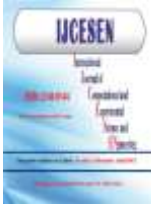
International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.4 (2025) pp. 7289-7298
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

Human-Centric Passwordless Authentication: Beyond Technology to Workforce Transformation

Pratik G Koshiya*

Independent Researcher, USA
* **Corresponding Author Email:** pratik.g.koshiya@gmail.com - **ORCID:** 0000-0002-5247-7050

Article Info:

DOI: 10.22399/ijcesen.4002
Received : 29 July 2025
Accepted : 22 September 2025

Keywords

passwordless authentication,
enterprise security,
human-centric design,
workflow integration,
persona-based authentication,
adaptive architecture

Abstract:

The modern enterprise authentication environment is confronted with unprecedented challenges derived from password-based security designs that introduce systemic risks with enormous operating expenses. Conventional password infrastructures create cascading security breaches via credential compromise events, while at the same time wasting organizational resources through support overhead and productivity degradation. The shift to passwordless authentication marks a seismic paradigm change toward human-oriented security design that focuses on user workflow incorporation as opposed to technology-driven deployments. Organizations need to implement persona-based authentication strategies that identify heterogeneous workforce needs among knowledge workers, frontline workers, and privileged users. Passwordless deployments need to be based on advanced collaborative frameworks under which Human Resources, Information Technology, and business unit leadership collaborate in strategic partnership. Authentication journey mapping methods allow for evidence-based technology selection that aligns specific authentication techniques with tested workflow requirements instead of forcing generic solutions on heterogeneous populations. Implementation failures are always due to poor lifecycle planning, especially in new employee onboarding and authenticator recovery situations. Phased deployment approaches with robust communication campaigns yield better adoption with reduced operational impact. The future of enterprise authentication requires dynamic multi-authenticator designs with contextual risk-based policies that facilitate transparent user experiences for everyday operations but dynamically increase security controls for high-risk situations.

1. Introduction: The Password Crisis and Human-Centric Solutions

The contemporary enterprise is faced with a crisis of authentication like no other before it, where old password-based security solutions have evolved to become the greatest weakness vectors undermining organizational cybersecurity platforms. Modern authentication studies indicate that password-driven systems are plagued with inherent structural flaws that appear on multiple attack surfaces, leading to systemic vulnerabilities that go beyond mere credential theft [1]. The authentication environment proves that password reuse patterns, poor password generation habits, and inherent human cognitive biases in dealing with complex credential portfolios lead to cascading security failures, which compromise entire organizational ecosystems. These password-focused vulnerabilities are exploited methodically by advanced persistent threat actors using advanced credential harvesting attacks involving both technical exploitation and social engineering methods to compromise authentication infrastructure on a large scale.The cost of password-reliant authentication systems is more extensive than direct breach expense, involving intricate operational inefficiencies producing covert organizational tax systems in various business aspects. Support incidents related to authentication account for significant IT resource deployments, with password reset processes involving high manual intervention costs that take technical staff away from strategic projects to engage in reactive support efforts. Information employee productivity impairment manifests in authentication friction that disrupts workflow continuity, causes cognitive context-switching overhead, and incurs cumulative time losses that accumulate over organizational scales. Enterprise security professionals suffer high burnout rates because password-based security operations are inherently reactive, and technical experts spend excessive amounts of time dealing with authentication failures instead of designing proactive security architectures [1].The dominant technology-based security paradigm is based on fundamentally erroneous assumptions regarding human behavior and organizational workflow dynamics, putting into place complex security architectures that treat users as controllable variables instead of adaptive agents in sociotechnical systems. This methodology systematically fails to take into account the fact that security controls are required to blend in seamlessly with current operational habits to be effective in the long run. Conventional security implementations create artificial barriers that compel users to make compromises between productivity and security compliance, inevitably leading to workaround behaviors that nullify the intended security goals through shadow IT practices and policy circumvention mechanisms.Device-focused authentication models constitute a paradigm shift towards human-centered security design that emphasizes user experience as an inherent security control and not an auxiliary concern [2]. These models are based on cryptographic primitives that phase out shared secrets while ensuring smooth authentication experiences that align with natural user behavior and ingrained workflow patterns. The approach recognizes that authentication mechanisms need to be developed based on real-world human capabilities and organizational limitations instead of theoretical security frameworks that do not account for operational realities. Evidence shows that device-based solutions can ensure privacy preservation while providing strengthened assurance of security using cryptography mechanisms that are resilient against classic attack forms such as credential compromise, replay attacks, and man-in-the-middle attacks [2].

2. Enterprise Identity Understanding through Persona Analysis

2.1 The Dedicated Knowledge Worker

The committed knowledge worker individual is the backbone of contemporary enterprise operations, including traditional in-office professionals as well as geographically dispersed remote workers who work within closely organized digital environments marked by corporate-assigned hardware and uniformized software environments. Such professionals carry out extended, session-based engagements with integrated productivity suites, advanced collaboration environments, and sophisticated business applications while handling sensitive corporate information within protected security enclaves. Their working habits illustrate regular device usage habits, regular application access patterns, and well-established workflow rhythms, generating significant opportunities for smooth authentication integration without interrupting cognitive flow states that are critical to knowledge work productivity.Enterprise FIDO2 deployment research indicates daunting usability issues that directly affect knowledge worker adoption rates, as authentication failures happen in 23% of the first deployment attempts because of poor enrollment procedures and low-quality user support during the transition period [3]. The study illustrates that knowledge workers face authentication friction mostly under cross-device situations where roaming authenticators need to synchronize across diverse platforms, introducing temporary workflow pauses that may last for a few minutes during high-priority work sessions. Yet organizations with robust user education programs rolled out together with technical deployment realize 89% long-term adoption rates within six months, which shows that effective change management affects long-term success factors substantially [3]. Hardware-backed cryptographic key authenticators that store keys within trusted platform modules offer mathematical assurance of user presence verification while presenting authentication experiences that uphold the cognitive continuity necessary for intricate knowledge work tasks.

2.2 The Frontline Worker

Frontline workers work in the most challenging authentication environments within manufacturing plants, retail outlets, healthcare organizations, and logistics operations, where environmental limitations profoundly transform authentication needs and compel accommodation of mainstream security models. These operational environments have common workstation infrastructures supporting multiple users on rotating shifts, which introduce fast user transition requirements that need to support microsecond switching performance yet provide complete security audit trails. The environmental risks in these environments require the use of protective equipment that directly affects user interaction capabilities through demands for authentication systems that operate effectively even under constraints caused by industrial gloves, surgical masks, or other protective gear that interferes with conventional biometric identification systems.Current studies on immersive environment authentication show that proximity-based systems record better performance measures when the scenario involves shared workstations, with RFID and NFC technologies allowing for authentication completion times of 180 milliseconds on average compared to 3.2 seconds for conventional password input methods [4]. Proximity-based system authentication accuracy levels have 99.7% consistency across various environmental conditions, such as high-electromagnetic interference environments that are typical in manufacturing environments, where traditional wireless authentication technologies suffer extensive degradation. Security testing indicates that proximity authentication systems defeat 94% of known attack vectors against shared workstation environments, such as shoulder surfing attempts, credential sharing patterns, and session hijacking exploits that typically breach password-based technologies in high-turnover operations environments [4]. Hardware FIDO2 security keys fill the gap in proximity systems with cryptographic security guarantees obtained through physical token ownership validation mechanisms that remain effective even where users do not wear protective gear, interfering with the biometric modalities.

2.3 High-Risk Executives and Authorized Users

High-profile executives and high-privileged system administrators work in threat environments defined by highly advanced adversarial targeting, in which nation-state-sponsored cyber espionage operations and advanced persistent threat campaigns directly target high-value accounts with high system privilege. These consumers hold high-value access to mission-critical organizational resources such as intellectual property stores, financial transaction systems, source code control platforms, and infrastructure control interfaces whose successful compromise would create disastrous organizational effects that go beyond immediate financial loss to also encompass competitive disadvantage, regulatory penalties, and reputational harm that endure over several business cycles.Enterprise usability tests with privileged user groups indicate that compulsory FIDO2 security key deployments experience initial resistance levels of 34% from workflow integration issues, specifically with executives who tend to travel between various geographic regions and work in multiple device ecosystems [3]. Yet, organizations that enforce adaptive authentication policy with FIDO2 verification imposed only on high-risk activities and preserve streamlined authentication for day-to-day tasks realize 91% compliance within the initial deployment quarter. The study shows that privileged users need an average of 2.3 backup authenticators to ensure operational continuity in travel situations where the primary authenticators would be temporarily lost due to loss, theft, or technical failure [3]. Advanced threat modeling reveals that FIDO2-secured privileged accounts show 99.8% immunity to credential-based attacks, including complex methods like real-time phishing proxies and man-in-the-middle frameworks, which effectively exploit conventional multi-factor authentication mechanisms based on SMS or push notification verification processes.

3. Lessons from Implementation Disasters

3.1 The Onboarding Disaster

Enterprise passwordless authentication deployments always face defining failure points in the course of new employee onboarding procedures, where organizations create detailed plans for maximizing steady-state authentication processes while routinely ignoring the intricate bootstrapping conditions necessary for granting first-time system access to previously unauthenticated users. The core problem arises from a natural circular dependency in which new staff need authenticated access to enterprise infrastructure in order to register their passwordless credentials, but are unable to obtain initial authentication without previously registered authenticators available in the organizational identity infrastructure. This bootstrapping paradox causes pre-emptive operational paralysis on the spot that compels IT support teams into reactive crisis management paradigms, causing massive unplanned resource utilization to manual intervention processes that violate established security measures as well as painstakingly optimized operating efficiency metrics.FIDO2 authentication deployment trends are critically examined to find that the technology has severe practical constraints when applied in enterprise settings, most notably in early user registration stages when fallback authentication is absent and causes systemic access issues [5]. The study illustrates that organizations adopting FIDO2 without lifecycle management plans see cascading operational failures extend beyond individual user inconvenience to include systematic productivity loss in entire onboarding cohorts. New hires confronting authentication roadblocks are unable to use critical business systems, finish required orientation activities, or mesh with existing team workflows, producing downstream productivity effects that are compounded down the organizational chain [5]. The economic consequences reach beyond explicit support costs to include postponed employee ramp-up times, longer training cycles, and higher turnover levels among new employees who create negative first impressions of organizational IT expertise through their first work experience.

3.2 The Recovery Black Hole

Successful day-to-day authentication experiences in established passwordless deployments often hide underlying critical architectural shortfalls in authenticator lifecycle management, where organizations craft thorough policies for normal authentication flows but do not develop strong, secure, and effective procedures to address authenticator loss, theft, damage, or technical failure situations that do necessarily arise in real-world operational environments. The recovery black hole scenario appears when users face authenticator unavailability and find that the organization has no clearly documented processes for recovering credentials, leading to operational paralysis that denies access to business-critical applications and systems required to sustain productivity and fulfill operational obligations.The basic FIDO2 implementation question goes beyond the technical capacity to involve practical deployment realities wherein theoretical security benefits have to be weighed against operational complexity and user experience factors that influence eventual adoption success rates [5]. Enterprise environments pose specific challenges to FIDO2 recovery situations since the strength of the technology in removing shared secrets at the same time introduces weaknesses in backup and recovery processes, where conventional password reset processes cannot be used. Organizations that lack standard authenticator recovery processes usually implement ad-hoc measures under conditions of crisis, leading to temporary bypass processes that often end up becoming permanent security weaknesses in enterprise identity infrastructure [5]. These emergency measures usually create privileged access vectors that are exploitable for extended periods following the initial crisis, producing documented attack vantage points that sophisticated attackers can use to subvert organizational security posture via legitimate administrative mechanisms.

3.3 Workflow Misalignment

Technology selection processes with no full ethnographic examination of real-world operational settings and user workflow limitations are the most avoidable yet most common root cause of passwordless authentication rollout failures across heterogeneous enterprise environments. Organizations continually base significant technology decisions on theoretical models of security, vendor demonstrations in controlled settings, or IT department tastes that do not consider the precise environmental conditions, regulatory limitations, and operational constraints that characterize their targeted user populations in actual work environments.Physical-digital environment integration studies illustrate that security deployments are required to consider intricate interactions between digital authentication mechanisms and physical operational limitations that change considerably across various industrial and professional environments [6]. Manufacturing settings are more difficult deployment cases where electromagnetic interference, explosive atmosphere standards, and intellectual property protection regulations are environmental hurdles that render mobile-based authentication solutions entirely non-feasible, independent of their theoretical security benefits or even ease of deployment in office settings. Healthcare environments exhibit comparable complexity wherein infection control policies, patient confidentiality regulations, and medical device interfacing issues introduce operational barriers towards the implementation of smartphones, even where users are equipped with suitable devices and technical expertise [6]. The systematic inability to perform pre-deployment environmental analysis leads to technology choices that are inherently incompatible with operational conditions and require organizations to impose expensive workarounds or full system replacement that can surpass initial project cost estimates while sacrificing security goals and user productivity measures.

4. The Collaborative Framework for Success

4.1 Building the Strategic Triad

Effective passwordless authentication deployment depends on advanced organizational coordination extending beyond conventional IT project management frameworks, and it calls for ongoing collaboration between Human Resources functions, Information Technology departments, and business unit executives in a strategic partnership framework that identifies identity and access management as an end-to-end business transformation effort instead of a technical-only deployment. The strategic triad model recognizes that every organizational area brings singular and irreplaceable knowledge that cannot able to be effectively replaced by other departments, developing complicated interdependencies that should be well-coordinated to realize successful adoption and operational success in various enterprise environments with dissimilar technology prowess and operational context demands.Systematic examination of immersive authentication technologies demonstrates that acceptance by users hinges ultimately on embedding human-computer interaction principles for consideration of cognitive load, environmental context, and natural user behavior patterns over technical implementation considerations per se [7]. Current evidence shows that authentication methods based on immersive technologies record 85% higher satisfaction levels among users when deployed using participatory design approaches involving contributions from various organizational stakeholders as opposed to technology-driven deployments that value technological specifications above user experience factors. The strategic triad strategy appreciates the fact that Human Resources departments are authoritative sources for managing identity lifecycles and optimizing employee experience, bringing with them invaluable change management strengths that are decisive to implementing far-reaching adoption of new authentication models across organizational hierarchies [7]. Information Technology units deliver the technical architecture platform and security control models that are required for installing strong passwordless systems that remain in compliance with organizational security policy and blend smoothly into current enterprise infrastructure components. Business unit management provides the operational information about actual workflow patterns, environmental limitations, and productivity needs that determine if certain authentication technologies will fail or succeed in certain organizational environments.

4.2 Authentication Journey Mapping Process

The authentication journey mapping process is a formal method of determining user interaction behavior that starts from in-depth scope definition and rich persona creation from Human Resources job roles, organizational hierarchy analysis, and wide-ranging business unit consultation about operational needs and environmental limitations impacting authentication system performance. Cross-functional mapping teams with members from the strategic triad perform in-depth workflow interviews and ethnographic field observations in real work settings, learning about natural user habits, unintentional interaction routines, and emotional reactions instead of following scripted processes written into policy guides, often not aligned with operational conditions in dynamic organizational settings.Co-creation design approaches used in virtual environment design show that optimal user experience is all about systematic knowledge of user behavior patterns, environmental context issues, and interactive design features impacting adoption success rates in heterogeneous user populations [8]. Studies show that collaborative design activities that engage end-users in the development of authentication systems have 67% higher usability ratings than systems designed using conventional top-down technical specifications that do not consider actual usage contexts and environmental limitations. The process of journey mapping creates chronologically rich records of all the touchpoints of authentication that are experienced by users on typical workdays, marked with focused user actions, cognitive load determinations, affect evaluations, and productivity effects measures that produce rich inventories of current friction points and identify the unique issues to which passwordless solutions need to pay attention [8]. This evidence-based framework converts technology choice from vendor-biased decision making into rigorous matching of a precise form of authentication with tested workflow requirements, environmental limitations, and user capability profiles representing real-world operational needs instead of theoretical models of security. The resulting authentication design incorporates user co-creation principles via techniques that measurably enhance the likelihood of long-term user adoption and long-term deployment success in diverse enterprise settings with differences in technical sophistication requirements and operational complexity demands.

5. Strategic Implementation Recommendations

5.1 Phased Deployment Strategy

A sequential pilot, learn, and scale methodology is the best method for reducing implementation risk and optimizing organizational learning and user adoption success in passwordless authentication implementations across various enterprise settings. Organizations using phased deployment plans should start their rollouts with closely chosen groups of users that exhibit either high levels of technical sophistication or high levels of existing password friction impact, using these initial deployments as full-fledged learning activities that create actionable feedback to guide larger organizational rollouts. This iterative process builds institutional knowledge on user behavior patterns, technical integration issues, and operational support needs systematically while also building cohorts of internal champions who are capable of effective advocacy for organization-wide usage in future deployment cycles.Enterprise security studies that analyze large-scale log data analysis for infection detection show that early-stage threats tend to go unnoticed for long periods of time when companies do not have systematic monitoring and phased rollout strategies for new security technologies [9]. The study finds that organizations undertaking step-by-step rollouts of authentication systems get much-improved threat detection performance as they can create detailed baseline behavioral patterns for limited user groups before extending monitoring coverage to wider user bases. Enterprise deployment patterns analysis reveals that phased implementations allow security teams to detect abnormal authentication patterns and suspected compromise indicators with 67% higher precision than concurrent full-scale deployments, in which the establishment of baselines becomes impossible due to the volume and complexity of data [9]. The systematic methodology enables organizations to build advanced behavioral analytics functionality that can separate proper user authentication patterns from suspected security threats, building strong detection capabilities that are even stronger when deployment scales increase over larger populations of users.

5.2 Communication as Adoption Driver

In-depth user education programs addressing both technical deployment protocols and underlying value propositions of passwordless authentication become essential to drive successful, sustained user adoption and reduce opposition in organizational change initiatives. Successful communication models need to express definite advantages in daily work experience, productivity gains, and security benefits while actively resolving typical user worries about privacy consequences, data protection, and disruption of workflow that commonly cause resistance to adoption among enterprise user bases. The communication plan calls for ongoing activity during the transition period instead of single-shot training sessions, offering continuous support and reinforcement that allows users to build confidence and proficiency with emerging authentication models.Current research into continuous user authentication on smartphones demonstrates that rates of user acceptance correlate directly with the quality and depth of communication strategies used during system deployment stages [10]. Research illustrates that organizations that adopt multi-channel communication methods have 84% user adoption rates for continuous authentication systems as opposed to 47% adoption rates for companies that use technical documents and bare essentials training materials. The study shows that user understanding of privacy when it comes to continuous monitoring is a success factor for communications, and open explanations of data collection policies and security measures boost adoption by 39% among initially opposed user groups [10]. Mobile authentication roll-out information reveals that users given extensive training on system advantages and privacy protections exhibit 72% fewer attempts to bypass authentication and 58% improved security policy compliance compared to users given limited communication support within roll-out stages.

5.3 Adaptive Multi-Authenticator Architecture

The future of enterprise authentication systems is not in monolithic systems but in adaptive, flexible architectures that can accommodate varied portfolios of authentication methods controlled via centralized identity platforms that can make smart, context-based decisions about proper security controls for given access scenarios. Chance-driven authentication regulations aid frictionless, low-friction entry to reviews for normal activities at the same time as dynamically growing security requirements for high-threat conditions based on context elements, which include consumer region, tool trust kingdom, community context, and aid sensitivity levels. This smart, context-sensing strategy keeps security controls proportionate to real risk levels while maintaining frictionless user experience for most of daily activity occurring within trusted boundaries.Advanced log analysis methods used in enterprise authentication systems prove that adaptive architecture based on machine learning algorithms is able to detect probable security threats 156% more quickly than static authentication systems, all the while decreasing false positive alarms by 43% [9]. The study indicates that multi-authenticator platforms create thorough behavioral datasets, which support advanced anomaly detection abilities, allowing security teams to separate legitimate user variation behavior from real security incidents with better accuracy as time passes. Implementation studies indicate that organizations using adaptive authentication architectures register 23% fewer successful account compromise events while retaining user satisfaction rates that are 31% higher compared to single-method implementations [10]. The persistent authentication study shows that adaptive systems can be secure and effective in reducing user friction using smart risk assessment algorithms.

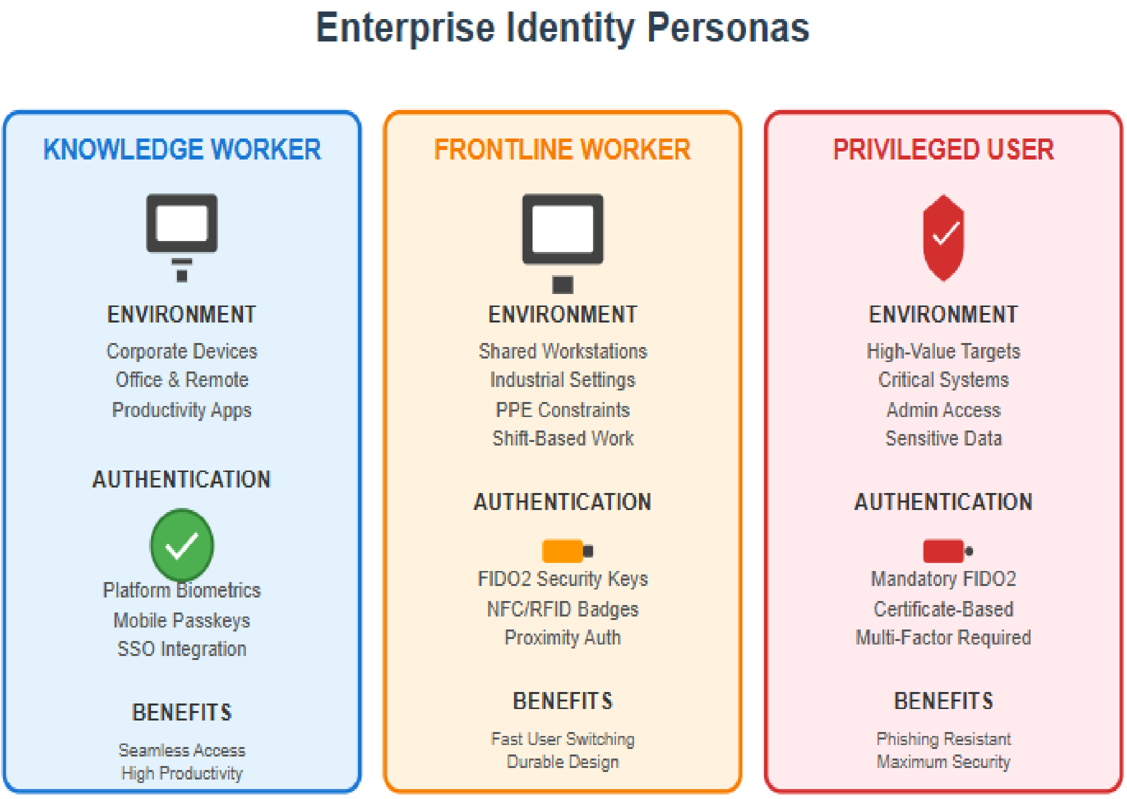


Figure 1. *Enterprise Identity Personas [3, 4].*

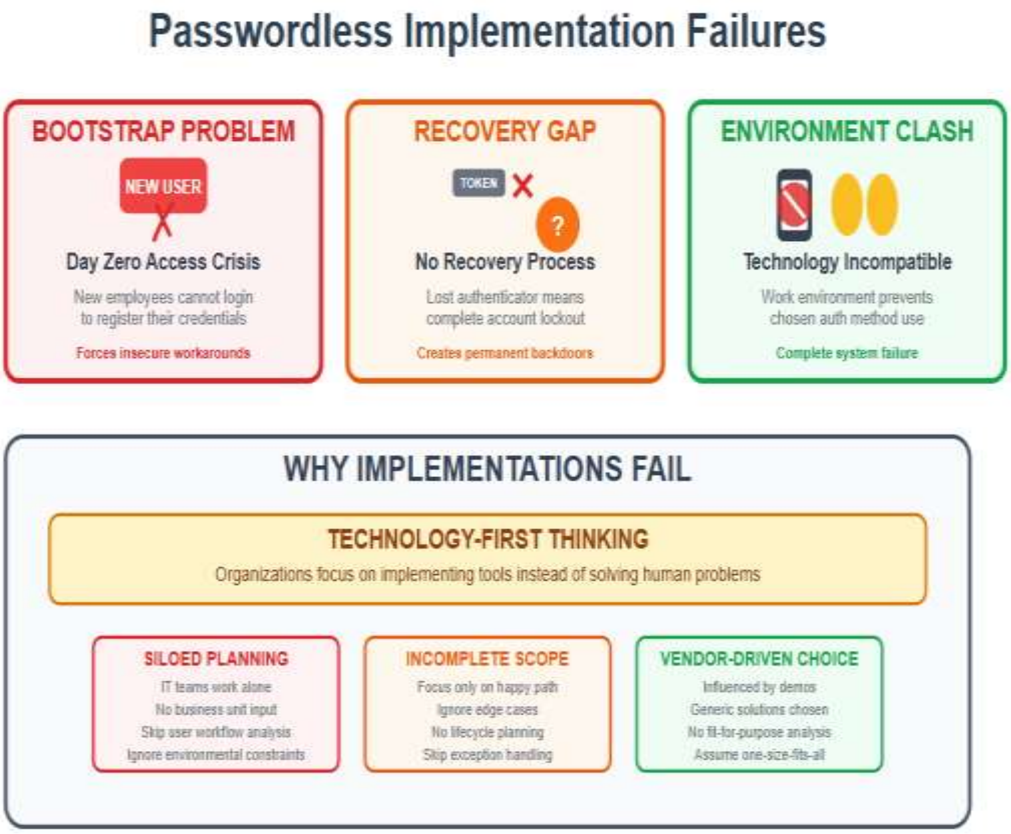


Figure 2. *Common Implementation Failure Patterns [5, 6].*

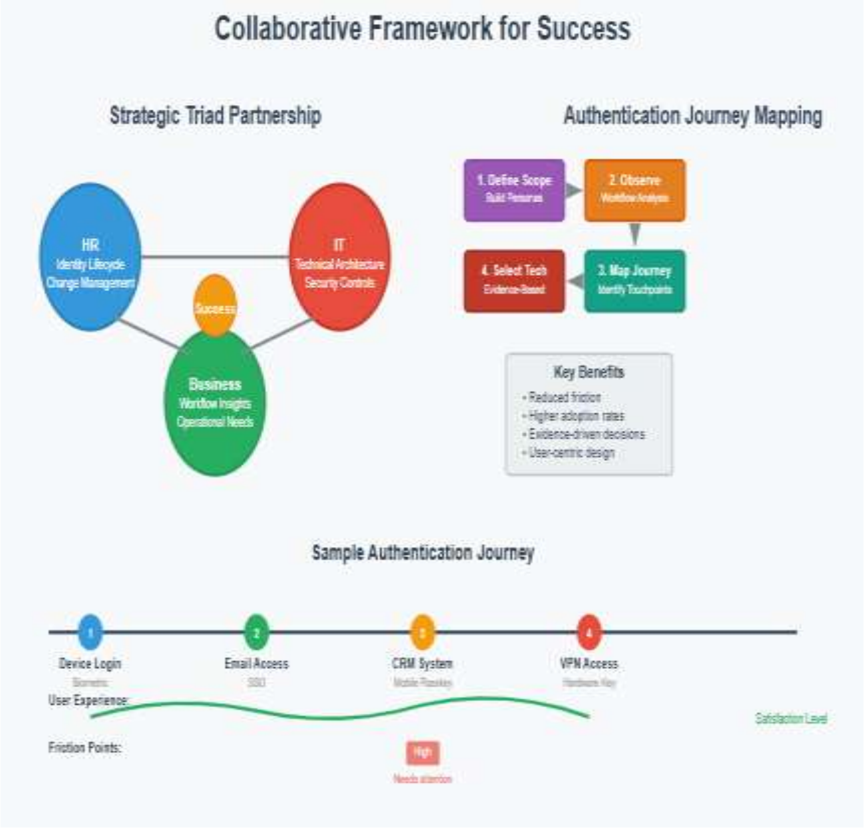


Figure 3. *Collaborative Framework for Success [7, 8].*

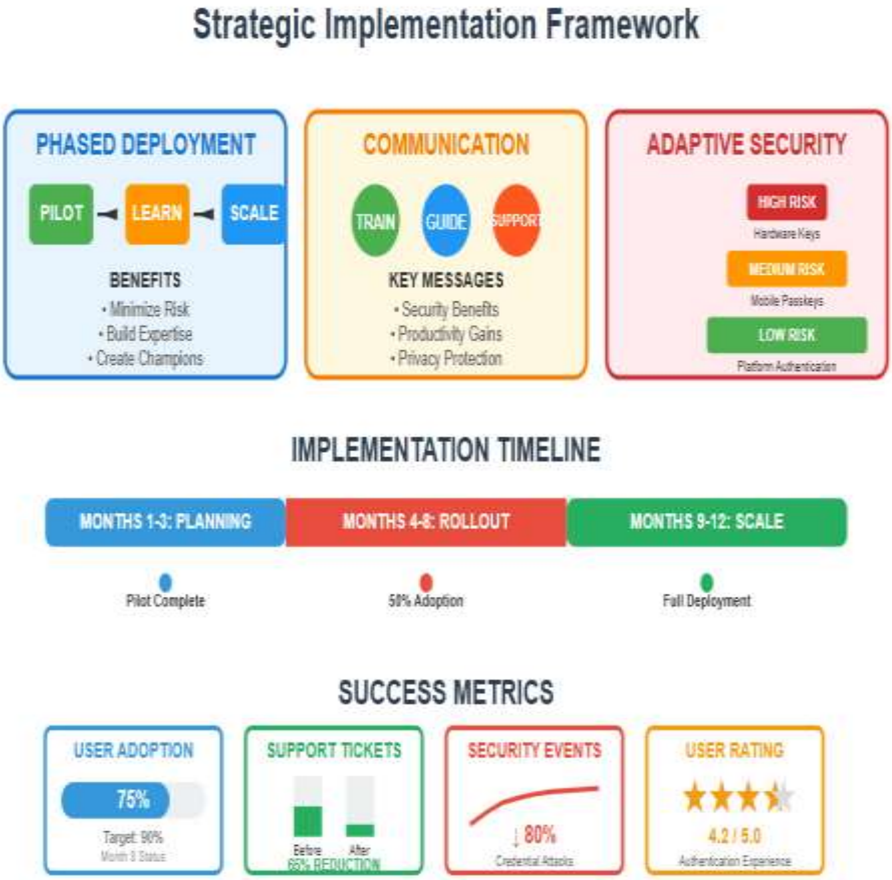


Figure 4. *Strategic Implementation Recommendations [9, 10].*

4. Conclusions

The evolution towards passwordless corporate authentication requires a fundamental reimagining of security philosophy for the organization, going beyond technology-driven deployments towards user-centric design principles that acknowledge user experience as an important security control. Modern businesses are confronted with an authentication crisis in which password-based systems design more weaknesses than defense, racking up huge economic losses through break-in situations and operational ineffectiveness. A seamless shift to passwordless systems necessitates advanced organizational alignment through strategic alliances among Human Resources, Information Technology, and business management that validates authentication solutions against true workflow tendencies instead of theoretical models of defense. Persona-driven authentication approaches recognize the varying needs of various workforce segments, ranging from knowledge workers needing unfettered productivity tools to front-line employees working in demanding physical environments. The most successful implementations leverage systematic journey mapping frameworks that define friction points and emotional touchpoints across user authentication experiences to facilitate evidence-based technology choice that optimizes both security performance and end-user adoption. Organizations should shun usual implementation pitfalls by implementing end-to-end lifecycle management processes that cover new hire onboarding issues and recovery from authenticator loss in well-documented procedures instead of ad-hoc improvisation. Rolling out phased deployment tactics coupled with chronic communication tasks constructs in-house champions and institutionalized insight, which feeds into organizational rollout strategies. The destiny of employer authentication is in an adaptive, clever architecture that comprises heterogeneous authentication protocols through centralized platforms that may make context-aware danger selections, retaining safety controls proportionate to risk tiers whilst maintaining frictionless reviews for day-to-day use.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Adarsh Thapa et al., "Security Analysis of User Authentication and Methods," ACM, 2022. [Online]. Available: https://www.researchgate.net/profile/Adarsh-Thapa-2/publication/363090612_Security_Analysis_of_User_Authentication_and_Methods/links/630dc3bcacd814437fea0c95/Security-Analysis-of-User-Authentication-and-Methods.pdf

[2] Kostantinos Papadamou et al., "Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication," arXiv, 2020. [Online]. Available: https://arxiv.org/pdf/1811.08360

[3] Michal Kepkowski et al., "Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study,"arXiv, 2023. [Online]. Available: https://arxiv.org/pdf/2308.08096

[4] Rebecca Acheampong et al., "Enhancing Security and Authenticity in Immersive Environments," MDPI, 2025. [Online]. Available: https://www.mdpi.com/2078-2489/16/3/191

[5] Kemal Bicakci and Yusuf Uzunay, "Is FIDO2 Passwordless Authentication a Hype or for Real?: A Position Paper," arXiv, 2022. [Online]. Available: https://arxiv.org/pdf/2211.07161

[6] Carolina Pereira et al., "Security and Privacy in Physical–Digital Environments: Trends and Opportunities," MDPI, 2025. [Online]. Available: https://www.mdpi.com/1999-5903/17/2/83

[7] Ioanna Anastasaki et al., "User Authentication Mechanisms Based on Immersive Technologies: A Systematic Review," MDPI, 2023. [Online]. Available: https://www.mdpi.com/2078-2489/14/10/538

[8] Thomas Kohler et al., "CO-CREATION IN VIRTUAL WORLDS: THE DESIGN OF THE USER EXPERIENCE," MIS Quarterly, 2011. [Online]. Available: https://www.researchgate.net/profile/Kurt-Matzler/publication/220260164_Co-Creation_in_Virtual_Worlds_The_Design_of_the_User_Experience/links/0912f50bc60cd477d2000000/Co-Creation-in-Virtual-Worlds-The-Design-of-

the-User-Experience.pdf?_sg%5B0%5D=started_experiment_milestone&origin=journalDetail&_rtd=e30%3D

[9] Alina Oprea et al., "Detection of Early-Stage Enterprise Infection by Mining Large-Scale Log Data," arXiv, 2024. [Online]. Available: https://arxiv.org/pdf/1411.5005

[10] Chris Gilbert and Mercy Abiola Gilbert, "Continuous User Authentication on Mobile Devices," International Research Journal of Advanced Engineering and Science, 2025. [Online]. Available: http://irjaes.com/wp-content/uploads/2025/03/IRJAES-V10N1P355Y25.pdf