identity proofing is a significant step to closing these gaps and freeing organizations from proprietary, platform-centric user stores. These have always been plagued by inaccuracy and both privacy and security challenges, particularly under the load of increasingly remote users, modern hybrid computing architecture and ubiquitous end user devices of various models and capabilities. In the spirit of diversity, equity and inclusion, whatever approach is selected, it needs to be available to all, not just a privileged few with the latest smartphones.



4

There are four categories of net gains to be had from successfully managing this transition. These are materially significant and achievable with the right technology enabler:

Cost Savings: Simplified IAM IT Infrastructure / Vendor Consolidation

- Reduce or eliminate legacy authentication methods, fees and related management costs
- Reduce or eliminate OTP messaging costs (and associated systemic security risk)
- Reduce fees, maintenance and support costs by managing all users in a single instance

Operational Efficiency: Administration, Overhead, and User Productivity

- Eliminate 30-50% helpdesk calls related to password management / reset
- Reduce administrative overhead for new user onboarding and system provisioning
- Improve the average time it takes for a user to login dozens of times / day / employee
- Recapture lost worker time and value related to password recovery
- Improve fraud management by eliminating stolen / synthetic identities before onboarding

Customer Experience and Loyalty

- Modernize user experience and improve satisfaction for higher lifetime value
- Accelerate new account origination with fewer abandonments and faster time to value
- Improve adoption of new business services, lines of business, and high value digital transactions

Security and Risk

- Reduce risk of business disruption and financial loss from credential-based phishing, data breach and ransomware attacks
- Reduce risk of customer turnover and losses from account take-over
- Reduce risk and fines for GDPR / PII and KYC identity proofing non-compliance

To achieve the benefits of passwordless technology, organizations need a controlled rollout and migration of users to a new, modernized login process that merges identity proofing and authentication. This form of identity-based passwordless MFA is critical to digital transformation, determining whether organizations compete or become uncompetitive. Successfully managing organizational change is crucial to transitioning users from passwords to a more secure and convenient login method that has linkages to a real-world identity.

This makes successfully managing the related organizational change the determining factor to either a productive or destructive "disruption" to the status quo. Success here hinges on how adept organizations become at re-engineering the online habits of users grooved over decades and who need to be gracefully transitioned from trusting, even expecting, passwords to using their likeness and trusting that privacy and security have improved as much as user convenience.

Prepare for Change

Password-based security is at its breaking point. Passwords and traditional multi-factor authentication (MFA) are being hacked and compromised at scale. Legitimate users innocuously share credentials, sometimes for convenience, but inadvertently giving others privileged access that can be misused. Other times access is shared in a form of collusion, such as offshoring their work to further a side hustle.

These security vulnerabilities have always been present, but now it's common for one person to have hundreds of passwords for hundreds of systems, each supposed to be unique, hard to guess and at the same time easy to remember. But we know that doesn't happen, and all too often, we accept the risks as the cost of doing business, because password-based authentication is so deeply baked into organizational culture and behavior.

And for good reason. Passwords, 2FA codes, physical and logical tokens, and even digital device recognition have stood in for identity over the past six decades. Still, in reality, they have all served as near proxies for identity. None of them prove a user's identity. It is easy to forget why we are challenging our users for an identifying factor.

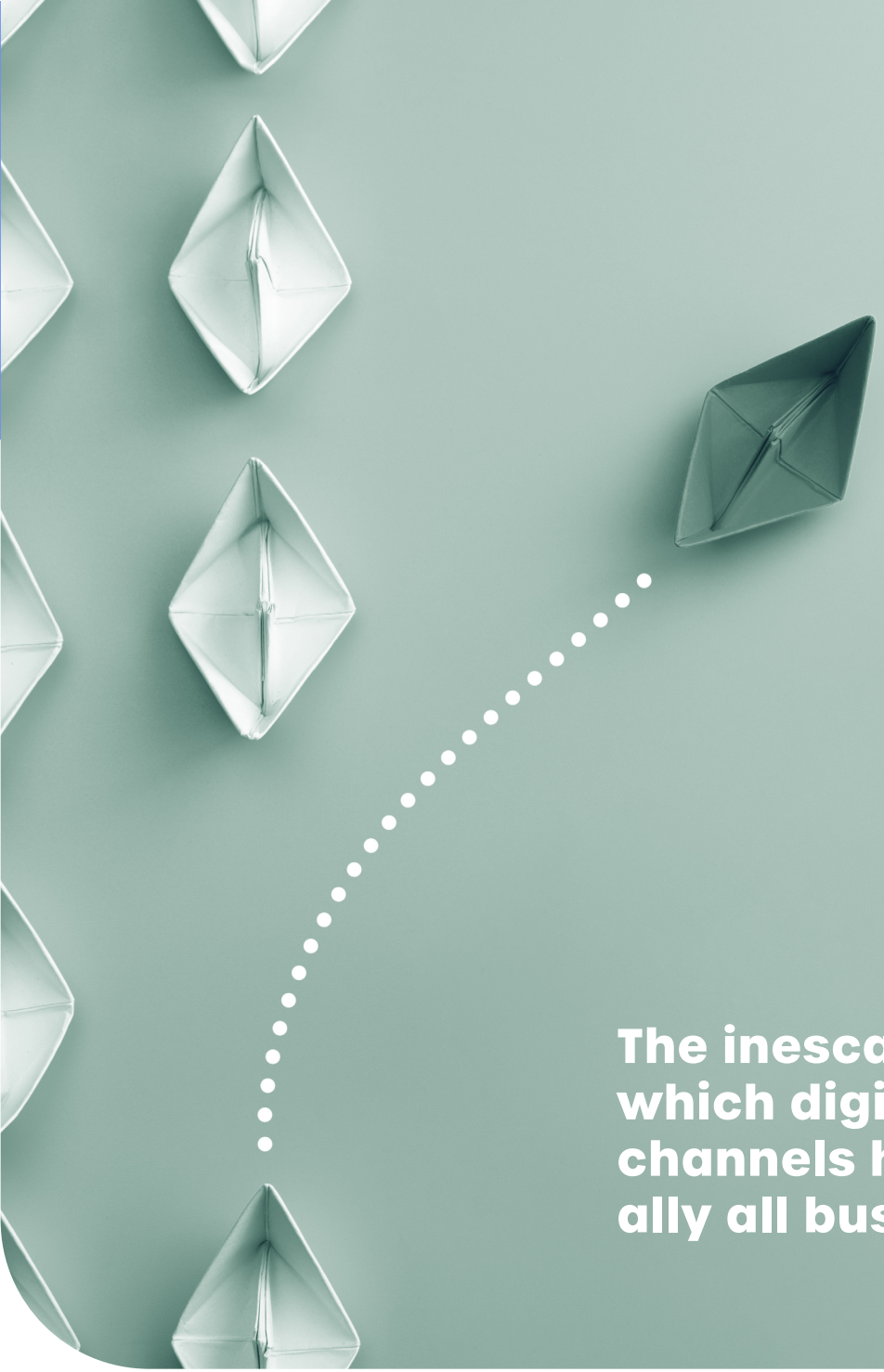
Biometrics are the latest entry into the authentication game and these biometrics such as TouchID and FaceID are considered strong authentication, but they suffer from two issues. First, modern smartphones support multiple fingers and faces (known as "alternate appearances") that are not linked back to a real-world person. This means that a spouse, family member, or other local actors can utilize this mechanism to get unauthorized access into corporate systems.

Second, when the device is initially set up, the identity of the person performing the action is not verified. This problem persists as devices get lost or upgraded. The device biometrics are enrolled again, and you are introducing the potential for threat actors to inject themselves into the process undetected.

One of the first challenges is recognizing passwordless MFA (the shiny object) from the business reality of enabling passwordless MFA across the enterprise. Drawing this delineation embraces technology as an enabler not just of identity and access management, but as a tool or facilitator to help IT control the roll out of passwordless across disparate IT and ease groups of users into their new user experience.

If we are to accomplish strategic advantage through this form of digital transformation, IT needs to engage LOB executives and key stakeholders in human resource management, customer acquisition, fraud management and all points at which users are onboarded or authenticated.

Naturally, this doesn't have to happen all at once, but it's essential to capture ready gains for the effort.



"Why?" Because misidentifying a user or allowing the wrong person access to digital services has been proven to be a significant productivity killer and can expose organizations to considerable risks and disruption. This makes knowing exactly who is logging in a mission-critical process that goes far beyond operational silos. When verified identity is so readily attainable, all sources of user acquisition, onboarding and engagement can and should be covered.

The inescapable truth is that the speed at which digital commerce and remote work channels have emerged has placed virtually all businesses at a digital crossroads. The challenge is to re-imagine user onboarding and authentication as core to the organization's ability to drive value. Because as this paper will describe, simply layering on another technology to eliminate passwords while ignoring fundamental shortcomings in legacy processes and technology exposes organizations of all sizes to needless cyber risks and drains to productivity.

The inescapable truth is that the speed at which digital commerce and remote work channels have emerged has placed virtually all businesses at a digital crossroads.

Tactical steps to prepare for change

Document applications, interfaces, operating systems, authenticators, user stores, and SSO

To gain a comprehensive understanding of the technology landscape, it is essential to assess the impact on users, the criticality of the applications, whether they are used on shared devices, and the potential risks associated with transitioning to passwordless authentication. This holistic approach ensures that organizations can make informed decisions and implement effective security measures that enhance their overall cybersecurity posture.

Itemize and prioritize systems and use cases

To achieve a successful passwordless deployment, it is critical to understand the variances in user journeys. This includes remote users, in-office users utilizing their personal devices, and those using corporate-issued devices. A thorough understanding of these variances is crucial in determining the most effective approach to passwordless authentication. By prioritizing both user needs and organizational security requirements, organizations can achieve a more secure and efficient authentication process.

Identify and categorize administrators and other groups of users

To ensure optimal security measures, it is essential to identify user privileges and associated risks to determine the appropriate level of authentication for each group of users. For instance, privileged access users require a higher level of authentication assurance compared to general users due to the sensitive nature of their activities.

Establish RACI engagement plan to inform and educate LOB leads and key stakeholders

To Identify stakeholders, including vendors and system integrators, mapped activities, requirements, and reporting structures ensuring clear lines of communication and deliverables. By taking a proactive approach to stakeholder engagement, organizations can build a collaborative environment that fosters effective communication and enhances project outcomes.

Frame communications plan

Establish a baseline and predetermined time frame for progress reviews with key stakeholders and communicate changes and progress to end-users. Then, ensure users receive a walk through of their journey, and embed a feedback loop for continuous improvement. This approach can help ensure that the program meets end-user needs and expectations, and ultimately leads to greater success in program management.

KEY CHALLENGE

Complicated Legacy IAM IT infrastructure

When we look at internal systems, there are three buckets of systems that all need to work together:

- **User Directories**
- **Authenticators, and**
- **OS and Applications**

Today, we do not have a secure way or even a remotely operational efficient way to accomplish this. Ever since users needed to login, we've had the concept of user directories or sources of truth for them to get into a system.

These are your user directories. Of course, the star of the show is Microsoft Active Directory, and as of the publication date of this paper many are moving to Azure AD. Over the past 10 years, many other prominent directories have popped up such as Ping, Forgerock, Okta, and we have many legacy systems from Oracle, Broadcom (formerly CA), IBM, and others.

Getting these to be 100% authoritative for all user data has always been a key challenge. In the late 90s Microsoft Active Directory was the main directory, and then every application had its own store, and we've replicated that model over the past 25 years.

Unfortunately, to access all these directories, single sign-on systems and custom applications, you need a username, password, and, of course, all kinds of different authenticators.

Virtually every user directory offers its own Authenticator, such as Microsoft Authenticator, Google Authenticator, Okta Authenticator, etc. But because they are not flexible enough, we have also deployed tokens, other standalone app-based authenticators, Windows Hello, Apple TouchID, and much more.

And why are we doing this? We use them to access all of our operating systems and applications. This creates complexity. Simply overlaying passwordless compounds complexity. Without addressing data quality or privacy this may provide backward compatibility of passwordless to what very well may be described as the legacy user authentication backbone of the enterprise, but it does little to simplify IAM infrastructure long term or reposition IT to manage customers, employees and various groups of users within one platform-agnostic instance.

Of course, nearly every organization is deploying single sign-on which helps reduce some of the burden. However, the single sign-on systems still need a username, password and 2FA. This creates an incredibly powerful vector for cyber attacks. We have seen these SSO systems become the target for hackers via the main signing certificate (i.e., the golden SAML Solar Winds attack) or by coercing administrative credentials from users.

With all of these directories, authenticators, and applications the legacy IAM infrastructure shows signs of stress, producing the lowest common denominator in terms of really understanding who the user is and giving threat actors multiple entry points obscured by complexity. No surprise cybercriminals log in as frequently or more often than they hack in.

KEY CHALLENGE

The Complicated Journey to go Passwordless

When multiplied by thousands of applications used by thousands of employees, contractors, partners and customers, managing users and then layering on passwordless becomes extraordinarily complex, even for the most sophisticated organization.

After decades of IT investment and years focusing on the integration, deployment, and end-user experience, this should come as no surprise. It's part of the reason help desk costs are exploding, particularly as password policies are evolving in light of increased vulnerabilities from the growing number of remote workers and customers on the go.

Viewed from this perspective, the actual technology to provide users with a passwordless feature pales in comparison to the organizational imperative to reduce systemic cyber risk, manage scarce IT resources, and in general, do more with less.

Without a comprehensive plan to get rid of 95% of passwords (as there will always be a few that just cannot be transitioned), passwordless projects tend to fail, and the net result is more tools and vendors added to the mix. While it makes sense to prioritize systems for passwordless access because this can drive early benefits that can fund downstream efforts, isolating attention to a few of the easier systems can offer short-term gains at the expense of long-term failure and a missed opportunity to create strategic advantage.

A comprehensive plan needs to address the various edge cases for passwordless across the enterprise, reduce the number of authenticators in use, free IAM architecture from platform-specific constraints and offer the organization a bridge to a web3 environment where a certified, standards-based IAM IT architecture can improve business agility, cut costs, improve security, and provide all users the modern convenience they expect.

Crafting a Vision

We want to use identity, instead of single sign-on authenticators, tokens, one-time passwords, secrets, and other tools to authenticate anytime, anywhere from any device.

This is what biometrics promise to do, but if we put a verified user identity at the center we then gain an important new construct in our IT arsenal that simplifies and helps control deployment, ultimately making it easier to train users for passwordless access and consequently easier for them to consume. This is a Web3 enabled, platform-agnostic identity easily accessible via a single API and certified to the highest industry specifications for identity (NIST 800-63-3), security (FIDO2 and iBeta) and interoperability (SAML, oIDC, oAUTH, RADIUS and more), devoid of proprietary, platform-specific protocols.

Along your multi-year, passwordless journey, we want to phase out the many fragmented authenticators giving you considerable operational resources back and saving potentially dozens of dollars per user per month that you are currently paying. We're also going to fix the broken user experience with a consistent, seamless experience along the way.

The definition and capabilities around identity have changed quite a bit over the past few years, but the Web3 definition of identity is very simple and, now, technically very possible. It is a combination of a user held and managed credential, otherwise known as a public-private key pair, matched to their real identity, and has undeniable proof of its use every time.

Think about your experience with a police officer or airport security agent. You present them with a credential, and they verify your physical appearance. This is all now possible today with an amazing remote experience that enables a digital connection with an extraordinary level of trust.

Many companies offer authentication via push messages, hardware tokens, one-time-code apps, etc. It is important for the new approach to accommodate those as well. These legacy authenticators will need to be phased out over time, so the new approach should upgrade to a single, certified standards-based authenticator.

We need a convenient way to roll out passwordless multi-factor authentication across the enterprise. This means it has to be easy for the users to consume and also not be a burden for IT staff to administer and deploy.

Another factor to consider is how identity authentication can and should be tailored to specific business and security objectives. To give one example, you may have a higher-risk application or a population of users, and you need to know, without a doubt, that this is the person you hired and prove it before you give them access continuously. It's important here to introduce as little transactional friction as possible.

A critical standard here is FIDO authentication and a biometric-certified platform such as that afforded by the iBeta PAD2 standard. Then, you'll want to consider the technology to be used to verify the identity of a remote user, either when they set up their account for the first time or perform a critical activity.

Consider this, when a user transitions to new systems, it's difficult to ensure the user's identity because this use case requires the use of a username and password. Building "Trust on First Use" (TOFU) requires special attention as there is little organizations can do to solve this problem. Binding a user's identity to their credential means the user is not simply tied to a device (like Windows Hello for Business) but their authentication is based on a verified identity, meaning every login, including the very first login, is quick, seamless, and secure.

There are hundreds of providers that do identity proofing. And that is part of the problem. They are typically standalone applications that are cobbled together and do not allow for either a turnkey deployment or enablement for your developers to embrace them to make your applications use identity properly. You want loosely coupled systems with a cohesive platform.

The highest digital identity standard available is NIST 800-63-3. But, depending on the use case, you'll also want to accommodate verification via a trusted phone number, a banking identity, and for workers, even by matching to a prior HR or security photo or previously authenticated account. The key here is flexibility and interoperability. You'll want to avoid custom, one-off integrations.

While you are forming your digital identity transformation strategy, there will be three other important considerations.

- **First, the technologies that you deploy need to keep the organization free from privacy issues.**

GDPR and other mandates need to be incorporated and not as an afterthought.

- **Second, ensuring the authenticity of a device will ensure users are utilizing only approved authentication methods.**

An example of this would be preventing users from trying to authenticate with a jail broken device. A well-formed strategy would attest to the authenticity of a device seeking to use authentication, which allows relying parties to check that a security key or other client device is genuine. In doing so, preventing spoofing attacks using counterfeit devices. The attestation of the device, authenticator, and keys offers enhanced security as it ensures an uncompromisable environment and helps prevent spoofing attacks.

- **Finally, as you mature your zero trust strategy, one of the most important pillars of zero trust is identity.**

The only way to do zero trust from an identity perspective is with real biometrics. If you can give your authenticator or one-time code to somebody else, it is not zero trust. You're probably not going to use real biometrics for your initial passwordless strategy, but it needs to be considered and incorporated into the plan. Identity pundits and analysts all agree that real biometrics (e.g., matching a live face or voice) will enable the future of authentication.

Tactical steps to craft your vision

Establish strategic imperatives

- Security
- User Experience
- Privacy
- Interoperability

Develop supporting detail technical requirements / specifications

- See Example

Determine KPIs and how ROI will be measured

Project Scope: Supported Use Cases

Now, instead of all the systems having a separate username, password, and custom 2FA tools, your users need to have one authoritative system with a common experience for accessing everything.

Maybe users are authenticating into Bing, federated apps, Okta, your legacy SSO, or trying to get into a workstation or a legacy VPN system. Let's give all users a consistent set of tools and a common authentication experience with flexible options.

The idea here is to not just give users the wallet in the form of an app-based or appless experience but a platform that can deliver to your employees and / or customers an entire range of convenient login experiences.

If you can give them an app either by embedding the platform in an existing app or by branding a white-labelled app, it is the most secure and rich experience that they can have. Depending on the application a user authenticates into and on the desired user experience, here are some examples of the ways we can then engage with them.

If you can give them an app either by embedding the platform in an existing app or by branding a white-labelled app, it is the most secure and rich experience that they can have.

First, we can send a push to the authenticator, where they tap and do Face ID. The right app can handle industry-standard one-time codes (i.e. 6-digit code generators) and also fall back to codes verified via email and SMS. Authentication can be upgraded to a "live selfie" when the risk of a digital interaction requires you to know at a high level of certainty the user identity.

The ability to work offline in any environment, such as on an airplane, needs to be supported. Authenticating into a workstation before connecting to the Internet, zero trust checks (such as checking for a jail broken or current patch level) also need to be supported.

But, what if the authentication device gets lost or stolen? Users need recovery options that have minimal impact on both the user and on the operational staff.

Users will need support for multiple personas or accounts inside of the same application. For example, most domain administrators have an administrative account and a regular user account. You could support many AD, SSH, X509, LDAP, and other credentials inside of the same authenticator.

One other very important feature inside of an app is the ability to reset your existing legacy passwords. As you go passwordless, passwords become used far less often, which is obviously the objective. However, once you come across a system that still relies on an AD login, for example, and has not been migrated to a passwordless experience, we have just created a tremendous amount of friction because now the user needs to figure out how to reset their AD password to get in.

With an app, this can be automated with the press of a button combined with their Face ID, closing the security loopholes of legacy self-service password reset tools that are both expensive and frequently targeted by threat actors. We can also reclaim the cost of these other password reset systems.

Lastly, the same device or app used for virtual access can and should be leveraged for physical access control systems such as Honeywell or Lenel. This enables a person to use their mobile device or smartwatch to tap a building card reader and get into the building with one common experience. No more plastic card keys!

Phishing Resistant MFA

With an identity platform packaged in either an app or appless experience, we have more than an authentication tool. Sure, capabilities such as QR code scanning, push notifications to mobile, FIDO-certified authentication and device biometrics give us the power to have phishing-resistant passwordless MFA at our disposal. But there's more.

With minimal effort, an identity platform can support a passwordless authentication experience into just about any web application for "Universal Web Login." Here, there is almost 100% certainty that authentication to some applications cannot be handled by industry-standard federation protocols. A key obstacle is that the various directory providers will have no chance at addressing all of these authentication needs. To succeed, you need a purpose-built identity strategy, not one cobbled together by vendors that do not leverage the latest in identity and privacy standards.

For phishing-resistant MFA access to these systems, you'll typically be looking for purpose-built connectors, and likely dozens of them that will allow you to make it as easy as possible to establish the initial passwordless authentication experience.

Of course, you can't count on 100% coverage here either, so make sure your approach has support for other tools such as one-time codes and platform authenticators (e.g., FIDO, Windows Hello, Yubikey, OTP).

Implement Change

With the vision, key challenges, and scope fully developed, we're ready to talk about implementation. Let's prioritize a passwordless MFA deployment to give the best chance at success because if you don't get the deployment right and take your IAM engineering, helpdesk, and business objectives into consideration, the deployment takes twice as long as it should or ends up failing. If, for example, early stumbles cause executives to revolt against the user experience, it's game over.

The first two steps in the journey, employee enrollment, and password reset, set the stage to let you move forward at any pace you desire. Enrollment is the obvious starting point. There are many ways to get users into the system, such as point-and-click invitations, bulk invitations, or self-service.

Password reset can be delivered out of the box. Practically speaking, once enrollment is complete, just about the only thing to do here is to let your help desk and users know about this amazing feature.

Next, by targeting the three most heavily used systems, early gains can be achieved. For most organizations, this will be virtual or personal desktops, remote access, and the single sign-on gateway. This often represents 80% of the password-based interactions for your users.

Not only does this produce early payback in reduced friction and genuinely excited users, but it will also lower your attack surface tremendously. Most importantly, these target systems allow you to deploy passwordless without impacting your existing authentication processes. It can be deployed in parallel and very rapidly.

Remember, people resist change, even if it's for the betterment of their login experience. So while no one likes passwords, they dislike change even more. So, consider a coexistence strategy for deployment. Provide a side-by-side login experience where users can choose to log in as before or passwordless. Allowing users to choose when to make the switch will improve the acceptance rate, and as laggards see the experience others have adopted, their move to passwordless will be out of excitement and curiosity vs resentment and resistance.

Once we have this scoped out and underway, a second and third phase can be determined to cover the entire organization. There are many changing applications that your users will constantly need to access. The beauty of moving authentication outside of the applications and single sign-on systems is it makes switching from one to the other a completely seamless operation from the user's perspective.

We have seen amazing successes, for example, where one VPN product is changed for another, and you avoid the pain of having to issue users a new username, password, and 2FA experience. Instead, users can simply scan a QR code and then scan their face to gain access. Otherwise, they don't even need to know that anything has changed. This makes it easy for both users and operational staff.

With verified identity, identity is proven at first and every access. The proof of identity over and over again in a very simple way and via a great user experience enables digital business at scale. The goal is to get workers and customers into a modern authentication experience (i.e., passwordless MFA, non-phishable MFA) and to do so with very high assurance that the user on the other end of the digital connection is who they claim to be. Verified identity is essentially the only way to do this.

This fulfills the end goal, which is to conduct business and transact online in much the same way we do in person, without disruptions, with minimal fraud and with the ability to manage to fraud targets utilizing fewer resources for manual reviews while avoiding the ever present threats of ransomware and data breach from credential-based attacks.

Review Progress and Analyze Results

When an organization decides to move to passwordless authentication, it is important to review and analyze the change management process to ensure that the transition is successful. Without tracking progress, there is little to prove the value of the investment. Based on our experience, the following are ways to track progress based on actual results:

Establish clear goals and metrics

Before implementing passwordless authentication, it is essential to define clear goals and metrics for success. This includes establishing baseline metrics for the current authentication system, the deployment timeline, helpdesk times, and administration cost, defining the target metrics for passwordless authentication (like adoption rates) and outlining the key performance indicators (KPIs) that will be used to measure progress. Overlooking this step will set a path where it would be difficult to determine the success rate of passwordless deployment.

Conduct user surveys and feedback sessions

It is essential to gather feedback from users to understand how the new authentication system is being received. This is a step often overlooked or skipped by IT teams. But for a successful deployment, it's critical to ensure users experience minimal friction or impact on their day-to-day workflow. This can be done through user surveys or feedback sessions, where users can provide insights into the user experience, ease of use, and any challenges they may be experiencing. The information gained here will ensure the long-term success of the move to passwordless.

Monitor performance metrics

Monitoring performance metrics such as login success rates, time to authenticate, and user adoption rates can help track progress and identify any issues that need to be addressed. These metrics are easily measurable, can prove time to ROI, and can also provide insight into the effectiveness of the passwordless authentication system overall.

Regularly review and adjust the strategy

Change management is an ongoing process and should be treated as such, and therefore it is essential to regularly review and adjust your passwordless strategy with the key stakeholders as needed. This includes identifying any areas where the authentication system may be falling short and implementing changes to address those issues. Consideration must also be made for new technologies, as they are considered and added to the stack, where they fit into the passwordless strategy. Regular reviews can also help ensure that the passwordless authentication system is meeting the organization's goals and objectives.

Connect with 1Kosmos

If you'd like to learn more about 1Kosmos BlockID solutions, Contact Us >>

About 1Kosmos

1Kosmos BlockID is a distributed digital identity platform supporting both business-to-employee and business-to-consumer services that easily integrates with existing operating systems, applications, and IT security infrastructure to perform strong, verified Identity Based Authentication – eliminating the need for passwords, one-time codes, and more. By simplifying identity infrastructure, 1Kosmos drives both cost savings and user convenience while securing businesses and individuals from the harm and inconvenience of identity fraud. The company is headquartered in East Brunswick, New Jersey.

For more information, visit www.1kosmos.com or follow @1KosmosBlockID on Twitter.