okta

MFA Evaluation Guide

Okta Inc.
301 Brannan Street, Suite 300
San Francisco, CA 94107

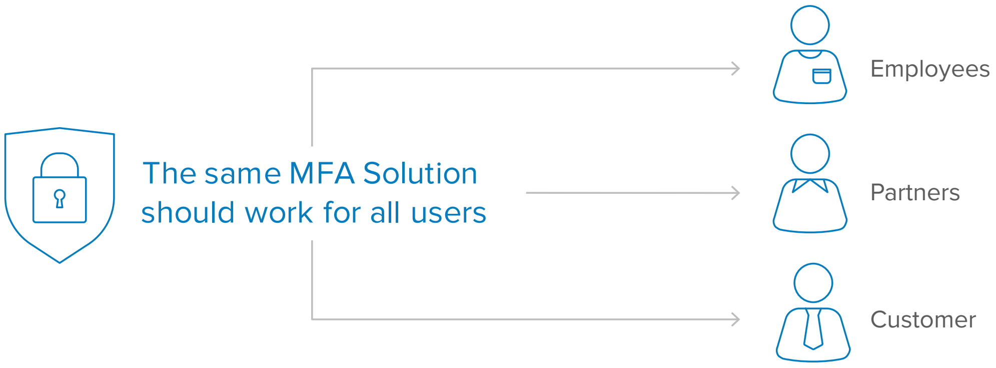
info@okta.com
1-888-722-7871

4 Key Considerations to Guide Your Choice in MFA

Multifactor authentication (MFA) is a critical security requirement for every organization, regardless of size and industry. But not every MFA solution is created equal. Your investment in MFA should be well-thought-out. Not only does your chosen MFA solution need to meet the requirements you have today, but it needs to enable and secure the future growth and evolution of your business. This evaluation guide will help you understand the key factors you need to consider when investing in MFA.

1—One Solution for Every User: Your MFA Must Support Workforce and Your Customers

Most security journeys begin with meeting internal needs. The same is true for MFA. You start out looking for a solution to enable your employees and contractors to securely authenticate to your enterprise servers and applications. As your organization grows, your digital presence will expand to offer services to your customers that also require strong authentication. It might be through mobile apps, website portals, or other digital venues that require customer logins.



The same MFA Solution should work for all users

While many of the core aspects of identity and access management span the needs of both workforce users and customer users, each audience has different needs. For example, while some organizations might not worry about giving their internal users a frictionless MFA experience, they will understand that such frictionless experiences are vital requirements to keep customers happy and engaged. The ability to address customer specific needs must be a prerequisite for the MFA solution you choose if you want to be able to expand your service offerings to your customers. That said, your MFA solution shouldn't shortchange your internal users. It's just as important that your chosen MFA offering deliver the best possible experience for your internal users too.

Another problem can arise when security and marketing teams fail to communicate. Your security team might be fully engaged in driving an MFA initiative to address compliance or data security needs, while marketing on its own decides to develop and release an app for customers without understanding the need to incorporate MFA. That puts your customer data in peril, jeopardizing your corporate reputation, setting you up for future lawsuits, and putting you in financial risk.

If your existing MFA solution can't adequately handle customer authentication needs, you're left with the choice of replacing that MFA solution or investing in a second one. While having two MFA solutions in place might seem like an okay solution, it usually causes ongoing problems and difficulties. First of all, maintaining two separate MFA solutions substantially increases your licensing costs, administrative efforts, and help desk burden. Second, it can lead to inconsistencies in MFA policies and capabilities that create gaps in your security posture. Often those gaps go on undetected until damage is done to your reputation and financial standing.

A worse scenario is when an organization simply decides it doesn't need MFA for its customer users. With 81% of data breaches leveraging weak or stolen passwords, a considerable number of public apps—such as Google, Facebook, Twitter, and Dropbox—are implementing MFA to better protect their customers. if you don't have MFA for your customer experiences, you're putting your reputation at significant risk. You might even be opening the door to direct financial attacks, such as would be the case if your customer experience includes shopping cart accounts that are not MFA protected.

When evaluating MFA solutions, think holistically and plan with the future in mind. Choose a solution that fully addresses the authentication needs of your internal workforce and your external customers. Your MFA solution should be able to facilitate your ability to incorporate MFA into ad hoc projects created by marketing or other departments with speed-to-market as a priority and without placing a burden on your development teams. Your MFA solution also needs to present frictionless experiences for all your users, especially your external customers.

2—Your MFA Must Support Multiple Factors

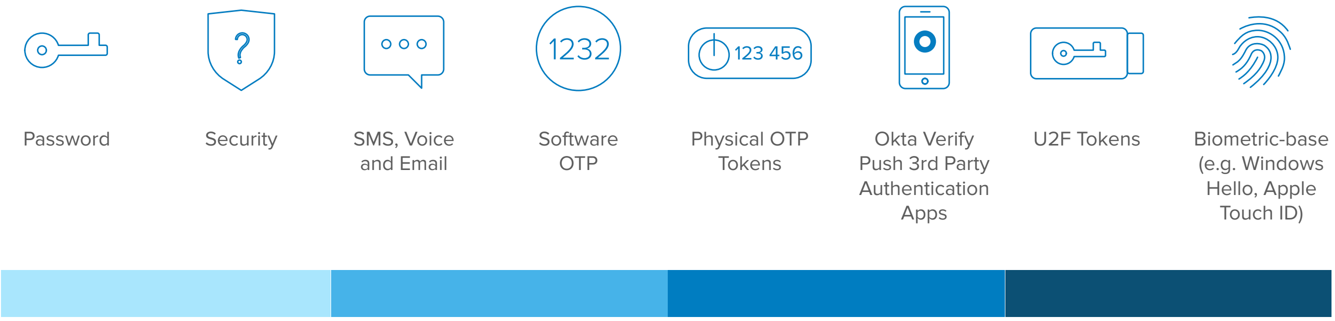
When evaluating MFA solutions, a top priority should be finding one that offers an extensive variety of factors—i.e. SMS, third-party factor like Authy, push notifications, and hardware tokens. This is because different types of users need different levels of security and identity assurance. Additionally, you need to be able to offer multiple options to ensure users have frictionless experiences.

Maybe you want your office employees to use push verification as their primary MFA factor. But what happens if one of them accidentally leaves their mobile phone at home? You can give them the option to use a voice call to a corporate landline.

[1] 2017 Data Breach Investigations Report, Verizon

You might want to require your engineers and maybe even executives, to use either U2F or some form of biometrics to heighten protection of their access to super sensitive information. You might also have legacy systems that require support for outdated or expensive hardware tokens that you don’t want the bulk of your users to use as their MFA factor.

An array of MFA factors also enables your customers to have positive, yet secure experiences with your apps and websites. For example, you might want to let your customers choose from factors such as push verifications or a third-party factor like Authy. But what if some of your customers don’t have smartphones or don’t want to install an app? In lower risk situations, you might choose to give them other options, such as voice call authentication, email, or perhaps SMS authentication with the warning that it’s not as secure.


1232
123 456
Password
Security
SMS, Voice and Email
Software OTP
Physical OTP Tokens
Okta Verify Push 3rd Party Authentication Apps
U2F Tokens
Biometric-base (e.g. Windows Hello, Apple Touch ID)

There is no one-size-fits-all when it comes to MFA factors. Choose an MFA solution that lets you meet the unique flexibility, security, and usability needs of your different users, as well as one that allows you to choose cost-effective factor options when appropriate.

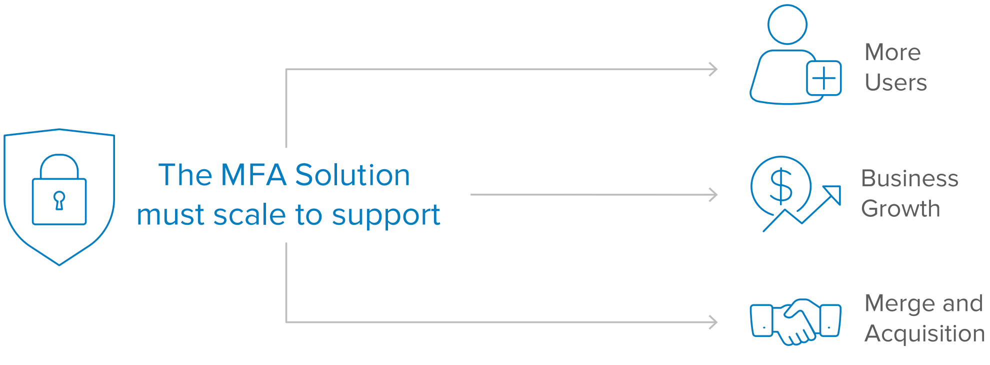
3—Your MFA Solution Must Be Part of a Platform That’s Future-Proof and Easy To Extend

Growth and evolution is a natural outcome for any successful business. Your MFA solution needs to enable that growth and facilitate the evolution of your business in a variety of different areas:

- Handling business growth
- Adding other identity management capabilities
- Expanding MFA coverage

Handling Business Growth

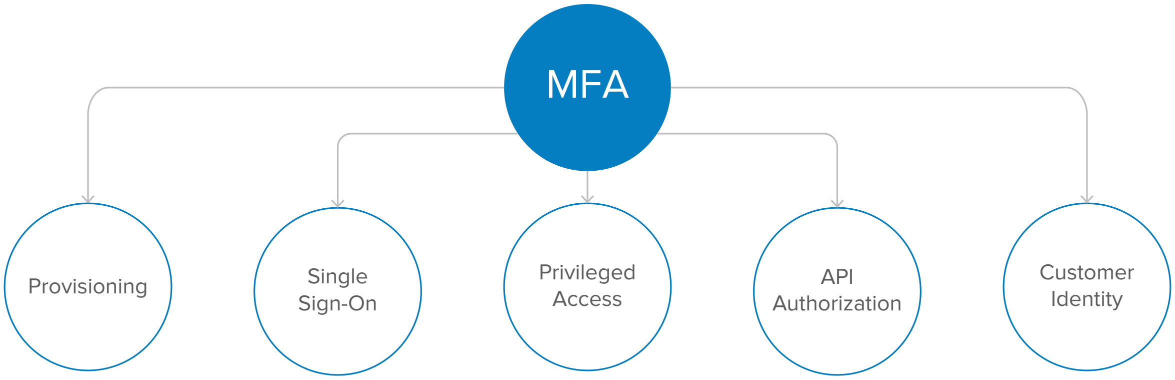
You need to choose a MFA solution with growth in mind. As your business expands to more employees, contractors, and customers, your MFA solution needs to handle that expansion without requiring you to redeploy or procure new systems. Not only does that mean it needs to be able to easily scale, but it needs to make onboarding of new users a simple and seamless experience.



Business growth can also lead to new partnerships or even mergers. What if one of your new business units, partners, or contractors has their own identity management (IDM) system? Will your chosen MFA solution integrate with that system using federation? What if these new businesses or partners bring on new users in less traditional ways, such as through mobile or web apps? Will you have to invest in added technologies or different point solutions to allow your chosen MFA solution to integrate with these different types of methodologies? When evaluating MFA solutions, make sure you choose one that has the flexibility you need to support multiple, diverse ways of bringing on new users.

Adding Other Identity Management (IDM) Capabilities

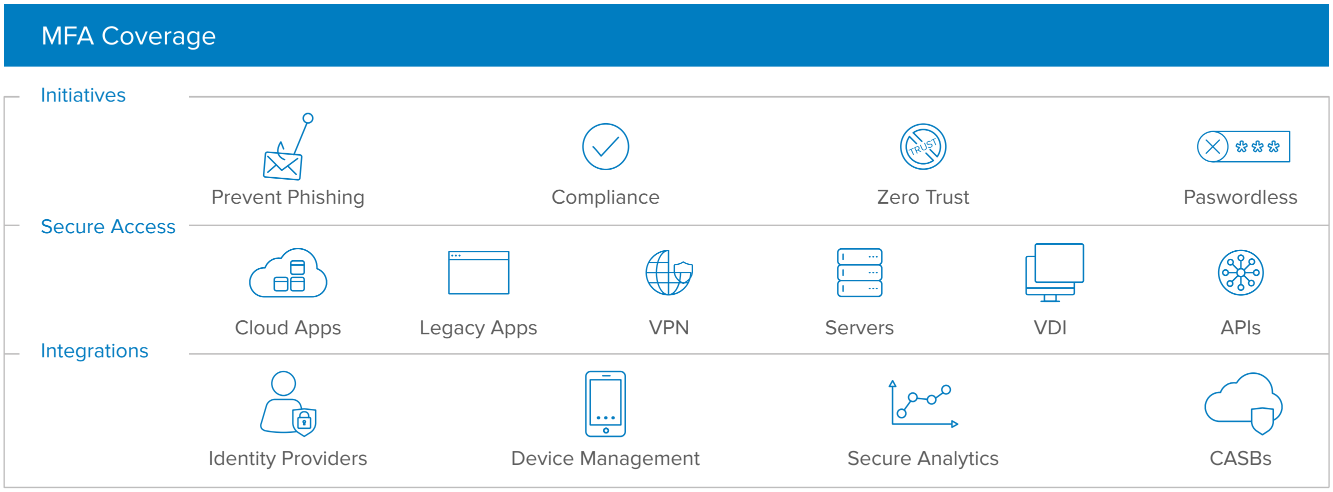
MFA could be the start of your IDM journey, but it very likely won't be the end of that journey. As your business grows, you might want to add additional capabilities such as single sign-on (SSO), account lifecycle management, and even API-based authorizations. Adding these other capabilities shouldn't require a major overhaul of your environment or significant integration effort to make them work with your MFA solution.



For example, implementing an SSO solution can save your users a lot of time, and create a more seamless and frictionless authentication experience. But some MFA solutions simply require you to procure, implement, and integrate SSO manually once you decide to expand. And worse, they require you to keep syncing disjointed data for years. Ideally, you want to choose an MFA solution that supports additional IDM capabilities on the same platform. Expansion needs to be turnkey and not require additional planning, migrating, and syncing of user data, or more. Your MFA choice should offer a full range of solutions to choose from that you simply turn on and you're ready to go. When you're ready to broaden your capabilities, you don't want to be slowed down and frustrated by integration hassles. You want a MFA solution that lets you seamlessly and quickly expand your IDM functionality as your business grows.

Expanding MFA Coverage

MFA rarely supports just a single authentication experience. If you don't already, over time you will likely want to integrate MFA into several different types of services or user experiences that you offer. This could include help desk ticketing, human resource services, customer management, project management, development platforms, application delivery controllers, and any number of clouds apps, services, and platforms.



MFA Coverage

Initiatives: Prevent Phishing, Compliance, Zero Trust, Paswordless

Secure Access: Cloud Apps, Legacy Apps, VPN, Servers, VDI, APIs

Integrations: Identity Providers, Device Management, Secure Analytics, CASBs

Before you invest in a MFA solution, make sure it provides an extensive selection of out-of-the-box integrations to cover your current offerings and potential future ones. Beware of solutions that only integrate with leading solutions or are vendor-biased. Unless the integrations span the gamut of large and small offerings, as well as established and innovative new solutions, you could end up spending significant time and expense developing or paying for those integrations yourself. Even worse, you might find you're not able to integrate at all.

In addition to having a large library of pre-built integrations, make sure your MFA choice offers a robust API with easy-to-use SDKs, documentation, and widgets to facilitate integrating MFA with custom web apps, server solutions, as well as iOS and Android apps.

4—Your MFA Must Support Modern Capabilities

MFA has evolved significantly over the years. It began with two-factor authentication, also called 2FA, which was the first answer to the problem of password security simply not being sufficiently secure. 2FA typically consisted of using a pre-defined PIN number or a SMS to verify an individual's identity. Implementing 2FA usually was a manual effort that required in-house development to integrate it into SMS gateways or whatever system or application you were offering.

The second generation stepped up identity verification considerably with the use of hardware tokens. Their compact nature made them easy for users to take with them wherever they went, but hardware tokens can also be easily lost or stolen. Even though their approximate $20 cost per token seems low, rolling them out to every user in a large organization and keeping multiple servers on-premises to validate tokens gets cost-prohibitive.

The third generation of MFA moved into the cloud with software-based mobile verification factors such as one-time passwords (OTP) and push notifications. It offers the same capabilities and level of security as hardware tokens, but it's easier to take advantage of with a lower cost and better mobility. While MFA in the cloud brought significant advancement to MFA in terms of security, mobility, usability, and flexibility, it still falls short in terms of the more adaptive, seamless, frictionless, and intelligent capabilities that today's modern users and organizations demand.

The latest generation of MFA expands the cloud MFA to a broader platform and offers a full range of capabilities without additional integration pain. Organizations are quickly recognizing the need to make sure their choice in MFA offers these capabilities, which include the following:

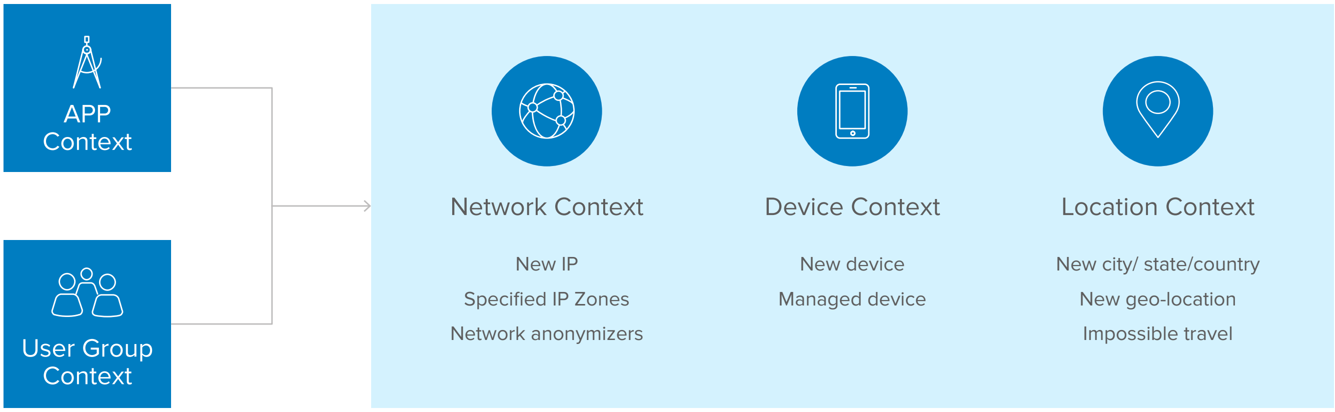
- Adaptive MFA
- Authentication intelligence and insight
- Responsible password-less authentication
- Identity provider discovery and routing
- Seamless expansion to single sign-on, account lifecycle management, and custom integrations via APIs and SDKs

Adaptive MFA

Adaptive MFA takes a dynamic, risk-based approach to MFA that enables organizations to significantly strengthen authentication security, while delivering a more seamless and frictionless experience for users than ever before possible. It leverages contextual attributes of the user and device to gauge on-the-fly the risk level of an access request, and then subsequently determines if authentication requirements for that request should be denied, stepped up, or even stepped down. It can take into account things such as changes in user behavior, device behavior, or location. Is the user authenticating from an unfamiliar location or new device? Is a weak password being used? Are there brute force attack indicators? Are there anomalies in the user's behavior? Did the user attempt to log in from a location thousands of miles away from a location that they just logged in from minutes or hours ago?

When the contextual indicators suggest a higher level of risk such as in the above cases, policy can trigger the need for multiple layers of MFA or even deny access. Additionally, if the contextual indicators in adaptive MFA suggest lower risk, policy could lessen the requirement for multiple factors.

Adaptative MFA-Contextual Access Management



The power of adaptive MFA is that it reduces user friction when friction is not necessary, and it can tighten security access when it detects certain risk factors. This balance between being secure and user-friendly can be illustrated with how you might configure access policies in an environment without adaptive MFA versus an environment with adaptive MFA. For example, without adaptive MFA you might deny access to anyone who is trying to authenticate from certain foreign countries where you don't do business and that are known originating locations for hacker activity. This strict rule can help keep your organization safe, but it can also cause significant business disruptions for salespeople or executives who in the future might visit that country to explore new opportunities.

This scenario can be handled in a secure, but more user-friendly way with adaptive MFA. Instead of writing a policy that denies all access from a certain location, the policy could prompt for certain MFA factors when access attempts originate from that country. The adaptive MFA policy could also look at a variety of contextual conditions, such as time of day, device being used, geographical anomalies, and more, to further tighten or loosen authentication requirements.

Authentication Intelligence and Insight

Your MFA investment should also leverage authentication intelligence to easily tell the difference between suspicious login behavior and normal login behavior. This requires gathering authentication information from thousands of different organizations and continually analyzing and comparing the attributes of millions of different login attempts.

Such intelligence gives you visibility into login attempts that might seem innocent, but based on past analysis reveal that under this certain condition it has a high likelihood of being nefarious. With that indication of suspicious activity, the MFA solution should enable you, by policy, to determine your course of action, including denying access or requesting additional MFA factors.

Responsible Password-Less Authentication

People sometimes have a resistance to MFA since it often adds extra steps to authentication. But when you can leverage authentication intelligence and combine it with the dynamic and contextual response capabilities in adaptive MFA, you put yourself in a position to actually reduce authentication steps and user friction. This includes the ability to introduce “responsible” password-less authentication, where instead of prompting for a password, you simply prompt for some other MFA factor, such as a biometric or push verification. It’s referred to as responsible password-less authentication because before it ever allows password-less authentication, it validates the trust and risk level of the access by comparing its contextual knowledge of the access against real-world relevant authentication intelligence.

Basic password-less authentication has been available for awhile, where users can access a system without a password by using some predetermined authentication factor. The problem with this basic level of password-less authentication is that you don’t have a clear way of knowing if you can trust the user. For example, if a hardware token is your authentication factor, how do you know if it’s really being used by an authorized user? What if the token was lost or stolen? What other unknowns might raise the risk level of that access?

With adaptive MFA and authentication intelligence, you can gain a high level of confidence that the person trying to authenticate is who they say they are. Scenarios where responsible password-less authentication might be automatically enabled could include a user trying to access a system from a network the user has used several times before, access to the system during business hours from a known trusted network such as your intranet, or accesses that follow the user’s known pattern of access, such as at the same time and place.

One of the powerful aspects of combining adaptive MFA and authentication intelligence to enable responsible password-less authentication is that you can employ several layers of security without the user having to do anything. You can use knowledge of the device being used, the location, time of access, past access patterns, and other contextual information to create an extremely frictionless, yet secure experience.

Identity Provider Discovery and Routing

When you deploy MFA you typically integrate it into the workflow of your organization’s identity and access management (IAM) framework. But how do you handle authentication and MFA for your partners and contractors who need access to your internal systems? Do you go through the work of onboarding them into your IAM framework? You might if it only requires onboarding a few people. But what do you do if it’s more than a few?

Your MFA solution should offer identity provider discovery and routing so you don’t have to worry about onboarding. It should give you the option to allow your partners or contractors to use their own internal or third-party identity provider system, while enabling you to still enforce MFA according to your own policies.

For example, when your partners’ users log in to your portal, the MFA solution can detect by the username that those users need to use the partner’s identity provider system and then automatically and transparently leverage that system for authentication. However, if that partner’s identity provider system doesn’t use MFA, once users authenticate to the partner’s authentication system, your MFA solution can require them to respond to your MFA requests before they can access your environment. That capability facilitates your ability to allow contractors and partners to use their own identity providers, while enabling you to secure access to your internal resources according to your defined MFA policies.

Choose Your MFA Wisely

Your MFA choice determines how well you can protect access to all your internal resources, as well as your ability to provide frictionless experiences for your internal employees and external customers. Your MFA choice also impacts your ability to grow your business and take advantage of emerging technologies and future innovations. As part of Okta's identity-led security framework, Okta Adaptive MFA delivers on the key considerations that need to be part of your search for a solution that meets all your MFA requirements today and in the future.

Okta Adaptive MFA enables you to address the different levels of security and identity assurance of all your different user types, including your internal workforce, partners, contractors, and customers. Its wide range of authentication factors give you the flexibility you need to deliver secure and frictionless user experiences, while keeping your costs low. The extensible nature of Okta Adaptive MFA and its more than 5,500 out-of-the-box integrations make it easy to implement MFA across all aspects of your environment, including your on-premises systems and applications, third-party hosted platforms, cloud services, mobile apps, and more. The Single Sign-on, Lifecycle Management, Universal Directory, and API Access Management services in Okta's Identity Cloud allow you to turn on additional identity management capabilities with ease whenever needed. With Okta Adaptive MFA's modern, next-generation MFA capabilities, such as Adaptive MFA, responsible password-less authentication, authentication intelligence with Threat Insight, and IDP discovery/routing, you can future-proof your ability to meet the MFA requirements your organization and users demand today and will need tomorrow.

For more information on how to take advantage of Okta Adaptive MFA, visit www.okta.com.

okta