



WHITE PAPER

Secure your AWS environment with highest-assurance phishing-resistant MFA

Stop account takeovers and go passwordless for a wide variety of AWS use cases



Contents

The critical need to protect AWS environments	3
Choosing the right MFA approach	4
What qualifies as phishing-resistant MFA?	5
Secure, easy authentication with AWS and the phishing-resistant YubiKey	6
Modern, phishing-resistant authentication and passwordless with the YubiKey	6
Protecting the software supply chain with the YubiHSM	6
AWS authentication scenarios supported by the YubiKey	7
AWS support for the YubiKey	7
AWS root users	8
AWS IAM	8
AWS IAM roles anywhere	8
YubiHSM 2 and AWS IoT Greengrass	9
Amazon Cognito	9
AWS SSO	9
AWS GovCloud	9
What is attestation and why does it matter?	9
Getting started is easy	10

36%



global CISOs in 2023 have started to **implement components of Zero Trust**¹

82%



of breaches involve **data stored in the cloud**³

62%



of organizations can partially attribute a **data breach to remote work**.⁴

74%



of data breaches can be traced back to the human element including situations such as **stolen credentials and phishing**.⁵

The critical need to protect AWS environments

Powering most modern work environments and digital capabilities of today are a mix of on-premise solutions alongside a suite of cloud, intelligence and emerging technologies—globally, 32% of cloud infrastructure services are provided by Amazon.¹

As organizations mature their digital capabilities leveraging Amazon Web Services (AWS) solutions to build and manage applications and workloads, it becomes increasingly important to adopt strong phishing-resistant multi-factor authentication (MFA) and security frameworks such as Zero Trust to better protect people, devices, applications and data in the workplace and along the supply chain.

Digital transformation and remote work have introduced new elements of risk, making traditional perimeter-based security models ineffective—82% of breaches involve data stored in the cloud² and Symantec identified that 77% of mobile apps contain valid AWS access tokens for logging into private AWS cloud services while another 47% contained AWS access tokens to data housed in Amazon S3 buckets, potentially leading to the exposure of sensitive data or, in the case of one supply chain vulnerability, the biometric digital fingerprints used across five mobile banking apps.³

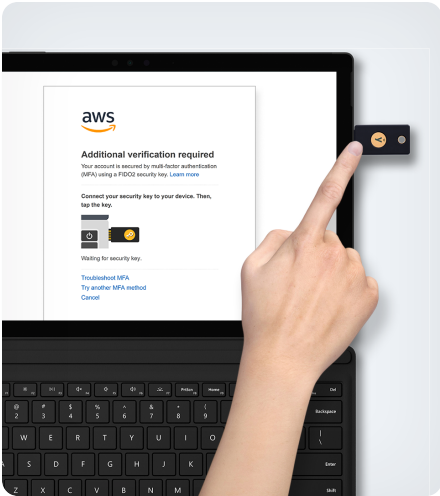
While the average data breach costs \$9.48M in the US and \$4.45M globally,⁴ cyber attacks can have severe and long-lasting consequences for organizations including damage to physical assets, customer trust and brand reputation, increased cyber insurance premiums, and potential loss of intellectual property.

When tracing these breaches, it is apparent that attacks against identity are pervasive; 74% of data breaches can be traced back to the human element including situations such as stolen credentials and phishing.⁵ Furthermore, 62% of organizations can partially attribute a data breach to remote work.⁶

Modern cyber attacks require modern security approaches to mitigate risk. In addition to architecting its cloud technology to high security standards, Amazon is taking a leadership position to help customers on the journey to MFA, Zero Trust and passwordless.⁷

A Zero Trust strategy reduces risk by assuming all users, devices, applications and transactions are potential threats that should be verified and authenticated before access is granted. For AWS environments, supporting the identity pillar of Zero Trust includes adopting strong phishing-resistant MFA in tandem with the enforcement of access control decisions by using an Identity and Access Management (IAM) tool such as AWS IAM, Ping Identity or Okta.

This whitepaper will outline key considerations when choosing authenticators and provide specific AWS use cases that can be supported by phishing-resistant MFA and passwordless authentication.



Choosing the right MFA approach

Identity is fundamental to strong cloud security and is the foundation of a strong Zero Trust strategy. The Zero Trust model involves having a strong level of trust in the authentication mechanisms of every user from every device attempting to access AWS resources, whether inside or outside the network perimeter. A critical part of building out Zero Trust access policies within AWS is understanding how users are establishing their identity and what level of trust can be attributed to that mechanism. In this step, it becomes apparent that while any form of MFA will offer better security than passwords, **not all MFA is created equal**.

Conventional MFA solutions including SMS, OTP, and push notifications are increasingly susceptible to account takeovers from phishing, attacker-in-the-middle and social engineering attacks at a penetration rate of 10-24%.⁸ Furthermore, security is just one reason that organizations are turning to MFA—they are also using it to support remote access (34%), support privileged access (26%), improve user convenience (24%), support Zero Trust initiatives (25%) and meet compliance requirements (21%).⁹ MFA and, more specifically, phishing-resistant MFA, is now a standard requirement for many global cybersecurity regulations and is a growing requirement for organizations to either qualify for cyber insurance or eliminate costly increases in premiums, sub-limits or exclusions.

Drivers for adoption of phishing-resistant MFA



For US federal agencies, the requirement to advance toward Zero Trust and use phishing-resistant MFA originates from the White House Executive Order 14028,¹⁰ Office of Management and Budget (OMB) Memo 22-09¹¹ and the National Security Memorandum/NSM-8.¹² However, there is global cross-sector pressure to adopt phishing-resistant MFA from NIS2¹³ in the EU as well as the global PCI DSS v4.0 standard for those organizations that handle payment card data,¹⁴ with additional regulators likely to follow suit.



What are passkeys?

Passkeys are a new term in the industry, but the concept is not new. Passkeys are a new name for FIDO2 passwordless-enabled credentials, a standard that is replacing passwords and phishable MFA logins with more secure passwordless experiences. There are different passkey implementations:

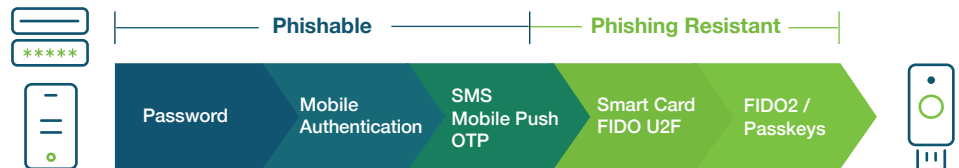
Synced passkeys live in the cloud, which means credentials on a smartphone, tablet or laptop can be shared between devices. While synced passkeys enable easier credential recovery in the case of a lost or stolen phone or laptop, the FIDO credential is harder to track, so it is suitable for lower security assurance scenarios.

Device-bound passkeys offer enterprises greater control of their FIDO credentials compared to synced passkeys. However, there are different types of device-bound passkeys—those that reside in general purpose devices such as smartphones, laptops and tablets, and those that reside in hardware security keys purpose built for strong security. Device-bound passkeys in modern FIDO security keys offer the highest security assurance and provide enterprises with trusted credential lifecycle management and attestation abilities. With this passkey approach enterprises can deliver the simplest user onboarding and credential recovery experience across devices and platforms, all while staying in compliance with the most stringent requirements across industries.

What qualifies as phishing-resistant MFA?

Phishing-resistant MFA refers to an authentication process that is immune to attackers intercepting or even tricking users into revealing access information. It requires each party to provide evidence of their identity, but also to communicate their intention to initiate through deliberate action.

According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, two forms of authentication currently meet the mark for phishing-resistant MFA: PIV/Smart Card and the modern FIDO2/WebAuthn authentication standard.



While PIV/Smart Card met the needs for traditional perimeter-based authentication requirements, the modernization of IT and growth of remote work requires an alternative high assurance authentication solution that can help organizations transition from passwords to passwordless and Zero Trust.

The future is passwordless

Given the inherent weaknesses associated with passwords, both from a security and from a usability perspective, a global best practice that has been adopted, is moving toward passwordless authentication—authentication that does not require the user to provide a password at login.

Going passwordless is a journey for most organizations, not necessarily an overnight change—first moving away from passwords and legacy forms of MFA, which are all highly vulnerable to phishing, and moving to a modern MFA approach which offers strong phishing-defense. Once there, an organization is well poised to move to passwordless and Zero Trust.

Modern authentication standards, including PIV/smart card and FIDO, enable strong two-factor, multi-factor, and passwordless authentication. FIDO2/WebAuthn is the most recent iteration of the FIDO standard, and uses public key cryptography for high security, where the private keys never leave the authenticator, enabling modern two-factor, multi-factor and even passwordless authentication.



Protecting the software supply chain with the YubiHSM

Increasingly sophisticated attacks are targeting software supply chains as an entry point to compromise financial systems and data, with 82% of CIOs stating their organizations are vulnerable to software supply chain attacks.¹⁸ For example, in 2021, developer auditing tool maker Codecov suffered a compromise of its Bash uploader script that could export information stored in user environments.¹⁹ Further, both the EO 14028²⁰ and the FDIC²¹ have indicated that agencies/organizations will be held accountable for third-party weaknesses.

Whether you use code that's been developed by internal teams or from external sources (e.g. third party developers, open-source frameworks, libraries), it is important to always deploy phishing-resistant MFA, the YubiKey, for code access and to implement trusted code-signing via the YubiKey 5 Series or a hardware security module such as YubiHSM 2.

Secure, easy authentication with AWS and the phishing-resistant YubiKey

Modern, phishing-resistant authentication and passwordless with the YubiKey

Yubico created the YubiKey, a hardware security key that supports phishing-resistant two-factor, MFA and passwordless authentication at scale with an optimized user experience for AWS environments.

The YubiKey is a multi-protocol key, supporting both PIV/Smart Card and FIDO2/WebAuthn standards along with OTP and OpenPGP, integrating seamlessly into both legacy and modern environments, helping organizations bridge to a passwordless future. For the highest level of security, the YubiKey 5 FIPS Series is FIPS 140-2 validated, FIDO Level 2 certified and DOD-approved,¹⁵ meeting the highest authenticator assurance level 3 (AAL3) requirements.

The versatile YubiKey requires no software installation, battery, or cellular connection, making it ideal for shared workstation and mobile-restricted environments, and offers a frictionless authentication workflow that is 4x faster than login with SMS. A single YubiKey conveniently works across multiple devices including desktops, laptops, mobile, tablets, and notebooks.

The YubiKey is proven to reduce risk of account takeovers by 99.9%¹⁶ while delivering a great user experience, letting users securely log in with a single tap or touch. The total economic impact of YubiKeys includes:¹⁷

The total economic impact of YubiKeys⁴¹:



Strongest Security

Reduce risk by

99.9%



High Return

Experience ROI of

203%



More Value

Reduce support tickets by

75%



Faster

Decrease time to authenticate by

>4x

The YubiKey can be used for simple, secure authentication to AWS accounts and the AWS console—via a root account, IAM, commercial or AWS GovCloud, a desktop or a supported mobile platform—as well as offering secure code signing to secure the software supply chain. In addition, AWS Single Sign On (SSO) support for WebAuthn allows the YubiKey to be used for high-assurance phishing-resistant security across multiple AWS accounts and applications.

YubiKeys work with over 1,000 products, services and applications including IAM platforms (e.g. AWS IAM) as well as privileged access management (PAM) solutions. With the improved support for device attestation, IAM policies can now also enforce

AWS support for the YubiKey

- ✓ AWS root users
- ✓ AWS IAM
- ✓ AWS IAM Roles Anywhere
- ✓ Amazon Cognito
- ✓ AWS SSO
- ✓ AWS GovCloud
- ✓ Attestable
FIPS 140-2 validated

the use of phishing-resistant or FIPS-certified devices such as the YubiKey FIPS Series to provide the highest level of security and compliance needs.

The YubiKey can be used for multiple credentials, giving users flexibility to secure all AWS accounts as well as personal accounts—all on the same key.

AWS authentication scenarios supported by the YubiKey

Adding MFA for your AWS IAM users, AWS root users and Amazon Cognito immediately enhances your security posture and follows modern security best practices to effectively counter modern cyber threats, helping meet you wherever you are on your journey to MFA, passwordless and Zero Trust.

YubiKey deployment to your AWS environment can be supported by identifying the highest priority use cases and user populations based on risk and business impact:

Top scenarios for phishing-resistant MFA



Privileged access

Targeted employees who have elevated access to systems or data.



Shared workstation

Employees who need access to shared computers and devices (e.g. customer facing environments and call centers).



Hybrid and remote work

Employees who require remote access to VPN, IAP, IAM, & IdP platforms.



Mobile-restricted

Sensitive environments where mobile devices are not allowed (e.g. call centers, manufacturing environments, server rooms).



High security

Federal and tightly regulated organizations who require a FIPS 140-2 validated solution.



Software supply chain

Access and data exchange associated with third party software and code.

User groups



Office workers

Office workers who can be targets of elaborate credential phishing schemes.



Third party

Third parties who need access to systems and data.



End customers

Customer accounts are susceptible attacks & fraud; build loyalty and trust.

Amazon best practices for root users:²²

When possible, use a hardware-based MFA device that does not rely on a battery to generate the one-time password (OTP) and enable at least two MFA devices so that you have a backup in case a device fails or is lost. Don't re-use a physical MFA device for any other purpose than protecting the root user credentials. Store the MFA device according to your information security policy, but not in the same place as the associated password for the root user.

“ Having strong authentication is a foundational security component of a Zero Trust architecture. Yubico and YubiKeys help fill the gap, for example, where weak passwords have been used, by providing validated, phishing-resistant security keys.”

John Kindervag | Creator of Zero Trust

AWS root users

An AWS root user is the single sign-in identity created with an AWS account who has complete or privileged access to all AWS services and resources. Like other privileged users who have elevated access to systems, software, data and infrastructure, root user credentials should be protected by MFA, and ideally hardware-based phishing-resistant MFA such as the YubiKey.

AWS IAM

AWS IAM best practice is to require all root and IAM users to sign into the AWS Management Console with MFA.²³ AWS and YubiKey bridge convenience with the ability to use a single YubiKey to access multiple IAM and root users across multiple AWS accounts, as well as any other application that supports U2F. AWS also supports enrolling a U2F credential on behalf of another user for organizations that need extra control over their AWS console credentials.

AWS IAM roles anywhere

YubiKey | YubiHSM 2

AWS IAM Roles allows the same IAM policies and IAM roles be used for AWS resources to extend to workloads running inside and outside AWS, including servers, containers and applications. Rather than storing cryptographic keys in software, which is highly vulnerable to a variety of attack vectors, keys can be stored in the YubiKey 5 Series, which supports public-key infrastructure (PKI) via PIV / Smart Card.

For developers, the YubiKey can be used with AWS long-term credentials to provide secure programmatic access to AWS for organizations that aren't yet ready or able to use identity federation.

For a production server, the same protection can be found with a hardware security module such as the YubiHSM 2.



YubiHSM 2 and AWS IoT Greengrass

The YubiHSM 2 / YubiHSM 2 FIPS is a game changing hardware solution for protecting data from being copied by attackers, malware, and malicious insiders, no matter where it lives. This includes advanced protection for CA root keys, database master keys, code signing, authentication/access tokens, manufacturing processes and component authenticity checks, IoT gateways or proxies such as AWS IoT Greengrass, file encryption, cryptocurrency exchanges, and more.

The YubiHSM 2 offers a higher level of security for cryptographic digital key generation, storage, management and cryptographic capabilities that include hashing, key wrapping and attestation, with full support for the PKCS#11 industry standard. This world-smallest HSM offers superior cost effective security and easy deployment, making it accessible for every organization.

AWS IoT Greengrass allows users to securely and locally run compute, messaging, data caching, sync, and machine learning inference capabilities for connected devices. The YubiHSM 2 can be used to perform the cryptographic operations for AWS IoT Greengrass to be able to securely store private keys.

Amazon Cognito

Amazon Cognito enables identity and access management for developers to create enterprise or consumer web and mobile applications, acting both as an OpenID Connect and identity provider (IdP). Amazon Cognito includes support for MFA and hardware-based phishing-resistant MFA such as the YubiKey.

Further, for developers looking to transition users away from passwords, the Yubico WebAuthn Starter Kit provides a turnkey passwordless reference architecture based on AWS.

AWS SSO

AWS Single Sign-On (SSO) allows organizations to easily assign and manage employee access to multiple AWS resources as well as other cloud services (e.g. Salesforce, Box, GitHub). By default, when a user signs in to the user portal, they sign in with their email address and password (the first factor). With the added integration of WebAuthn, AWS SSO enables you to secure user access to AWS accounts and business applications using MFA and FIDO-enabled security keys such as the YubiKey.

The YubiKey can be used with single sign-on providers and AWS SSO to provide a phishing-resistant passwordless login flow to the AWS ecosystem.

AWS GovCloud

AWS GovCloud provides cloud services across all classification levels to US Federal, Department of Defense, State and Local Governments. In June 2023, AWS IAM announced support for FIDO2 security keys in AWS GovCloud, allowing the use of the FIPS-validated YubiKey to provide the highest level of security and compliance. Additionally, AWS has improved support for device attestation in all regions, supporting IAM policies that can be used to enforce enrollment with FIPS-certified devices.

The YubiKey 5 Series, YubiKey 5 FIPS Series and YubiKey Bio Series provide the highest level of security for your AWS environments.



What is attestation and why does it matter?

Attestation enables validation that the authenticator hardware is from a trusted manufacturer and that the credentials generated on that device have not been cloned. Attestation is a critical piece of Zero Trust, since there is no implicit trust in an authenticator in a Zero Trust model.

There are two types of authenticators—platform authenticators and portable authenticators. Trusted platform authenticators (TPM) are built into modern devices such as laptops and smartphones and rely on a user-supplied biometric (face or fingerprint) as an authentication factor. Portable authenticators, such as hardware security keys, 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. Attestation can be provided by some TPMs, but it is also built into the FIDO standard and can additionally be provided by some hardware security key vendors, like Yubico, to support smart card deployments.

While platform authenticators are user friendly, they can introduce portability issues across devices and visibility challenges that make it difficult to receive valuable signals on how credentials are protected and pose a significant risk if the device is compromised. To bolster security, a TPM can be used in combination with a possession-based authenticator such as the YubiKey for high assurance and FIDO2 phishing-resistant authentication.

“ If your organization is still early in adopting MFA, the free security key is another way to help protect your AWS account credentials, as well as to jump start your MFA journey by showing how convenient modern security keys are to use. As you expand your AWS usage, all your users should obtain and enable MFA.”

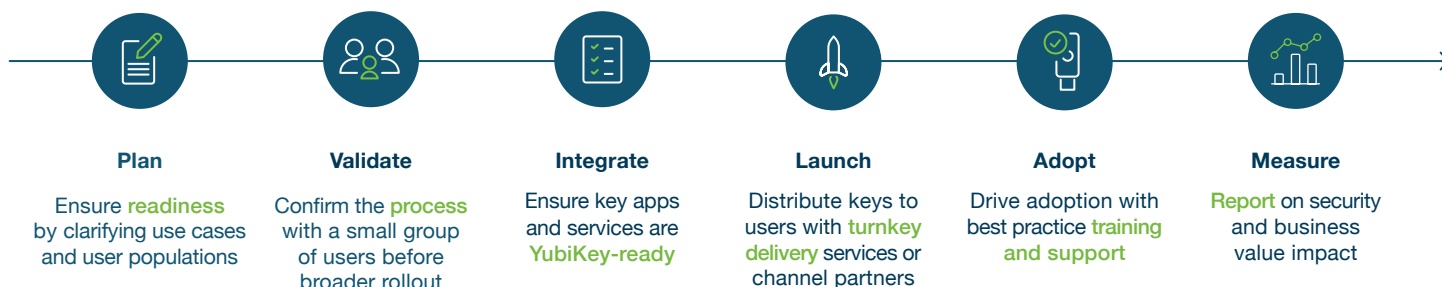
CJ Moses | CISO | AWS

Getting started is easy


The YubiKey provides public and private organizations with phishing-resistant, strong hardware-backed authentication that is ready to use with AWS and is simple to deploy across multiple applications as well as modern devices with single sign-on (SSO) capabilities for a smooth user experience when accessing apps and services.

In fact, AWS believes so strongly in MFA and the YubiKey that they have been giving away a free key—the YubiKey—to eligible AWS account owners in the US:²⁴

When you're ready to deploy the YubiKey at scale, we have made it easy to get started to with a simple 6 Step Best Practice Deployment Guide: [6 Step Best Practice Deployment Guide](#):



 **Contact us** yubi.co/contact

 **Learn more** yubi.co/partner-aws
yubi.co/wwwyk
yubi.co/yes

Yubico also offers YubiEnterprise Services, consisting of **YubiEnterprise Subscription** and **YubiEnterprise Delivery**, to help simplify procurement and distribution of YubiKeys. If you want a closer partnership on any of the six steps of this plan, [Yubico's Professional Services](#) team is here to help.



YubiEnterprise Subscription

With YubiEnterprise Subscription, organizations receive a service-based and affordable model for purchasing YubiKeys with benefits such as predictable spending, upgrades to the latest offerings, customer support and more.



YubiEnterprise Delivery

With YubiEnterprise Delivery, agencies experience turnkey authentication with shipping of YubiKeys, tracking, and returns processing of Yubico products handled seamlessly by logistics experts, so organizations can focus on what matters—securing the workforce.



Sources

- ¹ Synergy Research Group, [Cloud Provider Market Share Trend Q2 2023](#), (August 3, 2023)
- ² IBM, [2023 Cost of Data Breach Report](#), (July 24, 2023)
- ³ Kevin Watkins, [Mobile App Supply Chain Vulnerabilities Could Endanger Sensitive Business Information](#), (September 1, 2022)
- ⁴ IBM, [2023 Cost of Data Breach Report](#), (July 24, 2023)
- ⁵ Verizon, [2023 Data Breach Investigations Report](#), (June 6, 2023)
- ⁶ Fortinet, [2023 Work-from-Anywhere Global Study](#), (March 7, 2023)
- ⁷ Mark Ryland and Quint Van Deman, [Zero Trust Architectures: An AWS perspective](#), (November 23, 2020)
- ⁸ Kurt Thomas, Angelika Moscicki, [New research: How effective is basic account hygiene at preventing hijacking](#), (May 17, 2019)
- ⁹ S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
- ¹⁰ The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- ¹¹ OMB, [M-22-09](#), (January 26, 2022)
- ¹² The White House, [Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems](#), (January 19, 2020)
- ¹³ European Parliament, [The NIS2 Directive](#), (February 2023)
- ¹⁴ PCI, [PCI DSS: v4.0](#), (March 2022)
- ¹⁵ DOD OCIO, [Memo](#), (December 20, 2019)
- ¹⁶ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- ¹⁷ Forrester, [The Total Economic Impact of Yubico YubiKeys](#), (September 2022)
- ¹⁸ Venafi, [CIO Study: Software Build Pipelines Attack Surface Expanding](#), (June 2022)
- ¹⁹ Ax Sharma, [Hundreds of networks reportedly hacked in Codecov supply-chain attack](#), (April 20, 2021)
- ²⁰ The White House, [Executive Order on Improving the Nation's Cybersecurity](#), (May 12, 2021)
- ²¹ FDIC, [Third-party arrangements: elevating risk awareness](#), (2007)
- ²² AWS, [Securing the credentials for the root user](#), (Accessed October 5, 2023)
- ²³ AWS, [Multi-Factor Authentication \(MFA\) for IAM](#), (Accessed October 5, 2023)
- ²⁴ AWS, [Protect Yourself Online with a Free Multi-Factor Authentication Key](#), (Accessed October 5, 2023)



About Yubico

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, a hardware security key that is the gold standard in phishing-resistant multi-factor authentication (MFA). Yubico's solutions offer organizations and users deployment expertise and operational flexibility as YubiKeys work across hundreds of consumer and enterprise applications and services.

Yubico is a creator and core contributor to the FIDO2/passkey, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and is a pioneer in delivering modern, hardware-based passkey authentication security at scale to customers in over 160 countries.

For more information, please visit: www.yubico.com.