



The What, Why and How of **Phishing-Resistant MFA**

A Tale of FIDO, PIV, CBA, WHfB, and More



Table of Contents

What: Key Elements of Phishing Attacks	4
Why: Reasons to Prioritize Phishing Resistance	9
How: Best Practices to Prepare for a Phishing Attack	14
Start with the Fundamentals	15
Be Realistic About What you Already have	17
Leverage the Right Authentication Methodology	20
Pursue the Challenge Holistically	24
Balance Protection with Usability	27
Operationalize the Authentication Lifecycle	29
Conclusion	31
About Axiad	32

Phishing attacks are on the rise around the globe, and they are becoming **more efficient and more costly to organizations that are unprepared**. Cybersecurity advisors and watchdogs, including the White House Office of Management and Budget, NIST, and CISA are well aware of the escalating threat. They advise security executives to prioritize a **technology-centric defense strategy**. But with so many options available – many of which have critical gaps that can be exploited by bad actors – how do you move forward in a pragmatic fashion? This eBook leverages insights from some top security insiders to help you prepare.



What: Key Elements of Phishing Attacks

The Fundamentals of Phishing

Phishing is a malicious activity that uses some form of social engineering to gain access to personal, sensitive, or proprietary information; or the goal may be to penetrate the victim's infrastructure and deploy malevolent software such as ransomware. It can target a specific person or group (called spear phishing) by leveraging details that aren't widely known to create a false sense of security, or it can apply to a wide population. Other variations include vishing, trap phishing, whaling phishing and email phishing scams.

These ill-natured attacks can come in many forms. The most common, according to **National Institute of Standards and Technology (NIST)**, are the following:



Impersonated Website

The use of fake authenticators at illegitimate websites.



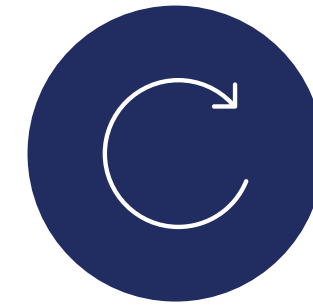
Attacker-in-the Middle

When an attacker captures authentication data from the user and relays it to an illegitimate website.



User Entry

When authentication data is manually entered, which can be compromised.



Replay

The use of captured authentication data at a later point in time.



Another emerging threat vector to be aware of, which is a close cousin to phishing attacks, is called **prompt bombing**. This strategy is designed to circumnavigate multi-factor authentication (MFA) with sheer force. By methodically and continuously sending second-factor authentication requests to a user by email or phone (OTP) in a condensed time frame, the sender is counting on the user to become frustrated and

approve the request. This can provide the “**keys to the kingdom**” with access to a variety of applications, systems and services, and it can also provide additional information that can be leveraged for a successful phishing attack.

At the root of each of these examples is a well-tuned strategy executed by cybercriminals to subvert the authentication process.

A Brief History of Successful Phishing Attacks

Phishing attacks aren't new. Some of the most-famous attacks are now almost a decade old and materially impacted the targeted organizations. Here are a few:

Facebook and Google

When a bad actor discovered that both organizations used the same Taiwanese infrastructure supplier, he sent out a series of invoices to them between 2013 and 2015 that led to a series of scams costing more than \$100M.

Fischer Advanced Composite Components AG

An employee at the Austrian aerospace parts manufacturer transferred about \$42M to a fraudulent account in 2016, based on a phony email from the company's CEO.

Sony Pictures

In 2014, a criminal group lured top executives to provide their credentials on a bogus website, which were later used to leak terabytes of data that reportedly cost the organization more than \$100M.

Upsher-Smith Laboratories

A company employee paid out more than \$50M through a series of transfers to multiple bank accounts in 2015, after falling victim to fake CEO requests.

Colonial Pipeline

Access to an employee's password, likely from a phishing email, led to a ransomware attack that crippled a major U.S. fuel supplier in 2021 and led to a \$4.4M ransom –plus untold millions in operational and reputational damages.

Today, phishing remains a top concern for security professionals. A Verizon 2022 Data Breach Investigations Report lists phishing and stolen credentials as two of the four **“key pathways”** that organizations must be prepared to address in order to prevent breaches¹.

In many cases, employee training may have helped prevent the damage. But usually, training alone isn't enough to fend off sophisticated attackers who leverage an array of resources, information, and tactics that would rival a spy novel. To counter these attacks, technology must be leveraged as well.

1. Verizon: Data Breach Investigations Report: January 2023



Why: Reasons to Prioritize Phishing Resistance

Overwhelming Market Data

In a 2022 security report, phishing was cited as the second-most common cause of a breach (compromised credentials was number one), but it was also captured as the most expensive to an organization at an average cost of \$4.91M².

This aligns with other market data that has been published recently. In a 2022 identity security report³, for instance, it was reported that:

"An alarming 84% said their organization had experienced an identity-related breach in the past year. When asked what kind of breach, the most common answer was phishing attacks (59%), whether broad-based attacks or spear phishing."

2. IBM: Cost of a Data Breach Report, July 2022

3. Identity Defined Security Alliance: Trends in Securing Digital Identities, 2022



It's not just that the number of phishing-related attacks is increasing, but the concern also stems from the fact that they can be highly effective. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) noted that 80% of organizations had at least one individual who fell victim to a phishing attempt by CISA Assessment teams⁴. That's why there is a long list of successful breaches reported in the last year, including Twilio, Acorn Financial Services, Mailchimp, and more.

\$4.9M

Average cost of phishing attack⁵.

59%

Experienced a phishing attack in last year⁶.

4. CISA: Phishing Infographic, 2022

5. Identity Defined Security Alliance: Trends in Securing Digital Identities, 2022

6. CISA: Phishing Infographic, 2022

Cybersecurity-Related Watchdog/Regulator Guidance

As the risk on the ground has increased, organizations that are designed to help fight the battle against phishing-based attacks are responding in kind. In January 2022, the U.S. White House Office of Management and Budget (OMB) issued a memorandum⁷ that addressed the concept of phishing resistance 23 times – in just 29 pages of total text.

This guidance, formulated based on the research of many top minds in cybersecurity, is most applicable to the U.S. Federal Government, as related organizations must comply with the guidance by the end of the fiscal year 2024. But organizations doing business with the federal government, and in fact those organizations that simply want to adhere to emerging best practices, are also in line of sight.





CISA followed that guidance by stating in an October 2022 alert that it “strongly urges all organizations to implement phishing-resistant MFA to protect against phishing and other known cyber threats”⁸

And in January 2023, NIST issued a blog⁹ on the importance of implementing phishing-resistant authenticators. In this blog, NIST noted:

“Due to their effectiveness and simplicity, phishing attacks have rapidly become the tool of choice for baddies everywhere. As a tactic, it is used by everyone from low-level criminals looking to commit fraud, to the sophisticated nation state attackers seeking a foothold within an enterprise network.”

Three different authorities on cybersecurity lining up behind a single topic within a short period of time – with strong caution and guidance – is meaningful. It tells you that phishing-based attacks aren’t isolated and/or going away anytime soon.

8. CISA: CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication, October 2022

9. NIST: Phishing Resistance – Protecting the Keys to Your Kingdom, February 2023

A Countermeasure to Hidden Costs

Naturally, the primary and most visible costs of a phishing attack – for organizations that were unsuccessful in thwarting such an attack – are incurred shortly after a breach. Employee downtime, opportunity cost, and impact to brand is often significant. Fines and sanctions are also possible.

But a new and increasingly important cost to organizations is also starting to surface earlier on, even for those who are unscathed by such an attack: the increased cost for cyber insurance. As the volume and voracity of phishing-based attacks has increased, these entities have been subject to massive and

repetitive financial payouts. As a result, cyber insurance providers have raised the bar on security for companies before they can be insured, and they have materially increased premiums as well – with many rates having gone up anywhere from 50-100 percent in the last several years.

Dozens of cyber insurance providers, including Chubb, Travelers, AIG, CyberPolicy, and others have kicked off education campaigns to help their customers better prepare for phishing attacks. Many of these organizations have reported that a key to lower insurance rates is taking proactive measures to address the wide range of phishing tools and techniques that are currently in play.





How: Best Practices to Prepare for a Phishing Attack

With market data, industry watchdogs/regulators, and cyber insurance providers all underscoring the need to proactively prepare for a phishing-related attack, it's no surprise that one out of every two senior security and IT executives said that becoming more phishing resistant was their top cybersecurity priority in the next 12 months¹⁰. The big question for many is how to sift through the noise and accomplish this feat in a pragmatic fashion.

Here are some best practices gleaned from top cybersecurity experts:

10. Axiad: 2022 Authentication Survey Results, October 2022

1. Start with the **Fundamentals**

It's important to first do your homework and clearly define your requirements upfront. If you don't, you run the risk of getting lost in all of the products and features that are available. Some of the most common steps at this stage include:





Categorize End Users

Not all end users are the same, and applying the highest level of controls across the board may not be prudent. Place employees into groups by role (e.g., knowledge worker, compliance, IT, security, executives).



Map Authentication Levels

Armed with your categorization, map authentication levels to your groups. This might include different technology solutions for different categories of users.



Prioritize High-Risk Gaps

Look at the full risk landscape as you prioritize solutions for rollout. For instance, a finance executive with full access to financial systems is a higher risk for phishing than others. But perhaps entire groups – such as the Accounts Receivables team with access to both internal and partner teams – may cumulatively present a higher risk than an individual.



Avoid Easily Compromised Credentials

Passwords are passe for a reason – they are too easy to corrupt. In fact, there are 24 billion username and password combinations available on the dark web¹¹. Make sure you are planning to leverage advanced forms of authentication for all users.



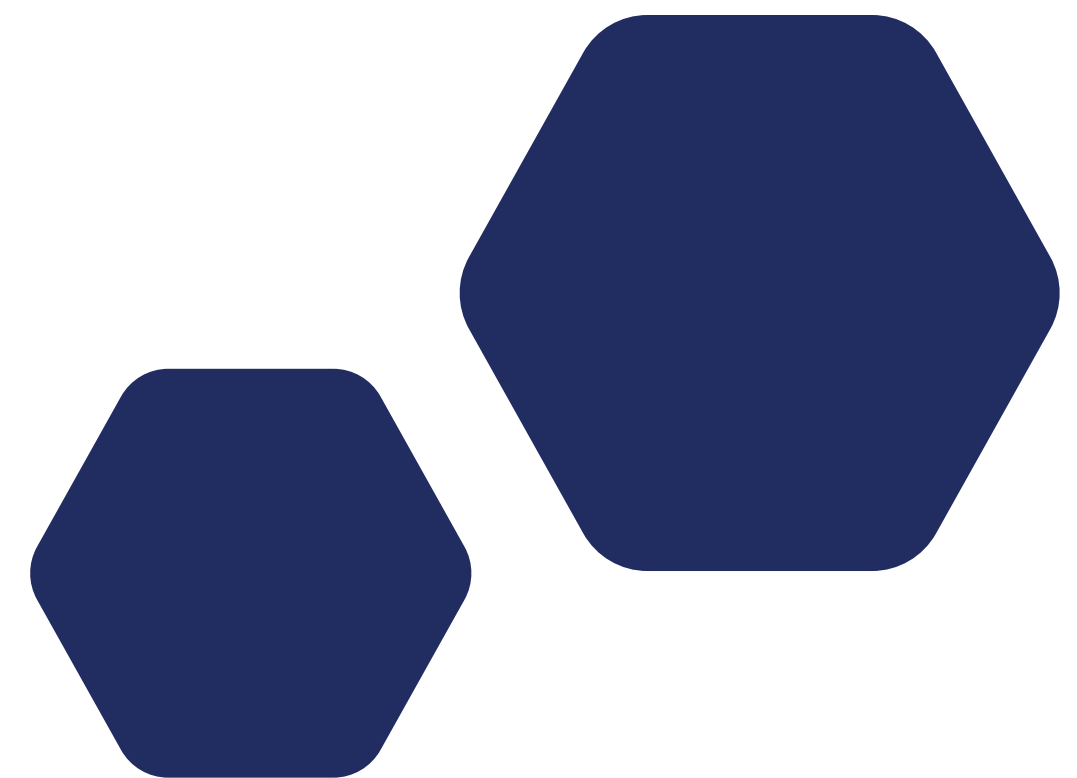
Enforce Day-One Enrollment

Take steps (perhaps through process initially and eventually through technology) to enforce critical policies for onboarding employees on their first day – so they aren't compromised before security controls are fully engaged.



2. Be Realistic about **What You Already Have**

The most common myth about becoming phishing resistant is that what you have in place today will protect you from what will come in the – sometimes near – future. Standard MFA and broad-based Identity and Access Management (IAM) tools are two of the most common tools that organizations tend to view as a panacea. The problem is, often they are not.





Not all MFA is the Same

Unfortunately, not all MFA is phishing resistant. Traditional MFA such as SMS authentication, OTP or even mobile push application notifications are all susceptible to phishing. In the Mobile Push scenario, the user accepts a push prompt sent to the mobile application to approve access. This approach is extremely vulnerable to prompt bombing attacks, as well as simple user error¹². Also, this approach is vulnerable to everyday man-in-the-middle attacks in which hackers intercept web traffic and insert themselves in the middle with fraudulent, lookalike login pages that not only accept user credentials but also deploy MFA to capture access.

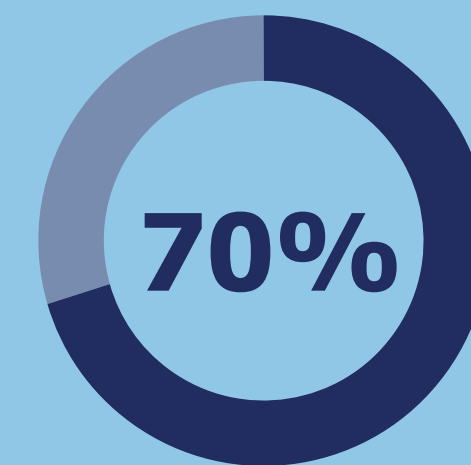


IAM Systems Can be Too Limited

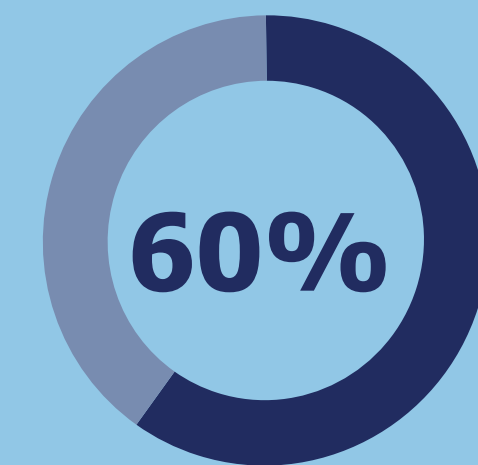
With all the good that IAM solutions do, protection against a phishing attack often isn't one of the primary benefits provided. Many of these solutions – particularly legacy solutions – leverage older MFA capabilities that can be compromised.



The challenges typically don't stop there if you are relying on IAM for phishing resistance. In a recent survey, it was found that 70% of organizations use three or more IAM systems across their organization, and more than half use four or more¹³. When authentication is completed in a fragmented fashion—sometimes caused by dividing efforts across multiple tools in place – it leaves the side door open for a phishing-related attack.



Have 3 or more IAM systems in place¹⁴



Leverage 5 or more authentication methods¹⁵

12. CISA: Fact Sheet: Implementing Phishing-Resistant MFA, October 2022

13. Axiad: 2022 Authentication Survey Results, October 2022

14. Axiad: 2022 Authentication Survey Results, October 2022

15. Axiad: 2022 Authentication Survey Results, October 2022

3. Leverage the Right Authentication Methodology

NIST concluded its recent guidance on the importance of being prepared for a phishing attack by stating:

*"In the end, phishing-resistant authenticators are a critical tool in personal and enterprise security that should be embraced and adopted."*¹⁶

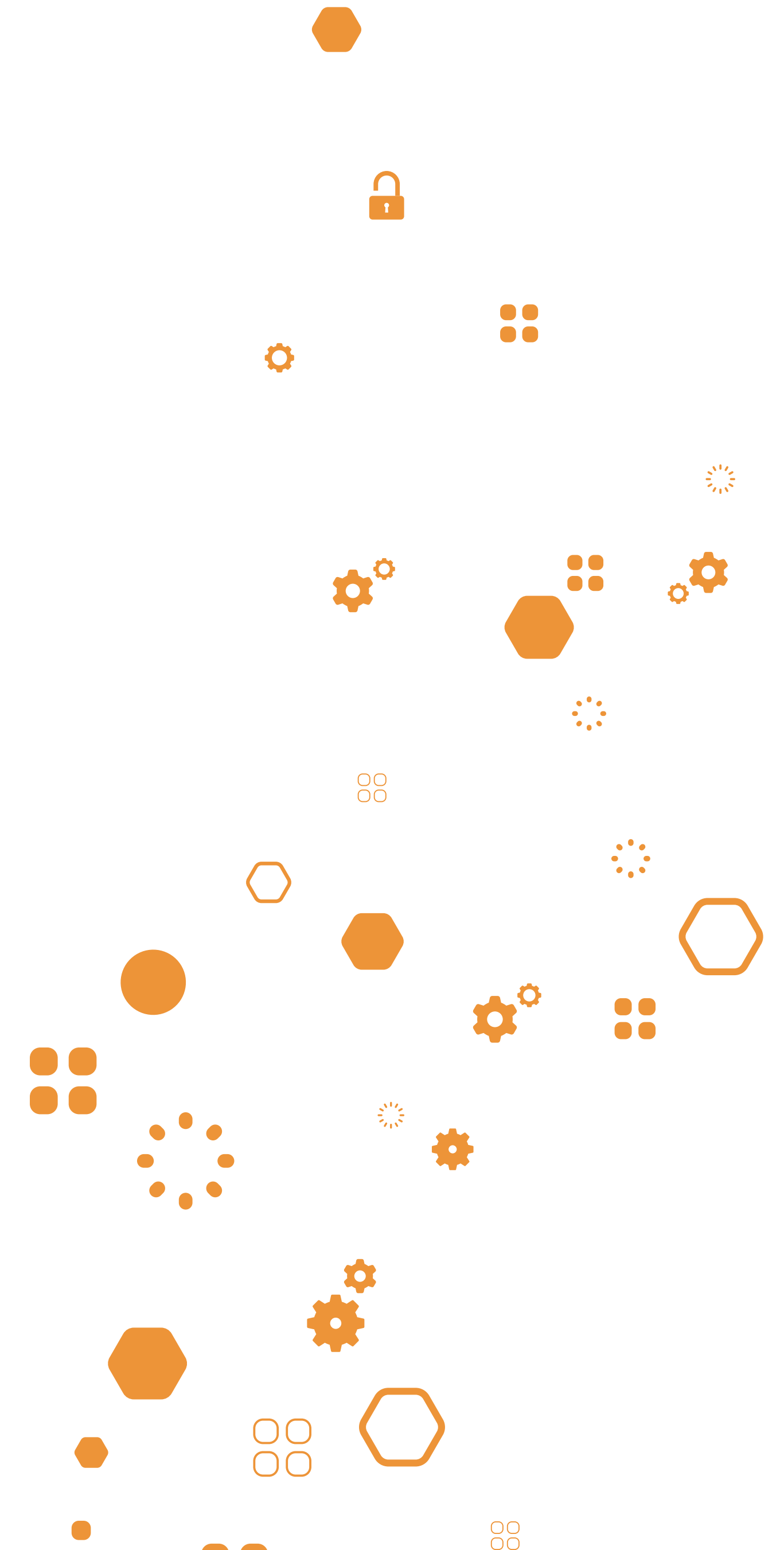
The challenge for many is to determine which ones, as there are several options to consider. Here are the most common and effective forms of phishing-resistant technology to evaluate:

Personal Identity Verification (PIV) Cards

PIV Cards are an integrated solution for U.S. Federal Government identity, credentials and management. This PKI-based credential is typically used by agencies that have the infrastructure to implement and administer it. While the PIV card infrastructure is relatively expensive and implementation times long, it is highly reliable, trusted, and proven. Further, as the PIV card can also be used as a physical identity card (with name, photo, etc.), it has multiple uses.

Certificate-Based Authentication (CBA)

This newer, simpler, more flexible form of PIV uses a strong token such as a YubiKey, a virtual smart card, or hardware device storage for authentication. Since the certificate is validated using secure communications and without shared secrets, CBA delivers phishing-resistant MFA. In addition, the process involves just the selection of the applicable certificate and the input of a PIN, so it is efficient for the end user. It's a great option for organizations in two major ways: 1) given the adoption of CBA by Microsoft, it works well with Azure AD; and 2) it can overlay an existing IAM ecosystem – or multiple IAMs – to effectively deliver an after-market kit for authentication and seamlessly upgrade them to phishing-resistant MFA.



FIDO

Fast ID Online (FIDO) represents an early and important advancement in authentication. To eliminate password storage on external servers, FIDO stores Personally Identifiable Information (PII), including biometric information, locally on the device. NIST says: “FIDO authenticators paired with W3C’s Web Authentication API are the most common form of phishing-resistant authenticators widely available today.”¹⁷ FIDO can take the form of separate hardware keys, or it can be embedded directly into platforms or hardware.

FIDO2

The latest iteration of FIDO enables users to leverage common devices to easily authenticate to online services in both mobile and desktop

environments¹⁸. With support of some of the biggest names in the technology industry such as Apple, Google, and Microsoft – and adoption by browsers such as Google Chrome, Microsoft Edge, Safari, and Firefox plus hardware such as Windows, Android and MacOS devices – this standard is unquestionably the future of phishing-resistant protection.

However, FIDO2 still must be integrated into the thousands of legacy on-premises applications that must be protected, many of which require special modifications. And securing internally developed and vendor-supplied applications further complicate matters and extend timelines.

It is important to know that the FIDO2 standard is evolving rapidly. A recent example is the introduction of the passkey (also called “multi-device passkeys”). As major vendors such as

Microsoft have not yet finalized their implementation of passkey, FIDO2 still requires meaningful work before it can solidify its place as the gold standard of phishing resistance.

Windows Hello for Business (WHfB)

This approach provides strong two-factor authentication on devices. Passwords are replaced with the WHfB credential that is tied to the device. This credential uses a biometric or PIN, rather than a password – working well for Microsoft accounts, Active Directory, and Azure AD. It is a strong option for Microsoft-centric environments, particularly those that are hybrid across on-premises and Azure AD.

17. NIST: Phishing Resistance – Protecting the Keys to Your Kingdom, February 2023

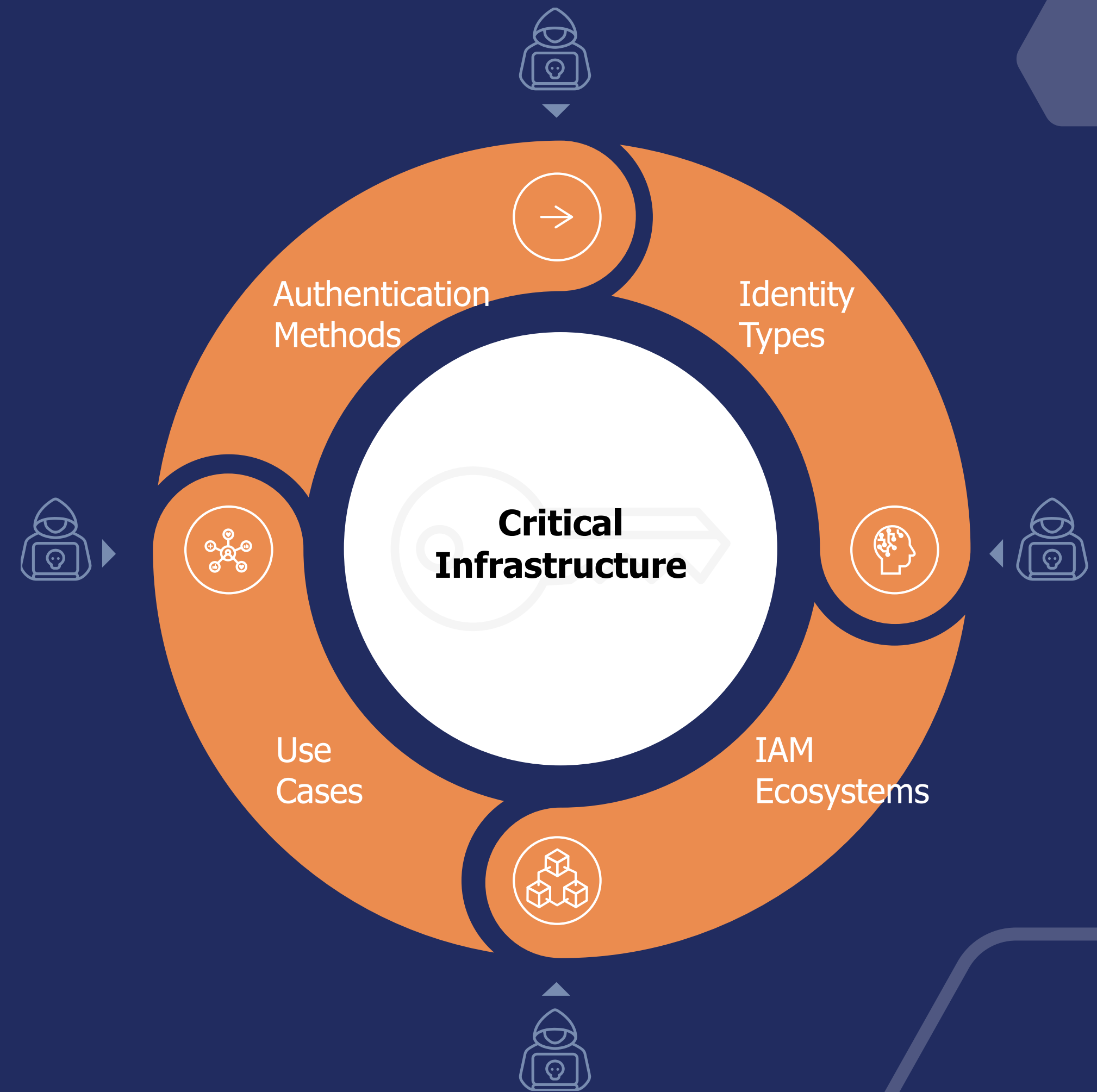
18. FIDO Alliance website: <https://fidoalliance.org/fido2/>

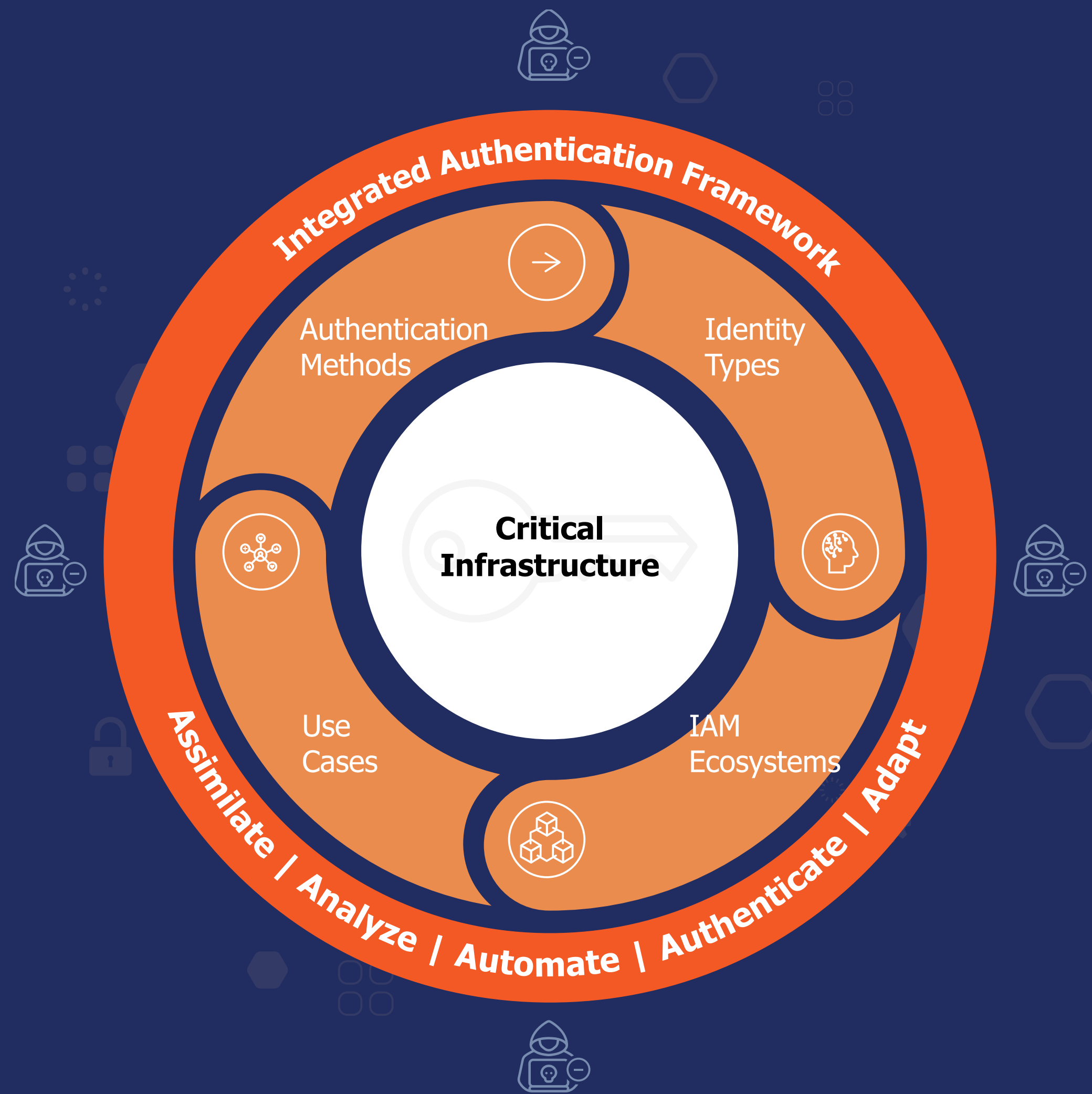


Organizations looking to achieve phishing resistance generally can't go wrong with any of those options, but **it is important to fit the right technology** (or set of technologies) **to the right problem**, at the right time to avoid unnecessary administrative costs, user challenges, and possible added risk if the wrong implementation decisions are made.

4. Pursue the **Challenge Holistically**

With multiple authentication alternatives to choose from, as well as so many authentication nuances to consider – including multiple operating systems perhaps in place, varying authentication methods in use, and user and machine identity types to secure – organizations run the risk of implementing phishing resistance in silos. The resulting gaps and inconsistencies can be exploited by bad actors.



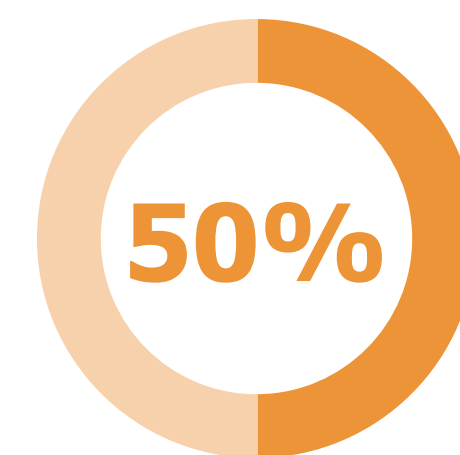


A smarter strategy is to shift from a fragmented approach to a single, **holistic strategy**: an integrated authentication framework. This strategy allows security executives to assimilate credentials, analyze in context, automate processes, authenticate uniformly, and adapt to emerging threats more efficiently. By systematically authenticating across all users, machines, and interactions – regardless of underlying IT complexity – organizations can not only improve their overall cybersecurity posture, but they can also can better **empower users and streamline processes for administrators.**

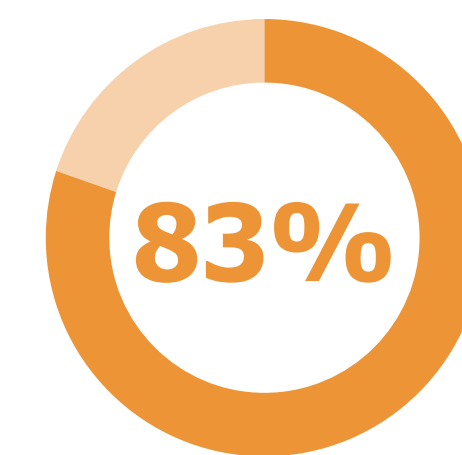


In the context of this analysis, an example of a holistic approach is that many organizations may require PIV/CBA and FIDO due to varying use cases, including authenticating to MacOS then O365. **And FIDO2 and CBA is the only way to deliver a truly passwordless experience for both user and machine authentication.**

Be sure you look at the big picture on what you're trying to accomplish, and then make the investments and develop the processes that will support that strategy over time. In a 2022 survey, 1 in 2 security IT executives said that are shifting from multiple, siloed tools for authentication to a holistic approach ¹⁹.



are shifting to a holistic approach ²⁰.



of organizations have at least 2 operating systems ²¹.

19. Axia: 2022 Authentication Survey Results, October 2022

20. Axia: 2022 Authentication Survey Results, October 2022

21. Axia: 2022 Authentication Survey Results, October 2022

5. Balance Protection with Usability

Becoming phishing resistant with advanced authentication techniques is a noble (and necessary) objective, but organizations can't afford to do so at any cost. Tighten the controls too much or make the authentication process too complicated, and you can negatively impact organizational efficiency. In fact, three in five users say that authentication practices have stopped them from doing their jobs²².



Worse yet, putting in too many perceived roadblocks for users may have unintended consequences from a risk perspective. It has been reported that a majority of users have bypassed security controls if they find them too stringent or difficult to navigate ²³.

To rectify these problems, enter passwordless authentication. This process, which uses factors like a user's device, biometrics, or behavioral analytics to verify identity instead of a password, can deliver on the promise of phishing resistance and reduce user friction at the same time.

But be careful as you consider your passwordless options, however. Not all passwordless solutions are the same. Most options (61 percent²⁴) actually use a password or other shared secret. These solutions typically hide (or mask) the secret from the end user to deliver a passwordless experience. But behind the scenes, the shared secret is still there – and can be intercepted or read. Seek out a “no-password” passwordless solution to eliminate shared secrets that are open to compromise.

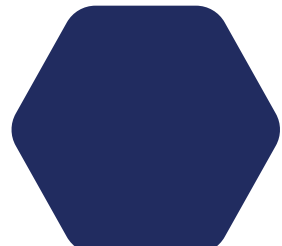
23. Axiad: 2022 Authentication Survey Results, October 2022

24. Cybersecurity Insiders: The State of Passwordless Security, 2021

6. Operationalize the **Authentication Lifecycle**

It's important to recognize that, in addition to the above, there is yet another weak link in authentication: the authentication lifecycle. This multi-step process spans authenticator enrollment, credential issuance, account recovery, credential (especially certificate-based) renewal, and revocation.

Once phishing-resistant MFA becomes the standard, bad actors focus on the vulnerabilities exposed during the lifecycle. An example of this kind of attack is hackers forcing the authentication to go to account recovery mode in order to exploit a weak link. For example, account recovery models that rely on personal information, such as your mother's maiden name, are a weak link since that information can be intercepted and then reused many times.





In addition to being secured at every stage, the lifecycle must be operationalized with the right tools and capabilities for IT to manage efficiently. And since IT cannot practically manage all stages of the lifecycle, user self-service – where secure emergency access is provided through face-to-face or remote authentication – must be enabled. Self-service also benefits the organization by reducing end user friction and driving down administrative costs.

Conclusion

Phishing resistance is not a **'nice to have.'** With attacks becoming more common, and more effective, cybersecurity watchdogs/regulators, cyber insurance providers, and security professionals are all lining up to help address this emerging threat vector. The path forward is difficult to navigate, but not impossible to tame. Make sure you:

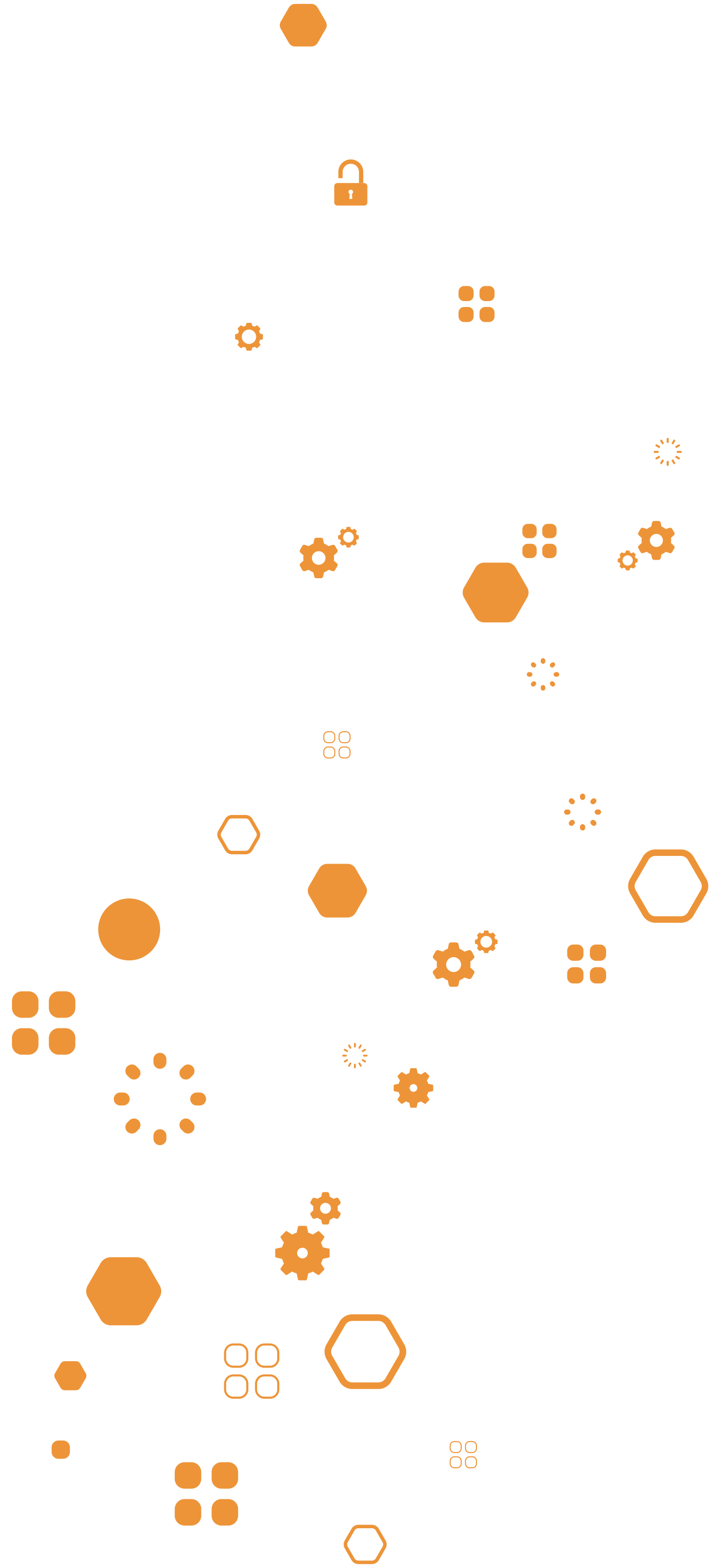
- 1** Are pragmatic and methodical in formulating your strategy
- 2** Take steps to leverage the right tools for the job
- 3** Think long term and future-proof your vision
- 4** Seek out technology that can help you integrate your approach and lower hurdles for your end users.

About Axiad

Axiad delivers organization-wide passwordless orchestration to connect people and machines to data and applications from anywhere with a comprehensive, secure, and efficient SaaS authentication platform. Unlike many approaches that are done in silos across multiple authentication methods, identity types, use cases, and existing IAM systems, Axiad allows customers to move to a passwordless future – and attain phishing resistance – without the friction and risk of fragmented solutions.

Axiad's flagship platform, Axiad Cloud, is a comprehensive, secure, and efficient authentication platform that delivers on the promise of integrated authentication orchestration. It supports PIV, CBA, FIDO, FIDO2, and WHfB, as well as the widest range of other credentials such as mobile MFA, YubiKeys, smart cards, TPM and biometrics.





Axiad's Certificate-Based Authentication for IAM extends the built-in functionality of a company's existing IAM system(s) to provide passwordless, phishing-resistant MFA for every user. Because it can overlay multiple IAM systems, use cases, and operating systems – including Microsoft Windows, Apple OS, and Linux – it can help organizations be more consistent and systematic in how they authenticate.



axiad