Making the Move to Dynamic Multifactor Authentication
# Table of Contents

Overview 1
The State of MFA Adoption

Defining Dynamic MFA 2

Five Reasons to Make the Move to Dynamic MFA 3

Conclusion 4
Overview

Passwords...the most hated thing we can't live without. The most annoying thing about passwords is their ineffectiveness at fulfilling their one true purpose in life, which is to help us stay secure online. There are alternatives, of course. This paper looks at new advances in multifactor authentication (MFA), which has the potential to take us to a passwordless future.

MFA works by requiring more than one method to authenticate the user of an application. Figure 1 depicts a standard MFA process. It is used mostly in situations where a lone username and password pair is not considered robust enough to establish user identity. Examples include knowledge-based authentication (KBA), which might ask for a mother’s maiden name, or one-time passwords (OTPs), which involves sending the user a unique identifying code they enter into the app to gain access.

MFA has long been considered superior to single factor, password-based approaches to access control. With MFA, assurance can be achieved by supplying not just “something the user knows,” like passwords and supposedly secret knowledge, but also “something they are” and something they “have,” like a known and recognized device. For many reasons, though, passwords have still predominated. Causes of MFA’s lack of strong uptake in security circles include user perceptions that the practice is inconvenient and confusing. MFA also suffers from architectural rigidity. It can be difficult for application owners to implement MFA consistently across all the various moving parts of their digital properties.

This is starting to change with the advent of Dynamic MFA, which adds a high degree of transparency and flexibility to the MFA process. “Dynamic MFA” provides an assortment of authentication options like traditional MFA tools, but allows the solution to adapt to changing risk conditions. Dynamic MFA uses the contextual state of the mobile device itself to respond to authentication requests. With advances in APIs and standards, it is now possible to implement Dynamic MFA that can adapt to context and present fewer hurdles for the user ... or more hurdles if there are indicators of risky transactions or sessions.

The State of MFA Adoption

Digital organizations are under pressure to implement MFA. Once a user stores a password, that password can be stolen from an online credential store. Indeed, some of the biggest identity and credential databases have been breached in recent times. Over a billion passwords were either compromised or discovered to have been compromised in previous breaches in the last year alone. This risk is greatly reduced with MFA. When authentication depends on independent variables that are not centrally stored, it becomes much more difficult to impersonate users or steal their personal information.

Password vulnerabilities are extensive. Industry experience shows that consumers typically use the same password for all of their online accounts — a pattern of behavior that exacerbates their risk exposure.
A password breach is bad for business. It damages the reputation of the organization that suffers the breach and may cause lost revenues and customer trust.

All of these risks have driven the security industry to desire that future passwordless state. It’s slow in arriving, however. Why is it taking so long? In large part, users rely on passwords so extensively. It’s not realistic to just rip-and-replace a solution everyone knows how to use — and is relatively easy to administer.

Despite the need for MFA, some organizations find it challenging to implement in ways that users will accept. It’s a convenience issue, partly. Some users may find it confusing to have to authenticate themselves one way for a standard transaction but be required to use OTPs for other interactions, e.g. a bank might require MFA for an address change but a simple password for a balance transfer.

The nature of MFA is also changing due to the evolution of the cybersecurity environment. In one instance, NIST, the National Institute of Standards and Technology, has recommended deprecating the use of SMS text messages for out-of-band (OOB) MFA in their most recent guidance for digital identification (SP 800-63-3). The reason for the deprecation itself is revealing. Text-based OOB was once considered an effective way to mitigate the risk of a “Man in the middle” attack, where a hacker could eavesdrop on a user and then impersonate the user when accessing a system. Now, with advances in off-the-shelf device-spoofing technology and the rise of cybercrime-as-a-service, the man in the middle can easily take over a phone and capture the SMS texted one-time password.

**Defining Dynamic MFA**

The tension between rising demand for MFA and the obstacles to its use have created a need for a new approach to multifactor authentication. Dynamic MFA offers a solution. It addresses both the technological and user experience challenges with MFA.

Dynamic MFA enables greater flexibility in MFA implementation and a more intuitive, context-aware experience for the end user. These outcomes are achieved through a combination of standards and architectural innovations. Dynamic MFA is also predicated on the reality that mobile devices are becoming the de facto standard for access to online properties. Research shows that Internet users access the Internet through mobile devices 51% of the time, and that the disparity between mobile access and browser access is growing.

Dynamic MFA focuses on two areas of risk that are transparent to traditional MFA solutions. First, there is the risk in the device itself: Dynamic MFA solutions, such as Iovation LaunchKey, can leverage external information to determine if a device has been used for malicious acts, is being emulated, arriving through a proxy, or if it is located in a suspicious time and place.

These factors, combined with permanent identifying traits of the device, allow the MFA solution to step up the rigor of the authentication process to provide better assurance that this is, indeed, the correct user.

The second area of risk is the risk inherent in the user’s request itself. Dynamic MFA allows a casual banking user to enter a relatively simple authentication action, like entering a PIN, when they want to review their balance information. But if the same user wants to send a large online money transfer to a new payee, the Dynamic MFA solution may request additional authentication factors on top of this PIN. It might request a thumbprint scan from the device, the entry of a graphic circle code, or the presence of some other known and registered wireless device, like an Apple Watch or wireless headset.
Figure 2 shows a simple representation of how Dynamic MFA works. The connections between the elements of a Dynamic MFA solution might be achieved through the use of standards such as OAuth, and use standard platform technologies like XML and JSON. In contrast to the basic MFA depicted in Figure 1, a Dynamic MFA process routes authentication requests based on usage context. So, if the user is trying to log on to his or her account, the MFA solution might require one type of MFA, such as a PIN. For additional flexibility the end user can be given some discretion in choosing which technique he or she prefers. They may prefer graphic Circle Codes to represent “something they know,” or they may prefer to always use thumbprint to confirm requests using “something they are”. These options might also include geofencing or time fencing parameters that require users to be coming from a known location, or to be working in a specified time range. In other cases, the MFA solution might enable authentication simply by using a strong digital fingerprint from a recognized and registered mobile device as an authentication factor.

Five Reasons to Make the Move to Dynamic MFA

Now is the time to start making the move to Dynamic MFA. The security environment grows more threatening. Consumers are less and less willing to tolerate breaches of their privacy and access credentials. With that in mind, here are five reasons to make the move to Dynamic MFA:

#1: MFA Is Your Friend
Consumers understand the value of MFA for their online activities that require an extra level of security. Now, with Dynamic MFA, it’s possible to make the experience easier to handle. When driven through mobile devices, MFA becomes more secure, more usable, more unified and more flexible than passwords, KBA or text-based two-factor authentication (2FA). With the right Dynamic MFA solutions, MFA can be added to any number of existing applications and workflows.

#2: Context Matters
Dynamic MFA enhances security by adding contextual indicators that pick up on risks and anomalies or evidence of device spoofing. Being context-aware makes a difference in the ability to balance security and user experience. For instance, if the user is a customer with no anomalies in their device or session, a Dynamic MFA solution can expedite their experience and get them to their goal as fast as possible. Alternatively, if there are indicators of an account takeover or device compromise, the Dynamic MFA solution can slow things down and add some authentication rigor.

#3: The Customer is King
Product owners and UX managers may want a better authentication experience for the end user. However, the InfoSec team may want to implement authentication processes that are not customer-friendly. Requiring a complex password or a code-embedded “fob” may turn customers off. What works internally, inside the firewall, may not be
the best approach with consumers. Dynamic MFA allows a host of different methods to be presented to the consumer, with the user selecting the methods they prefer to use within the constraints set by the administrator.

#4: Authentication Unification
In the old world, every user came through the digital front door, which was guarded by a username and password (because that’s what we knew how to do). Now there is omni-channel access through web sites, micro sites, mobile apps, kiosks, and even call center agents and in-branch tellers. Customers don’t want five different ways to authenticate themselves just because they can reach a business in five different ways. Dynamic MFA offers a unified system that allows a common authentication process through any of these channels, whether digital or physical.

#5: Think “End-to-End”
It’s time to tear down the common front door so new can provide a better overall experience for every customer (see #4). This means thinking about delivering just the right authentication at just the right time in their end-to-end customer journey. Delivering risk-appropriate authentication only when it’s needed means that easier, more frictionless methods can be used at other points in the customer journey, like transparent possession factors. This leads to better experience, greater user acceptance, and speeds up realization of the customer’s “lifetime value”.

Conclusion
Dynamic MFA offers a way to accomplish two sometimes contradictory goals: Improving security and user experience at the same time. By being flexible and context aware, Dynamic MFA diminishes the tradeoffs presented by earlier approaches to MFA. The time is right to make the move to Dynamic MFA. The security environment makes it essentially non-negotiable. The public demands better security for their personal information while also expecting ease of use. Dynamic MFA is the answer. It gives product managers and InfoSec teams the ability to make authentication a seamless part of the end-to-end about user experience.