1Kosmos and Microsoft

1Kosmos adds verified identity and passwordless access to help organizations build on their Microsoft investment

Modernizing identity and access management (IAM) with Microsoft Entra ID is a big step forward to protect new account openings, secure logins, and prevent fraud, but it is not enough. Organizations need to consider passwordless access when moving from Active Directory to Entra ID. Additionally, this migration may inadvertently introduce security gaps due to a siloed approach when securing systems that fall outside of the Microsoft environment.

The 1Kosmos Advantage

1Kosmos gives organizations using Entra ID a safe and secure way to get new users and new organizations rapid access to digital services without flooding the Service Desk with requests for account opening and password reset.

Through a powerful self-service identity verification workflow and a passwordless MFA credential, user can scan a QR code or click a smartlink to reset passwords or initiate their onboarding journey.

Security teams set the identity assurance levels for different users and systems based on business needs. 1Kosmos does the rest, providing a consistent passwordless MFA experience across Active Directory, Windows, Mac, iOS, Android, Linux, Unix, plus legacy systems.

Key Use Cases:

1. Deploy 1Kosmos as an External Authentication Method (EAM) within the Entra Platform
2. Facial Biometrics with Liveness
3. Passwordless MFA for more environments
4. Identity Verification up to IAL2
5. Interoperability and Extensibility
6. Authentication Resiliency
7. Self-Service Password Reset and Account Recovery
8. Upgrade to decentralized Identity
9. Passwordless Access for Restricted Environments
10. Secure Remote and Virtual Desktop Login

1Kosmos can easily enhance an organizations Microsoft investment by filling in the identity and authentication gaps a Microsoft deployment can introduce.

1KOSMOS FEATURES AND BENEFITS

→ **Extend Passwordless:** Provide passwordless access to macOS, Linux, and Unix and non-SAML based applications and services.

→ **Virtual and Higher Privilege Environments:** Implement passwordless access to domain controllers, remote desktops, and virtual machines.

→ **Legacy Technology**: Provide interoperability with legacy/internally built technologies.

→ **Integration with AD and Entra ID**: Off-the-shelf connectors enable quick and easy deployment including WS-Fed and WS-Trust protocols.

→ **Authentication:** Leverage any of the 11 authenticators, matching to risk or levels of identity assurance.

→ **Ensure Authentication Resiliency:** Leverage 1Kosmos as the default authenticator to cover all use cases and use the native MSFT Authenticator as a backup.

About 1Kosmos

External Authentication Method (EAM)

Organizations can leverage 1Kosmos as a Microsoft External MFA provider to protect all resources behind ADFS or Entra ID. Use conditional access to manage roll out to select groups of users or applications. Leverage any of the 11 authenticators matched to risk or levels of identity assurance, including facial biometrics.

Verified Identity

Ease employee onboarding and deliver a high level of trust behind every login for specific systems or groups of users by implementing high assurance identity verification. Suitable to support even the most privileged, mission-critical functions. Verification support for 158 countries and 1000's of documents to protect Entra or non-Entra applications, services, data, and systems.

Interoperability and Extensibility

Utilize fifty out-of-the-box connectors, an open API framework, plus a flexible SDK, to standardize authentication across the enterprise. Coverage provides a more flexible framework spanning Entra, Active Directory, SSO, PAM, plus all additional authentication requirements.

Password Reset & Account Recovery

Users can reset their password through the 1Kosmos platform for applications where passwords cannot be eliminated or recover an account due to a hardware upgrade or lost device.

Trust on First Use (TOFU)

Eliminate the "Trust on First Use" (TOFU) gap when users transition to new systems via a passwordless experience into new devices, eliminating the previously required username and password.

Restricted Environments / Shared Workstations

Enable phishing-resistant passwordless multi-factor authentication option for Sensitive Compartmented Information Facilities (SCIF), manufacturing clean rooms, customer help desks, higher education labs, retail bank branches, healthcare providers and other restricted environments.