okta

# Security Built to Work Outside the Perimeter

## 3 Reasons to Choose Adaptive Multi-Factor Authentication

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

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

# Table of Contents

# People are the Perimeter

We all know that the days of working within four office walls are long-gone, in fact 43%[4] of Americans work remotely at least some of the time. Your team works from their desks, but also from home, from the airport, from the coffee shop around the corner—the list goes on. Your employees are using modern cloud applications that allow them to work from anywhere, but is your security solution keeping up with this new perimeter? Keep your company out of the headlines and your end users happy and productive.

## Threat Actors are Becoming More Sophisticated:

**SMSishing**
“Trojan horse” text messages hackers will send to phones and then steal your data.[1]

**Phantom Fingerprints**
Hackers can lift fingerprints from photos taken up to 10 feet away.[1]

**Security in a borderless world:**
7 of the 15 fastest growing apps in Okta’s network in the past year (Jamf, KnowBe4, DigiCert, Cisco Umbrella, Mimecast, Sophos, and CloudFlare) are security tools or have security use cases.[3]

## People are the Perimeter:

81%
of data breaches involve stolen or weak credentials.[2]

73%
of passwords are duplicates.[2]

17%
is the percentage of Passwords that are 123456.[2]

A data breach can cost a company
$3.6 Million[2]

# What is the Difference Between 2-Factor Authentication, Multi-Factor Authentication, and Adaptive MFA?

91% of phishing attacks target credentials.[2] To prevent phishing attacks and meet a growing list of compliance requirements (PCI, HIPAA, NYDFS, NIST, and more) you need an authentication solution. But how do you choose between the complex options available? We made some sense out of all the acronyms for you:

## 2-Factor Authentication (2FA)

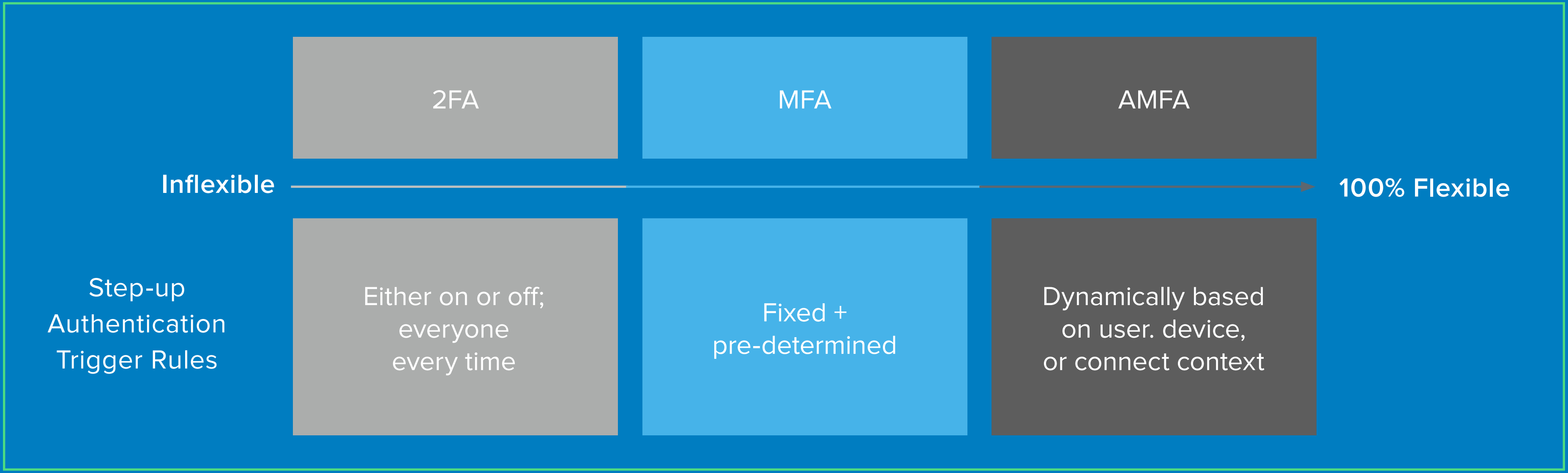
- **How it works:** Users must supply another, secondary factor after the primary factor (typically a password) to prove identity.
- **Potential gaps:** Only one additional layer of identity assurance with limited flexibility. Plus, it can be annoying to the end user to always require a second factor.

## Multi-Factor Authentication (MFA)

- **How it works:** You prompt the user and grant access based on a spectrum of possibilities, including inside/outside corporate networks, blacklisted/whitelisted sets of IPs, and application policies. You can set this up based on multiple data points and factors derived from login attempts, such as third-party tokens, biometrics, and SMS.
- **Potential gaps:** Static rules may not be as flexible and can still overburden the end user; does not surface unusual authentication behavior.

### Adaptive Multi-Factor Authentication (AMFA)

- **How it works:** A flexible system for prompting for additional identity assurance. Okta’s Adaptive MFA solution determines when to prompt for step-up authentication prior to granting access based on device and user context. Prompts are dynamic based on user and device context to prevent over-burdening the end user.



| | 2FA | MFA | AMFA |
|---|---|---|---|
| Inflexible → 100% Flexible | | | |
| Step-up Authentication Trigger Rules | Either on or off; everyone every time | Fixed + pre-determined | Dynamically based on user. device, or connect context |

**Here’s why Adaptive Multi-Factor Authentication is the secure, “won’t generate tons of helpdesk complaints” option you’ve been looking for.**

# 1. Use Factors and Policies You are Comfortable With

You have to balance security and end user flexibility to meet security and compliance requirements for your organization. Some end users might be at their desk, others might be on the go, and end users aren't just your employees any more. Customers, partners, and suppliers are all demanding access on-the-go and on multiple devices—3-4 on average.

When you have enterprise-grade security standards, device context between any two BIG-IP devices on the network is also critical. In addition, you want the flexibility to leverage various factors for authenticating your users, whether it's security questions or including biometrics, no matter where they are.

## No matter the factor or the policy, Okta's Adaptive MFA can handle it

Are your users team-Apple or team-Windows? Split? Of course. Okta Adaptive MFA supports biometric-based factors for all the fans such as Windows Hello and Apple Touch ID. Prefer another hard token? Yubikey is your new best friend. This flexibility allows you to provide an extra layer of defense to confirm all the identities before to providing access.

On top of that, why limit yourself to mobile? Adaptive Multi-Factor Authentication allows you to choose the second factor authentication needed based on employee role. So Bob in Accounts Payable can verify via mobile SMS, and Jan in Customer Success can authenticate via Google Authenticator, and Alex in the call center, who cannot use his mobile device, can use Windows Hello. Bob, Jan, and Alex don't hate IT for making access difficult and you rest easy knowing they're keeping your data safe.

Don't leave the team frustrated. To ensure strong authentication services from standing in line at the airport to the dining room table, Okta Adaptive MFA allows you to set organizational rules using trusted device policies. This ensures that users are accessing resources on known, trusted devices you've already vetted and given the thumbs-up to. This also means employees won't be pulling their hair out when faced with excess security factors every time they check email on their cell phone. Seamless end user experience, secure data, and enterprise compliance requirements met? Win, win, win. Go you.

# 2. Add Context to Your Policies

Threat actors can come from all around the world. 48% of threats are coming from IPs geolocated in China, but that means 52% are coming from elsewhere, including 7.7% in the United States and 23% from the unknown corners of the dark web.[3] Their mission? Penetrate your systems and applications and take all the data. In order to keep it secure, you have to understand who is accessing your data and from where.

Adaptive MFA is all about visibility into your data and control over the policies that permit access. Customers with Okta Adaptive MFA can apply a range of policies to trigger MFA or step-up authentication based on various scenarios that you define based on your unique needs. These include access networks, geographic location, or other anomalous behaviors like requested access from a proxy or Tor networks. When you have more context around the user trying to access your systems or applications, you can layer in protection based on suspicious behaviors that aren't on-par with your team's day-to-day behaviors. Centralized, real-time reporting of all authentication events also enables you to investigate red-flag events further or integrate with other security analysis and reporting tools.

# 3. Supported Security Integrations

Want more visibility into your organization’s security? Identity plays nice with your existing security solutions! Just up your game by adding and correlating authentication data with your other security logs. AMFA logs can provide a wealth of additional information into who is logging into what, when, and where.

Okta Adaptive MFA allows you to integrate authentication syslogs and reports with your other security tools via API. You’ll have insight into what apps users are logging into as well as be the first to know if something unusual is happening like multiple failed login attempts across many accounts which may be an indication of a cyber attack.

This will give you the centralized visibility and integration that meets your security needs as well as access management clarity to fulfill compliance requirements.

# Inspired Security: See How Three Organizations are Changing the Game with Adaptive Multi-Factor Authentication

flex

## Flex Tackles the Constant Change with Okta

Flex faced several challenges when it came to meeting end user productivity and security requirements—staying innovative, using best-of-breed applications, protecting customer data, keeping suppliers in the loop, and securing employee access to critical applications Customers' concerns are no longer about physical security, but how Flex is securing their IP and their data.

To tackle the changing cybersecurity landscape and remain innovative and productive, Flex chose Okta as their identity standard. Flex leverages Okta to provide strong authentication for their employees and constantly rotating suppliers. A self-service portal for suppliers to reset their own passwords also eases the burden on IT.

> "Okta plays a role in all three of my initiatives: Cybersecurity, business productivity, and best of breed. It fits all three, so it's a perfect match."

**Gus Shahin**
CIO, Flex

View the full story,
https://www.okta.com/customers/flex/

## Funding Circle Enables 100% of Their Employees to Be Secure

Funding Circle was challenged to federate their identities across multiple applications within the cloud and to ensure they kept a consistent user experience, but still meet complex financial compliance requirements.

With Okta they now have a robust set of access policies based on their users data such as location, IP address, or device, and they leverage step-up authentication MFA factors like Google Authenticator, SMS push, and the Okta Verify with Push mobile app. The IT team gets the security they need while the end-users have the simplicity that is important to them, and the company meets all its compliance requirements.

81%

reduction in password resets for Okta-integrated applications

100%

of employees protected with Adaptive MFA

View the full story,
https://www.okta.com/customers/funding-circle/

ThoughtWorks®

## ThoughtWorks Sees Increased Productivity, Security, and Savings

ThoughtWorks wanted to protect against loss of intellectual property with a growing dispersed workforce. They were struggling with 35% of helpdesk tickets related to issues with physical RSA security tokens, and employees were often disabled more than 30 minutes during MFA and password-reset cycles. It was time to move to the cloud and scale to meet their growing company and security needs.

In order to support open-standards and move to a more cloud-first strategy, ThoughtWorks partnered with Okta to meet the flexibility employees needed and the security their organization demanded. With Adaptive MFA, the total helpdesk tickets for password resets and MFA credential resets have decreased by 90 percent. End users spend significantly less time responding to MFA prompts with Okta Verify with Push and a flexible policy framework.

$400K
productivity improvement

$800K
time-savings in password and MFA credential resets

$400K
realized in security improvement

View the full story,
https://www.okta.com/customers/thoughtworks/

# Final Thoughts

We get it. Your end users are more globally dispersed than ever and demand a great experience while the business is constantly on the defense against bad actors and demands the best security. Figuring out the best authentication solution for your organization is hard. We're here to make sure your employees remain happy and productive and IT and security teams meet their compliance goals, and sleep better at night too.

Suggested resources to learn more about Adaptive Multi-Factor Authentication:

- Adaptive MFA Demo: Okta Adaptive MFA Get a Demo
- Meet Dave Fend, Your Okta Adaptive MFA Expert Podcast
- Adaptive MFA Instructor-Led Training: Get Some Hands-On Experience and Test-Drive the Product for Yourself
- Security without Compromise

[1] YOU Magazine

[2] Verizon DBIR 2017

[3] B@W report 2018 - https://www.okta.com/businesses-at-work/2018-01/

[4] NY Times article - https://www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html

### About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device. Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

You can learn more about Okta at okta.com.