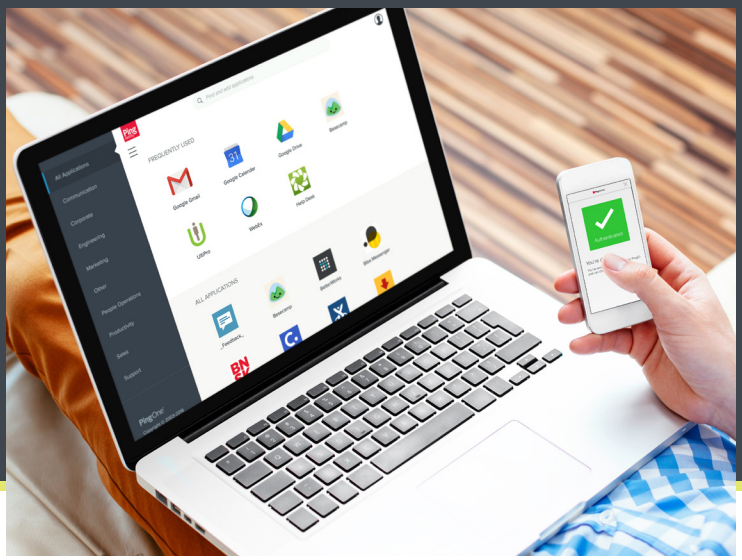

THE SECURITY LEADER'S GUIDE TO MULTI-FACTOR AUTHENTICATION

Password isn't exactly a four-letter word, but as a security leader, it should be just as cringe-worthy. You don't need to read every study or article about the weaknesses of passwords—though there are plenty—to know that single-factor authentication is putting your enterprise at risk.

Two-factor authentication (2FA) provides an extra layer of protection. Is it a step in the right direction? Sure. But it leaves something to be desired in terms of both security and experience. Not only is 2FA notoriously unpopular with your users, it's also not the sharpest security knife in the drawer, particularly if the second factor is delivered via text message.

> "[For those that] only offer second factor protections that depend on SMS, it's time to wake up, smell the targeted attacks, and give users better options.[2]"
>
> Andy Greenberg, Wired

This weakness came into the public light in 2016 when attacks on political figures were found to be a result of intercepted SMS messages. Around the same time, the National Institute for Standards and Technology (NIST) stopped recommending 2FA systems that use SMS, because of their many security weaknesses. While 2FA is correct in theory, "using SMS text messages isn't technically two-factor at all," according to security researcher and forensics expert Jonathan Zdziarski.[1] He asserts there are better tools that can actually prove possession of the "what you have" factor.

He's right. And that better tool is multi-factor authentication, or MFA.

[1] Andy Greenberg, "So Hey You Should Stop Using Texts for Two-Factor Authentication," Wired, June 26, 2016, accessed Feb 23, 2017 at https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/
[2] Ibid

01

HOW & WHY MFA WORKS

Multi-factor authentication begins with the notion that you can and should provide multiple factors for authentication, not just a single static means. MFA goes beyond 2FA by requiring users to authenticate via two or more different authentication factors as shown in Figure 1. By definition, it doesn't limit the number of authentication factors, but emphasizes the use of a broader set of factors across three main categories: what you know, have and are. This provides flexibility and a better user experience, not to mention a stronger security stance.

Combining multiple authentication factors results in a higher Level of Assurance (LoA) that the user attempting to authenticate is who the user claims to be. The theory is that if one of the factors has been compromised, the chances of the other factor also being compromised are low.

Authentication mechanisms can be distinguished by whether they use the same channel where the user accesses the application, or a separate channel that's dedicated for authentication. There's also value in authenticating via multiple factors of the same type, as long as compromising one factor doesn't mean compromising the other.

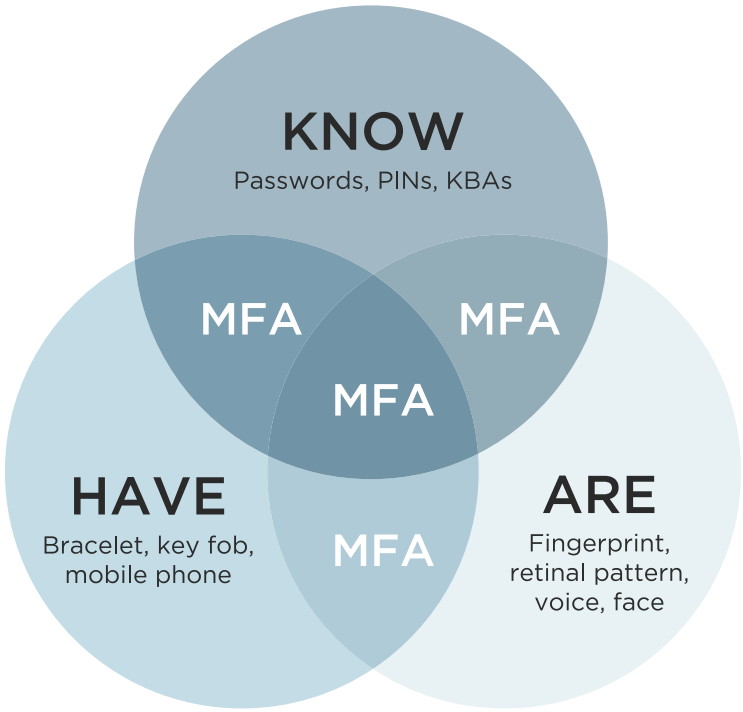

Figure 1: MFA requires users to identify themselves via two or more categories of authentication.

02

THE CASE FOR MFA

Digital transformation poses exciting opportunities for business and unprecedented challenges for security leaders. You need to adopt new applications and cloud technologies to remain competitive, but you must also minimize risk. On top of that, you need to place a larger focus than ever on user experience to keep pace with competitors, encourage adoption and, ultimately, achieve success.

Hitting the trifecta of security, cost and user experience isn't easy. But it's exactly what modern MFA was made for.

REDUCED RISK OF BREACH

Using MFA makes it more difficult for hackers to steal credentials or use brute force and discretionary attacks to breach your systems. Given the magnitude of costs associated with a typical breach—not to mention the lost revenue and damage to your company's reputation—reducing your risk can have a substantial impact on your top and bottom lines.

LOWERED COSTS

When it comes to cost, hardware-based token solutions can't hold a candle to utilizing a user's mobile device. Inherently flexible, modern MFA solutions allow you to step requirements up or down depending on the risk of a particular activity. Doing so reduces the cumulative costs of one-time SMS passcodes, voice calls or push methods by employing those controls only when warranted. The investment in MFA is typically offset by these cost reductions, coupled with the decrease in administrative costs associated with reduced help desk intervention.

BETTER USER EXPERIENCE

At the core of delivering an exceptional experience is giving users access to the information they need, when and where they need it. This is what MFA is made for, and it does so in a secure and frictionless way. By providing the flexibility to choose from a number of authentication mechanisms to address the preferences and constraints of your users, MFA allows you to deliver the type of experience they expect with the level of security you demand.

For customers-facing enterprises it is beneficial to embed MFA capabilities into your own mobile application. This can give customers secure MFA without requiring them to download a third-party MFA application or use less secure second factors.

03

STEPPING UP YOUR SECURITY

When choosing the right authentication method for your enterprise, you want to consider a number of factors. While not an exhaustive list, here are some of the most important:

- **Strength:** How well does it protect against common threat actions?
- **IT cost & overhead:** What is the cost per user? Will it require additional resources?
- **Ease of use:** Will it be easy for users to adopt? Do they have a choice of authentication mechanisms? Does it have a mobile SDK so you can embed MFA into your own mobile application?
- **Ease of implementation:** How easy is it to deploy and maintain?
- **Industry compliance:** Does it meet the compliance standards you must adhere to?
- **Standards:** Does it support identity standards, like FIDO?
- **Flexibility:** Will it support dynamic, step-up authentication?

The last point speaks to applying risk-based (or step-up) authentication to dynamically assess the risk associated with the request and apply only the necessary amount of security. To step up your own security and user experience, you can combine step-up authentication with passive contextual mechanisms.

Contextual MFA passively collects and analyzes contextual, behavioral or correlative factors, like geolocation, computing environment and nature of the transaction being attempted. It collects data about the user to establish a typical behavioral profile. If the user's behavior falls outside of this, it steps up authentication requirements. These operations are invisible to the user, so experience isn't compromised, and also highly reliable, minimizing vulnerability to attack.

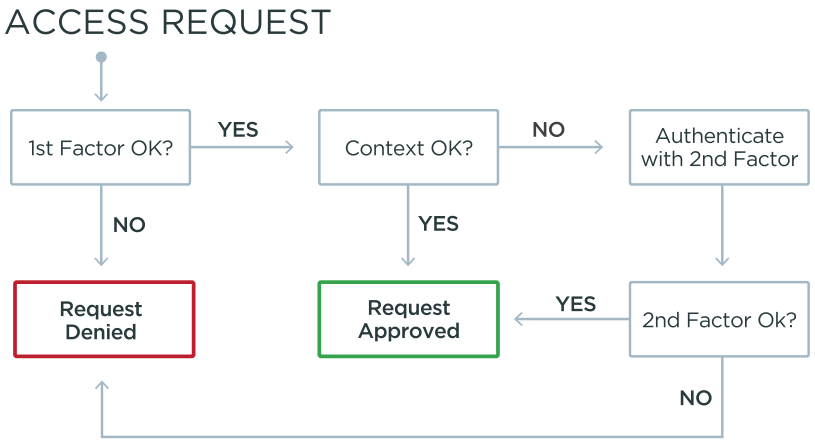

Figure 2: Risk-based step-up MFA is triggered by atypical and anomalous context or behavior. It's only when the context collected via the first authentication factor indicates something unexpected that a second factor of authentication is requested before access is granted.

04

MOVING BEYOND PASSWORDS

According to the latest Verizon DBIR, 81% of breaches in the enterprise were a result of weak or stolen credentials. And many, if not all, of them could have been prevented with a stronger authentication method.

By authenticating users on something they know (like a password), combined with something they have or are, MFA provides a stronger level of security against attack. Stepping up MFA with a risk-based approach using passive contextual authentication delivers the ultimate combination of security, usability and cost-effectiveness.

If you're ready to move beyond passwords—and we both know you are—we invite you to discover how MFA can strengthen your security posture. Read our Ultimate Guide to Enterprise User Authentication to learn more.