



# The Authentication Horizon 2026

From Password Fatigue to Frictionless Trust.

**AUTHENTICATION IS NO LONGER JUST ABOUT LOGGING IN.  
IT'S THE FOUNDATION OF DIGITAL TRUST.**

//

By 2026, over 60% of large enterprises and 80% of the Fortune 500 will have implemented advanced passwordless authentication strategies, moving beyond legacy MFA to unphishable, user-centric models."

— Gartner, Inc. (Adapted Projection)

In partnership with industry innovators, including





# THE BURNING PLATFORM



**Why the Status Quo is Failing.**

**81%**

of confirmed data breaches leverage stolen, weak, or default passwords

— Verizon DBIR 2025

**\$4.9M**

is the average global cost of a data breach

— IBM Cost of a Data Breach 2025 2025

**67%**

of help desk calls are for password resets, costing organizations an average of \$70 per call

— Forrester

**45%**

of users will abandon a cart or service if the login process is too complex

— Industry Research

## **The Cost of Complacency is Catastrophic**

The password-centric model is a direct liability to security, budget, and user experience. Organizations that continue with legacy authentication are not just behind—they're actively vulnerable.

# THE EVOLUTION OF AUTHENTICATION

## A Timeline of Digital Identity.

**1980S-2000S**

### The Password Era

Single Factor Authentication (SFA). The beginning of digital identity, but inherently weak.



**2010S-2020S**

### The Multi-Factor (MFA) Patch

SMS, TOTP, Push Notifications. A significant step, but now targeted by sophisticated phishing and SIM-swapping attacks.



**2023-2025**

### The Passwordless Dawn

FIDO2/WebAuthn standards gain traction. Biometrics and Passkeys emerge, but adoption is fragmented.



**2026 & BEYOND**

### The Era of Unphishable Identity

Decentralized Identity, True Passwordless Access, and Continuous Trust. Identity becomes a verifiable credential.



## The future is identity centric

We're moving from "What do you know?"  
to "Who are you, provably?"

# INTRODUCING THE NEXT GENERATION

**What True Passwordless Means**



**It's More Than Just "No Password." It's  
Verified, Frictionless, and Use-Centric**

**TRUE PASSWORDLESS  
IN 2026 IS DEFINED BY  
THREE PILLARS:**

# 1



## Inherently Strong

Uses biometrics (face, fingerprint) or a local PIN—secrets that never leave the user's device. Based on unphishable FIDO2/WebAuthn standards.

- Device-bound biometrics
- FIDO2/WebAuthn standards
- No network transmission of secrets

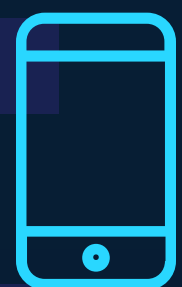
# 2



## Identity-Verified at Source

The initial identity proofing is as strong as the authentication itself. Is the person creating the account really who they claim to be?

# 3



## Portable and User-Controlled

The digital identity is not locked to a single device or provider. It's a part of the user's digital wallet, usable across services.

- Cross-device portability
- User-owned credentials
- Platform independence

# The Critical Gap That Basic Passkey Solutions Miss

Most passwordless solutions focus on the authentication part but ignore the crucial question: How do you know the person creating the passkey is really who they claim to be?

**"Identity-verified passwordless authentication is the only way to achieve true zero-trust security."**

# 2026 AUTHENTICATION LANDSCAPE

## Key Trends Shaping the Future



# 1

### Phishing Resistance is Non-Negotiable

Legacy MFA is no longer sufficient. The market demands cryptographic proof (public/private keys) that cannot be intercepted.

Cryptographic Proof



# 2

### The Rise of the Identity-Bound Passkey

Passkeys are just the start. The future is in verifiably binding that passkey to a real, proven human identity at creation.

Identity-Bound



# 3

### Decentralized Identity (DID) Goes Mainstream

Users own and control their identity attributes, presenting verifiable credentials without relying on a central database of PII.

User-Controlled



# 4

### Regulatory Pressure Intensifies

Digital Identity Guidelines (NIST 800-63-4), eIDAS 2.0, and other global mandates explicitly require phishing-resistant authentication.

Compliance Mandatory

# BREAKING NEW FRONTIERS

The 1Kosmos Approach

**While the industry talks about the future, one platform is already delivering it.**



## Verified Identity First

Users prove their identity once with government-issued ID and live biometrics. This creates a high-assurance digital identity.

KEY BENEFIT

Trust from Day One



## True Passwordless MFA

This verified identity is then bound to unphishable, biometric-backed passkeys for everyday access.

### KEY BENEFIT

Unphishable Access



## Built on Blockchain

For immutability and user control, identity events are recorded on a private, permissioned blockchain.

### KEY BENEFIT

Immutable Trust

# HOW IT WORKS

## The Journey of a Verified User

1

### Step 1: Onboarding & Identity Proofing

User downloads the 1Kosmos LiveID app. They capture a government ID and take a live selfie for liveness detection.

#### RESULT

A verified, reusable digital identity is created.

2

### Step 2: Secure Credential Binding

The platform generates a private key, secured by device biometrics, cryptographically bound to verified identity.

#### RESULT

An identity-proofed passkey is born.

3

### Step 3: Frictionless Authentication

To access an application, the user simply scans a QR code and approves with their biometric. No passwords.

#### RESULT

A secure, seamless user experience.

4

### Inherently Strong

The platform can periodically re-verify the user's presence using passive biometrics.

#### RESULT

Ongoing security assurance.

# TANGIBLE IMPACT

## The Business Case for 2026

### Return on Investment Highlights

**\$2.1M**

Help Desk  
Cost Savings  
annually

**98%**

Security Breach  
Risk Reduction  
vs. password-based

**15hrs**

User Productivity  
Gain  
per user/year

**\$800k**

Compliance Cost  
Avoidance  
annually

#### Immediate Benefits

- Eliminate 95% of password-related security incidents
- Reduce authentication time from 30+ seconds to under 3 seconds
- Cut help desk authentication requests by 92%

#### Long-term Impact

- Build a competitive moat through superior user experience
- Future-proof authentication infrastructure
- Enable zero-trust architecture implementation

# USE CASES

## Securing the Enterprise and Beyond

### Zero-Trust Architecture ENTERPRISE SECURITY

The perfect foundation for a ZTA, providing verified identity as the new perimeter.



### Remote Workforce Access REMOTE WORK

Secure, simple access to corporate networks, VPNs, and cloud applications.



### Customer Identity & Access Management E-COMMERCE

Offer customers a supremely secure and easy login experience, reducing cart abandonment.



### Financial Services FINTECH

High-assurance authentication for banking, trading, and financial applications.



# AUTHENTICATION IS IDENTITY



By 2026, the distinction between  
"authentication" and "identity  
verification" will have blurred into a  
single, continuous process of  
establishing trust.

“The future of authentication isn’t passwordless - it’s trustless verification of boundless identity.”

## Leading the Transition

Platforms like **1Kosmos** are not just part of this transition; they are **architecting its foundation.**



The Identity-Bound Passwordless Platform

Visit [1kosmos.com](https://1kosmos.com) to see how the future of authentication works today.