okta

Okta Adaptive Multi-Factor Authentication

Intelligent security for all your devices, apps and infrastructure

In today's landscape, hackers no longer break in, they log in. The continuous increase in identity based attacks proves that all entry points to your corporate resources should be secured—whether that's on-prem apps, cloud apps, or even infrastructure. And on top of all this, we also need to remember securing access to applications that are accessed by your customers, and your customer's customers. Okta's adaptive authentication products—Adaptive Multi-Factor Authentication and Adaptive Single Sign-On, secure your organization from data breaches by taking a contextual access approach in enforcing security. Leveraging device, user, user behavior, and location context through an adaptive, risk-based approach, Okta's adaptive authentication products offers security for all access points to your corporate resources.

Why choose Okta Adaptive MFA?

Flexibility in securing accounts. Okta protects access to data regardless of where that data resides, where your users are located, or which devices users choose to stay productive on. Built to be flexible in all environments, Adaptive MFA protects cloud resources in addition to your on-premises needs for VPN, RDP, and SSH, as well as custom built web and mobile apps accessed by your workforce, partners, customers and consumers.

Adaptive MFA addresses common pain points in deploying a multi-factor solution with the following capabilities:

1. A one size fits all solution for all user types. Whether you need to enforce MFA and adaptive policies for your own employees, suppliers, contractors, customers or consumers, Okta has you covered. Policies can be applied to any web or native mobile app—you can even use Okta as the auth provider for your custom built apps.

2. Dynamic response based on login context. Multi-factor authentication isn't great when all you can enforce is a basic "yes" or "no." Okta enforces step-up authentication when it makes sense based on historical context on the user paired with their device, location and IP and many more login characteristics.

3. Make passwords less significant. Even with reasonable password policies in place, users still tend to be the weakest link in the chain. Give your end users a simple login experience while staying secure by using strong auth factors like Okta Verify, biometrics, and FIDO2.0 tokens to replace passwords.

Key Features

Choose the factors that best fit your organization

Okta offers a wide range of multi-factor auth methods out of the box, and also lets you use any SAML or OIDC auth provider as a factor.

Risk-based authentication to identify login anomalies

Okta uses a machine learning model to categorize anomalies as high, medium or low. Use risk-based auth to pair a risk level with the appropriate factor.

Provide users with secure, passwordless logins on any device

Enforce device trust and make great use of strong auth factors like Okta Verify and FIDO2.0 by using these as a method of primary auth to replace passwords.

Okta ThreatInsight prevents large scale identity attacks

Okta's network effect captures billions of logins across all orgs. With ThreatInsight, admins can block access from suspicious IPs pre-authentication, thereby preventing account takeover and account lockout for your workforce, customers, and consumers.