RAPIDIDENTITY MFA

Advanced Multi-Factor Authentication Platform for Flexible & Frictionless Verification
Step-up Security with Multi-Factor Authentication, Tailored to the Way You Work

With 81% of all hacking-related breaches leveraging weak, default, or stolen passwords,* even complex passwords aren’t enough to stop today’s sophisticated attackers. Deny password-based breaches with advanced, multi-factor authentication (MFA). RapidIdentity MFA can replace passwords altogether or add extra layers of protection to all access entry points, including Active Directory, offline desktop, on-premise applications, cloud applications, employee and customer portals, and remote access using VPN and other technologies.

RapidIdentity MFA deploys in just days or weeks and is available as a standalone platform or can be fully integrated with RapidIdentity IAM for a complete solution that includes MFA for privileged accounts.

*Safeguard company data and systems being accessed via remote access solutions (VPNs, portals, virtual desktop infrastructure, remote desktops, SSH, etc), and verify the identities of all remote users.

Approve or deny access rights, while tailoring authentication methods with Risk-Based Authentication. RapidIdentity MFA adapts to how your organization defines risk levels, unlike the one-size-fits-all approach of other solutions.

Seamlessly perform secure, fast user-switching and direct authentication to Microsoft, RDS, Citrix® XenApp and XenDesktop, as well as to VMware® Horizon View.

Authenticate employees to Windows®, thin-clients, zero-footprint clients, local and remote applications, and Citrix, and also perform transaction-based authentication.

Deploy the right mix of authentication factors, while providing your users with fast, secure Windows logon. Windows login supports a wide variety of authentication methods to secure access to your users’ PCs and local application.

All RapidIdentity MFA authentication methods work online, with the majority working offline as well, provided the user has logged in online at least one time prior.

*Verizon 2017 Data Breach Investigations Report
The Broadest Range of Authentication Methods Available

Risk-Based / Adaptive Authentication - Adapts the stringency of authentication processes based on the likelihood that access to a given system could result in it being compromised using a risk scoring system.

Fingerprint Biometrics - A form of Biometric Authentication, this method automatically compares a user’s fingerprint to a stored fingerprint template to validate a user’s identity.

Push Authentication - Known as RapidIdentity PingMe within RapidIdentity, this method sends out-of-band push notifications to a pre-registered mobile phone or other device.

One Time Password (hard token, soft token, SMS, email, backup codes) - OTPs are unique passwords that are only valid for a single login session and defined period of time.

Bluetooth Authentication - This method leverages Bluetooth Low Energy (BLE) technology to enable users to effortlessly lock and unlock their computers when they approach or leave.

FIDO U2F Tokens - Universal 2nd Factor, or U2F, is an emerging universal standard for tokens with native support in platforms and browsers. U2F tokens are typically used for VPN authentication, web-based access, and Windows logon.

Smart Cards (contact / contactless) - Smart cards contain a cryptographic module that facilitates the generation and security of public key infrastructure (PKI) keys and certificates that are used for authentication.

RFID - Radio Frequency Identification (RFID) utilizes radio waves to communicate a unique identifier between a tag embedded in an RFID card and an RFID reader to verify a user’s identity and grant access.

QR Code - A QR code on a printed badge acts as a contactless card; however, instead of using a traditional card reader, a computer’s internal camera is used to read the QR code badge.

Pictograph - Instead of entering username and password credentials, users select the images that comprise their password from a pool of images. This method is ideal for younger users, such as K-5 students.

Magnetic Stripe / 2D Barcode - Cards utilizing magnetic stripe or barcode technology are presented to and read by a magnetic stripe or optical reader.

Social Login - Enables end-users to conveniently register and log into sites and user portals using their existing social network identities from Facebook, Twitter, Google+, and LinkedIn.

Challenge Response Questions - Utilizes previously answered challenge questions to authenticate a user and can be configured to be used in lieu of a password or to reset “something” a user should know, like a PIN or a password.
IMPROVE SECURITY WITHOUT IMPACTING USER EXPERIENCE

Strike a balance between usability and protection that drives user adoption with RapidIdentity MFA. Implement context-based policies that govern which multi-factor authentication method is actually needed—based on criteria, such as time of day, location, and network device settings. Users can even choose from a variety of authentication methods, like cell phone based soft tokens, one-time passwords, and biometrics, to best fit their situation.

LEVERAGE EXISTING SECURITY INVESTMENTS

Take advantage of existing investments in physical access by leveraging the same proximity card technology your employees already use to unlock and open doors to also open Windows™. Additionally, with such deployments, RapidIdentity MFA can be up-and-running in just hours with minimal end-user impact or training.

COMPLY WITH REGULATIONS THAT REQUIRE STRONG AUTHENTICATION

Deploy authentication technology that helps your organization satisfy regulations that require or strongly recommend strong authentication, such as SOX, CJIS, DFARS, HIPAA, HITECH, EPCS, Positive ID, and PCI-DSS. With RapidIdentity MFA, your organization can achieve compliance, while at the same time, improve the experience of end-users by streamlining authentication processes and reducing the amount of passwords that must be managed.