yubico

ZERO TRUST WHITE PAPER | MAY 2023

Accelerate your Zero Trust strategy with phishing-resistant MFA

Seven best practices to jumpstart your journey

Introduction

Last week I got an email with the kind of subject line you have to read twice: “The Zen of Zero Trust.” It was an invite to a webinar billed as “a lively exchange of perspectives, opinions and best practices on the path to data security enlightenment.”

That email is a good example of the marketing buzz around Zero Trust. Fact is: there’s nothing zen about Zero Trust and even less enlightenment. Everywhere they turn, CISOs are being told that they absolutely must implement Zero Trust. All of your friends and competitors already have strategies. And if you don’t, well, it can feel like you’re late to the game.

The principle of Zero Trust might be right for this moment, but it’s understandable if you’re struggling to move to a Zero Trust framework or infrastructure. The fact of the matter is, getting started on the Zero Trust journey and continuing to build on it is not easy—no matter how many CISOs claim they’re doing it.

If you’re a CISO who’s still trying to get your arms around the authentication aspects of Zero Trust, this whitepaper is for you. It focuses on key considerations and the practical steps you can take to make Zero Trust a livable, workable strategy starting with some key building blocks that will allow you early wins on your Zero Trust journey.

Demystifying Zero Trust

While the concept of Zero Trust has been around for a while, and in many organizations Zero Trust initiatives are well underway with the goal of protecting the company’s most important assets, it still means different things to different people. There may be many roads to Zero Trust cutting across the network, identity, and access control, and the array of definitions or ways to get there are dizzying.

To cut through all the noise, simply put, the Zero Trust framework implies that an organization should trust no individual or thing unless properly verified before being given access to the network and data. Can you imagine going grocery shopping and thinking that everybody entering the store was untrustworthy and was going to attack you, and possibly compromise your well-being? A sobering thought, and now having experienced the pandemic, a feeling that we’re all too familiar with.

But that’s exactly how a zero trust system works. Your network believes everything that comes from outside or within the system is hostile. Zero Trust means you can’t trust anything—not the user, not the computer, not the communication.

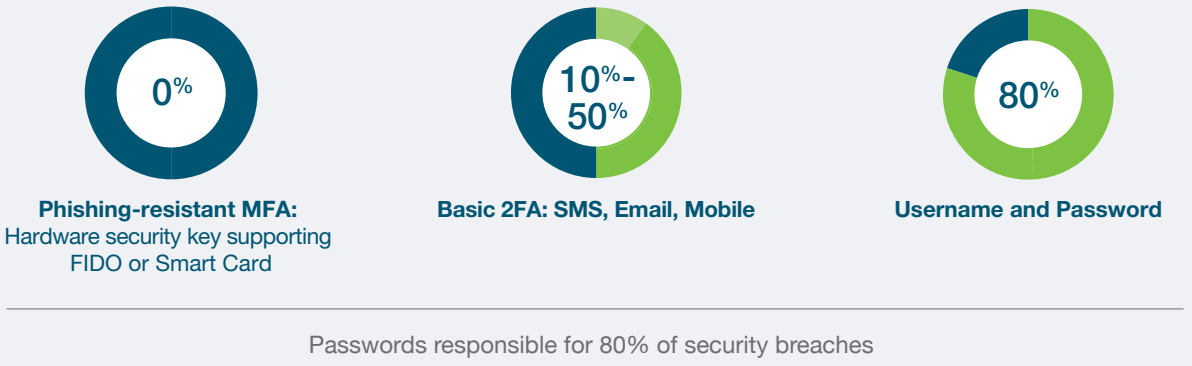
You have to validate and authenticate every user who is entering the network. You have to install monitoring agents on every endpoint. They have to validate that the device is trustworthy and provide attestation. You have to expire a user’s session and make them re-authenticate frequently. Doesn’t that sound like a horrible user experience? It can be if not approached with not only the organization’s security in mind, but the user experience as well.

Accelerate Zero Trust with phishing-resistant MFA

The Zero Trust model involves having a strong level of trust in the authentication mechanisms of every user from every device attempting to access company resources, whether inside or outside the network perimeter. Adopting strong authentication as a core building block of your Zero Trust strategy will jumpstart the security posture of the organization with strong identity management and authentication. By contrast, an organization that starts with network access, re-architecting network elements can be a much more complex process and take a lot longer. Re-architecting your network with zero trust principles is important but with strong authentication and an access control framework in place, you have a foundational Zero Trust component that can be leveraged along the journey. Additionally with an Identity framework in place, you can know who the users are, the strength of their authentication, and how they are connected so that unusual behavior can be detected.

No matter how one tackles this broad framework, it is important to start by creating a trusted identity with strong authentication for the user as a baseline as it provides immediate benefits across the organization that can be built upon as you further build out zero trust access policies. A critical part of this is looking at how users are establishing their identity, and what level of trust can be attributed to that mechanism. If users are using passwords alone to verify their identity, then the organization has no assurance of security no matter how nuanced and well thought through the rest of the Zero Trust strategy may be. Passwords are known to be highly vulnerable to remote and Man-in-the-Middle (MiTM) attacks, and stolen passwords are responsible for 80% of costly data breaches. SMS, email and mobile authentication offer more security for user identities than passwords but still fall down as they are so vulnerable to remote and phishing attacks.

Figure 1: Varying attack penetration rates of different user verification approaches



In a Zero Trust approach, mitigating known vulnerabilities that expose sensitive data is critical. Given that user access is a fundamental risk to protecting sensitive data, it is critical to implement strong authentication measures.

Unfortunately, one of the most common pitfalls organizations may fall into is to think of Zero Trust initiatives as one initiative, and think of strong authentication as another initiative altogether, as part of perhaps a regulatory mandate or related workstream. A real life example may be to have Zero Trust policy engines, and the identity authorization governance/policies as separate systems. A better and faster way to set things up well from the ground up is to think of strong authentication as a fundamental aspect of Zero Trust, and tying strong authentication into the broader Zero Trust initiative.

Establish trusted user identities using modern MFA

Modern multi-factor authentication (MFA), as part of strong authentication, can prevent network access with stolen passwords. Strong authentication using modern MFA enables phishing-resistant user authentication before access is provided. Legacy multi-factor authentication (MFA) methods such as SMS, authenticator apps and the like have been proven to be highly phishable. The authentication in these models are not truly bound between what the user has and the service allowing for access codes to be intercepted and replayed. If a user is using these methods to verify their identity and enter the network, the account can be compromised allowing for the attacker to gain a foothold that leads to lateral movement that can be difficult to find. As a result, the industry is moving away from symmetric based secrets (passwords, OTP) to more advanced asymmetric solutions that are bound in physical devices.

In order for it to be a secure Zero Trust framework, user accounts should be established using modern 2FA or MFA, using purpose-built hardware security keys that deliver the strongest levels of phishing defense and secure user access. With hardware security keys using modern phishing-resistant authentication protocols, users can register one single security key to hundreds of services with a unique public/private key pair generated for each service, and the secrets are never shared between services. And the private key is stored in the secure element on the hardware key and cannot be exfiltrated. In this manner hardware security keys stop remote, MiTM and phishing attacks as only the registered service is allowed to initiate the authentication ceremony unlike SMS or any mobile app authentication.

Figure 2: Strong authentication enabled with modern 2FA/MFA

Something you know (PIN) or (biometrics) unlocks the device

Private/Public key pair ceremony to validate the credential

A user can register one hardware security key to hundreds of services with a unique public/private key pair for services with secrets never shared.

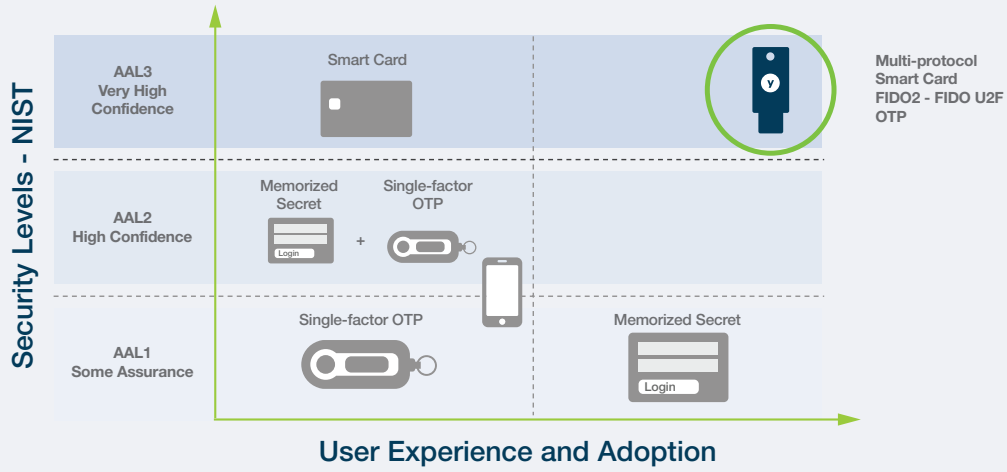
Top 7 strong authentication best practices to support Zero Trust

Zero Trust is a journey, with the first step being establishing a user trust framework. The following seven best practices will ensure that you are on your way to protecting a user's access as a foundational element of building your Zero Trust architecture.

1. Deploy strong phishing-resistant MFA

With the FBI stating that cybercrime has skyrocketed by 300% since COVID-19, and with a remote or hybrid workforce, organizations recognize the need to bolster security for user authentication with multi-factor authentication (MFA). As mentioned earlier, not all forms of MFA are created equal and below are some considerations when choosing authenticators that establish user identities.

Figure 3: Not all forms of MFA are created equal



Hardware security keys offer strong security and great user ease

When considering authenticator capabilities an organization should consider the following:

- **Security:** Is it a purpose-built security-focused hardware device or one built primarily for communication (such as a phone). Does the authenticator add other complexities such as the user having to download additional applications or software? And, does it provide 100% protection against phishing attacks? From a zero trust perspective, enabling strong security while reducing complexity should be a key design goal. A dedicated security-focused device allows for easier and more consistent monitoring.
- **Standardized access:** Is the authenticator based on open standards which means it will authenticate in a consistent and secure fashion across a range of platforms and services. Leveraging open standards allows for hundreds of integrations out-of-the-box, and requires limited configuration, which keeps proprietary solutions to a minimum. Additionally, open standards drive the industry to follow standard deployment patterns which in turn means that vendors will deploy solutions in a common way reducing complexity for enterprises. FIDO and smart cards (PIV) standards are the default strong authentication standards that the industry has and is building around.

- **Deployability:** Can the authenticator provide security across multiple devices, and can it work offline across mobile- or other types of restricted areas, in completely remote locations, or across shared workstations? We know that not all applications or environments can accommodate strong authentication protocols like FIDO or smart cards (PIV). An authenticator, and your IAM system, needs to be able to bridge the gap from OTP-based solutions to more secure solutions. When a system is ready to use stronger authentication, all your endpoint authenticators should not need to be replaced. Is it durable to handle the daily abuse across various hostile environments and continue working? And finally, is this a solution that is easy to manage for the organization and the user, with turnkey delivery to the user no matter where they are and with simple user self-service options to get up and running in minutes.

The right strong authentication solution should be able to address all of these considerations for best results for the organization and its users.

2. Attestation is important for Zero Trust

In a Zero Trust model, you cannot have implicit trust in the authenticator. With a Zero Trust mindset, strong authentication is very important but you still need to validate the hardware device itself to ensure it is coming from a known source and not compromised. Endpoint management is an important component of a Zero Trust framework as phones and computers are susceptible to malware. Attestation enables validation that the authenticator hardware is from a trusted manufacturer and that the credentials generated on that device have not been cloned.

There are two types of authenticators—platform authenticators that are built into modern devices such as laptops and smartphones. And then there are portable authenticators that are external to the computer and phones and can be carried around with the user, either on a keychain, or a small version that can be plugged into the computer.

Related to this is the process of attestation of a particular authenticator. Attestation is a key pair that is burned into the device during manufacturing providing important details such as manufacturer and device model. There has to be trust that the service knows the origin of the authenticator, and allows for cryptographic verification that the “attestation signature” on the newly created public key came from the trusted device. Attestation concepts are built into the FIDO standard and some vendors, like Yubico, also include attestation capabilities for smart card deployments. Additionally attestation is available in computers that have a secure element like a TPM or a Secure Enclave. Not all computing devices have a secure element by default. Additionally computer systems that OEM components will have secured elements from many third parties that you would need to track.

FIDO credentials, now called passkeys, can either be exportable or not exportable. Synced passkeys are automatically exported and copied across known devices. This provides a convenient way for consumers to use phishing-resistant authentication but comes with trade-offs. The very nature of FIDO credentials that are copied between devices makes it very difficult to attest to the protection of the credential on a particular device. At this time, there is no attestation for synced passkeys. Hardware-bound passkeys, which security keys support, are generated on the device and cannot be exported. As a result, the established FIDO attestation control provides cryptographic proof that the credential is protected by a known device.

Platform authenticator (built into the device) and FIDO synced passkeys make it challenging to receive valuable signals of how credentials are protected. Additionally, if the device is compromised the authenticator itself has a higher risk of being compromised as malicious code has more opportunity to find and exploit vulnerabilities. It's essentially a single point of attack. By contrast, using a single purpose portable authenticator that cannot have third party software loaded onto it, has a higher level of assurance that the private key material is known, authentic, and protected. This aligns with Zero Trust principles. Ultimately, it comes down to this simple fact, if you cannot trust, or have no visibility of the authenticator, then you can't trust the authentication either.

3. Strong authentication for all access points

Most organizations are using Identity and Access Management (IAM) platforms as core components of their Zero Trust framework. IAM is essential for securing the hybrid multi-cloud organization. Done right, modern IAM solutions can deliver a frictionless and secure experience for every user, asset and data interaction providing a foundation for a Zero Trust strategy. These solutions can grant access rights, provide single sign-on from any device, enhance security with MFA, enable user lifecycle management, protect privileged accounts, and more. When considering MFA in support of Zero Trust, it is a prudent architectural approach to decouple the authenticator from the IAM platform. This allows for an authenticator that can work with a wide array of IAM solutions. Choosing products that leverage open standards allow for the same authenticator to work across various IAM solutions which dramatically reduces the deployment impact on end users. A user should be empowered to be productive on a new IAM system, or a non-federated access point, using the same authenticator within minutes not weeks.

In addition to solutions centering around identity, there are solutions focused on network access and virtualization that play an important role in setting up a Zero Trust architecture. An ideal strong authentication and modern MFA solution should also work with these types of solutions to help jumpstart a Zero Trust posture. Strong authentication with smart cards has been available for years on networks and FIDO based solutions are now coming to market. There is no "one size fits" in the area of Zero Trust. Regardless of where the organization begins the journey, a future-proofed strong authentication solution can be achieved and be implemented early. As mentioned earlier, some legacy systems might have limitations where strong MFA is not initially possible without additional efforts. A transitional architectural approach is to leverage a physical authenticator that can support legacy OTP MFA as well as your target state strong authentication approach. A user can leverage the same physical and portable authenticator minimizing deployment complexities and disruptions to the user.

4. Strong authentication for non-user accounts

Accounts that are used to run services are vulnerable to compromise. Just as discussed for user accounts, service accounts need to be heavily protected, monitored, and properly scoped as well. Too often these types of accounts have been protected with static passwords. Unfortunately a number of IT and OT systems have limitations on authentication options. It is common though that many of these systems can leverage asymmetric cryptographic authentication built into commonly used Public Key Infrastructure (PKI) environments. A cryptographic certificate based authentication provides strong authentication as there is no password that can be stolen. It is critical though that the private key material be stored in hardware to ensure it cannot be stolen. The industry best practice is to store private key material in hardware security modules (HSMs), dedicated security hardware that come in different sizes from large physical appliances to small USB devices. HSMs generate the private/public key pairs that are used for authentication, and the private key does not leave the HSM. Architecting an HSM system should be addressed early on as deployment models can be centralized or decentralized depending on the use cases. It is not uncommon for companies to have different HSMs to meet different scenarios.

5. Sign to prove that it is you over time

Strong authentication is critical to a Zero Trust approach but how do you know that an authenticated person did the work, and that that work can be attested to over time? In the physical world a person would sign a document with their signature to approve a contract or some other legal document. In the digital world, it has been possible for quite some time to digitally sign email and electronic documents. This has been a somewhat cumbersome process in the past, but now with personal authenticators and inexpensive HSMs, signing electronically has become much easier and stronger. Cryptographically based signing ceremonies, backed by hardware, ensures that content was in fact created by the signer. Signing processes are well defined but they are a process that needs to be integrated into the various content creation systems. Software development management systems are probably the most mature systems to allow for signing procedures and a really good place to start. For a company, the code that runs your business is critical and is highly targeted by adversaries. In this modern age, it is hard to find a company of any size that is not developing software at some level. Therefore this code needs to be protected by strong authentication and signing processes.

6. Implement risk-based authentication

The Zero Trust framework involves implementing real time risk-based access policies based on signals and risk scores. This framework should allow automated controls and decision makers ready access to application information, knowledge of where users are coming from, allowing for easy differentiation between types of accounts, and device fingerprints. A strong authentication solution that is hardware-based and highly trusted can elicit a high trust score, thus allowing for higher privileged access. Once verified, that highly vetted and verified user can conduct more sensitive transactions such as making a large dollar transfer as part of a financial transaction, or fulfilling a medical prescription, and many other such sensitive transactions. A trusted strong authentication approach allows for step-up authentication based on risk, thus protecting the user and the organization while increasing productivity.

7. Plan for a passwordless future

Over the past few years, the term “passwordless” has gained momentum and now it is used by many security, authentication, and identity solution providers—each with their own unique nuance. For clarity, it is best to use a broader definition.

At Yubico, we have adopted the following:

> “Passwordless authentication is any form of authentication that doesn’t require the user to provide a password at login.”

Achieving secure passwordless login across desktop and mobile and into a wide array of services requires a rich ecosystem and a consistent framework for authentication. Specifically, it takes a rich open standards ecosystem built to achieve security and usability, while also satisfying the need for portability, compatibility, and interoperability to scale to the masses. Since our inception, Yubico has advocated for open security standards to achieve these goals. Yubico paved the way by pioneering the WebAuthn and FIDO open standards, and worked with tech giants like Google, Microsoft, and Apple to integrate these standards into the operating systems, and browsers we use every day. These standards, paired with a YubiKey, allow for strong authentication across devices, apps, and services without any additional proprietary software. It just works.

Identity and access management (IAM) solutions (e.g. Azure Active Directory, Okta, Duo, Ping and many others) have also embraced open standards by layering on top of the platform giants to deliver the functionality and scale that enterprises need to adopt strong passwordless authentication for business critical applications and services.

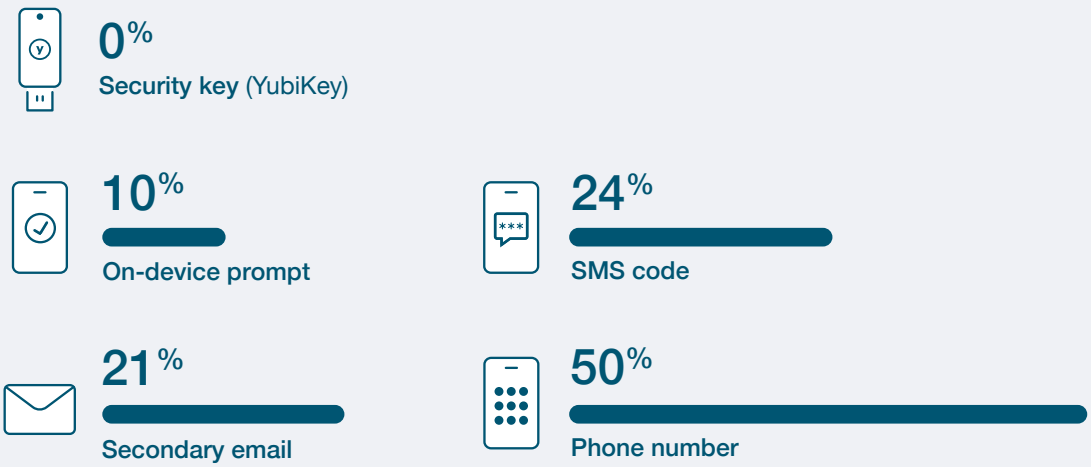
Organizations can embrace all the roads to passwordless by following a smart card passwordless, FIDO2/WebAuthn passwordless or a hybrid passwordless approach that uses the combination of smart card and FIDO2 passwordless, depending on their business scenarios and their internal infrastructure environment. Organizations that have a lot of legacy systems and on-premises infrastructure would be wise to pursue a smart card passwordless strategy, whereas cloud-first organizations can confidently explore FIDO2 passwordless. Or, in a third actionable scenario, organizations may choose to employ a dual approach. As an example, customers are opting to go with FIDO2/WebAuthn passwordless for computer login and federated web apps, while choosing a smartcard passwordless approach for secure on-prem network access (RDP, VPN, VDI). In this manner organizations can adopt a passwordless strategy to map to specific use cases, given their environments and user segments. Yubico can support Zero Trust initiatives and help organizations on their passwordless journey across all of these scenarios.

YubiKeys and the YubiHSM create a strong baseline of trust in a Zero Trust world

In the Zero Trust world that we now live in, especially during and after the Covid-19 health crisis where work-from-home and hybrid work policies have become the norm for many companies across many industries, CISOs need to figure out a way of enabling a Zero Trust architecture without hampering user productivity as they embrace remote work and cloud applications.

Yubico's phishing resistant hardware security solution—YubiKeys—supports the "Trust nothing, verify everything" Zero Trust approach with strong user identity and device authentication. YubiKeys are purpose-built for security and designed to stop phishing and other forms of account takeover in their tracks, delivering strong authentication at great scale.

Figure 4: Risk of account takeover with YubiKeys



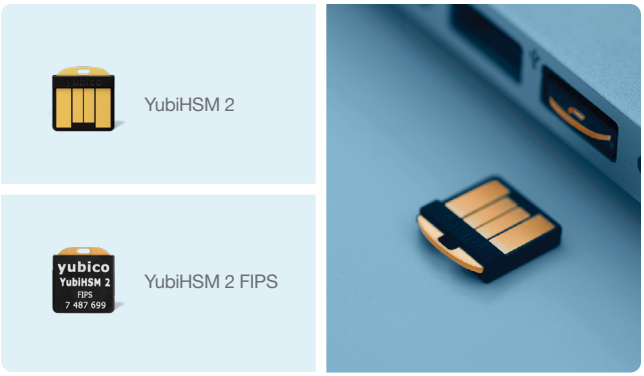
Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks. Source: Google Security Blog, How effective is basic account hygiene at preventing account takeovers.

Leveraging the modern FIDO2/WebAuthn authentication standards, YubiKeys work seamlessly across on-premises or cloud environments, do not rely on shared secrets between registered services, store no data and require no cellular connectivity. In other words, YubiKeys can work offline, anytime, anywhere providing always-on security for the user and their identity. And with a FIPS 140-2 validated lineup that meets the most stringent Authenticator Assurance Level 3 (AAL3) requirements, it delivers strong security with an intuitive user experience.

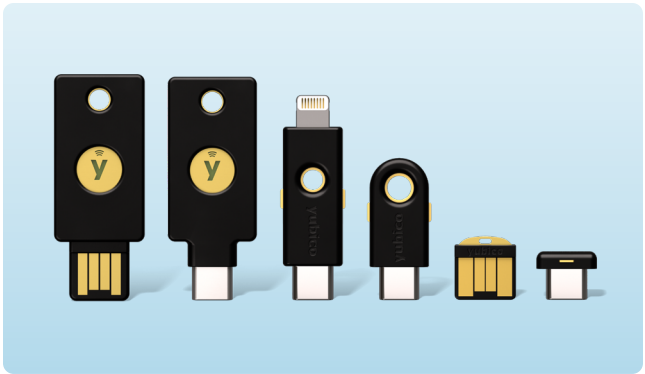
YubiKeys can be delivered to users easily, whether at corporate or residential addresses, ensuring the remote or hybrid workforce is secured efficiently. And with security keys that offer easy user self-registration, and integrate with your existing security infrastructure, identity and access management platforms, and hundreds of other services right out-of-the-box, user identities can be protected in just minutes. With YubiKeys an organization can experience strong security, a fast and easy user experience, and lower TCO.

The YubiHSM 2 is available as a FIPS 140-2 validated, Level 3 solution, or as a non-FIPS solution, both with the same capabilities. Both solutions ensure uncompromised cryptographic hardware security for applications, servers and computing devices at a fraction of the cost and size of traditional HSMs.

YubiHSM 2 can protect and be easily deployed to any:				
USB slot on servers	Databases	Robotic assembly lines	Applications	IoT devices in the field



YubiHSM 2 and YubiHSM 2 FIPS—The world's smallest HSM secures modern infrastructures other traditional HSMs with a bigger footprint simply can't.



The YubiKey 5 Series–from left to right: YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano and YubiKey 5C Nano.

Getting started on your modern MFA journey

There is no question that phishing-resistant MFA is the solution that's going to be required to adequately protect users as cyber threats evolve and become more sophisticated. Though the path to phishing-resistant MFA and passwordless can seem daunting, it doesn't have to be.

Don't know where to start?

Yubico's Professional Services team offers expert consulting services at every stage, from deployment planning and technical integration assistance to user training and support. Choose from the turnkey Deployment 360 Program for full end-to-end planning or individual workshops or engagements to supplement internal deployment activities.

Customer best practices—YubiKeys rollout at speed and scale

Plan

Ensure readiness and alignment ahead of execution

- Clarify goals, use cases / user groups
- Assemble project management / tech integration teams
- Engage Yubico experts as needed / Deployment 360

Validate

Confirm the process with a small group of users before broader rollout

- Select a few key workflows that can benefit from a raised bar for security to protect user identities and corporate data

Integrate

Ensure key apps and services are YubiKey-ready

- Ensure YubiKeys are integrated with the key applications and services you wish to secure

Launch

Cover all elements of YubiKey lifecycle management

- Determine YubiKey delivery and distribution
- Create policies for new users / lost and revoked keys
- Prepare user communications
- Go live! Kick off with a pilot

Adopt

Activate user training and support materials / processes

- Deliver user training and support materials
- Establish help desk support processes
- Educate on user self-service

Measure

Report on security and business value impact

- Track user activity and adoption
- Determine impact to helpdesk / reduced calls and cost savings
- Gauge how security as a differentiator may have driven additional revenue

Top misconceptions about Zero Trust

"Zero Trust is a product"

- Zero Trust is not a product, but rather a design approach and framework within which several solutions can play a role in working together to ensure access to sensitive data is limited based on need and risk scores.

"There is only one way to achieve Zero Trust"

- There are many roads to implementing a Zero Trust framework, and many specific initiatives may exist under the Zero Trust umbrella framework or architecture. Additionally, Zero Trust is a design approach so every project moving forward should be approached with that lens.
- However, a great way to jump start the Zero Trust journey is to ensure that all users accessing the network are strongly verified and that the authentication mechanism they use can be trusted.
- Remember! Despite all of the other controls that are put in place in support of Zero Trust, if the user accessing the network or data cannot be trusted, the whole model breaks down.

"Zero Trust is only for privileged users"

- In any organization that has data to protect from inside or outside threats, every user should be considered a privileged user, not just the few who are in important or visible roles.
- In today's hyper connected and agile corporations sensitive data can exist in many locations being accessed by many levels of the organization.
- Therefore an organization should verify every user, and not just those users who are considered "privileged" using a narrow definition.

"Zero Trust is only for large enterprises"

- Zero Trust is applicable for companies of all sizes.
- It is certainly relevant for larger organizations where different types of users are accessing different systems from anywhere, but this framework and design approach is not relegated to big companies only.
- In fact, Zero Trust may be even more relevant for SMBs given their cloud app heavy environments.

"Zero Trust is only for organizations in regulated or high risk industries"

- Zero Trust is not only meant for organizations that have specific compliance mandates to ensure data or network security.
- Any organization that has sensitive data or intellectual property to protect should consider adopting a Zero Trust model given the ever evolving threat landscape with greater risk vectors.

"Zero Trust will become less relevant as users go back to the office"

- It is safe to say that this is definitely not the case.
- As companies adopt a hybrid working model, Zero Trust will stay just as relevant as users will be working from anywhere into the foreseeable future.

Conclusion

Implementing a Zero Trust architecture can be a long and complex process. Deploy strong authentication upfront as a strong foundation when building out the Zero Trust strategy and as you're embarking on the journey. Strong authentication solutions have been tried and true for years and can heighten your security posture quickly and easily. Many of the deployment challenges of providing hardware backed security have dramatically improved with FIDO. Additionally Yubico has revolutionized and reinvigorated the use of smart cards with its easy to use technology. In this manner strong authentication can give you an early win as you roll out your broader Zero Trust initiative. While bringing the broader Zero Trust framework could take a while to fully bring to life, organizations can quickly establish trusted user authentication that are fundamental to a Zero Trust framework.

Focus on implementing modern MFA and not just "good enough" MFA, as the threat landscape is only becoming more sophisticated and considering a future-proofed solution is the appropriate architectural approach. With modern phishing-resistant MFA using hardware security keys, authenticator attestation builds trust that private key material is protected, and offers security against external malicious threats and also insider attacks.

Finally, marrying a strong authentication with ease of use for the user is a powerful combination. YubiKeys can deliver users a secure passwordless login experience, reducing user friction, fewer calls to the helpdesk and significant cost savings for the organization. In fact, based on interviews with 5 Yubico enterprise customers, Forrester created a composite organization and cited that YubiKeys had helped reduce risk by 99.9%, delivered ROI of 203%, and reduced support tickets by 75%. All in all, Zero Trust is no doubt a complex journey. Make it easier by thinking of strong authentication first and add the power of modern MFA and passwordless to your Zero Trust strategy shortlist.

Contact us yubi.co/contact

Learn more yubi.co/zero-trust

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.