Passwordless 360°

Protecting Your Business, Empowering Your Users

cpl.thalesgroup.com

THALES
Building a future we can all trust

Contents

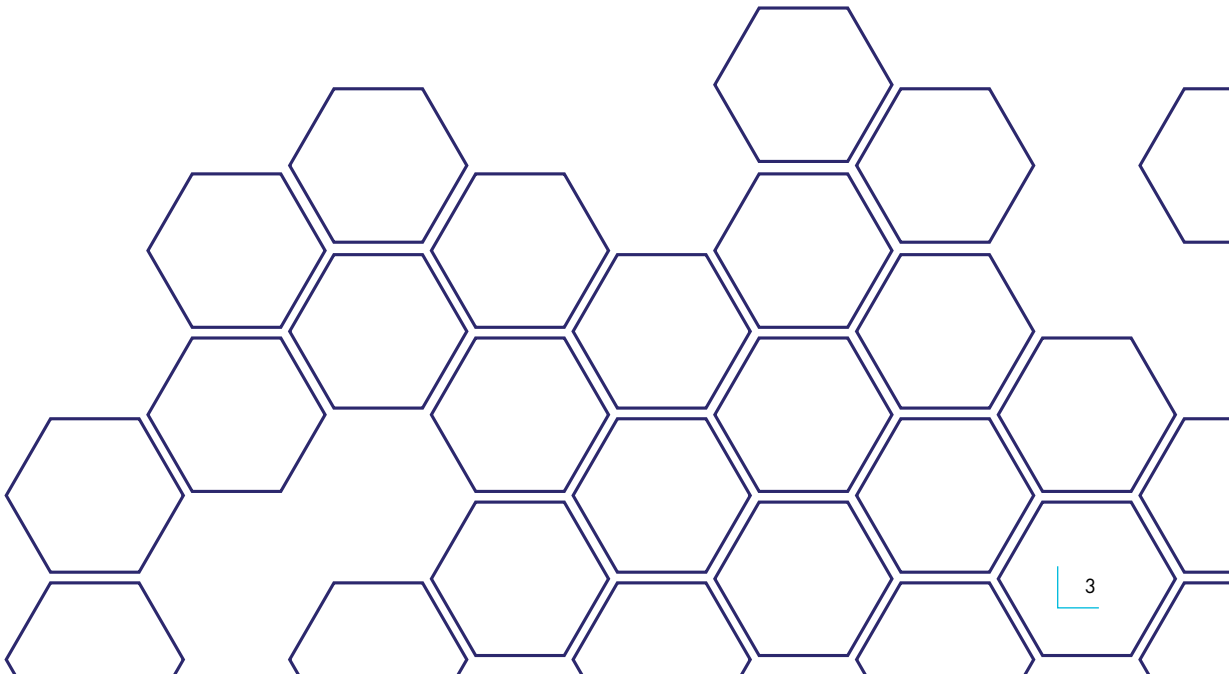
Executive Summary

Traditional password-based authentication is fundamentally broken. Relying on easily compromised secrets poses a significant security risk to individuals, organizations, and their extended ecosystems. The costs of data breaches, compliance violations, and lost productivity due to password struggles are staggering. Consumers, employees, and third-party users like suppliers or partners demand a secure and frictionless approach to digital interactions.

Passwordless authentication offers a transformative solution. Utilizing more robust methods like biometrics, hardware security keys, and user-friendly Passkeys eliminates the vulnerabilities inherent in passwords. However, organizations struggle to implement passwordless authentication at scale, leading to siloed and piecemeal implementations that fail to deliver on the passwordless promise. Maximizing the benefits of passwordless requires a holistic approach– Passwordless 360°.

This strategy extends passwordless beyond siloed use cases, encompassing users the entire business landscape. It empowers organizations to protect sensitive data, meet stringent compliance requirements, and gain a competitive edge. It offers a superior user experience that fosters consumer trust while streamlining employee login processes.

Embracing a Passwordless 360° strategy is an investment in a more secure and efficient future. By proactively transitioning to this model, organizations can stay ahead of evolving cyber threats, enhance operational efficiency, and meet the rising expectations of a digitally connected world.



The Authentication Paradox: Security vs. Convenience

For decades, passwords have been the primary means of authentication. However, this reliance exposes critical flaws: outdated technology, inherently weak security, and the limitations of human behavior. These factors converge to make passwords a major liability for individuals and organizations alike.

Vulnerabilities abound in password-based systems. Users frequently choose weak, easily guessed passwords, or reuse the same password across multiple platforms. This opens the door to brute force attacks, where cybercriminals can systematically try different password combinations until they succeed. Human error adds further risk. Phishing scams, social engineering, and other tactics prey on users' trust, tricking them into revealing passwords.

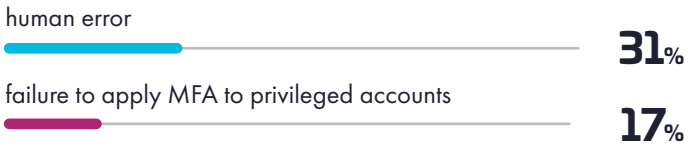
Passwords highlight a dangerous intersection where outdated technology, flawed processes, and human limitations collide to undermine security. Their reliance on knowledge-based secrets burdens users to remember unique, complex passwords for every account. This inevitably leads to insecure practices, creating a fertile ground for cyberattacks.

68% **of breaches involve a non-malicious human element.**

31% **of breaches in the last decade involve stolen credentials.**

60 seconds **is the time required for a person to fall for a phishing email.**

Causes Of Cloud Data Breaches



Source: Thales 2024 Data Threat Report

The Consumer Conundrum

Consumers struggle to create complex, unique passwords for a multitude of online accounts. Password fatigue leads to password reuse, a critical security lapse. When a data breach involving a reused password occurs, consumers face a domino effect of compromised accounts, financial losses, and identity theft. The erosion of trust with service providers further compounds the issue.

The Workforce Challenge

Within organizations, weak password hygiene significantly threatens sensitive data and critical systems. Many businesses still rely on simple usernames and passwords, making phishing campaigns a serious security (and trust) issue. Phishing attacks continue to exploit human error, tricking employees into revealing passwords or clicking on malicious links. A compromised employee account can be a springboard for attackers to gain access to an entire network, potentially disrupting operations and causing significant financial damage.

Even organizations that have migrated their email to cloud services, such as Microsoft 365, are still susceptible because, in most cases, cloud-based email and other cloud services are only protected by simple passwords. According to the FBI, cybercriminals are earning $2.9 billion from business email scamming.[1]

Xfinity Data Breach:

36m

In December 2023, Xfinity, a Comcast business, suffered a breach where the data of roughly 36 million people was exposed. The data included names, contact information, account usernames, and passwords, among other sensitive data. As a result, even the customers who weren't affected by the hack were forced to change their passwords, leading to disgruntled customers. (ref: CBS News)

MailChimp Breaches:

3attacks

MailChimp, an email marketing company, suffered from three data breaches in a span of 12 months, arising due to social engineering attacks. The attacks happened by phishing employees and stealing their credentials. (ref: ComputerWeekly)

1 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

The Third-Party Risk

The interconnected nature of modern business extends beyond the internal workforce. Reliance on third-parties like partners, vendors and suppliers introduces additional security considerations. The Verizon DBIR 2024 report[2] indicates that 15% of data breaches involved a third-party. Weak password practices by external partners can create exploitable entry points for cybercriminals. A breach suffered by a vendor can ripple across the supply chain, impacting multiple organizations and exposing vast amounts of sensitive data.

UK Metropolitan Police Service supplier breach

47k

The UK MPS suffered a data breach of 47,000 officers and staff due to unauthorized access to the IT system of a Met supplier. The breach was highly sensitive as it revealed the names and photographs of undercover officers, leading to significantly endangering their lives. (ref: CPO Magazine)

2 **https://www.verizon.com/business/resources/reports/dbir/**

The Passwordless Imperative

The ever-growing volume of data breaches and the sophistication of cyberattacks necessitate a move beyond passwords. Passwordless authentication offers a robust solution, mitigating the risks associated with traditional methods and generally relies on more robust methods like biometrics, hardware security keys, and possession-based factors. This minimizes the attack surface, making it exponentially more difficult for malicious actors to gain unauthorized access.

Businesses stand to gain considerably by embracing a holistic Passwordless strategy that encompasses all stakeholders – consumers, workforce, and third-party partners. Benefits include:

- **Enhanced Security:** Drastically eliminating passwords reduces the most common attack vectors.
- **Improved User Experience (UX):** Passwordless methods create a seamless, frustration-free login experience.
- **Significant Cost Reduction:** Organizations save on help desk time spent on password resets and the potential financial impact of a breach.

Despite growing awareness of passwordless advantages, many organizations fail to realize its full potential due to fragmented implementation approaches. Departmental silos often lead to isolated passwordless projects. For example, product teams might focus on consumer-facing authentication to enhance user experience, without coordinating with IT security who manage workforce authentication. Conversely, IT security might bolster workforce logins for higher security without addressing external user vulnerabilities.

This piecemeal strategy exposes organizations to severe risks. Uncoordinated deployments open significant attack surfaces. Even if internal workforce authentication is robust, neglecting external users (e.g., customers and partners) can undermine overall security. Disjointed approaches also hinder cost savings and operational efficiency, as they may require multiple solutions and lack centralized management.

To truly harness the power of passwordless authentication, organizations need a holistic strategy. This involves aligning consumer and workforce authentication and ensuring adaptive security standards across all user types. A strategic approach enables centralized policy control, streamlined user experience, and maximized cost benefits.

The Passwordless Tipping Point

The case for passwordless authentication extends far beyond mere security benefits. A confluence of factors drives a paradigm shift, making this the pivotal moment for organizations to make a strategic move. Let's examine why the landscape is ripe for passwordless adoption:

The Evolving Threat Spectrum: Traditional perimeter-based security models can no longer keep pace with the sophistication of modern attacks, paving the way for identity-centric security models. Ransomware campaigns weaken organizations, while supply chain attacks highlight the far-reaching impact of third-party vulnerabilities. Passwords represent a prime target, and a proactive stance means strengthening the most vulnerable link in the chain.

The Cost of Compromise: Data breaches exact a staggering financial toll. Beyond compliance penalties, organizations face lost productivity due to downtime, irreversible reputation damage, and missed opportunities due to stalled growth initiatives. The costs can quickly spiral out of control and erode long-term competitiveness. Passwordless adoption represents a proactive investment that significantly mitigates these risks.

Compliance as Catalyst: Stringent regulations like GDPR, CCPA/CPRA, and industry-specific standards like PCI DSS 4.0 emphasize the need for robust identity and access management. Passwordless authentication offers a compelling method to demonstrate compliance while reducing the business risks associated with data breaches.

User Expectations Reshaped: Consumers have come to expect seamless digital experiences across platforms, bleeding into expectations for workplace interactions. Password resets, frequent lockouts, and complex password rules are significant sources of employee frustration, impacting productivity and morale. Passwordless offers a way to meet user demands for convenience without compromising security.

Technology in Lockstep: The maturation of FIDO standards, widespread adoption of biometric capabilities on personal devices, and the emergence of consumer-friendly Passkeys demonstrate the industry-wide push for passwordless solutions. Technology is no longer the barrier; it's the enabler of a more secure and user-centric authentication model.

This shift is about more than just replacing passwords; it represents a fundamental change in how we approach user experiences for building digital services.

Passwordless authentication represents a technological leap that addresses the inherent limitations of passwords. It leverages stronger forms of authentication, offloading the burden from users and onto more robust systems. Passwordless solutions can break the chain of exploitable weaknesses by streamlining processes and removing the need for human recall, protecting users and organizations.

Organizations that embrace passwordless authentication position themselves as trailblazers, gaining a competitive advantage in security, user experience, and operational efficiency. Delaying this transition only creates more opportunities for adversaries and risks falling behind in an inexorably connected world.

Your Passwordless Toolkit: Technical Overview

Passwordless is exactly what the name implies – the absence of passwords. However, not all passwordless authentication methods are created equal. Here are a few examples to illustrate the different shades of authentication.

Biometrics: Fingerprint scanners, facial recognition, and iris scans offer convenient authentication. Note: it's important to select biometric systems that mitigate spoofing risks (e.g., advanced liveness detection) and carefully consider privacy implications.

FIDO Security Keys: These hardware tokens (USB, NFC, Bluetooth) provide robust multi-factor authentication. FIDO2 protocols offer strong phishing resistance. Consider vendor options and support for both FIDO U2F and the newer FIDO2/WebAuthn standards.

Synced Passkeys: This emerging technology leverages platform-based authenticators, simplifying passwordless access across devices. Passkey's cryptographic architecture enhances security and user experience.

Mobile Authentication Apps: Apps like MobilePASS+ generate one-time codes or handle push-based approvals. Ensure the app uses secure communication channels and consider biometric protection for the app itself.

Certificate-Based Smart Cards and Tokens: Immune to phishing attacks, like FIDO security keys and Passkeys, X.509 certificate-based authenticators provide a high level of assurance when accessing sensitive data hosted in legacy systems not supporting FIDO.

Pattern-Based Authentication: A convenient authentication solution that overcomes the weakness of passwords without the need for software to be installed or hardware to be provisioned. The end user just needs to remember a pattern on a grid instead of a password or a PIN code.

PKI to FIDO Migration

Hybrid Tokens: Industry experts recommend a phased transition, allowing for existing PKI infrastructure alongside FIDO adoption. Hardware tokens supporting both FIDO and PKI standards ease migration for organizations and users. In addition, organizations can benefit from the best of PKI, combining authentication with digital signature or file encryption use cases.

For a comprehensive list of available passwordless authentication options offered by Thales, see our portfolio here.

Passwordless Across Your Business Ecosystem

The transformative potential of passwordless authentication is best realized when organizations break down silos and embrace a holistic, Passwordless 360° strategy. This approach transcends the tendency to address consumer logins, workforce security, and third-party access in isolation. While each domain has distinct drivers, unifying these efforts unlocks technological streamlining, operational efficiencies, and more significant cost savings and maximizes the benefits of passwordless security.

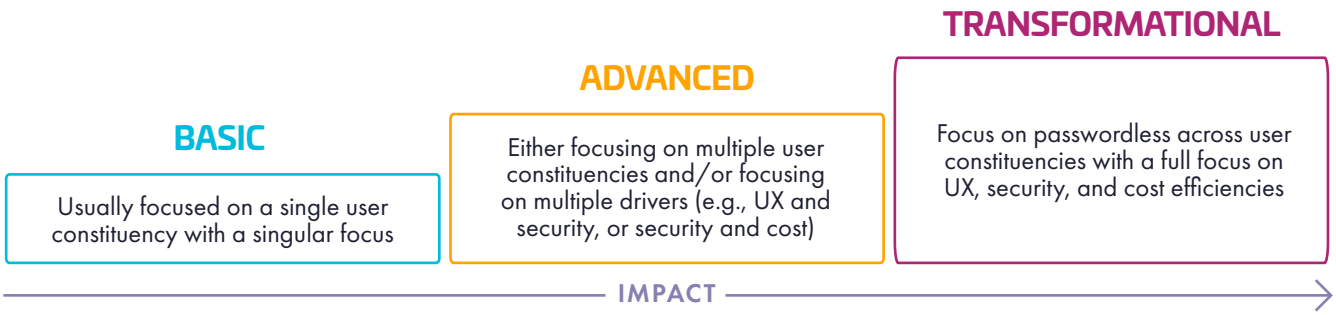


Figure 1: Passwordless authentication models

Basic passwordless implementations often operate within departmental silos. This fragmented approach might prioritize consumer login convenience or workforce security enhancements in isolation. While these initiatives have merit, they fail to optimize security, user experience, and operational efficiency across the organization. Overly strict security for all users can introduce unnecessary friction, while isolated improvements neglect other vulnerable areas.

The Passwordless 360° Approach

The Passwordless 360° approach provides a comprehensive framework for planning and evaluating passwordless implementations. Key steps include:

1. **User Ecosystem Mapping**
   Chart internal and external users (employees, customers, partners, suppliers). Evaluate their access levels, transaction types, and associated data sensitivity. This exposes potential security gaps in current and planned passwordless coverage.

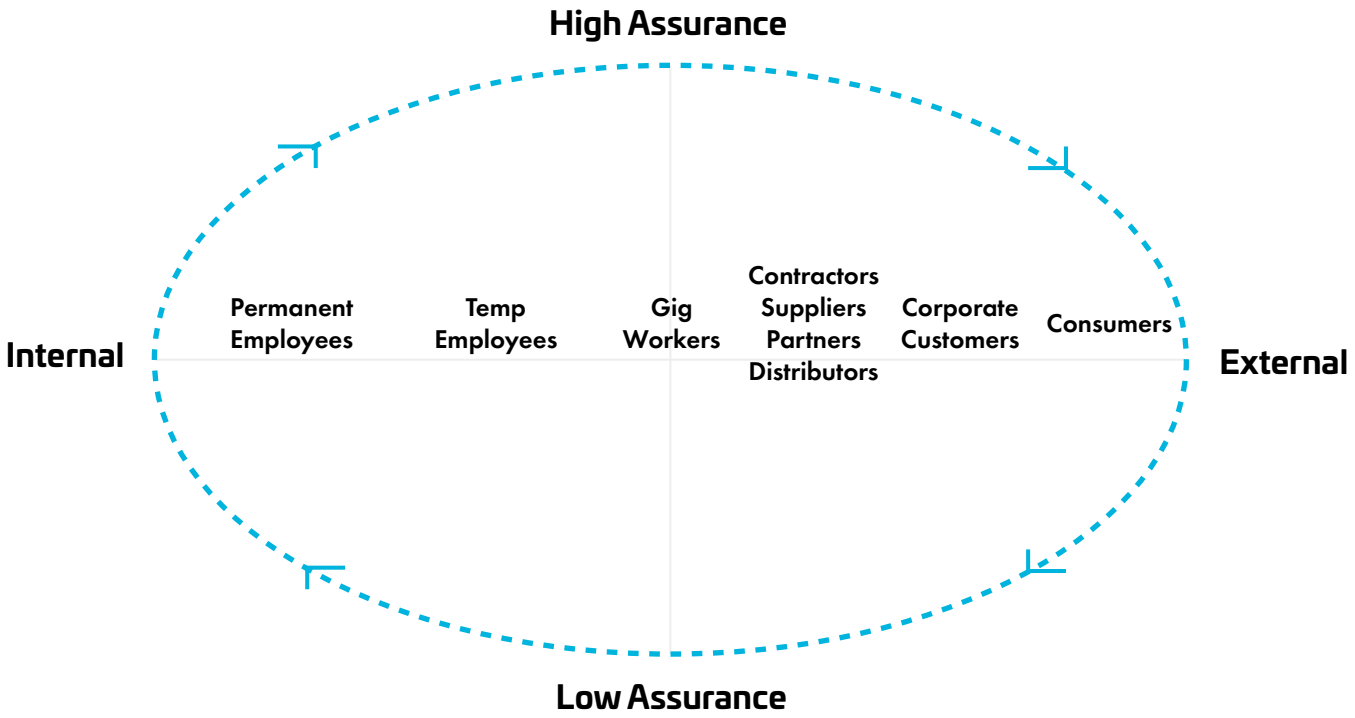


Figure 2: User ecosystem mapping

2. Risk-Based Assurance Levels

Determine appropriate authentication strength for each user group. High-risk scenarios necessitate robust multi-factor (e.g., hardware keys + biometrics) while streamlining low-risk access enhances convenience.

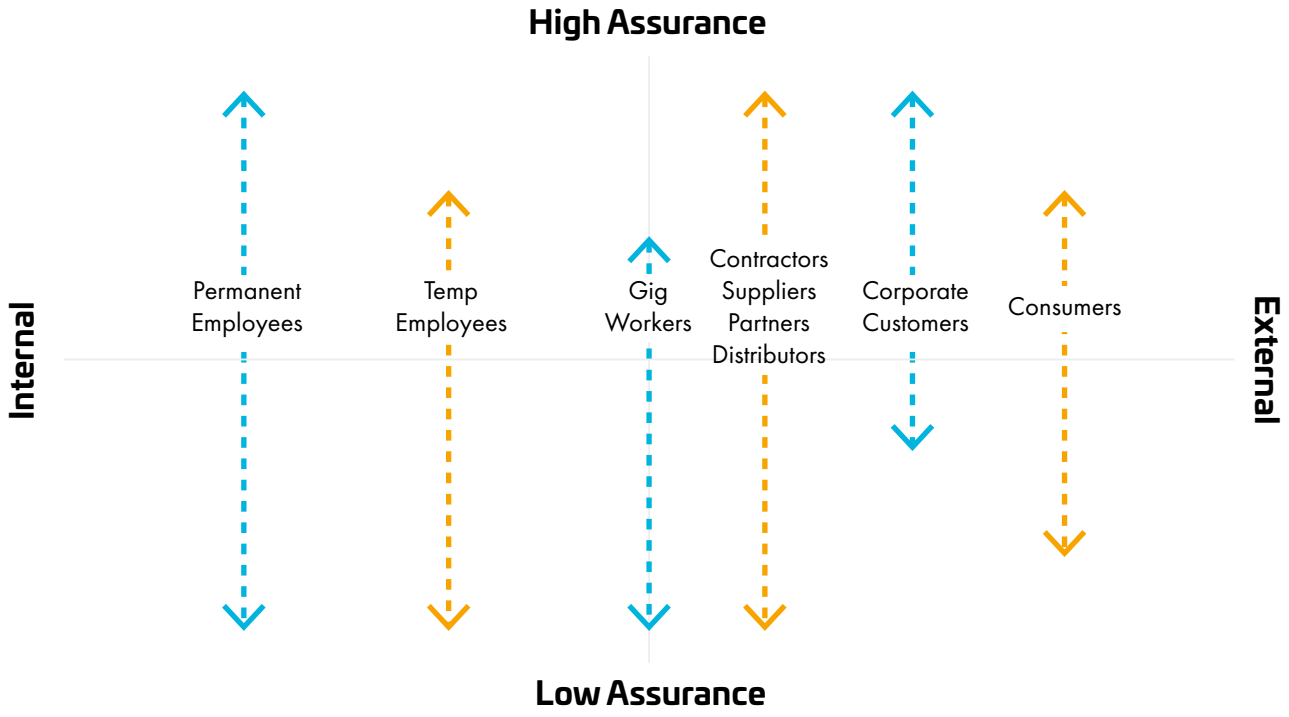


Figure 3: An example of mapping the spread of assurance levels needed for different types of user constituencies

3. Gap Analysis

Overlaying existing passwordless deployments onto the map highlights remaining vulnerabilities. For example, strong authentication for internal supply chain staff might not address equally sensitive access by external collaborators.

The Passwordless 360° model is customizable. For example, a Y-axis may represent user experience (UX) tolerance. Businesses can map user groups based on their sensitivity to friction. This informs decisions on where seamless login methods are paramount and where stricter security is acceptable. Organizations may also define the Y-axis to represent the password reset costs and analyze helpdesk costs associated with different user groups. This will highlight areas where passwordless will generate significant operational savings.

Overall, the Passwordless 360° model empowers IT leaders to visualize complex passwordless needs, justifying investment to stakeholders and prioritizing a phased rollout for maximum impact.

Let's examine how Passwordless 360° strengthens each pillar of the business ecosystem.

Workforce Authentication

Modern organizations must accommodate a diverse range of identities within the workforce – full-time, part-time, remote, and deskless workers, all with varying device needs. The correct passwordless authentication implementation offers the adaptability to meet these needs without compromising security. However, phasing out passwords requires careful orchestration to ensure a seamless transition away from legacy authentication systems, boosting adoption and minimizing user frustration.

A passwordless approach also aligns seamlessly with BYOD (Bring Your Own Device) policies, where robust authentication methods become critical for mitigating risk in complex device landscapes. Notably, the gig economy demands agile and secure techniques for onboarding and offboarding contractors and freelancers, and passwordless mechanisms ensure smooth and auditable access control.

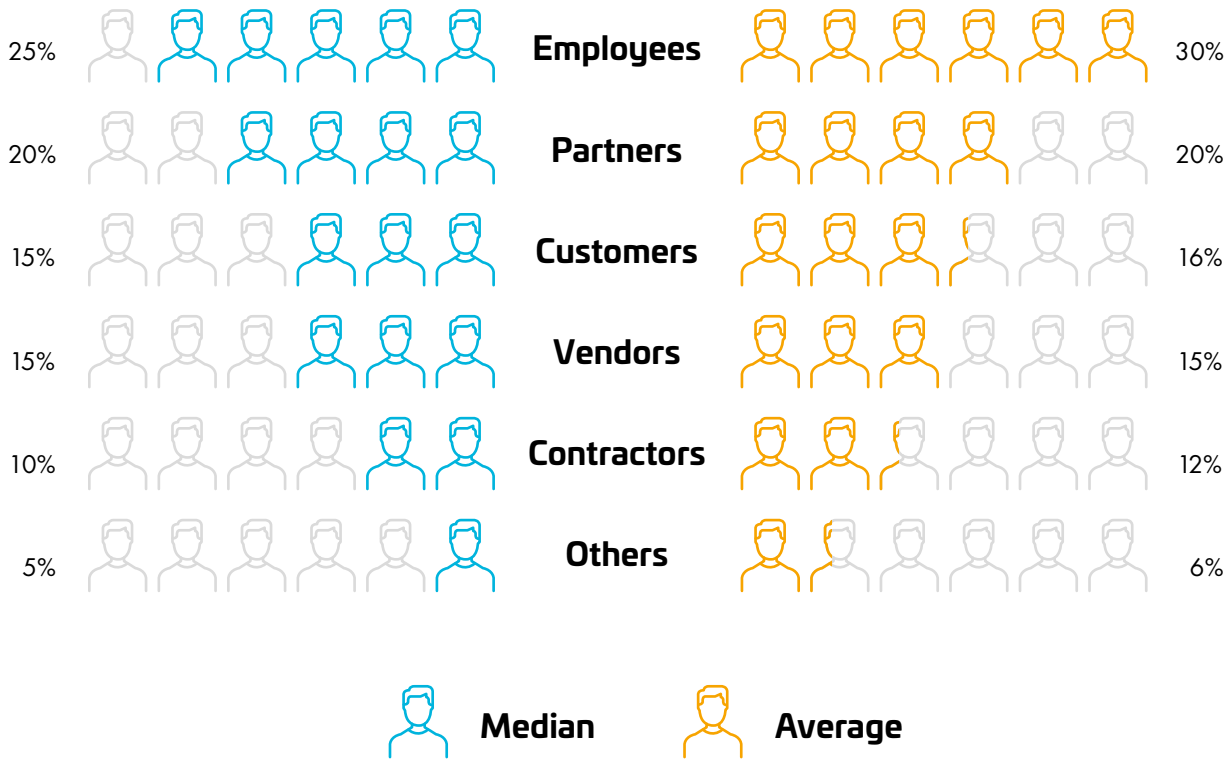
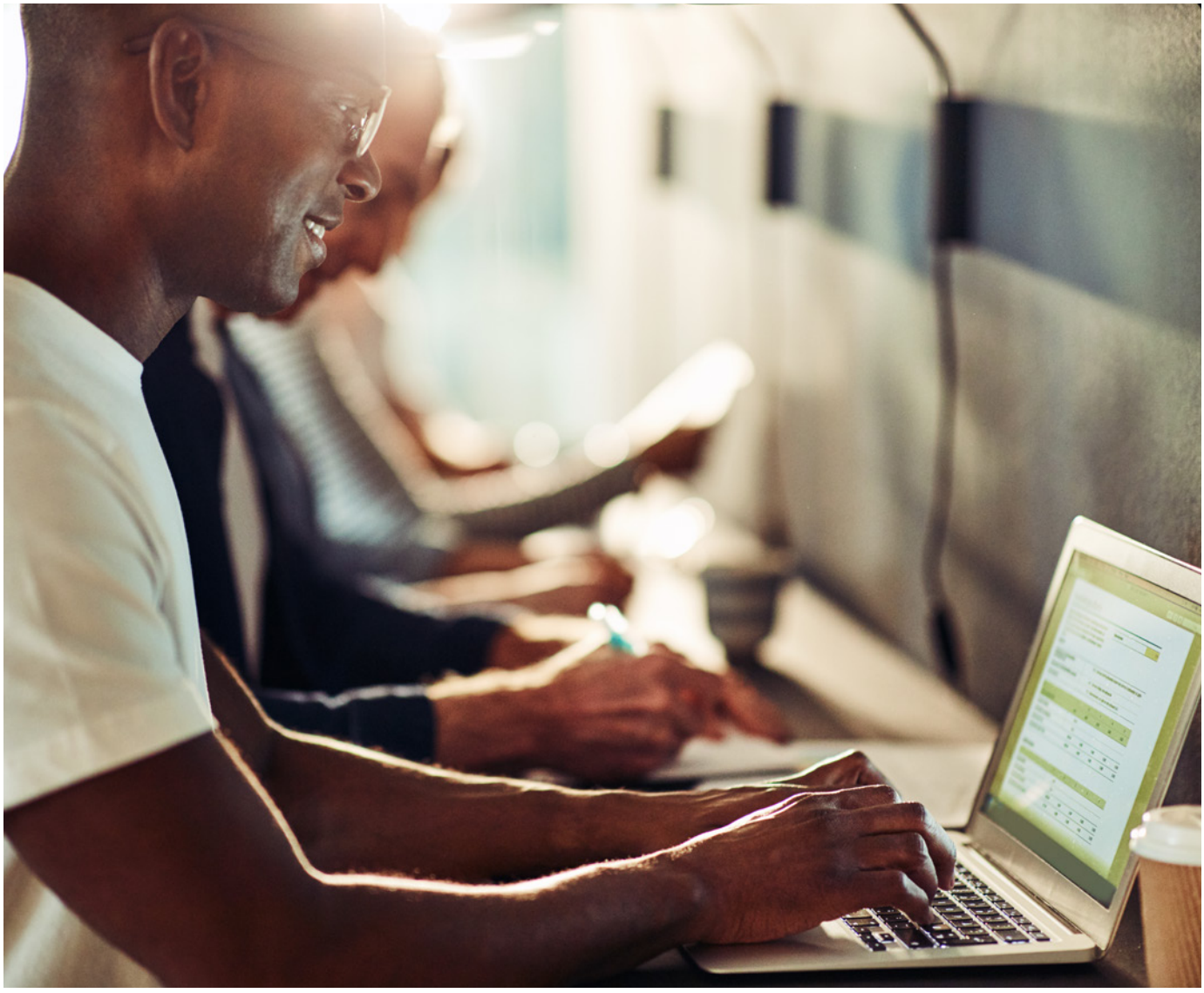


Figure 4: Identity Diversity in Modern Businesses. Source: Thales 2024 Data Threat Report

Passwordless authentication and Passkeys bring a measurable positive impact on an organization's security, IT, and business operations. A recent survey revealed that 65% of people reuse passwords across accounts, and nearly half hadn't changed their passwords in over a year, even after a known breach[3]. Growing awareness of this fundamental security flaw has made passwordless authentication, including Passkeys, one of the biggest trends in cybersecurity.

Fully passwordless authentication — where no password or similar secret is shared between the person and service — is far more secure than password-based authentication. Credentials never leave the user's device and are not stored on a server, so they are not vulnerable to phishing, password theft, or replay attacks.

3 https://techreport.com/statistics/password-reuse-statistics/



Passwordless Windows Logon

Protect the Edge

Before accessing any business applications, users must authenticate themselves on their desktop, laptop, or console, and typically, the only security measure in place for these enterprise systems is a password. Yet, protecting the edge is critical as a desktop provides access to numerous applications and data that users may have saved on the local drive, and even communication apps can be used to stage attacks.

One Solution, Many Secure Interactions

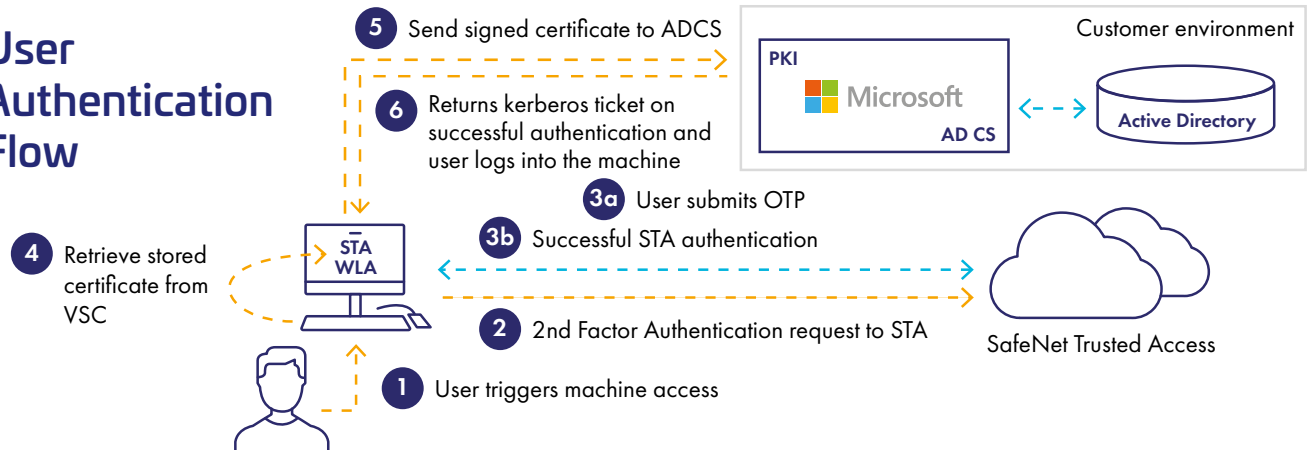
Organizations need one integrated solution that provides passwordless MFA from OS login to the user's remote applications, including Remote Desktop Protocol (RDP). The solution needs to be flexible enough to accommodate the organization's particular needs and provide a consistent user experience regardless of the method used for authentication. It should not burden the user by requiring them to authenticate multiple times.

Thales SafeNet Trusted Access: Your Passwordless Windows Logon Ally

Thales SafeNet Trusted Access provides passwordless, phishing-resistant MFA that begins at Windows Login and further augments the secured access of a SafeNet Agent for Windows Logon-protected machines by eliminating the AD password for machine access use cases. Enhancing the enterprise's security posture further eliminates end-user friction through an excellent end-user experience. End-users are no longer required to manage or remember their passwords.

- MFA by design for online and offline use cases
- Supports on-prem and hybrid AD deployments
- Supports all STA OTP authentication methods
- Supports SSO for web applications and extends the passwordless experience through SSO
- Easy to adopt in an existing landscape

User Authentication Flow



Securing Third-Party Access

Third-party relationships are notorious sore points for businesses, as breaches increasingly originate from supply chain vulnerabilities. A passwordless strategy allows organizations to extend frictionless yet robust authentication to partners, vendors, and suppliers. This eliminates the risks of shared secrets or weak passwords, streamlining collaboration and enhancing compliance. More robust third-party identity management bolsters regulatory confidence and protects sensitive data assets across the extended enterprise.

Passwordless for the Consumer

Finally, the consumer-facing side of the business stands to gain immensely from adopting passwordless technologies. Passkeys epitomize this shift – a familiar, intuitive, and remarkably secure way for customers to interact with digital services. This leads to higher conversion and lower cart abandonment, fostering trust and loyalty in an era where privacy concerns are paramount. Businesses that position passwordless as a commitment to both security AND superior customer experience can gain a clear competitive advantage. It is worth noting, though, that not all types of Passkeys are created equal. In fact, in certain regulated industries, such as banking, synced Passkeys may not provide sufficient assurance levels to comply with regulations like PSD2.

By embracing Passwordless 360°, organizations shift away from a reactive posture towards a proactive security model designed for the challenges of an interconnected world.

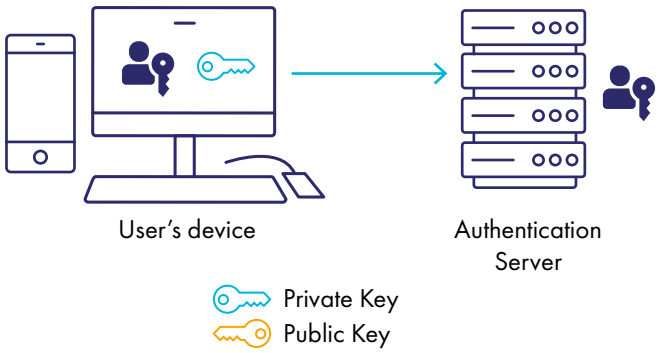
Passkeys: A Passwordless Future

Say goodbye to passwords!

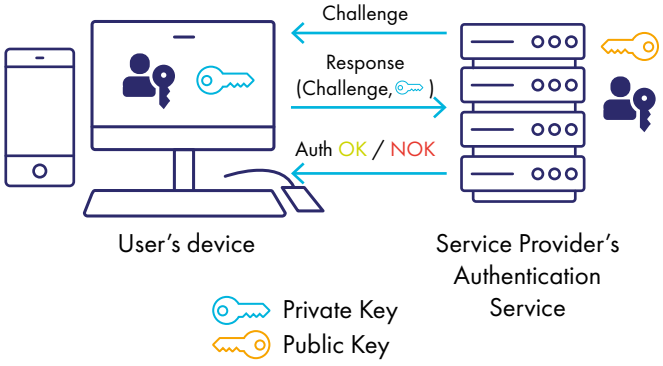
Backed by the FIDO Alliance, Passkeys are **secure credentials** stored on your device that replace the need to remember complex passwords for online accounts. Passkeys are cryptographic credentials that binds a user with a service. It consists of two keys: public and private. Unlike passwords, Passkeys are always strong and phishing-resistant. Major websites and apps already offer Passkey support, including Adobe, Amazon, Microsoft, Google, LinkedIn, Nintendo, Nvidia, and others.

How it Works:

Creation: After successful biometric verification, a Passkey is generated on your device. Websites or apps help you generate a unique public-private key pair. The private key is securely stored on your device; the public key is sent to the website.



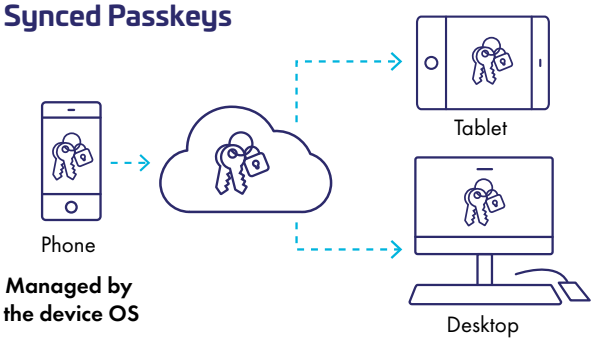
Login/Authentication: To sign in, you authenticate with your device (biometric, PIN, etc.), which uses the private key to prove your identity. After successful biometric verification, the authentication server sends a random challenge to the device. The device generates a cryptographic signature to the challenge with the private key of the Passkey and sends it back to the authentication server. The Authentication server verifies the response from the device using the public key and delivers an OK/NOK response to the authentication attempt.



Two Flavors:

Like other authentication methods, not all Passkeys are created equal. Passkeys can be implemented in two flavors: synced Passkeys and device-bound Passkeys.

Synced Passkeys

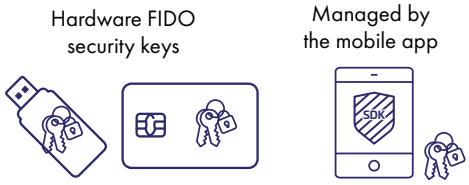


Managed by the device OS

Synced passkeys are exported to the cloud and propagate to other devices

Great for **Password Replacement**

Device-bound Passkeys



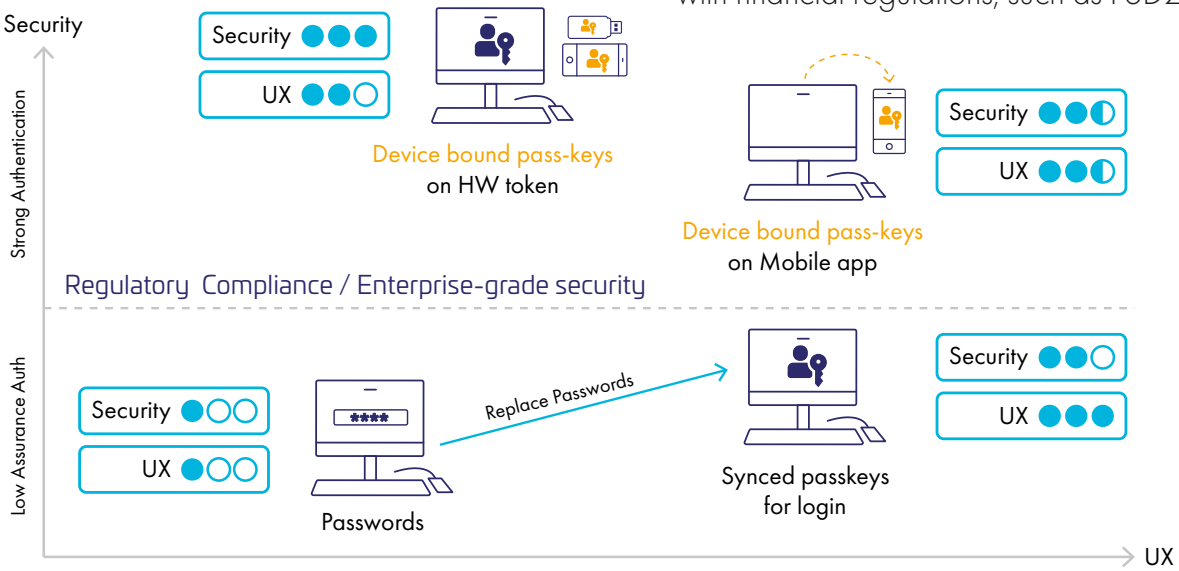
The private key never leave the device

Great for **MFA/SCA**

Synced Passkeys: Backed up to the cloud, allowing access across multiple devices for a seamless multi-device experience. Synced Passkeys are ready for mass adoption, as they offer a great alternative to passwords.

Device-bound Passkeys: Live on a single device and offer convenient login for local accounts. Unlike synced Passkeys, device-bound Passkeys provide a much higher level of assurance.

Combining synced with device-bound Passkeys: Synced (or multi-device) Passkeys provide a seamless user experience and better security than passwords. Synced Passkeys, however, do not reach the level of protection required by most financial regulators for Strong Customer Authentication (SCA). This is why, for SCA, banks should also enable device-bound Passkeys, using synced Passkeys for login and view use-case and relying on device-bound Passkeys on financial transactions for higher assurance. This joint implementation example of synced and device-bound Passkeys improves security and guarantees compliance with financial regulations, such as PSD2.



The Implementation Blueprint: Your Passwordless Journey

Depending on the industry and the sensitivity of data that is being exchanged, the passwordless mechanism needs to be adapted. A knee-jerk reaction to implementing passwordless is to resort to FIDO Security Keys. While these are arguably the best options for authentication, there are adjacent use cases that might not make it the most usable option. Take the example of factory workers that might require a badge for physical access or sometimes even rely on a zero-factor mechanism on the factory floor. Another example could be in the pharmaceutical or banking industry where sensitive data may need to be encrypted and digitally signed before being transmitted between multiple parties. In such scenarios, relying on PKI is a much better alternative, as it still gives you a phishing-resistant passwordless authentication mechanism while allowing you to leverage PKI for the encryption and digital signing applications.

Embarking on the passwordless journey requires a considered approach that goes beyond simply adopting new technologies. Here's a blueprint for a successful implementation:

Planning Essentials

Stakeholder Collaboration: Secure executive buy-in and foster cross-functional cooperation from the start. Identify stakeholders across IT, such as security and risk management, UX/CX teams, product managers, and other relevant departments. Craft a compelling business case that demonstrates the ROI of passwordless, clearly outlines cost implications, and anticipates the need for change management initiatives. Establish a steering committee to maintain alignment and support throughout the transition. Use the Passwordless 360° mapping to align stakeholders and executives.

Strategic Prioritization: Success hinges on identifying high-impact use cases from the beginning. Analyze your authentication workflows, pinpoint current weaknesses, and consider critical systems housing sensitive data or those prone to attacks. Carefully designed pilot programs offer initial proof of concept within well-defined environments. Focus on areas where passwordless will deliver the most impactful security improvements or significant user experience gains.

Authenticator Selection: Choose authenticators that align with your organizational needs. Evaluate compatibility with devices (considering both built-in biometrics and external hardware options), the technical ability of your users, and budgetary constraints. Assess vendors thoroughly, considering their security credentials, usability, and overall cost models.

Authenticator Life Cycle Management: Consider your approach to managing passwordless authenticators throughout their life cycle, including activation to end-of-life processes, and how you plan to assist users who have forgotten or lost their authenticators. Would you rather have IT maintain control of this management, or would you prefer to decentralize and empower end users with various operations? By addressing these questions, organizations can determine the most suitable authenticator management platform that aligns with their requirements.

Understanding Authentication Factors

Not all logins are created equal! Understanding the different authentication factors strengthens your cybersecurity posture. Here's a quick breakdown:

Zero Factor - No verification required. A simple signal, like presence detection, can be used for granting access to a resource.

Single Factor (Something You Know) - Basic password protection. Vulnerable to breaches and stolen credentials.

Multi-Factor (Something You Know + Something You Have + Something You Are) - Strongest defense! Combines knowledge (password) with possession (FIDO security key) or biometrics (fingerprint) for a layered approach.

When selecting an authentication model, ensure it is aligned with business needs, data sensitivity, and user experience expectations.

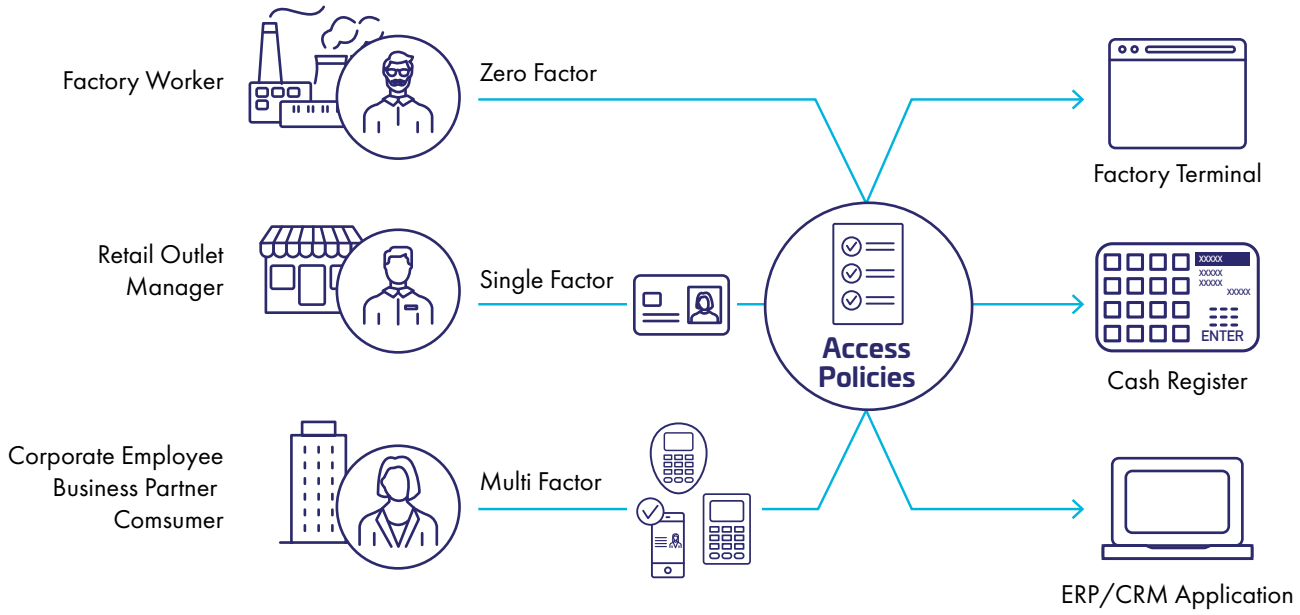


Figure 5: Authentication Journeys

FIDO Key Management

Deployment approach → / Migration ↓	Decentralize FIDO key life cycle	Control FIDO key life cycle
	Self-Service Driven	Admin Driven
PKI to FIDO	Hybrid PKI/FIDO keys + SafeNet Trusted Access + FIDO key Manager	Hybrid PKI/FIDO keys + SafeNet Trusted Access + VSEC:CMS
Password to FIDO	FIDO keys + SafeNet Trusted Access + FIDO key Manager	FIDO keys + SafeNet Trusted Access + VSEC:CMS

The need for FIDO key life cycle management

To effectively deploy FIDO authentication, organizations must define how they will deploy FIDO keys to their employees and how to manage them. The primary consideration should be how to deploy the keys securely so employees can use them quickly to access multiple digital resources. Do they want to delegate the enrollment to the end user or keep control of the management to ensure a highly secure onboarding? How do they deal with lost or forgotten FIDO keys?

A solution adapted to each approach

Thales helps organizations whatever their deployment and migration approach.

For organizations adopting FIDO with a decentralized approach, Thales provides a utility tool, the SafeNet FIDO Key Manager, that end users can download on a variety of devices to configure the FIDO key (e.g., set up or change the PIN) and can self-activate the key within SafeNet Trusted Access to access web applications.

For organizations migrating from PKI to FIDO, who want to control the FIDO key life cycle in the same way they manage their PKI credentials, SafeNet Trusted Access combined with VSEC:CMS allows them to let IT administrators control the FIDO key enrollment and secure access to their web apps in no time.

Deployment Best Practices

Communication and Training: Proactive communication and comprehensive user training are crucial. Develop clear messaging around the benefits of passwordless and provide robust resources to ensure a smooth transition.

Adaptive Security: A proper passwordless strategy doesn't equate to single-factor authentication. Strengthen security with context-aware authentication, risk-based assessments, and additional layers of protection. Well-defined access policies will guide the various authentication journeys.

Adopt the right MFA for balancing UX and Security: adapt to use case

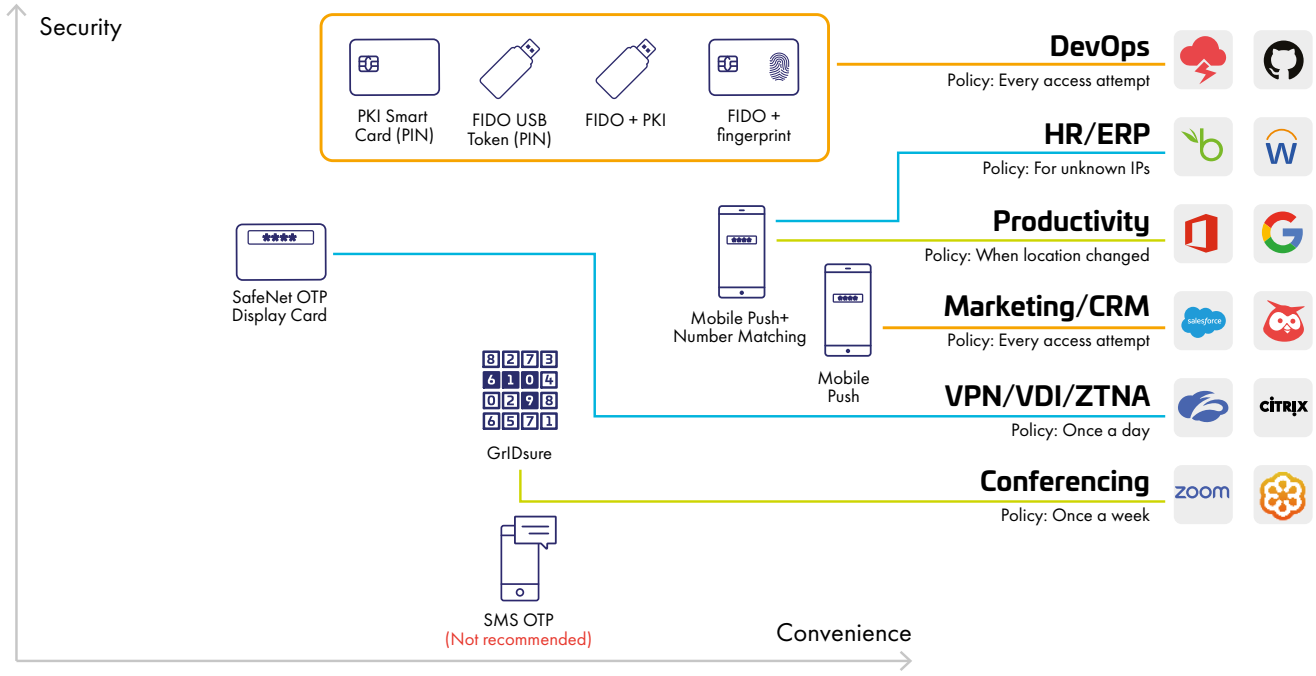
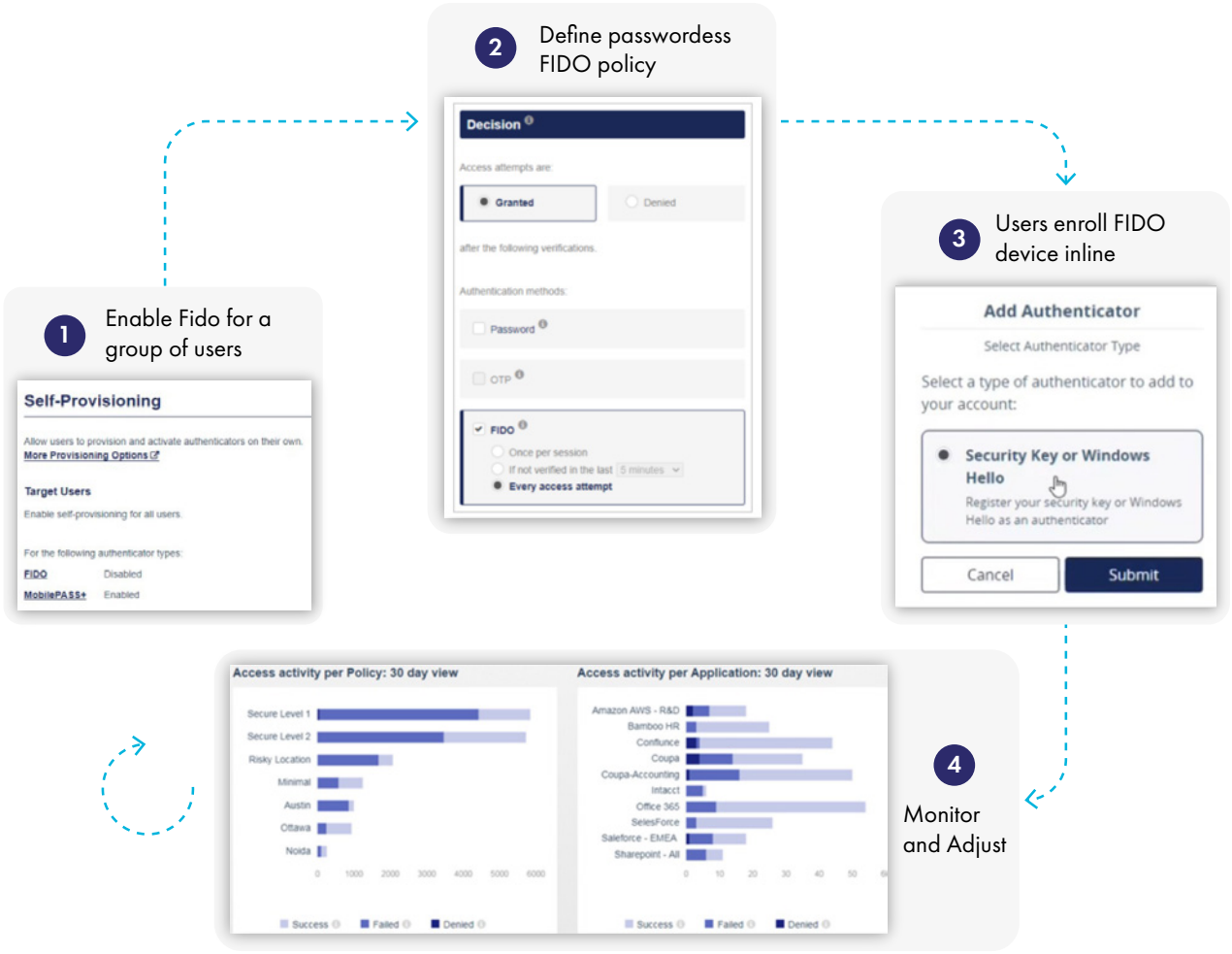


Figure 6: Adaption to use case

Monitoring and Optimization: Track critical metrics like success rates, adoption, and help desk ticket reduction to gauge progress. Gather user feedback to refine the experience and inform future improvements. Stay abreast of the rapidly developing passwordless landscape to adapt your strategy as technologies and standards evolve.

Activate FIDO Authentication with SafeNet Trusted Access



Sunsetting Passwords: A Managed Approach

Gradual is the Way: Don't treat password removal like ripping off a bandage; phase out passwords with careful consideration of applications and user groups. Maintain support for legacy systems as needed during the transition. Where applicable, offer alternatives with robust MFA as a temporary bridge solution.

UX is Paramount: Throughout the entire password elimination process, prioritize a seamless and secure user experience to drive acceptance without causing unnecessary frustration.

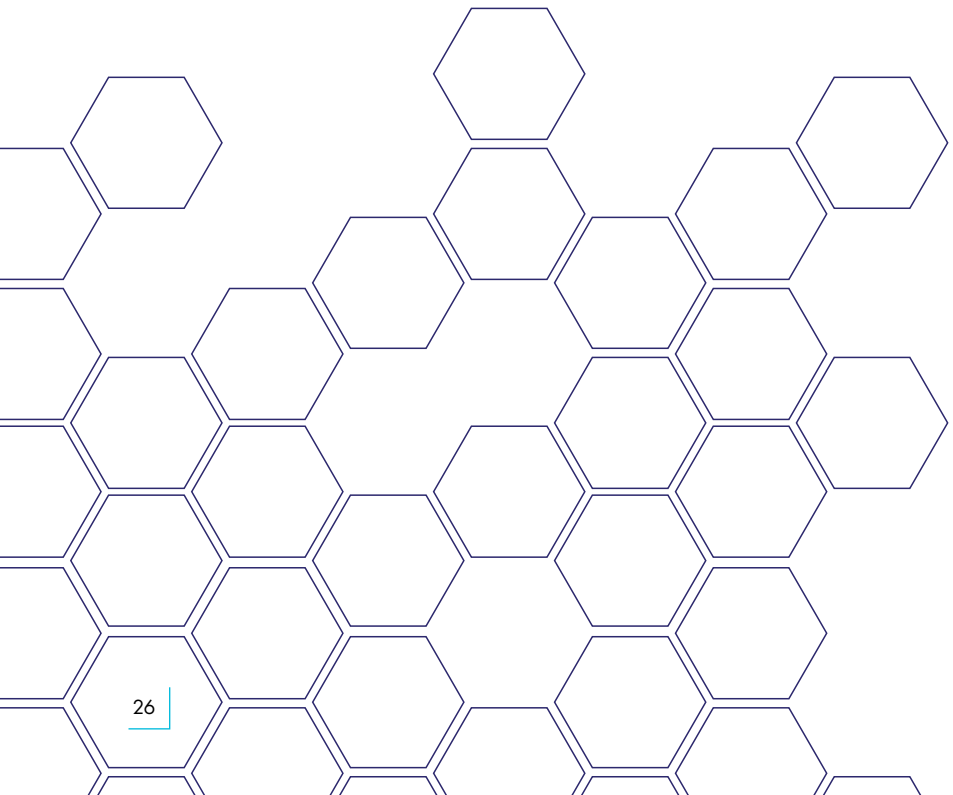
By following this strategic roadmap, organizations can lay a firm foundation for a successful Passwordless 360° implementation, enjoying the enhanced security, optimized user experiences, and significant cost savings that this transformative authentication model promises.

Conclusion: The Future is Passwordless

The benefits of passwordless authentication are undeniable - heightened security against sophisticated cyber threats, friction-free user experiences that increase productivity and satisfaction, and cost savings for businesses. In today's digital landscape, where breaches and compromised credentials are rampant, passwordless authentication stands out as a proactive countermeasure that organizations can no longer afford to ignore.

By embracing this transformative shift and adopting the holistic Passwordless 360° approach, businesses become more resilient against cybercriminals' evolving tactics. Employees are empowered with convenient login methods without sacrificing security, and customers enjoy seamless experiences that build trust and loyalty.

The time to explore passwordless solutions is now. As technology giants push for consumer-oriented standards like Passkeys and the wider industry offers increasingly mature and accessible options, the opportunities for implementation have never been more significant. Begin your journey towards Passwordless 360° and unlock a new era of secure, convenient, and cost-effective digital interactions.



Passwordless 360 - Thales's Approach To Get Full Passwordless Coverage

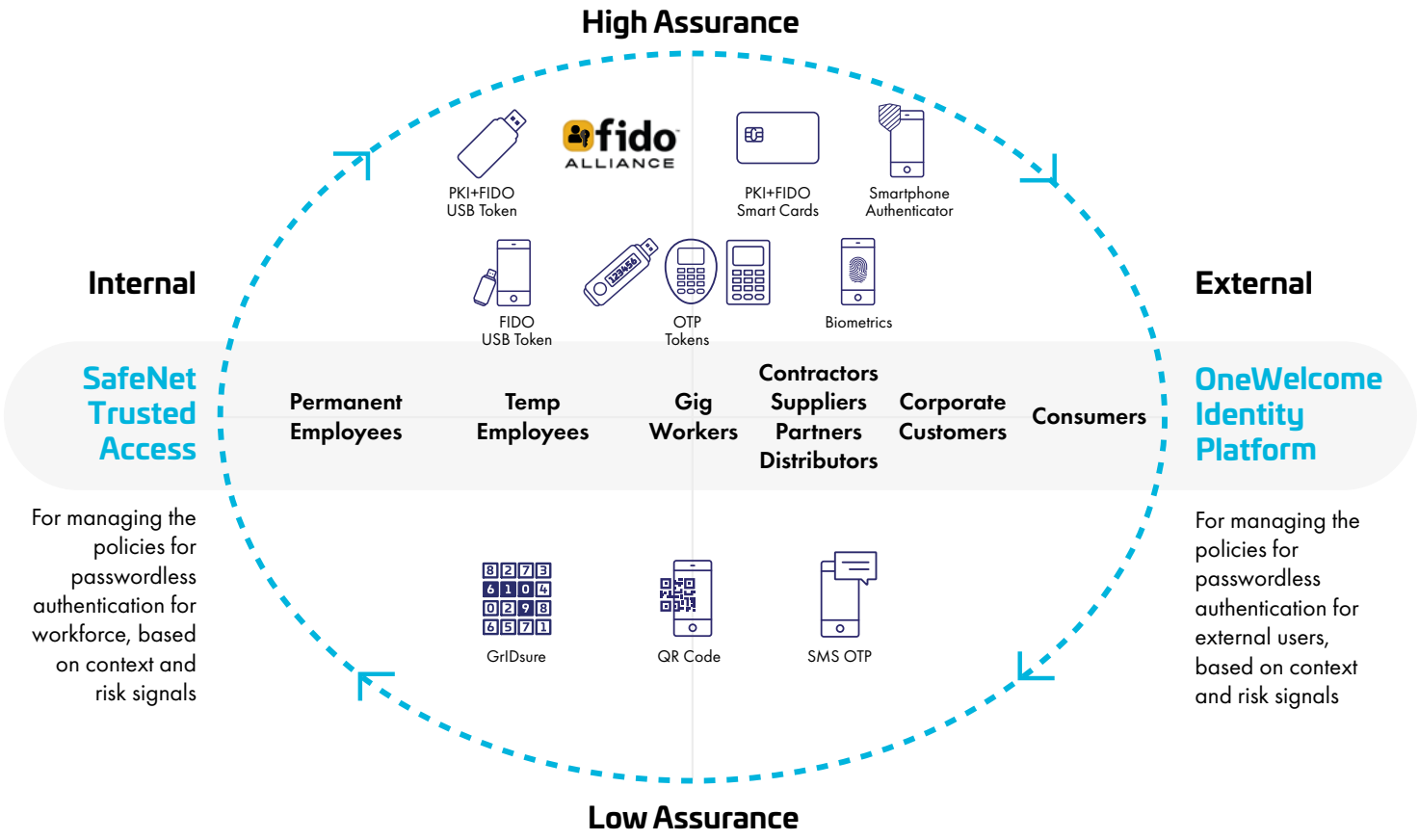


Figure 7: Passwordless 360

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com