Okta Adaptive Multi-Factor Authentication (AMFA)

okta

Protect against Account Takeover Attacks and fraud

Account Takeover (ATO)—An increasingly common consumer attack method wherein a bad actor gains illegal access to a user's account, and can exploit that access for financial or informational gain. Every digital business featuring a login page is at risk to this method.

$6B	120%	659
Losses due to Account Takeover Gartner	Increase in ATO since 2016 Javelin Research	Identity theft incidents in H1-2018 Breach Index

Account takeover at a glance

These attacks can be either human-driven or automated using bots. In large-scale automated attacks, botnets disguise themselves by rotating between IP addresses and generating new signatures. This allows them to avoid being discovered by device or browser tracking solutions. To prevent account takeovers, you need an identity platform that combines security with a seamless user experience. See how Okta identity and security solutions can help you in this journey.

Use Okta to Stop Account Takeover Attacks and Fraud

Strong Account Security

Seamless User Experience

Easy Integration and Management

Trusted by leading organizations to protect against Account Takeover

FARMERS INSURANCE

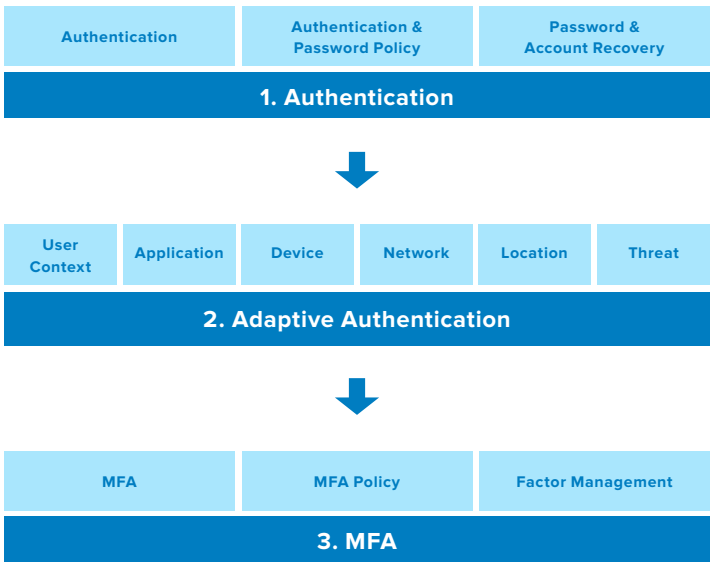
bazaarvoice

Northwestern Mutual

Okta's Account Takeover Prevention Stack

Okta offers a three-layer stack to prevent account takeovers.

1. **Okta Authentication:** Enforce primary authentication and password policies. This includes easy password and account recovery capability.
2. **Adaptive Authentication:** Automatically assess login risk based on normal user login patterns. Variables include user context, device, network, location, and threats.
3. **MFA:** Enforce strong authentication using a range of factor options including knowledge, possession, and biometric factors. This includes self-serve factor management options.



Okta AMFA—Adaptive Authentication

How your users access their data—and the risk associated with those methods—is constantly changing. Your security should be able to keep up. Okta Adaptive MFA allows for dynamic policy changes and step-up authentication in response to changes in user or device behavior, location, or other contexts. Adaptive MFA supports detection and authentication challenges for riskier situations like:

- Use of weak/breached passwords
- Proxy use
- Geographic location and zone changes
- Brute force and denial-of-service attacks
- Use of new devices
- Indications of other anomalous behaviors

Multi-Factor Authentication (MFA)

Different situations require different strategies for authentication and identity assurance. Not all factors are appropriate in every circumstance, and organizations typically want a variety of assurance levels—levels of proof that a user is who they say they are—based on security needs. That's why Okta offers flexible support for a wide range of second factors spanning all assurance levels, including:

- SMS, Voice, and Email
- One-time passwords like Okta Verify and Verify Push and third-party solutions, e.g Google Authenticator
- Physical tokens including support for RSA, Symantec, and Yubikey tokens
- Biometric factors including Windows Hello and Apple Touch ID

Managing factors should be as easy as possible. Okta's self-service factor reset capability allows end users to reset and enroll into factors without having to divert resources from the support team.

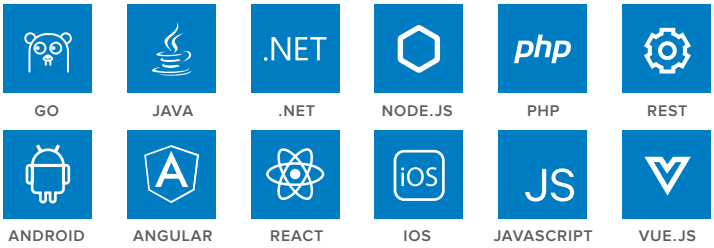
Seamless User Experiences

The enhanced security required to stop account takeovers shouldn't add friction to your users' experience.

- Combine Okta's adaptive authentication with MFA to intelligently detect high-risk logins and enforce a second factor only when necessary.
- Okta allows you to deploy MFA downstream in your applications when the user performs critical actions on your platform—just in case. This might include when a user attempts to transfer money, make changes to personal information, etc.
- Okta gives you the option to eliminate passwords from the authentication experience. You are free to establish high-assurance primary authentication factors, such as SMS, Email, Voice, or Google Authenticator, as sufficient means for app access.

Quick Integration, Easy Management

Adding security to your application should be easy and customizable. With support for all major programming languages and frameworks, Okta's prebuilt widgets and SDKs make adding security into your applications quick and easy.



Should you need a more customized experience, integrate directly with Okta's Restful APIs. Our detailed API documentation, user forums, and support engineers provide product builders with all the support they need to add security layers to their application.

Adding MFA is just the start. Okta makes managing users and application security simple. Okta's admin and user dashboard allows users, security teams, and support teams to quickly manage the factor experience, monitor suspicious activity, and enforce security measures as necessary.

Okta's reporting dashboard provides security teams with all the details they need within the admin console. The Syslog API allows you to get a real-time feed of login events into your internal systems. Pre-built integration with all major SIEMS ensures your SOC team can construct a complete picture of the risks involved.

Visit the API product page to learn more about how Okta can provide a secure and frictionless experience for users, as well as a manageable experience for product builders and administrators. Reach out to our product experts to learn more, and see how Okta can keep your service safe from account takeovers.