PARAVIEW

Paraview Multi-Factor Authentication

At A Glance

Multi-Factor Authentication (MFA) is a security mechanism that requires users to provide two or more verification factors to access an application, account, or system, enhancing protection beyond just a password.

MFA combines at least two of the following factors:
Something You Know: Password or PIN.
Something You Have: Smartphone, hardware token, or smart card.
Something You Are: Biometric data like fingerprints or facial recognition.

In a world of growing cyber threats, MFA provides a simple yet powerful solution to safeguard identities, maintain compliance, improve user trust.

Multi-Factor Authentication

Multi-Layered Authentication:
Paraview MFA supports a variety of authentication methods, including software OTP, hardware OTP, SMS/email verification codes, hardware tokens (e.g., RSA, YubiKey), facial recognition, fingerprint recognition, and mobile QR codes.

Policy-based dynamic access control:
Paraview MFA adjusts permissions in real-time based on user roles, context, and resource sensitivity, ensuring secure and flexible access aligned with security policies.

Adaptive MFA:
By collecting contextual information during user access, such as source IP address, geographic location, time, browser, and device details, and analyzing it through UEBA algorithm models, adaptive user risk interception strategies can be implemented. This enables dynamic and secure access control.

Seamless Integration:
Paraview MFA supports various integration methods, including single sign-on protocols such as OAuth2.0, OIDC, SAML, and CAS, as well as RESTful APIs for application integration. It also supports multiple authentication protocols, such as LDAP and RADIUS. For servers, it allows extending various MFA methods through plugin-based implementations.

PRODUCT BRIEF

KEY BENEFITS

Enhanced Security:
MFA significantly reduces the risk of account breaches by requiring multiple layers of authentication, ensuring stronger protection against cyberattacks.

Compliance and Trust:
Ensures compliance and builds trust by securing identities and data.

Improved User Experience
MFA offers flexible, user-friendly authentication options while seamlessly integrating with existing systems for a smoother login experience.

CRITICAL DIFFERENTIATORS

- **Authentication Methods:**
Supports a wide range of authentication methods, including software OTP, hardware OTP, SMS/email verification codes, hardware tokens (e.g., RSA, Yubikey), facial recognition, fingerprint recognition, and mobile QR codes, catering to various user and scenario needs.

- **Flexible Policy Customization:**
Allows for customized login strategies, secondary authentication, and risk-based policies based on user dimensions, enabling dynamic risk assessment and tailored authentication methods for enhanced security.

- **Extensive Industry Experience:**
Serves over 2,000 clients across industries like finance, manufacturing, healthcare, education, retail, and government, offering customized solutions backed by deep industry expertise.

Solution Overview

The following table shows the capabilities of Paraview MFA.

Paraview MFA Capabilities	
Self-Service	• User Dashboard: Provide a customizable workspace where users can manage and organize their applications and resources. • Password Reset and Recovery • Access Permissions Request and Approval
Single Sign-On (SSO)	• Single Sign-On (SSO): Allows users to access multiple applications with a single set of credentials, streamlining authentication. • Single Sign-On protocols: OAuth 2.0, CAS, OIDC, SAML2.0, form-based authentication etc.
MFA Core Capability	• Multi-Layer Authentication: Enhances security by requiring users to provide multiple forms of verification during login and when accessing applications. • Authentication Methods: OTP (software and hardware), SMS/email Verification Code, Facial Recognition, Fingerprint Recognition and QR Code. • Flexible Authentication Policies: Policies Based on User Groups, Organizational Dimensions, and more.
Customizable Policies	• Role-based authentication to apply stricter controls for privileged users. • Flexibility to select preferred authentication methods (e.g., SMS, email, biometrics) based on user profiles. • Supports two-step and three-step multi-factor authentication processes.
Risk-Based Authentication	• Unusual login attempts, such as from new locations or devices, trigger additional verification. • Sensitivity of requested resources (e.g., critical systems vs. general applications).
Windows/Linux Server MFA	• Windows MFA with offline OTP. • Linux MFA with offline OTP.
Directory Service	• Support for LDAP Protocol • Support for RADIUS Protocol
Audit & Analytics	• Auditing and Monitoring: Recording and monitoring user access to applications and resources to meet compliance and security requirements. • User Behavior Profiling: Analysis and Profiling of User Login, Access Behavior, Permission Changes, and Application Usage

PARAVIEW

For more information, visit our website at: www.paraviewsoft.com