ADAPTIVE MULTI-FACTOR AUTHENTICATION

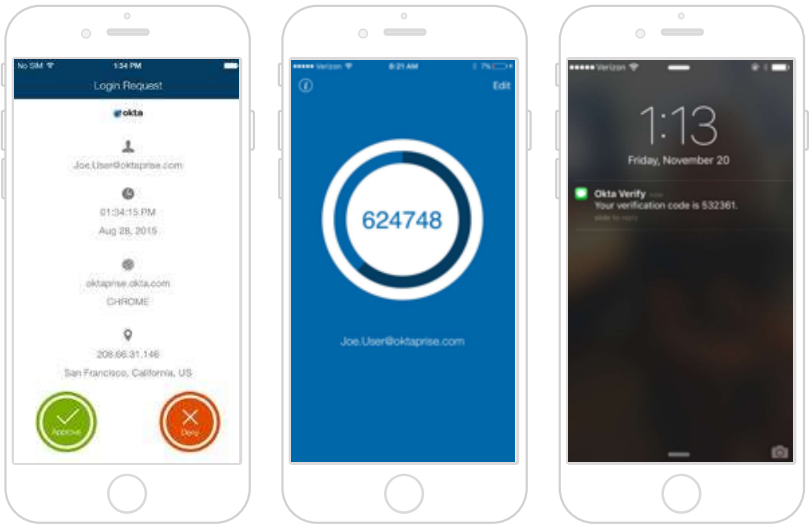
Whitepaper

Okta Inc.
301 Brannan Street
San Francisco, CA 94107

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

Executive Summary

This white paper provides an overview of Okta Adaptive Multi-factor Authentication (MFA). For security conscious organizations looking to protect applications and data, Okta Adaptive MFA is a comprehensive but simple strong authentication solution that provides policy driven contextual access management, supports a broad set of modern factors, leverages big data insights across thousands of enterprises, and integrates with the applications and VPNs organizations need. With Okta Adaptive MFA organizations can have enterprisegrade security with a great user experience.



Security Is a C-Level Issue

Security breaches are no longer just an IT problem. Securing organizations against the monetary and reputational damage caused by the theft of confidential data has become a top concern for C-level executives. On average, it takes organizations 205 days to detect a breach has occurred.[1] These breaches have a profound and lasting effect. Not only are compromised organizations liable for any damages, revenue can be impacted as consumers hesitate to make purchases and share their information with organizations unable to secure confidential data.

Traditional User Authentication Isn't Good Enough

Traditionally organizations have secured access to VPNs and applications with a single-factor of authentication: a password. But passwords, in addition to being difficult to manage, are vulnerable to a variety of common attacks. Hackers are phishing, social engineering, and using other increasingly sophisticated techniques to steal passwords for consumer, banking, and enterprise applications. As these attacks become more prevalent IT and security professionals have a responsibility to add new security controls to thwart these attacks.

[1] http://www.itsecurityguru.org/tag/breach

The percent that the cost of a data breach increases each year.[2]

The percentage of people who do open those phishing emails. Eleven percent click on the attachment.[3]

Percentage of web app attacks that originate with stolen credentials.[3]

In the case of the Anthem data breach, hackers stole personal records from Anthem's databases using compromised administrator credentials. Had multi-factor authentication (MFA) been in place, the hackers would have needed an additional piece of information beyond the administrator's password to access Anthem's data. That extra verification could have prevented the loss of almost 78.8 million people's data, including somewhere between 8.8 to 18.8 million non-Anthem customers.

The Impact of Mobility

The growth of the mobile workforce has changed how organizations must secure access to applications and data. Users are accessing applications from home offices, coffee shops and hotels, and from mobile devices. Users demand the flexibility to connect from anywhere, and IT and security professionals must adapt to secure access from unknown networks and devices.

The Benefits of MFA

MFA is designed to protect organizations against a range of attacks that use stolen credentials. MFA requires users to provide something in addition to their primary password—something the user is, has, or knows—before they are authenticated. With MFA in place, even if a user's password is stolen, the user account is protected from unauthorized access by requiring hackers to steal or spoof an additional factor.

[2] Ponemon Institute Report: 2015 Global Cost of a Data Breach.

[3] Verizon Data Breach Investigations Report.

Challenges of Legacy MFA Solutions

Poor User Experience

While the benefits of MFA are significant, MFA can be disruptive to end users in a variety of ways. Solutions that depend on hard tokens are complex to manage and expensive to maintain. The cost of tracking and replacing tokens is significant. End users find carrying hard tokens and entering passcodes cumbersome. For businesses with strict MFA policies, end users have to re-authenticate frequently throughout the day, reducing productivity and frustrating users.

Complex to Manage

Legacy stand-alone MFA products are hard to implement. IT teams need to integrate the MFA product with each application and system individually. Extending MFA protection to new applications and adding new users is complex, so scaling implementations is difficult. Building one-off point integrations is prone to creating coverage gaps as administrators either forget to enable, or are unaware MFA protection is required for new resources.

Difficult to Scale

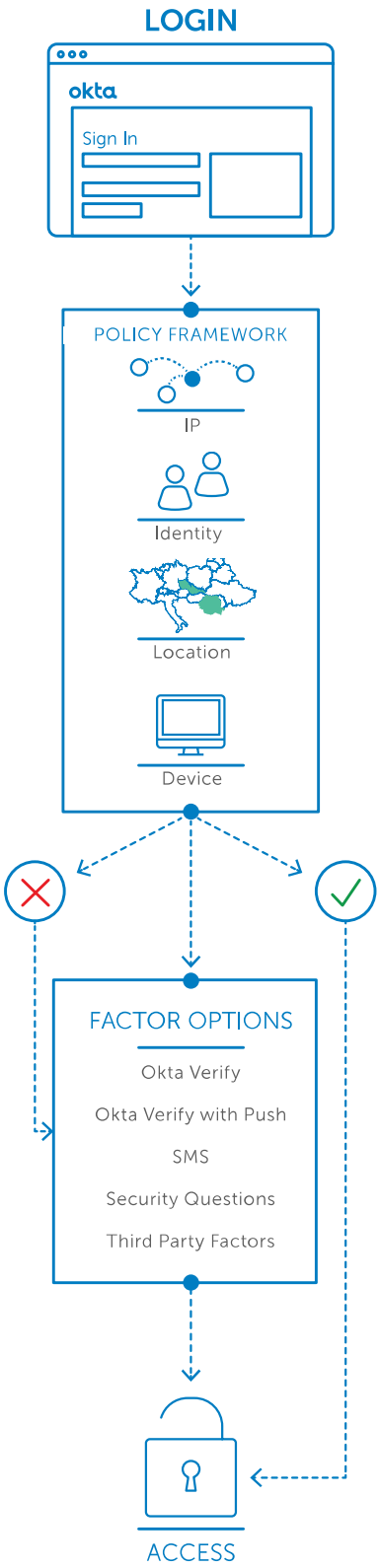
With stand-alone MFA products, organizations are dependent on applications and systems supporting vendor-specific integrations, inhibiting broad MFA protection for all apps and resources. As more organizations adopt cloud applications, they are finding many cloud apps do not support built-in integrations for their MFA vendor. Instead these cloud applications either do not support MFA, or use a native mechanism such as SMS-based passcodes or security questions. This adds confusion for end users who have to navigate separate credentials, and separate MFA factors for the various applications and services they access.

Unable to Protect All User Types

As the number and types of users within organizations continue to grow, a single MFA factor type may not scale to mobile or international users, or to specific groups of users who do not have access to smartphones due to their job functions. For example, many call centers do not allow employees to bring in personal mobile devices.

A New Approach to Security: Smarter, Easy to Use, and Comprehensive

Okta Adaptive MFA solves the challenges of legacy, stand-alone MFA products by offering enterprise grade security and a great user experience through policy-driven contextual access management, support for a broad set of modern factors, big data analytics, and built-in integrations to all the apps and VPNs that organizations need to protect.



Reduced Risk with Contextual Access Management

Okta contextual access management helps organizations reduce risk by examining when, where, and how users access applications and data. Organizations can choose to allow, require step-up authentication, restrict scope, or deny access based on who the user is, what network or country they are connecting from, and what device they are using. Administrators will even be able to adjust access based on what factors the user selects for verification, and how they performed primary authentication.

Okta Adaptive MFA's granular contextual access policies easily secure more resources with a second factor without impacting normal user activity. Users are only prompted for verification when necessary, not every time they attempt to login.

Comprehensive User Coverage through a Modern Set of Second Factors

Integration to a broad set of second factors and flexible enrollment policies mean IT no longer has to worry if users are equipped with the latest smart-phone, or located abroad with no access to a phone at all. Okta Adaptive MFA can secure access for all users with factors that make sense given the user's role, privileges, and work environment. Smartphone-based options like Okta Verify with Push offer end users a fast and easy way to verify their identity. For users without smart phones, Okta Adaptive MFA also supports other out of band factors like SMS passcodes. Okta also supports integrations with multiple third party factors like Yubikey, making it easy to migrate between factors, such as from RSA to Okta Verify with Push. Okta's enrollment policies enable administrators to select which factors are required, optional, and disabled for specific users and groups, and can be used to require the setup of redundant factors to reduce IT support costs.

Proactive Security and Risk-based Adaptive Authentication

Okta's big data analytics calculate risk scores based off rich user profiles to reduce false positives and proactively secure applications and data. Security teams can leverage Okta's insights into millions of users, devices, and authentication requests to identify possible attacks and prevent unauthorized access. Unlike stand-alone MFA products that only see a part of the picture, Okta Adaptive MFA has access to Okta's single sign on and enterprise mobility management data. Using this combination of contextual data from all of a user's authentication activity improves security by increasing the number of dimensions hackers have to spoof to impersonate a user.

More importantly, Okta Adaptive MFA does not just generate alerts. Because Okta centrally controls access to all applications, when Okta Adaptive MFA detects an abnormal authentication request it automatically stops the potential hacker, and gives administrators the option of totally blocking or limiting access to only certain resources to effectively reduce risk.

Simple Deployments with Built-in Integrations to Apps and VPNs

Okta's 100% cloud based Adaptive MFA solution enables organizations to deploy strong authentication security to all applications and critical infrastructure. Administrators can quickly add new applications and VPNs from the 500+ SAML and RADIUS integrations in the Okta Application Network (OAN). Central management of users, devices, and MFA security policies eliminates coverage gaps as users and resources are added, changed, and removed.

Available for Developers

Implementing MFA has traditionally been difficult for developers trying to build their own applications and portals. Okta Adaptive MFA is available through API's and the Okta Sign-on Widget, making enrollment, revocation, and authentication easy to implement. Developers can quickly add strong authentication into custom applications of all types. The Okta Adaptive MFA APIs also allow developers to fully brand the MFA experience so users get the security benefits and simplicity of Okta Adaptive MFA with a tailored look and feel.

Conclusion

Okta Adaptive MFA lets IT and security administrators deploy effective security controls to protect apps and infrastructure without sacrificing the end user experience. Okta offers a smarter MFA solution built on contextual data about users, devices, and behavior, and a comprehensive set of modern factors to support any user. Adding new applications and users is easy, offering rapid time to value and simplifying migrations from existing on-prem MFA products to Okta's more cost effective cloud based solution. With integrated single sign-on and enterprise mobility management, Okta makes it easy to secure users, devices, and applications.

okta

To learn more visit us at:
okta.com/learn/Adaptive-MFA