Multifactor Authentication Provides Low-Cost & Effective IT Solution

It's critical that your multifactor authentication (MFA) solution meets the basic requirements for secure identity and access management (IAM) solutions in a hybrid environment. Digital transformation today relies on a unified access management (UAM) platform that includes at least basic MFA. Use the checklist below to make sure your MFA solution offers the protection your company needs.

User Community Support

Does the MFA solution support all the user communities that access your sensitive data?

- Workforce (employees and contractors)
- Partners/Vendors
- Customers

Application Integration

Does the MFA solution work with the cloud and on-premises apps that are critical to your organization?

- Integration with cloud applications
- Integration with on-premises applications
- Integration with human resource management systems (HRMS), such as Workday or SuccessFactors
- Directory integration, such as Active Directory or LDAP

Enterprise Access

Does the MFA solution support the network access systems your organization uses or might use?

- VPN access
- WiFi access
- SSH/RDP access
- RADIUS integration

Authentication Methods

Does the MFA solution support the authentication tools that your organization uses?

- Native mobile OTP authenticator (push-based)
- Offline time-based verification codes (TOTP)
- Hardware tokens, such as Yubico YubiKey
- X.509–based certificates
- Legacy authentication methods, such as SMS, security questions, or email

Flexible Authentication Policies

Does the MFA solution enable flexible and sophisticated authentication policies at a granular level?

- Granular policies for different identities, apps, devices, and contexts
- Allows for definition of different policies for various identities, communities, or applications
- Customizable authentication flow
- Risk-based decisions

Developer Support

Does the MFA solution provide APIs and support for integration with your custom applications and third-party systems?

- MFA registration and life-cycle management APIs
- SDK for major platforms and languages

net-tech

Open Standards Support

Does the MFA solution support these popular, modern standards for secure connections to web applications?

- SAML
- OpenID Connect
- OAuth2

Reporting

Does the MFA solution provide reports that enable you to meet compliance requirements and enhance your security based on threat data?

- Ability to externalize authorization events to third-party SIEM solutions
- Out-of-the-box reports and audit trails
- Ability to effect system change based on authorization events
- Real-time information about access attempts

Advanced Requirements

Although any MFA solution should meet basic requirements, organizations making a successful digital transformation usually choose solutions that meet advanced requirements. MFA is evolving quickly. An advanced MFA solution ensures, from the start, that you aren't behind the curve.

Behavioral Analytics

Does the MFA solution use behavioral analytics to intelligently adapt and does it require different authentication factors?

- Familiarity signals
- Attack signals
- Anomalies (user behavior and context signals)
- Continuous authentication

Device Trust

Does the MFA solution take into account information about the device being used for authentication?

- Device health, including version, tampered, lock, encryption, browser plug-in, and more
- Device reputation
- X.509–based certificates
- Integration with mobile device management (MDM)

Users and devices

Does the MFA solution support user access via multiple devices and does it account for different types of users and user roles?

- Support for multiple devices
- Support for different user communities, such as employees, contractors, partners, IT administrators, and customers

General considerations

Can you integrate the MFA solution with your custom apps and in your organization without having to replace or significantly modify existing solutions?

- Enables integration into your custom apps via an API
- Enables incorporation of MFA without the need to rip and replace other solutions

How Net-Tech Provides Managed IT Services to Help With Your MFA

Don't let a bad actor exploit any cracks in the wall of your defense. It's crucial to take every step possible to increase your network security. Net-Tech can help you set up MFA correctly, test it, and guide you through scaling for your entire organization. Throughout the process, we will also provide administrative assistance and user training.

The Total Care Cloud subscription service from Net-Tech includes MFA setup and support. If you still have questions about implementing MFA or would like assistance with setting it up across the apps your employees use, please contact us.

Want to discover more ways to keep your systems safe?

Contact us for a complimentary IT analysis with one of our top cybersecurity experts today.

Call (425) 452-8324

net-tech