IDC PlanScape

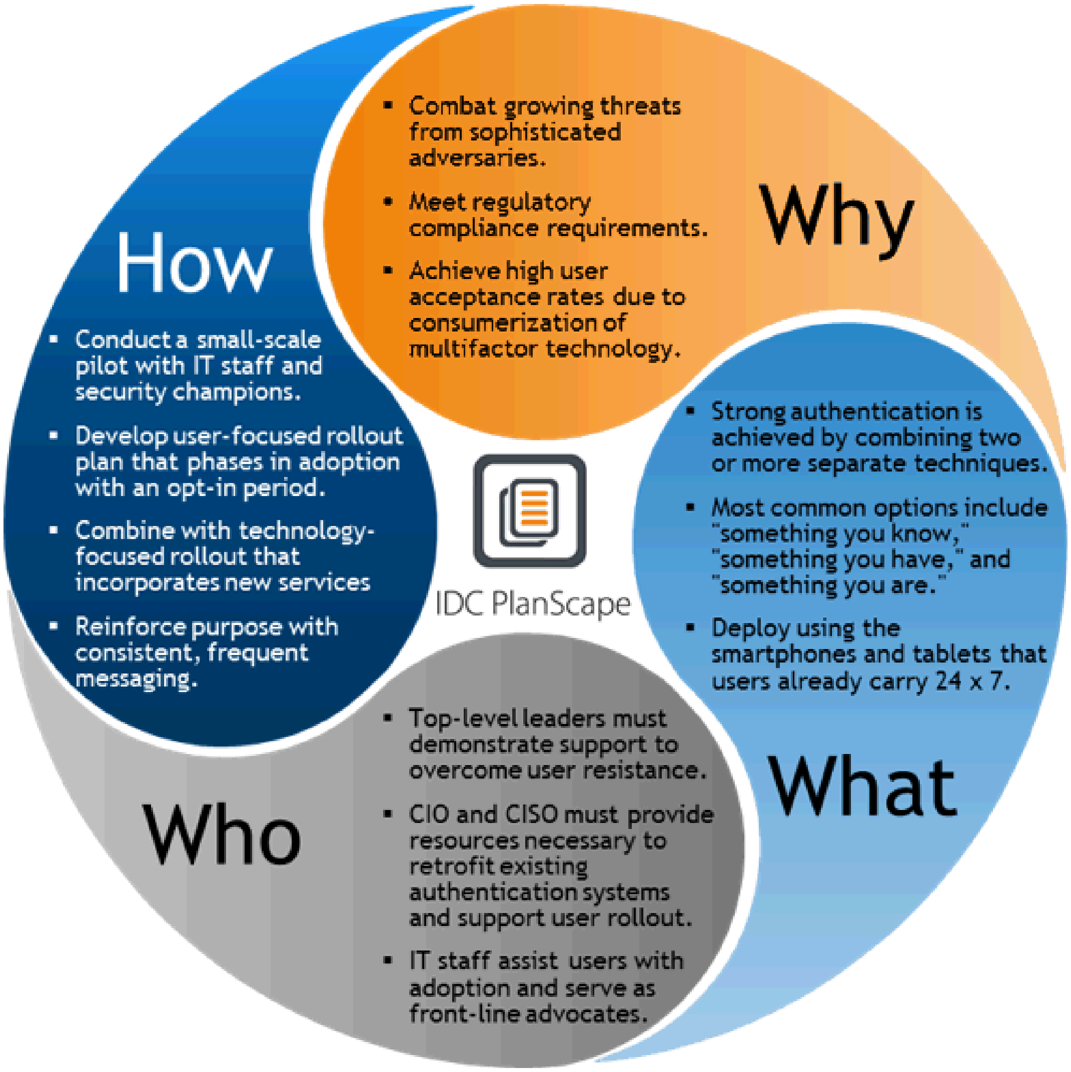
# IDC PlanScape: Deploying Multifactor Authentication

Mike Chapple

## IDC PLANSCAPE FIGURE

## FIGURE 1

**IDC PlanScape: Deploying Multifactor Authentication**



Why

- Combat growing threats from sophisticated adversaries.
- Meet regulatory compliance requirements.
- Achieve high user acceptance rates due to consumerization of multifactor technology.

What

- Strong authentication is achieved by combining two or more separate techniques.
- Most common options include "something you know," "something you have," and "something you are."
- Deploy using the smartphones and tablets that users already carry 24 x 7.

Who

- Top-level leaders must demonstrate support to overcome user resistance.
- CIO and CISO must provide resources necessary to retrofit existing authentication systems and support user rollout.
- IT staff assist users with adoption and serve as front-line advocates.

How

- Conduct a small-scale pilot with IT staff and security champions.
- Develop user-focused rollout plan that phases in adoption with an opt-in period.
- Combine with technology-focused rollout that incorporates new services
- Reinforce purpose with consistent, frequent messaging.

Source: IDC, 2017

May 2017, IDC #US42539517

## EXECUTIVE SUMMARY

Multifactor authentication provides organizations with an effective security control that overcomes the weaknesses of knowledge-based authentication and protects network, application, and data assets in an increasingly sophisticated threat environment. By combining passwords with physical devices and/or biometric measurements, organizations add a layer of strong security and protect themselves against password theft.

Recent advances in multifactor authentication make this technology more accessible to nontechnical end users and allow widespread deployment throughout the organization. Using multifactor authentication may now be as simple as clicking a button on a pop-up window that appears on the smartphone that a user was already carrying. The simplicity of this approach improves security while increasing user satisfaction.

Organizations planning the deployment of multifactor authentication should consider approaching both users and services in a phased approach that prioritizes high-risk users and applications to achieve the greatest benefit as early as possible in the deployment. Communicating frequently with both management and end-users increases the likelihood of a smooth deployment.

This IDC study provides senior technology leaders with a multifaceted approach to multifactor authentication.

"Multifactor authentication is a time-tested approach that is finally coming of age," says Mike Chapple, adjunct analyst with IDC's IT Executive Programs (IEP). "Organizations recognize that they face an increasing threat from the compromise of password-based credentials; knowledge-based authentication simply doesn't provide an adequate level of protection against those threats. Push-based authentication using smartphones is both simple for end users and cost-effective for the organization."

## WHY IS MULTIFACTOR AUTHENTICATION IMPORTANT?

Organizations that rely solely upon passwords for authentication are taking a significant risk in today's cybersecurity threat environment. While passwords remain a useful component of any organization's security program, they now fall into the category of "necessary, but not sufficient" as a means of proving user identity. Multifactor authentication approaches, long the realm of classified government agencies, financial institutions, and others with security postures bordering on paranoia are now a critical component of even the most routine technology services.

Data gathered from recent security incidents bears out this claim. In its "2017 Data Breach Investigations Report," Verizon examined the details of thousands of security incidents that took place in 2016. "81% of confirmed data breaches involved weak, default or stolen passwords," underscoring the fact that password authentication can simply no longer stand on its own for more than the most inconsequential of services. There is a high likelihood that any service that runs at scale and relies only upon password authentication is already compromised by adversaries if the service offers information or resources of any value.

## What's Wrong with Passwords?

The underlying problem with password authentication lies in the fact that passwords are simply static information that can be easily stolen and used by someone other than their rightful owner from anywhere the application is accessible, which often means around the world. Whether gathered from individual users through social engineering attacks or stolen en masse from a compromised website, attackers can steal passwords without the end user's knowledge and then use those passwords to assume that user's identity.

Compounding the insecurity of password authentication is the fact that users harbor an intense dislike of passwords due to the difficulty of memorizing complex passwords, leading them to reuse the same complex passwords across many business and personal sites. Attackers are wise to this behavior and will routinely steal passwords from less secure sites, such as a news or sports website, and attempt to use those passwords to log into more sensitive sites, such as a bank or corporate VPN. For example, a breach of Adobe's website in 2013 resulted in the publication of over 130 million passwords on the internet. An attacker seeking to compromise ABC Corporation could simply search that dump for accounts ending in @abc.com and attempt to reuse those credentials to log on to an ABC site. The chances of successfully finding a single reused password with this approach are quite high. In a February 2017 survey of smartphone users, Keeper Security discovered that more than 80% reuse passwords.

## Multifactor Authentication Builds Upon Passwords

Multifactor authentication provides enterprises with the ability to complement passwords with other authentication techniques that do not rely upon the user's possession of secret knowledge that may be stolen and reused. These techniques are not new. Security professionals coined the term *multifactor* decades ago and selectively deployed the approach in highly sensitive applications, such as when securing remote access to datacenter networks. However, dramatic changes in the cybersecurity threat environment including the rise of advanced persistent threats (APTs) and the open publication of data from massive password thefts are now leading organizations to deploy multifactor on a much more widespread basis.

## Regulation Often Drives Adoption

Some organizations are adopting multifactor authentication approaches due to external regulatory requirements:

- The *Payment Card Industry Data Security Standard (PCI DSS)* explicitly requires the use of multifactor authentication for administrative access to systems and networks that store, process, or transmit credit card information.
- While stopping short of mandating multifactor authentication, the *Federal Financial Institutions Examination Council (FFIEC)* issued guidance to banks and other financial institutions stating that the FFIEC members "consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties."
- Federal government regulations require the use of multifactor authentication to secure remote access to *sensitive government systems.*

In addition to these formal requirements, many auditors now expect that organizations will consider the use of multifactor authentication in their risk assessments and design of security controls.

## User Attitudes Toward Multifactor Are Changing

Users are now very accepting of multifactor authentication due to the convergence of several factors:

- Mainstream consumer services, including Google, Twitter, Facebook, and LinkedIn, support multifactor authentication, raising user awareness and acceptance of the technology.
- Media coverage of data breaches and nation-state sponsored attacks on major corporations increases user threat awareness.
- The widespread adoption of smartphones for multifactor authentication and their 24 x 7 availability to users eliminate the need for users to carry separate dedicated hardware devices that often get forgotten, lost, or stolen.

Deploying multifactor authentication technology reduces an organization's cybersecurity risk and allows it to continue to operate in an increasingly hostile threat environment.

# WHAT IS MULTIFACTOR AUTHENTICATION?

Multifactor authentication is requiring the simultaneous use of authentication technologies from two or more separate control categories to verify a user's identity. The three categories of authentication factors include:

- **Knowledge-based authentication.** These techniques fit into the category of "something you know" and rely upon the user's possession of secret information. The most common example of knowledge-based authentication is a password, but this approach also includes security questions, PINs, and similar techniques.
- **Possession-based authentication.** These techniques fit into the category of "something you have" and rely upon the user's physical possession of an object. Historically, security teams implemented possession-based authentication using hardware tokens that users attached to their keychains. This has given way to the use of smartphone- and smartcard-based authentication.
- **Biometric authentication.** These techniques fit into the category of "something you are" and measure a physical feature of the user. Biometric authentication techniques include fingerprint scanners, facial recognition, voice identification, and iris/retinal scanning.

Multifactor authentication requires the use of two or more authentication techniques representing at least two *different categories* of authentication. For example, an organization might combine knowledge-based authentication with possession-based authentication by requiring that users enter a password and then confirm their log-in using their registered smartphone. Similarly, a system might require the use of both a fingerprint (biometric authentication) and a password (knowledge-based authentication). For a detailed discussion of authentication factors, see *IDC TechScape: Worldwide Advanced Authentication* (IDC #US42418917, April 2017).

## What Isn't Multifactor?

Organizations seeking an expedient approach to satisfying regulatory or contractual requirements for multifactor authentication often consider using two knowledge-based authentication techniques in their log-in process. For example, many websites require that users not only confirm their identity using a password but also answer security questions based upon information appearing on their credit report. While this may provide marginal security benefits, it does not achieve the strength of a multifactor approach to authentication. The problem with this approach is that an attacker able to gain access to a user's password through a social engineering attack or other means is likely also able to obtain (or research) the answers to security questions using similar tactics.

When the FFIEC first incorporated guidance suggesting that financial institutions implement multifactor authentication, many banks responded by adding security questions to their log-in process. The FFIEC responded by releasing a FAQ that clarified their position:

> By definition, true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication.

Organizations seeking to deploy multifactor authentication should carefully assess the factors they are considering to verify that they are truly adopting factors from different categories and, therefore, different risk profiles.

## Smartphones Play a Critical Role in Multifactor Authentication

The widespread use of smartphones is one of the most critical factors driving user acceptance of multifactor authentication technology. Some of the benefits of smartphone use as a second factor are:

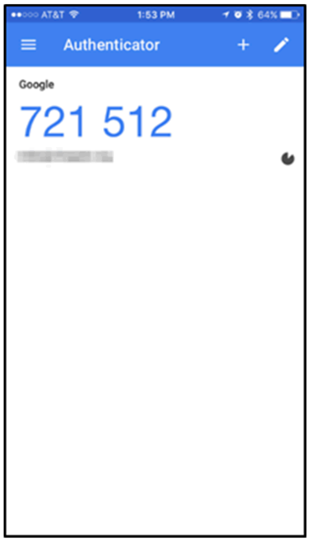
- Users already carry smartphones with them on a 24 x 7 basis, ensuring that they will have access to the device when they need to authenticate.
- Companies can often rely upon personally owned smartphones as a second factor for the vast majority of their users, avoiding the cost of purchasing dedicated hardware tokens and the overhead of managing those devices. This reduces the total cost of ownership of multifactor solutions.
- Users are comfortable with the process of authenticating to their phones through both passcodes and/or biometric authentication.

The first uses of smartphone apps as multifactor devices relied upon the use of passcode mechanisms, such as the Google Authenticator app shown in Figure 2. In a typical multifactor authentication process using this approach, users would:

- Access the application and log-in in with a username and password, successfully completing a knowledge-based authentication process.
- Provide the one-time password from their smartphone app. This code may be generated on demand or rotate periodically. If the user provides the correct code based upon the time or access sequence, this proves possession of the device and completes the second authentication factor.

## FIGURE 2

### Smartphone-Based Passcode Authentication



Google

721 512

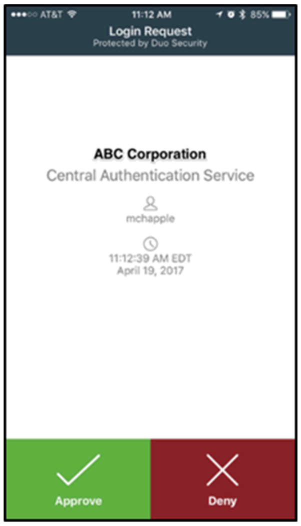
Source: Google, 2017

The passcode approach to multifactor authentication is cumbersome for users, who quickly become tired of opening the authentication app and entering the passcode in addition to their password. Recently, multifactor authentication vendors began moving to a "push" authentication approach that works slightly differently:

- The user provides a username and password in the same manner as other techniques.
- The authentication system automatically sends a push notification to the user's registered smartphone asking them to approve the log-in. An example of this notification from Duo Security appears in Figure 3.
- The user clicks a single button to approve the log-in request.

## FIGURE 3

### Smartphone-Based Push Authentication



Login Request
Protected by Duo Security

ABC Corporation
Central Authentication Service

mchapple

11:12:39 AM EDT
April 19, 2017

Source: Duo Security, 2017

The push authentication approach achieves the same security objective as the passcode approach but using an approach that is much more likely to gain acceptance among end users.

## WHO ARE THE KEY STAKEHOLDERS?

Successfully deploying multifactor authentication requires a partnership between business leaders, technologists, line managers, and end users. Individuals in each of these roles play an important part in rolling out multifactor authentication technology (see Table 1).

## TABLE 1

### Key Stakeholders

| Role | Responsibility |
|---|---|
| Senior business leaders | Demonstrate support for the multifactor initiative, preferably by becoming early adopters and evangelists for the technology. |
| Chief information officer (CIO) | Provide funding and staff resources required to support the deployment. Serve as the key contact for other senior executives with questions or concerns. |
| Chief information security officer (CISO) | Spearhead the multifactor deployment initiative, coordinating resources within the IT organization and ensuring that the deployment achieves security objectives. |
| Line managers | Support the initiative with end users, helping them understand the business case for multifactor authentication and direct users to technical support resources, as needed. |
| Legal counsel and IT compliance staff | Ensure that multifactor authentication deployments comply with any legal or regulatory obligations affecting the organization. |
| Information security staff | Serve as subject matter experts for the deployment and share technical ownership with the identity and access management team. Participate in communications and outreach efforts. |
| Identity and access management staff | Integrate multifactor authentication technology with existing identity and access management systems. Share technical ownership with the organization's information security team. |
| Application owners | Ensure that applications not using central authentication systems are properly integrated with multifactor authentication technology. |
| Front-line IT staff | Assist end users with device enrollment and authentication questions. Serve as front-line advocates for the initiative. |
| End users | Enroll multiple devices in the multifactor authentication system. |

Source: IDC, 2017

# HOW CAN MY ORGANIZATION TAKE ADVANTAGE OF MULTIFACTOR AUTHENTICATION?

Deploying multifactor authentication is certainly a significant technical undertaking for an IT organization, but it is even more so a change management effort. Organizations should carefully plan their multifactor deployments to increase user satisfaction and raise the likelihood of a smooth rollout process that minimizes business disruption.

## Begin with a Pilot Rollout

As with any major technology initiative, IDC recommends that multifactor deployments begin with a pilot initiative designed to serve as a proof-of-concept for the technology and resolve any technical issues before impacting larger numbers of users. During this pilot deployment, organizations should:

- Validate that the selected multifactor authentication technology integrates with existing infrastructure and services.
- Confirm that the enrollment experience for end users meets both technical and user experience requirements.
- Estimate the impact on the help desk and front-line IT support during the rollout process.
- Verify that routine authentication works as expected and prompts users to reauthenticate at the desired interval.
- Test communications tools to ensure that they adequately convey the rationale behind the initiative as well as clear steps that users should take to enroll their devices in the multifactor system.

Organizations conducting multifactor pilot projects are often tempted to limit the pilot to IT staff in an effort to "protect" end users from exposure to unproven technology. While this approach is well intentioned, it reduces the effectiveness of the pilot project by only exposing the technology to a technically sophisticated audience. Multifactor deployments have significant change management requirements, and organizations should include users with varying degrees of technical expertise in initial deployments.

## Add Users in Waves

Upon successful completion of the pilot initiative, the organization should begin planning the deployment of multifactor authentication to the full complement of users in a staged manner. Some factors to consider when designing the full-scale deployment are:

- **Availability of both tier 1 and tier 2 IT support resources to support the deployment.** Draw upon experience from the pilot initiative to estimate the support burden and size waves so that they do not overwhelm available IT support staff.
- **Prioritize high-risk users for early inclusion in the system.** Users with privileged access to systems and applications will have the greatest negative impact on the organization if their accounts are compromised and should be prioritized for multifactor deployment.
- **Events in the business cycle that may affect scheduling.** Schedule users to adopt multifactor around critical events. For example, finance personnel should not be scheduled for multifactor deployment during the week of year-end close. Similarly, salespeople should not be rolled into the system during an end-of-quarter rush to close deals.

One way to ease the burden on support staff and improve the end-user experience is to offer users an opt-in period where they may enroll themselves in multifactor authentication and begin using the technology immediately. Many users will choose to take advantage of this self-paced enrollment and then will not need to be part of the waves of mandatory enforcement that follow.

## Add Services on a Parallel Track

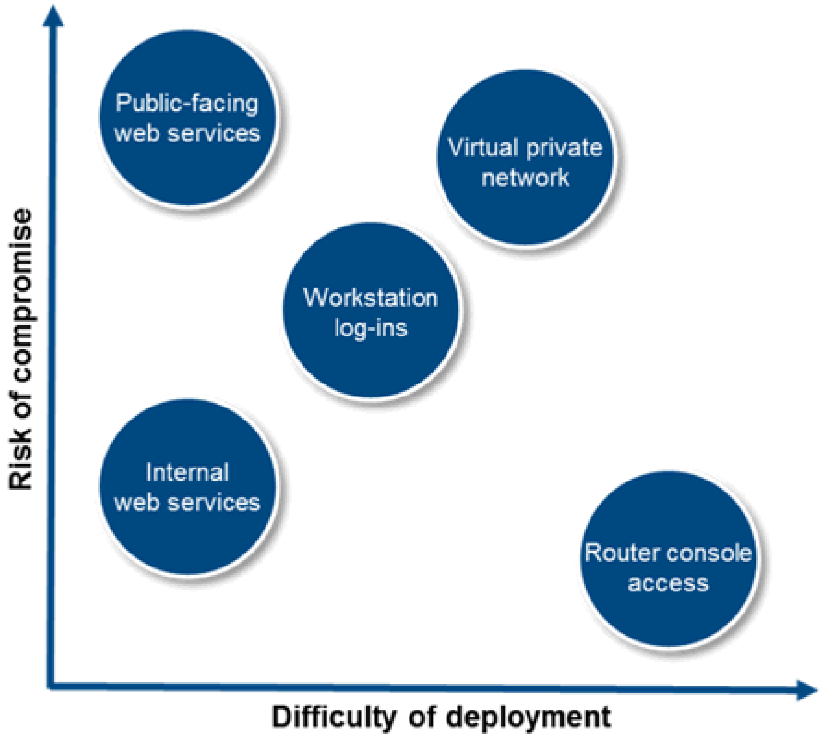
In addition to deploying multifactor authentication to users, organizations will also need to plan the deployment of multifactor authentication across its IT service portfolio. IDC recommends that organizations consider two major factors when planning their service rollout:

- **Risk of compromise.** Organizations should consider both the likelihood that an attacker will successfully compromise the service and the impact on the organization should such a compromise occur. Together, these two criteria determine the risk posed to an organization by the service. For more on evaluating risk, see *IT Security Foundation: Assessing IT Adversarial Risk for Digital Transformation* (IDC #US41083616, March 2016).
- **Difficulty of implementation.** The technical characteristics of the service and the organization's chosen multifactor authentication platform will create varying degrees of technical difficulty for service implementation.

Organizations may wish to develop a matrix similar to the one shown in Figure 4 to help them prioritize service rollout. The contents of the matrix will vary depending upon the organization's infrastructure and vendor choices. After developing this matrix, the IT team should generally begin by deploying multifactor to the high-risk/low-difficulty services in the upper left corner and progress in a down-and-to-the-right fashion, concluding with the low-risk/high-difficulty services in the lower right corner. This approach provides the greatest impact/effort trade-off.

### FIGURE 4

### Prioritizing Services for Multifactor Deployment



Source: IDC, 2017

## Communicate Frequently

We cannot overemphasize the importance of frequent communications with end users, management, and other stakeholders about the multifactor initiative. Changes to authentication are a frequent source of fear, uncertainty, and doubt among end users, and the project team should take care to assuage these concerns by communicating frequently and highlighting the stories of end users that successfully migrated and appreciate the added security offered by multifactor authentication.

Some organizations choose to replace the technically obscure language of "multifactor authentication" with a friendlier term when communicating with end users. For example, organizations might refer to the initiative as "two-step log-in" or "enhanced security."

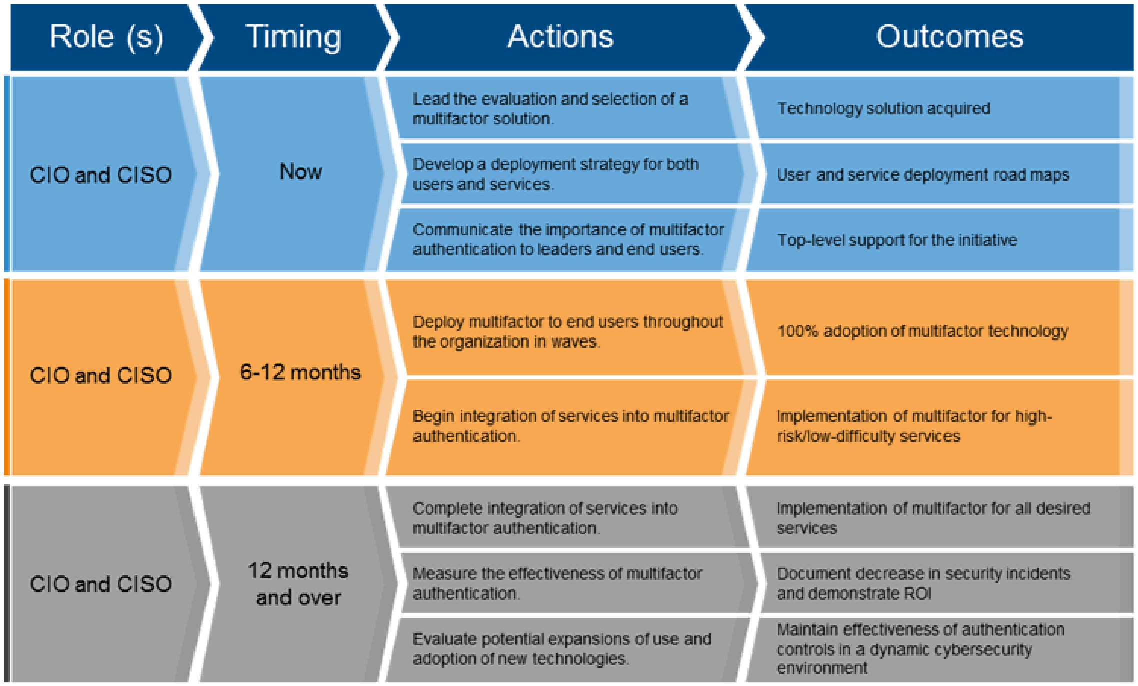
Successful communications efforts also sometimes draw parallels to the experiences that end users have with consumer-based multifactor authentication technology. They might say that this is "technology similar to what you might use to protect your financial, email, or social media accounts."

# ESSENTIAL GUIDANCE

Multifactor authentication plays a critical role in protecting an organization against increasingly common password-based attacks. IDC recommends that organizations that either have not deployed multifactor authentication or have only deployed multifactor to a limited subset of users consider full-scale implementations. Figure 5 provides our essential guidance on this subject.

## FIGURE 5

### Essential Guidance for Deploying Multifactor Authentication



| Role (s) | Timing | Actions | Outcomes |
|---|---|---|---|
| CIO and CISO | Now | Lead the evaluation and selection of a multifactor solution. | Technology solution acquired |
| | | Develop a deployment strategy for both users and services. | User and service deployment road maps |
| | | Communicate the importance of multifactor authentication to leaders and end users. | Top-level support for the initiative |
| CIO and CISO | 6-12 months | Deploy multifactor to end users throughout the organization in waves. | 100% adoption of multifactor technology |
| | | Begin integration of services into multifactor authentication. | Implementation of multifactor for high-risk/low-difficulty services |
| CIO and CISO | 12 months and over | Complete integration of services into multifactor authentication. | Implementation of multifactor for all desired services |
| | | Measure the effectiveness of multifactor authentication. | Document decrease in security incidents and demonstrate ROI |
| | | Evaluate potential expansions of use and adoption of new technologies. | Maintain effectiveness of authentication controls in a dynamic cybersecurity environment |

Source: IDC, 2017

## RELATED RESEARCH

- *IDC TechScape: Worldwide Advanced Authentication, 2017* (IDC #US42418917, April 2017)
- *The Era of the Password Has Passed* (IDC #lcUS41963216, November 2016)
- *Worldwide Identity and Access Management Forecast, 2016-2020: Mobile and User Behavior Analytics Drive Growth* (IDC #US41644516, August 2016)

## About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Trademark Notice