Whitepaper

Multi-factor authentication deployment guide

January 2023

Contents

Introduction: Hardening your defenses in the age of mega-breaches

Sophisticated cyber attacks continue to rise, and credential-based attacks constitute a large part of the increase. According to a recent report, email attacks against organizations rose by 48% in the first half of 2022. Relative to the previous six-month period, more than two-thirds of these attacks were credential-phishing attempts (an email containing a malicious link designed to steal sensitive account information). In these attacks, 265 individual brands were impersonated.

Threat actors have taken advantage of the shift to remote work by stepping up social engineering tactics like phishing, and by using data breaches to perform account takeovers. As a result, multi-factor authentication (MFA) has rapidly become a primary method for increasing the assurance that a user is who they say they are. MFA lets organizations secure access to all their resources, including consumer/enterprise web and mobile apps, in an increasingly remote and hybrid world. Governments, regulatory bodies, and corporations have come to understand its critical role in establishing a modern Zero Trust security posture (never trust; always verify).

Today, MFA has become essential to a robust, identity-first security strategy. As one example: A January 2022 executive order issued by the U.S.

President's Office of Management and Budget established phishing-resistant MFA as a fundamental requirement for modernizing cybersecurity across federal agencies. As governments, companies, and cybercriminals evolve, the nature of MFA is morphing too, including the rise of passwordless authentication and the increasing importance of devices (managed and unmanaged) for evaluating security posture.

This guide is designed to provide best practices for fully leveraging the promise of MFA, including upgrading to passwordless authentication. We'll review the results of a survey we conducted in partnership with IDG which demonstrates the powerful role Identity and Access Management (IAM) plays in modern auth and security, and which showcases the most recent priorities and adoption trends of your peers. We'll also use this space to help organizations understand important elements to consider in designing MFA solutions, such as

- Implementing phishing resistance
- Understanding policies and regulations, and
- Contemplating changing access needs.

Based on our observations working with engineering and product teams, we conclude with practical advice for those building MFA for their applications.

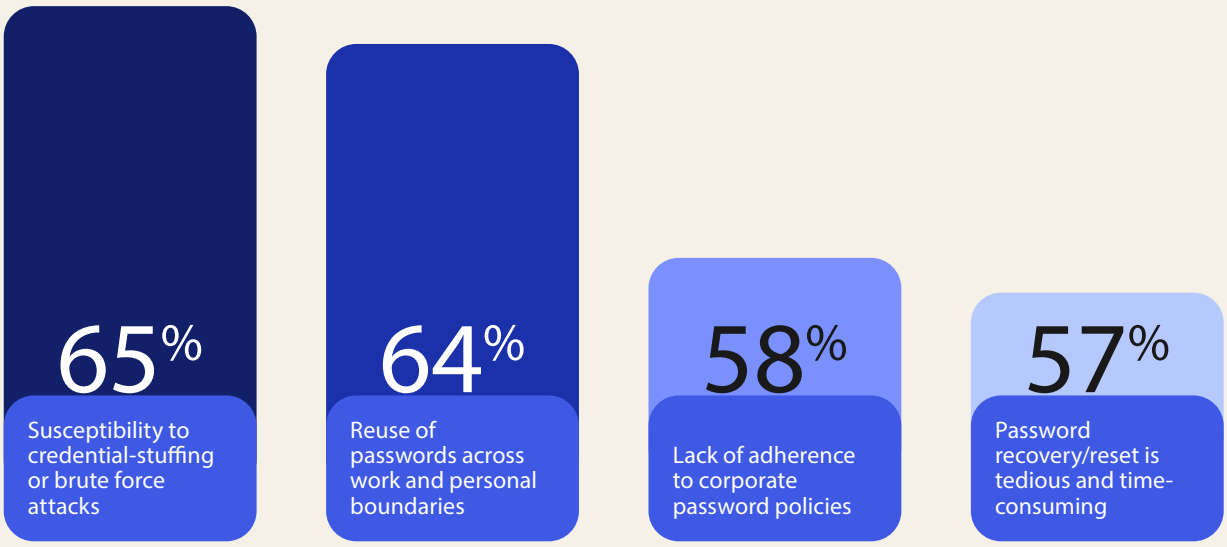
Deploy phishing-resistant MFA as part of a strong IAM strategy

Today's identity-based threats take many forms, including malware, hacking, and phishing. These assaults lead to downstream outcomes like credential theft, account compromise, and exfiltration of data. To prevent these common threats, organizations must elevate their security posture to meet them, and the first line of defense is Identity. Companies still relying on legacy identity approaches, like on-premises apps and firewalls, leave themselves alarmingly vulnerable to sophisticated attacks. In essence, they depend on a slow, complex, and fragmented framework to protect their organizations and employees.

But let's break this down: Our joint survey with IDG reveals some specific concerns and statistics regarding secure authentication from IT and Security leaders.

Top password-related concerns

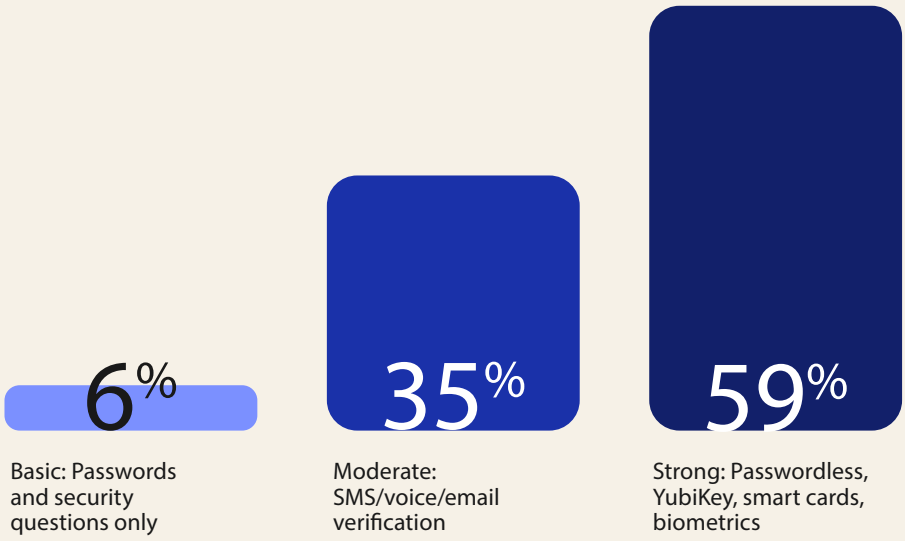
1,000+ employees 70%
500-999 employees 52%



Insight: Respondents cite multiple password-related concerns, including stolen credentials and re-use of passwords across work and personal accounts.

Level of MFA that makes the most sense for business

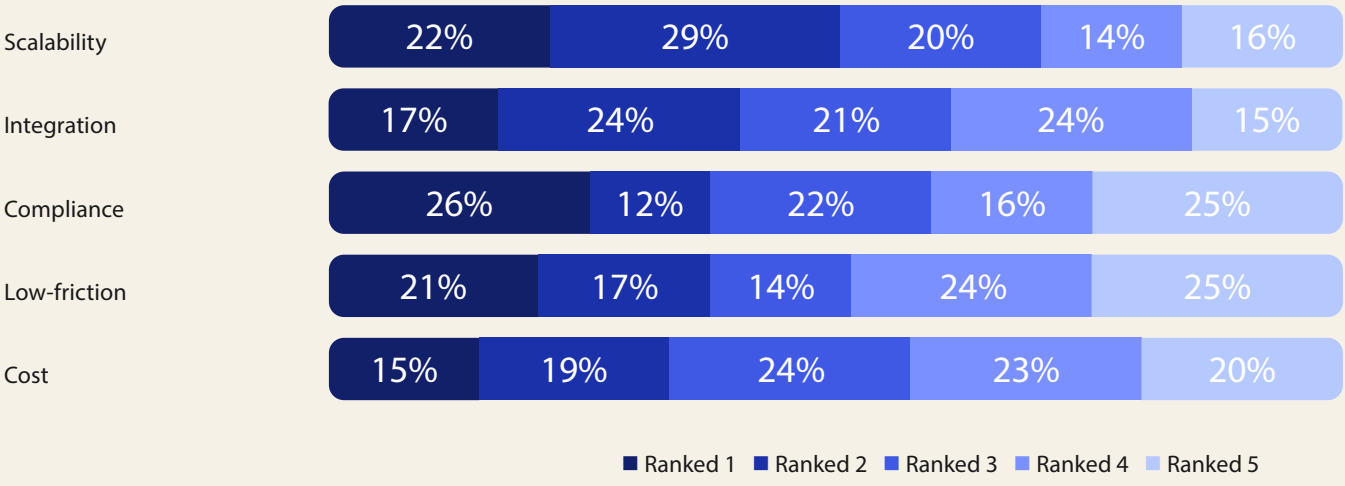
IT VP and above	73%
IT Director/Manager	53%



Insight: More than half (59%) say the strongest MFA solution available is the most appropriate for their business.

Importance of criteria when choosing an MFA solution

Organizations were asked to "stack rank" all five criteria from most to least important.



Insight: 51% rank scalability among their top two considerations when choosing an MFA solution.

Consider the assurance level of different authentication factors

Generally speaking, authentication validates identity using one of three types of factors:

- Something you know (a password)
- Something you have (a personal identity verification smart card)
- Something you are (a fingerprint)

For added security, MFA employs two or more types of factors. And while the most common version is still a password used in conjunction with a time-based token, a push notification to a mobile app, or a biometric factor, there are various approaches to MFA. They each present different tradeoffs.

Different types of authenticators are available with varying degrees of strength. At Okta, we rank authenticators by assurance levels as follows:

LOW: Passwords, security questions, one-time-passwords (OTPs) through SMS, voice, or email, and OTP apps like Authy and Google Authenticator

MEDIUM: Mobile push notifications and physical-token OTPs

HIGH: Personal Identity Verification (PIV) or Common Access Card (CAC) smart cards, FIDO 2.0 / WebAuthn + CTAP2

Of course, assurance level isn't the only consideration for organizations seeking to strengthen their MFA. Authenticators must also be easily deployable and put into use by workforces and customers. They must also be resistant to specific kinds of threats like man-in-the-middle (MitM) or adversary-in-the-middle (AitM) attacks. But there's no substitute for hardening security with the highest assurance factors.

Offering SMS as a factor, for example, may be a quick way to get users up and running with MFA, but it does not provide a high level of assurance. Common security issues, like SIM hijacking and large-scale smishing and vishing attacks, undermine the level of assurance that SMS authentication can provide. That's why we highly recommend utilizing stronger MFA factors, like Okta Verify Push, or biometrics (via WebAuthn or, in the case of the U.S. government agencies, PIV/CAC smart cards.)

Best practices for designing strong MFA

1. Consider (and reconsider) your MFA policies

Before deploying an MFA solution, you need to assess the security risks and specific threats your organization faces. Which resources and attack vectors are your primary concern? A well-considered, risk-based policy configuration should trigger "step-up" authentication challenges when the risk is particularly high.

For example, a policy could ensure that a second factor is required every eight hours when logging in from a known network, or only require that second factor when logging in from a new device or geolocation. Or, perhaps you have a certain group of user accounts with broad access to sensitive data—for them, you need a stricter policy. Examples might include developers in your organization with access to source code, or executives with access to sensitive data. You can require a stronger factor type or ask them to respond to additional MFA prompts. You might even consider implementing MFA for sensitive actions within applications. By allowing more fine-grained controls on operations that are deemed highly sensitive (such as approving purchase orders or transferring funds) you not only reduce risk, but can seamlessly implement security that meets ongoing compliance requirements.

Ultimately, any additional verification should be as transparent as possible and eliminate friction. It should foster a good user experience—without compromising security.

2. Plan and provide for a variety of access needs

For users with internet access but little or no service from their cell phone carriers—think a Wi-Fi-enabled airplane, a rural home, or the basement of a concrete building—voice and SMS may not be feasible. In these cases, Okta Verify with push or a one-time password (OTP) are better choices, as this communication is encrypted over the phone's internet connection. Hardware devices that generate event-based or time-based one-time passwords (TOTP) don't require a communication channel at all, and are difficult to tamper with or copy. However, physical devices can be costly to deploy, and easy for employees to forget at home or lose. For these reasons, factor types may not be the best choice for short-term contractors or high-turnover roles.

Organizations should choose MFA factors that solve for a wide variety of scenarios; there's rarely a one-size-fits-all solution to accommodate all situations. Generally speaking, the following deployment tips ensure both enhanced security and a great end-user experience:

- Provide users with multiple factor options, so they always have a backup. If one auth factor is a password, plan for breached password detection to alert users and to block the usage of any breached passwords.
- Only enable strong, phishing-resistant factor types and move towards passwordless MFA, or PIV/CAC smart cards for U.S. government agencies, whenever feasible.
- Check the origin of the web URL before authenticating. Credentials should be linked / bound to the domain from where the access request originates.
- Where your hardware supports it, allow users to use biometrics as their second factor (examples include Windows Hello and Touch ID). This simplifies end-user experience and increases the level of assurance that a user is who they say they are.

3. For sensitive apps, enforce high assurance and phishing-resistant authenticators as part of your MFA policies

As mentioned earlier in this guide, not all authenticators are phishing resistant. All authenticators offer varying degrees of resistance to social engineering, as all authenticators impose costs and risks on adversaries seeking to take over an account. For example, SMS-based OTPs can be intercepted fairly easily. Push authenticators offer greater resistance to static credential-phishing campaigns than authenticators that rely on OTPs.

Combining Push with Number Challenge, which asks the user verifying a push request to identify a number presented on the sign-in page, offers resistance to a broader set of adversary techniques including "MFA Fatigue" attacks. Hardware-based authenticators offer the highest levels of assurance.

The most reliable definition for phishing resistance is maintained by the US National Institute of Standards and Technology (NIST). According to NIST, phishing resistance requires that the channel being authenticated is cryptographically bound to the output of the authenticator. In simple terms, this means that the domain (i.e., address) of the website you are signing in to is tied to your authenticator. This ensures that it won't issue your credentials to a phishing web page.

Several authenticators available in Okta's platform meet this definition. Okta supports roaming FIDO2 WebAuthn authenticators (i.e., security keys) and device-bound FIDO2 WebAuthn authenticators (e.g., FaceID, TouchID, or Windows Hello). We also support using PIV smart card auth within an app's sign-on policies to access specific apps. Depending on your deployment model, FastPass (Okta's device-bound passwordless authenticator) also meets this definition. Mandating the use of at least one phishing-resistant authenticator eliminates the risk of sophisticated phishing attacks via social engineering and AitM attacks.

4. Check compliance requirements carefully

Most IT compliance standards, such as PCI DSS, SOX, and HIPAA, mandate strong user authentication controls—they're often prime motivators for an MFA deployment. If your goals include meeting such standards, ensure a detailed understanding of the requirements so you can tailor configuration and policies to them. For example, PCI and HIPAA compliance require strong authentication that includes at least two out of three strong authentication methods. SOX focuses less on technology and more on passing an audit– you'll still need to prove that your organization's finance and accounting data is secure. IT compliance requires implementing relevant standards and proving you've met them. Make careful documentation part of your configuration and implementation process so you can quickly generate proof in the event of an audit. Your future self (and your org) will thank you.

5. Model your MFA to secure the growing hybrid workforce

As remote and hybrid employees and contractors attempt to access their resources in the cloud, bolstering security is critical. Ideally, new employee onboarding should be done in the office, where existing employees have in-person access to IT. But remote work brings new challenges for MFA deployment and troubleshooting.

To speed MFA deployment, it's best to enable factors that allow users to quickly get up and running (like built-in device biometrics or mobile app authenticators like Okta Verify) rather than making them wait for a hard token to be shipped to them. This ensures they can quickly access the resources they need to get set up. For remotely onboarding new employees, some organizations now host virtual onboarding sessions and send setup instructions to the employees' personal email address, so they can convey information even before the new hires have access to their corporate email.

6. Have a plan for lost devices

Workplaces that allow BYOD (bring-your-own-device) have seen a sharp increase in employees using personal devices to access corporate assets. However, there are some significant security challenges that come with these unmanaged devices. Many companies with BYOD policies experience data breaches via employee devices, making it imperative to secure this open threat vector.

Device assurance policies let you check sets of security-related device attributes, such as OS version, disk encryption, and jailbreak/root detection, as part of your authentication policies. In this way, device assurance policies create an additional security layer on top of authentication policy rules to validate the security posture of the device in use.

Another consideration is the fact that employees routinely download company data to their desktop/laptops. For this reason, it is important to be able to require users to complete an MFA challenge after they enter a password to unlock their machine. Most compliance guidelines include MFA as a requirement, and the ability to do this at the machine-level prevents the risk of a desktop-related attack and protects data in the event a laptop is lost or stolen.

However, anything a user has, a user can lose, and a procedure for handling lost devices should be part of your comprehensive IT helpdesk playbook. For any devices used for MFA, ensure that reporting a lost device results in:

- Closing any current sessions and requiring the user to re-authenticate
- Disassociating the device from the user's account and access rights
- Remote wiping of corporate information on mobile devices (usually done on company-owned devices)

It's also important to audit the user account's activity prior to the point in time when the device was lost, to note any unusual activity. If you notice anything suspicious, consider the possibility of a breach and escalate accordingly. Once you handle immediate security concerns, focus on getting the employee back to work with a replacement device or login method. For example, an alternative process like calling the IT helpdesk to verify identity requirements can allow the employee to be productive while you implement replacement factors.

7. Consider adaptive MFA

Step-up MFA can allow fine-grained control over how and when MFA is applied, but it requires careful consideration to configure. In some cases, even for well-defined policies and criteria, you may want to be able to make dynamic access decisions based on changes to user or device context.

Adaptive MFA works by noting access patterns and then adapting the policy around each user or group. For example, an employee who routinely travels and checks email from overseas may only periodically require a second authentication factor, but an employee who never travels would immediately receive an MFA challenge when overseas. Risk-based policies, like prompting for a step-up authentication challenge when trying to access resources through an unauthorized proxy, or automatically blocking access from known malicious IPs, can also kick in when triggered by suspicious events. Adaptive MFA is a powerful tool to automatically derive dynamic policies over time—ones that are tight enough to give you the security your organization requires, but flexible enough to treat your users as individuals.

8. Phase your deployment

Complex deployments and policies rarely work perfectly right out of the gate. When a process change affects all employees, you should always track its effectiveness as it's deployed, and be prepared to refine policies based on observations. Phase your deployment so IT/Security start using MFA first; from there, you can expand to additional user groups. Get comfortable with the auditing functionality early in the process, which will be invaluable for troubleshooting and adjusting policy configuration in the future.

For example, once you've deployed MFA to a specific group of users, you

can use auditing tools to spot check adoption and use. Try implementing a mechanism for user feedback. Users may not always take the time to provide written feedback, but an audit trail gives you some visibility into what they experienced. Did it take them three tries to enter their OTP? Did they give up? Problems like these could indicate a misconfiguration, a gap in user education, or simply a scenario that wasn't considered in the initial rollout plan. Using audit tools and encouraging employee feedback assures all stakeholders that the system is working as intended and new security policies are successfully adopted.

9. Provide user education

Deploying MFA to reduce security risks from password-only access is an essential security practice in a highly digital world. But some users will see it as an inconvenience, worrying that this process change will consume valuable time during their busy day. It's critical to ensure that everyone—from management to IT teams to security teams to end users—is aligned on why you're making the shift to MFA. Achieving buy-in from the entire organization ensures everyone accepts and understands their role in keeping the company secure. Education can help users appreciate the security benefits of taking this additional step.

One common approach is for IT to send out emails announcing upcoming changes. Another is to carry out mock phishing drills in an organization to demonstrate how even the most seasoned employees can be tricked into revealing their credentials. Be sure to include screenshots, FAQs, and contact information so employees can easily reach out for assistance.

Understand and manage the vulnerability of your account recovery flow

Multi-factor authentication is only as secure as its account recovery flows. In highly publicized recent cases, attackers exploited vulnerabilities in the account recovery process to gain control of an account.

For example, imagine a company called Acme. Acme's web application provides for MFA based on a soft token app installed on a user's phone, and allows the user to enroll a phone number to receive a backup second-factor for account recovery in the event that the user is unable to access their soft token. The strength of Acme's second-factor now depends on the strength of the telecom provider's processes for authenticating the customer and forwarding calls or SMS. Will the attacker be able to impersonate the user and convince or pressure a customer service rep to route calls or SMS to a number she controls?

Because every second-factor will need a reliable method for replacement, organizations must design secure recovery flows. Different approaches will suit different circumstances, but here are some best practices to keep in mind:

Keep primary and secondary factor recovery independent.
It's important to separate the recovery of the secondary factor from the recovery of the primary factor. Otherwise, if an attacker gains access to the primary authentication factor, the second factor can't be relied upon, if it can be reset with the compromised password. The recovery flow for the second-factor should be completely separate from the recovery flow for the password; for example, if an email message is the recovery method, recover the secondary factor through a separate channel.

Involve an administrator.
An administrator can implement a sophisticated high assurance authentication method in various scenarios. In enterprise scenarios, companies are in the best position to authenticate members of their organization through shared secrets derived from the content of the employee's work or profile, the company, and human relationships. One notable approach is to ask an employee's manager to authenticate the user and then authorize IT to execute the MFA reset.

In consumer scenarios, an administrator can interrogate a user across a large set of shared secrets. For example, upon onboarding, consumer banking applications will collect a large set of obscure personal details that become shared secrets for account recovery. Recent events in the person's history with the application or company can also constitute viable

shared secrets. The evaluation of a set of shared secrets can be automated via web or voice and can in many cases provide better assurance than a human, because it's less vulnerable to social engineering.

Provide a backup secondary factor.
Many scenarios require an automated method for recovering the second factor (for example, products serving large numbers of users where 1:1 support is prohibitively expensive, or where operational costs need reduction). Enrolling the user in more than one second factor at the time of onboarding allows the user to recover a second factor by completing authentication through a backup second factor. One notable, simple, and low-cost example is to provide users with a card (either physical or printable) with a set of codes that can be used only once, and that can be used as a backup second factor.

Protect login flows from brute force and credential stuffing attacks

As the availability of inexpensive computing resources increases, so does the vulnerability of authentication systems to brute force guessing attacks. However, a few simple techniques can be used to significantly improve the security of your MFA when a password is compromised.

Analyze logs and alerts.
Collect and analyze unsuccessful secondary factor attempts. In the event of several failed second-factor challenges, alert the user or an administrator to this suspicious behavior, and prompt the user to enroll a new token.

Use an out-of-band token.
A second factor verified through a channel separate from the primary factor adds extra protection against brute-force attacks and phishing. For example, a popular new factor sends the user a push notification on a mobile phone with details about the authentication request and a prompt to accept or deny the request. This channel is inaccessible to a traditional brute-force guessing approach.

Design to manage risk, usability, and cost

The design of an MFA feature will have significant implications for security, usability, and cost, in any context. A higher assurance second factor can, in some cases, feel like an unnecessary extra burden for end users and administrators; this can impact the adoption of MFA for your product and thereby decrease security. Here are some best practices for balancing risk, usability, and cost:

Offer a spectrum of options to serve diverse user populations.
Different user populations present different levels of risk and therefore warrant different levels of assurance. For example, an administrator can have a larger scope of access than an individual user, so you may want to provide stronger second factors for administrators while offering more convenient options for the general workforce. In consumer scenarios, different users will have different preferences for the balance of security and usability they would like on their accounts. If a more familiar option with lower assurance such as SMS is used it may add more security than a high-assurance option that's not widely adopted.

Support federated identities and authentication.
Federated identity, also known as federated single sign-on (SSO), is a method of linking a user's identity across multiple identity management systems, allowing users to move quickly between systems while maintaining security. In enterprise scenarios, many companies are implementing authentication and MFA locally for identities they manage, and federating to resources. This approach allows product development teams to outsource the administration of policy and security processes to customers and partners. Enabling these users to implement MFA independently allows them to optimize across the aforementioned considerations according to their specific circumstances and constraints. For example, a partner can design the administration of account recovery to suit their specific IT function. This outsourced approach has the added advantage of allowing users to use one token to access all resources.

How Okta changes the game

Okta's modern approach to identity management is uniquely positioned to help businesses take control of identity management, including MFA, to reduce data breaches and other negative outcomes. Okta allows you to:

Quickly enable MFA for your workforce and customers.

- Deploy MFA quickly and easily, with more than 7,000 out-of-the-box connections on the Okta application network
- Extend coverage to on-premises applications via support for RADIUS, RDP, ADFS, and LDAP, as well as header-based auth and Kerberos via Okta Access Gateway
- Facilitate intelligent, contextual access decisions based on device and connection attributes
- Reduce dependency on passwords with single sign-on and passwordless authentication

Confidently centralize identity.

- Reduce account management complexity
- Unify access for users to eliminate passwords while providing a positive experience
- Mitigate risk and reduce identity sprawl by restricting access to services via intelligent SAML connections

Reduce the attack surface and respond rapidly to credential compromise.

- Automate provisioning and deprovisioning to accelerate consistent onboarding while eliminating orphan accounts
- Extend security policies to custom applications via SCIM, SDKs, and Okta's rich APIs
- Ensure the right level of access is granted to the right applications at the right time with access request workflows and complete identity lifecycle management

To see how easy it is to administer Okta's Adaptive Multi-Factor Authentication solution and pilot the authentication process, watch this demo.

Learn more about Okta's Adaptive MFA solutions at https://www.okta.com/products/adaptive-multi-factor-authentication/

Conclusion: A roadmap for MFA success

Multi-factor authentication has become a global best practice for application developers to secure access to their applications. But behind the scenes, you must take many steps to fully leverage the power of MFA security without disrupting the workforce. Best practices include analyzing second-factor recovery flow, designing systems to withstand brute force attacks, and finding the appropriate balance between security, usability, and cost.

A modern, automated approach to MFA can help organizations control access, safely automate recovery, and dramatically reduce the risk of data breaches.

Whitepaper

Multi-factor authentication deployment guide

okta

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871