DATASHEET

Adaptive Authentication

Orchestrate custom user authentication journeys to ensure users are who they claim be

Adaptive Authentication addresses authentication gaps by dynamically adjusting login requirements according to contextual risk factors exhibited by users like location, domain, and device used at run-time. By dynamically adapting authentication methods, based on a determined level of risk, security and IT teams will improve the user experience while stopping malicious actors from logging in.

The 1Kosmos Adaptive Authentication Advantage

1Kosmos Adaptive Authentication evaluates multiple signals, such as the device used, the origin of access—from within or outside the network—user behavior, including past login locations and frequency, to determine the user's legitimacy at the time of authentication.

1Kosmos assesses these signals and authenticates users based on the level of risk. It minimizes user disruptions by requesting less information from recognized users who exhibit expected results.

The authentication orchestration only intermittently prompts users for additional information, particularly when security risks are elevated. This results in smoother user experiences, reduced authentication barriers, and enhanced security levels.

What constitutes an appropriate level of assurance might differ from one organization to another, highlighting the importance of adaptability in the 1Kosmos approach.

1Kosmos Adaptive Authentication evaluates multiple signals to determine the user's legitimacy at the time of authentication

1KOSMOS FEATURES AND BENEFITS

- → Improve authentication journeys, eliminate security gaps and reduce risk when authenticating users
- → Orchestration is managed through a centralized hub, ensuring a consistent administrative experience
- → Leverage a single authentication platform to ensure a consistent user experience.
- → Collect workstation information for validating trusted endpoints
- → Easy integration via industry authentication standards such as OAuth, OIDC, SAML, FIDO and RADIUS
- → 50 out-of-the-box integrations and a robust API framework enabling quick integration into common technologies, including Azure, Ping, Okta, O365, and more
- → An immutable audit trail of all events enables visibility to all logins and access attempts

Reasons to consider

- Simple and flexible deployment model
- A single authentication platform meeting all risk and business requirements
- Compatibility with leading-edge and legacy technologies

Administration
The 1Kosmos control plane is a centralized hub that allows admins easy access to the platform's configuration and management. Admins can connect to applications and services, user stores, and set the corresponding policies and orchestration for all authentication journeys.

Authentication Orchestration
Implement various authentication methods based on user signals and associated risk. Administrators can implement several methods, including basic multifactor authentication (Push, OTP) plus - FIDO2, FIDO Passkeys and an AAL2 certified identity-based biometric (1Kosmos LiveID).

Compatibility
1Kosmos integrates via industry authentication standards such as OAuth, OIDC, SAML, RADIUS, and FIDO. Additionally, supports interoperability across Windows, Mac, iOS, Android, Linux, and Unix operating systems.

Event Logging
Each authentication is protected by an immutable audit trail. Events are logged in perpetuity and cannot be manipulated, giving a detailed and indisputable picture of access results and administrative changes for auditors.

Health Agent
Collects workstation information for validating trusted endpoints and injects additional information to the authentication events.

Authentication Methods
Users can authenticate via any identification methods, including LiveID, device biometrics, FIDO2, FIDO Passkeys, push messages, email/SMS/Token, hardware tokens, Windows Hello, and Mac TouchID.

About 1Kosmos

©2024 1Kosmos Inc., 1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education and healthcare organizations in the world.