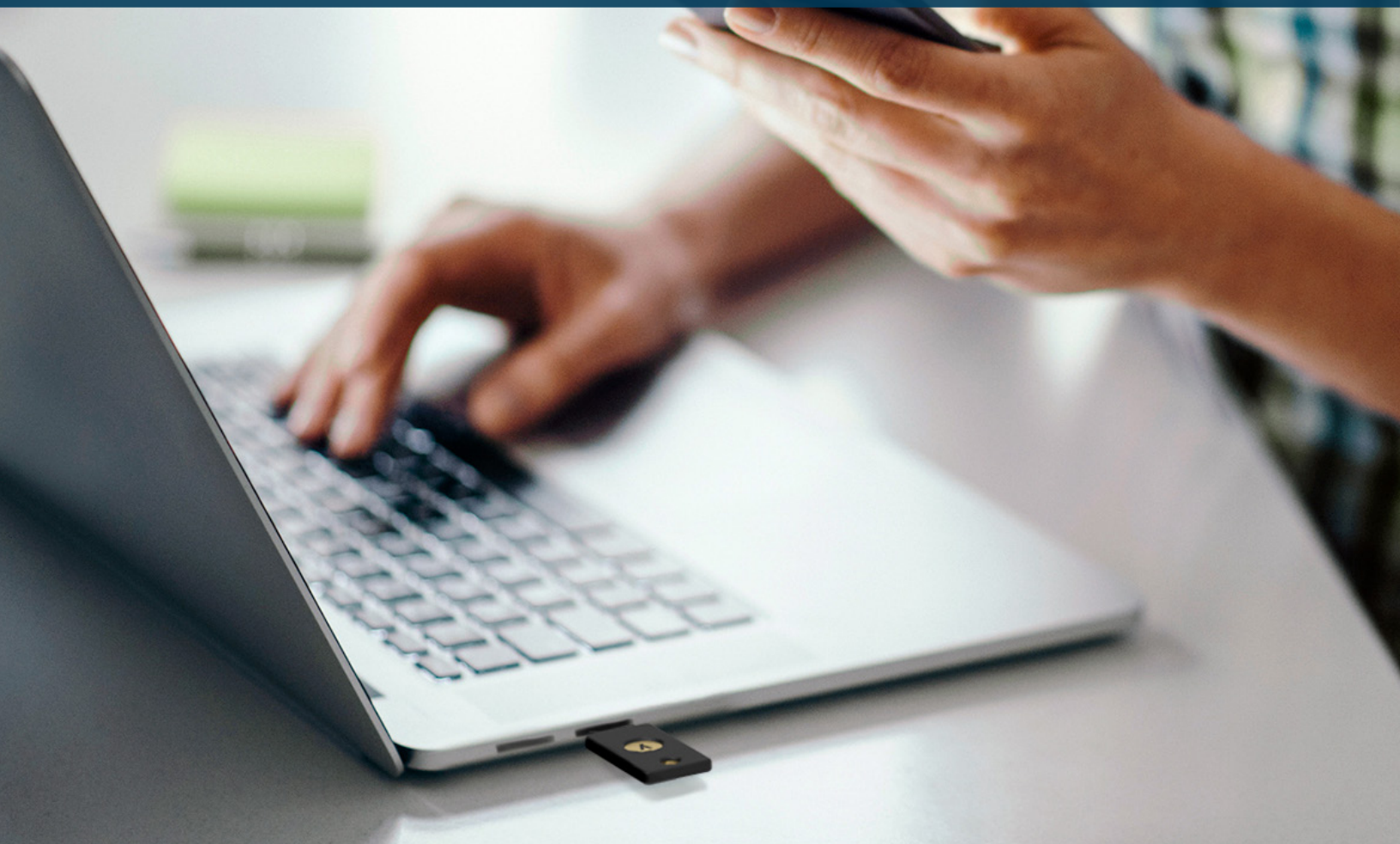
yubico

WHITE PAPER

Passwortlose Anmeldung im Zeitalter der Passkeys

Wichtige Überlegungen zum Lebenszyklusmanagement beim Aufbau einer sicheren, passwortlosen Strategie



Inhalt

Zusammenfassung

Wenn Sie in einem Raum voller Sicherheitsexperten das Wort „passwortlos“ sagen, werden Sie eine Reihe von Reaktionen hervorrufen. Das liegt daran, dass „passwortlos“ ein sich entwickelndes Konzept ist, das von verfügbaren Technologien, sich verändernden Cyberbedrohungen und unzähligen Anwendungsfällen beeinflusst wird. Der Zweck dieses Whitepapers ist es, den Hype um „passwortlos“ zu entmystifizieren und praktische Orientierungshilfen zu bieten, wie Unternehmen passwortlose Authentifizierungsoptionen im Zeitalter der Passkeys bewerten können. Das bedeutet, dass wir zunächst über Passwörter und Multi-Faktor-Authentifizierung (MFA) sprechen müssen. Mit einem soliden Verständnis der aktuellen Landschaft und der Risiken können wir uns dann darauf konzentrieren, aktuelle und zukünftige Probleme mit einer durchdachten passwortlosen Implementierung zu lösen.

74 %

der Datenschutzverletzungen sind auf menschliches Versagen zurückzuführen, z. B. Social-Engineering-Phishing-Angriffe, Missbrauch von Privilegien[1]

60 %

der Sicherheitsrisiken in Cloud-Umgebungen von Unternehmen sind auf schwache Passwörter oder geleakte Anmeldedaten zurückzuführen[2]

66 %

der Unternehmen haben, testen oder planen, innerhalb des nächsten Jahres passwortlose Authentifizierung einzuführen[3]

50 %

der Belegschaft werden bis 2025 passwortlos arbeiten[4]

Nicht alle Arten der MFA sind gleich

Passwörter bleiben die am häufigsten verwendete Form der Benutzerauthentifizierung, die von 91 % der Unternehmen verwendet wird.[5] Sie sind beliebt, weil sie eine universelle Authentifizierungsmethode darstellen, die sich für nahezu jede Anwendung eignet – portabel, kompatibel und interoperabel über verschiedene Geräte hinweg. Was Passwörter jedoch nie bieten konnten, ist eine angemessene Sicherheit.

Ein Passwort ist ein geteiltes Geheimnis. Das Geheimnis ist dem Benutzer und dem Validierungsdienst bekannt, wird oft auf verschiedenen Geräten gespeichert und kann sogar in Nachrichten oder auf einem Zettel weitergegeben werden. Wenn Unternehmen sich auf passwortbasierte Authentifizierung verlassen, sind sie anfällig für Angriffe, da Passwörter leicht gehackt, gestohlen oder einfach erraten werden können. Zudem fallen versteckte **Verwaltungs- und Supportkosten** verbunden für Passwörter und herkömmliche MFA an. Große Unternehmen geben schätzungsweise bis zu 1 Million US-Dollar pro Jahr für Personal und Infrastruktur aus, um Passwörter zurückzusetzen.[6] Die durchschnittlichen Kosten eines Datenverstoßes betragen weltweit 4,45 Millionen USD, wenn ein Passwort kompromittiert wird, und können je nach Größe der Organisation deutlich höher sein.[7] Berücksichtigt man darüber hinaus die Frustration der Benutzer im Zusammenhang mit Passwörtern und den schwer verständlichen Komplexitätsanforderungen, so wird schnell klar, welche Vorteile die Abschaffung von Passwörtern sowohl für die Benutzerfreundlichkeit als auch für die Kostensenkung mit sich bringt.

Obwohl jede Form von MFA eine bessere Sicherheit als ein Passwort allein bietet, **ist nicht jede MFA gleich**. Einfache oder veraltete Formen von MFA, wie SMS, mobile Authentifizierung, E-Mail-‚Magic Links' und Einmalpasswörter (OTP), können von böswilligen Akteuren leicht umgangen werden. Diese Methoden basieren auf geteilten Geheimnissen, die anfällig für Kontenübernahmen durch Phishing, Social Engineering und MITM-Angriffe (Man in the middle), mit einer Angriffsdurchdringungsrate von 10–24 % sind.[8]

66 % der Unternehmen geben an, dass sie im Zuge der Abkehr von problematischen Passwörtern und Phishing-anfälliger MFA eine **passwortlose Authentifizierung** testen, bereits eingeführt haben oder die Einführung planen.[9] Für die meisten Unternehmen ist der Weg zur Passwortlosigkeit eine Reise – der erste Schritt besteht oft darin, sich von veralteten Formen der MFA zu verabschieden und zu einer starken, Phishing-resistenten MFA mit dem FIDO2/WebAuthn-Standard zu wechseln. Sobald sie dort angelangt sind, sind Unternehmen bereit, passwortlose FIDO2-Zugangsdaten zu nutzen, die jetzt als Passkeys bezeichnet werden, um ihren Weg zur **Passwortlosigkeit** abzuschließen.

Heutzutage konzentrieren sich viele Passkey-Implementierungen auf die User Experience der Authentifizierung. Leider wird dabei der wichtige Bereich des **Konto-Lebenszyklus-managements**, einschließlich der Geräteregistrierung und des Account-Bootstrappings, einfach übersprungen. Viele Anbieter verwenden auch Passwörter und herkömmliche MFA, wodurch Angriffspunkte entstehen, die die beabsichtigte Sicherheit von Phishing-resistenten MFA-Lösungen umgehen und **Zero Trust untergraben**, das auf die ausschließliche Verwendung von Phishing-resistenten MFA zusteuert.[10]

Um einen sicheren Übergang zur Passwortlosigkeit zu gewährleisten, werden in diesem Whitepaper **wichtige Implementierungsfaktoren erläutert, die auf dem Weg zur Passwortlosigkeit mithilfe von Passkeys zu berücksichtigen sind**, um eine starke Sicherheit über den gesamten Authentifizierungszyklus hinweg zu gewährleisten.

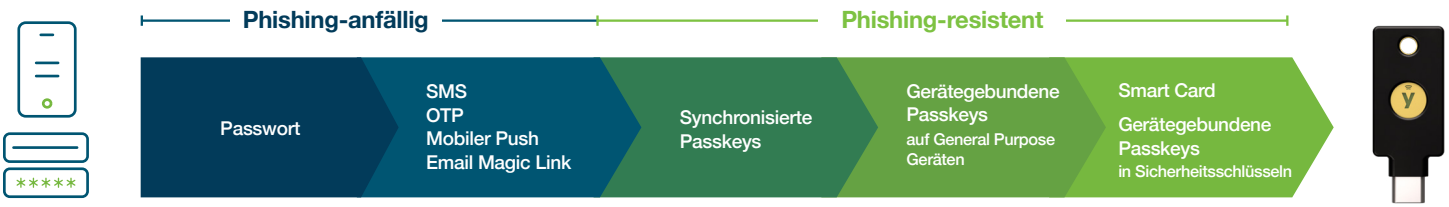
Was ist die passwortlose Authentifizierung?

„Passwortlos“ ist jede Implementierung einer Authentifizierung, bei der der Benutzer **während des gesamten Authentifizierungszyklus kein Passwort erstellen und/oder angeben muss**, einschließlich:

Herkömmlicher passwortloser Lebenszyklus	Moderner passwortloser Lebenszyklus				
Benutzeranmeldung	Onboarding/ Registrierung	Erste Anmeldung	Verbund und Single Sign-on	Kontowiederherstellung	Authentifizierung bei älteren Systemen

In den letzten Jahren hat sich immer mehr der Begriff „passwortlos“ hervorgetan. Inzwischen wird er von vielen Anbietern von Sicherheits-, Authentifizierungs- und Identitätslösungen verwendet. Wie bei anderen Schlagworten in der Branche ist der Begriff „passwortlos“ nicht eindeutig definiert, was zu einem Ökosystem führt, in dem **nicht alle passwortlosen Implementierungen den Schutz und die Benutzerfreundlichkeit bieten, die der Begriff verspricht**.

Viele Beispiele für passwortlose Verfahren beruhen auf der veralteten Definition von „passwortlos“: jede Form der Authentifizierung, bei der ein Benutzer bei der Anmeldung kein Passwort eingeben muss. Diese Definition führt dazu, dass viele ältere MFA-Lösungen wie **SMS**-Verifizierung und **Magic Links per E-Mail** als „passwortlos“ gelten, auch wenn diese Lösungen sowohl veraltet als auch sehr anfällig für Kontoübernahmen sind. Darüber hinaus lässt diese veraltete Definition eines passwortlosen Systems etwas vermissen, um sicherzustellen, dass **Phishing-resistente Authentifizierungsimplementierungen** bei der Geräteregistrierung, dem Bootstrapping von Konten oder der Authentifizierung bei älteren lokalen Systemen **nicht auf Passwörter oder herkömmliche MFA zurückgreifen**. Außerdem muss eine sichere passwortlose Lösung weiterhin mehrere Authentifizierungsfaktoren bieten, um den Zugriff zu schützen, wenn ein Gerät gestohlen wird, wie z. B. eine PIN oder einen biometrischen Faktor.



25 %

der MFA-Transaktionen, die ein Token verwenden, basieren auf der FIDO-Authentifizierung[11]

Die passwortlose Authentifizierung mit **Smartcards oder FIDO2** (FIDO2-Zugangsdaten werden jetzt durch **Passkeys** dargestellt) verändert die Art und Weise, wie Authentifizierungsfaktoren verarbeitet werden, grundlegend. Bei einem passwortlosen Modell verlagert sich die Validierung des ersten und zweiten Faktors ausschließlich auf den Authentifikator. Der erste Faktor ist in der Regel der physische Besitz des Authentifikators selbst und der zweite Faktor ist die PIN oder eine biometrische Validierung, um den Authentifikator zu entsperren und den kryptografischen Vorgang auszuführen.

Da diese „eigentliche“ Definition der passwortlosen Authentifizierung einen Großteil des Authentifizierungsprozesses an den Authentifikator verlagert, ist es von entscheidender Bedeutung, sicherzustellen, dass der private Schlüssel gesichert ist, damit er nicht gestohlen oder geklont werden kann. Ebenso wichtig ist es zu wissen, dass der Faktor tatsächlich in allen Authentifizierungsszenarien verwendet wird.

Bevor wir die Überlegungen zur Umsetzung eines modernen, starken passwortlosen Systems im Detail erläutern, sollten wir einen Schritt zurücktreten und **Phishing-Resistenzen und Passkeys**, die die Grundlage für die heutigen passwortlosen Implementierungen bilden, besser definieren.

Was ist Phishing-resistente MFA?

Als Reaktion auf Risiken und regulatorische Anforderungen setzen Unternehmen **Phishing-resistente MFA** in Form von **Smartcards (PIV/CAC)** und dem modernen **FIDO2/WebAuthn** ein.

NIST definiert Phishing-Resistenz in Special Publication (SP) 800-63 und Draft 800-63-4[12] als „die Fähigkeit des Authentifizierungsprotokolls, die Offenlegung von Authentifizierungsgeheimnissen und gültigen Authentifikatorausgaben gegenüber einer betrügerischen Partei zu erkennen und zu verhindern, ohne auf die Wachsamkeit des Abonnenten angewiesen zu sein“. Phishing-resistente MFA-Prozesse basieren auf einer kryptografischen Überprüfung zwischen Geräten oder zwischen dem Gerät und einer Domäne, wodurch sie ideal gegen Versuche geschützt sind, den Authentifizierungsprozess zu gefährden oder zu untergraben.

Smartcards (PIV/CAC) sind eine der effektivsten Methoden zum Schutz vor Phishing. Der Benutzer muss seine Smartcard in ein Lesegerät einführen und die Smartcard mit einer eindeutigen PIN validieren. Eine PIN bleibt lokal auf dem Gerät, wird nie übertragen und muss nie geändert werden, wodurch sie sicherer als Passwörter ist. In Fällen, in denen Smartcards aufgrund von Kosten, Zugriff auf Cloud-Dienste, mobilen Geräten, abgeschotteten/isolierten Netzwerken keine praktische Lösung darstellen oder von Auftragnehmern, Partnern oder anderen Dritten genutzt werden müssten, setzen Unternehmen auf FIDO2 und moderne passwortlose Anmeldeprozesse.

Der Authentifizierungsstandard **FIDO2/WebAuthn** wurde entwickelt, um moderne cloudbasierte Umgebungen skalierbar zu unterstützen. FIDO2/WebAuthn ist die neueste Version des FIDO-Standards, der Geräte zur einfachen Authentifizierung bei Online-Diensten nutzt. Bei der FIDO-Authentifizierung melden sich Benutzer mit Phishing-resistenten Zugangsdaten an, sogenannten **Passkeys**, und werden zusätzlich durch biometrische Daten oder eine eindeutige PIN verifiziert.

Passkey

ist eine neue Bezeichnung für **passwortlose FIDO2-Zugangsdaten**

Was sind Passkeys?

Passkeys sind ein neuer Begriff in der Branche, aber das Konzept ist nicht neu. Passkeys sind ein neuer Name für **FIDO2-Zugangsdaten ohne Passwort**. Dieser Standard ersetzt Passwörter und Phishing-anfällige MFA-Anmeldungen durch sicherere passwortlose Verfahren. Es gibt verschiedene Passkey-Implementierungen:

Synchronisierte Passkeys befinden sich in der Cloud, sodass Zugangsdaten auf einem Smartphone, Tablet oder Laptop zwischen Geräten geteilt werden können. Während synchronisierte Passkeys die Wiederherstellung von Zugangsdaten im Falle eines verlorenen oder gestohlenen Telefons oder Laptops erleichtern, sind FIDO-Zugangsdaten schwieriger nachzuverfolgen und eignen sich daher für Szenarien mit geringerer Sicherheitsgewährleistung.

Gerätegebundene Passkeys bieten Unternehmen im Vergleich zu synchronisierten Passkeys eine bessere Kontrolle über ihre FIDO-Zugangsdaten. Es gibt jedoch verschiedene Arten von gerätegebundenen Passkeys – solche, die sich in Allzweckgeräten wie Smartphones, Laptops und Tablets befinden, und solche, die sich in Hardware-Sicherheitsschlüsseln befinden, die speziell für hohe Sicherheit entwickelt wurden. Gerätegebundene Passkeys mit Sicherheitsschlüsseln bieten die höchste Sicherheitsgarantie und stellen Unternehmen bewährte Fähigkeiten zum Lebenszyklusmanagement von Zugangsdaten und zur Bescheinigung bereit. Mit diesem Passkey-Ansatz können Unternehmen die einfachste Benutzererfahrung beim Onboarding und bei der Wiederherstellung von Zugangsdaten auf allen Geräten und Plattformen bieten und dabei die strengsten Anforderungen in allen Branchen erfüllen.

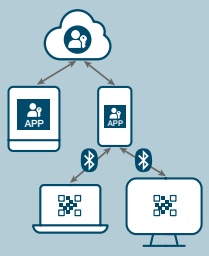
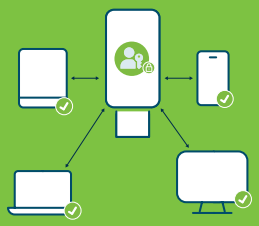
Welcher Passkey-Ansatz ist der richtige für Sie?

FIDO-Standards und **Passkeys** wurden von allen führenden Plattformen für Identitäts- und Zugriffsverwaltung (IAM), Lösungen für Identitätsanbieter (IDP) und Lösungen für die Verwaltung privilegierter Zugriffe (PAM) übernommen, um die Unterstützung von passwortlosen FIDO2-Erfahrungen in großem Maßstab für geschäftskritische Anwendungen und Dienste zu ermöglichen.

Synchronisierbare Passkeys sind großartige Lösungen für viele Verbraucher mit geringem Risiko und risikoarme Anwendungen. Da sie als weniger sicher gelten, sind sie jedoch im Allgemeinen nicht für Personen mit hohem Risiko oder Unternehmen geeignet. Sie erschweren die folgenden Aufgaben:

- **Prüfen** und Belegen, wie Passkeys synchronisiert oder geteilt werden, und Ermitteln, welche Kopie verwendet wird.
- Verwalten des **Lebenszyklus** des Passkeys, nachdem er erstellt wurde, da geklonte Passkeys, die gemeinsam genutzt werden, nicht vom Original zu unterscheiden sind.
- **Unterstützen** von Benutzern, die sich nicht mit ihrem Passkey anmelden können oder Hilfe bei der Wiederherstellung benötigen.
- Abdecken aller **Anwendungsfälle**, da synchronisierbare Passkeys auf mobile Konnektivität angewiesen sind, was sie für Umgebungen mit eingeschränkter Mobilität, luftleere oder isolierte Netzwerke und gemeinsam genutzte Arbeitsplatzgeräte ungeeignet macht. Außerdem unterstützen nicht alle Computer und Telefone Passkeys.

Gerätgebundene Passkeys werden nicht synchronisiert oder auf andere Geräte kopiert. In einem Szenario mit synchronisierten Passkeys, bei dem Passkeys zwischen mehreren Geräten verschoben werden können, könnte der Faktor, der zum Entsperren des Authentifikators verwendet wird, von einem anderen Benutzer stammen, da nicht alle Faktoren mit dem Passkey übertragen werden. Bei einem gerätegebundenen Passkey besteht eine höhere Sicherheit, dass der Benutzer, der das Gerät steuert, der Benutzer ist, der den Passkey verwenden soll, wodurch das Risiko eliminiert wird, dass der zum Entsperren des Authentifikators verwendete Faktor von einem anderen Benutzer stammt. Ein gerätegebundener Passkey bietet eine höhere Sicherheit, da der Passkey auf FIDO2-Sicherheitsschlüsseln basiert oder auf einer Plattform erstellt und in einem Trusted Platform Module (TPM) gespeichert wird, was der Funktionsweise von Windows Hello entspricht. Gerätegebundene Passkeys bieten die besten Kontrollen auf Unternehmensebene, die Unternehmen benötigen, um den Lebenszyklus eines Passkeys ordnungsgemäß zu verwalten und zu sichern. Dabei wird die Public-Key-Kryptografie für hohe Sicherheit genutzt, bei der die privaten Schlüssel den Authentifikator niemals verlassen.

Anforderung	Synchronisierte Passkeys	Gerätegebundene Passkeys auf Allzweckgeräten	Gerätegebundene Passkeys in Hardware-Sicherheitsschlüsseln
			
Zwischen Geräten synchronisiert/ gemeinsam nutzbar	Nicht verwaltete Synchronisierung	Verwaltete Synchronisierung	Keine Synchronisierung zwischen Geräten
Funktioniert über Apple/ Google/Microsoft	Funktioniert möglicherweise nicht	Funktioniert auf allen Plattformen	Funktioniert auf allen Plattformen
Benutzerregistrierung/ Onboarding	Schwach; wird durch Passwort unterstützt	Schwach; App durch Passwort unterstützt	Am sichersten bei Verwendung mit Yubico FIDO Pre-Reg, da die Benutzerregistrierung dann nicht passwortabhängig ist
Wiederherstellung der Zugangsdaten	Einfache Wiederherstellung	Zeit für den Austausch des Telefons und teuer	Am schnellsten mit einem Backup-Schlüssel
Compliance und Audit	Sicherheitsstufe 2 der NIST-Empfehlungen zur Authentifizierung (AAL2) Keine Bestätigung; unsicher, ob Benutzer den Passkey kontrolliert	Sicherheitsstufe 2 der NIST-Empfehlungen zur Authentifizierung (AAL2) Unterstützt Softwarebescheinigungen	Sicherheitsstufe 3 der NIST-Empfehlungen zur Authentifizierung (AAL3) Unterstützt Hardwarebescheinigungen
Risiko/Kosten	Gilt als „kostenlos“; hohe IT-/ Helpdesk-Kosten und ein höheres Risiko sind kostspielig	Gilt als billiger als HW, aber Lücken bei der Risikoexposition können langfristig kostspielig sein	Gilt als teurer im Voraus, ist aber aufgrund des geringeren Risikos von Verstößen und des geringeren IT-Aufwands kostengünstiger
Funktioniert auch außerhalb von Unternehmensszenarien	Nicht auf gemeinsam genutzten Arbeitsplatzgeräten mit Einschränkungen für Mobilgeräte	Nicht auf gemeinsam genutzten Arbeitsplatzgeräten mit Einschränkungen für Mobilgeräte	Funktioniert über alle Unternehmensszenarien hinweg

> Wenn Sie auf passwortlose Systeme umsteigen, vermeiden Sie, dass Benutzer ihr Passwort vergessen. Sie müssen sich keine Sorgen machen, dass sie sich aussperren, Passwörter auf einen Zettel schreiben oder Opfer eines Phishing-Angriffs werden. Sie entfernen also den menschlichen Faktor."
>
> **Jason Rucker** | Director of IT | City of Southgate, MI

So wählen Sie die richtige passwortlose Strategie für Ihr Unternehmen

Jedes Unternehmen befindet sich an einer anderen Stelle auf dem Weg zur Passwortlosigkeit. Aber jede noch so kleine Maßnahme, die auf eine Abkehr von Passwörtern abzielt, wird die Sicherheit verbessern, denn wir wissen, dass eine passwortbasierte Umgebung immer anfälliger für Phishing-Angriffe und weniger sicher ist.

Es gibt zwei Fragen, die Sie sich stellen sollten, um zu bestimmen, wie Sie Ihre Reise zur Passwortlosigkeit planen:

- **Arbeiten Sie in einer Cloud-, On-Premise- oder Hybrid-Umgebung?** Es mag beruhigend sein zu wissen, dass Sie unabhängig von der Art Ihrer technischen Umgebung heute eine oder mehrere sichere passwortlose Optionen nutzen können.
- **Wie priorisieren Sie Sicherheitsstufen, User Experience und Compliance-Kosten?** Diese Elemente stehen manchmal im Widerspruch zueinander, daher ist es wichtig zu wissen, wie Sie die Kompromisse aushandeln, wenn Sie schwierige Entscheidungen treffen müssen.

Diese Fragen helfen Ihnen, den besten Weg zu finden, um von der herkömmlichen MFA zu passwortlosen Smartcards, Passkeys oder einem hybriden Ansatz zu wechseln. Darüber hinaus hilft Ihnen die Frage bei der Bewertung von Passkey- und Authentifizierungsoptionen, die Ihrem Sicherheitsbedürfnis entsprechen, und bei der Erstellung einer Implementierungsstrategie, die zu Ihrem Risikoprofil passt.

Smartcard

Wenn Sie in einer lokalen Active Directory (AD)-Umgebung arbeiten oder veraltete lokale Systeme verwenden, ist eine passwortlose Smartcard-Implementierung wahrscheinlich die beste Wahl. Denken Sie an die Vorteile hardwarebasierter Sicherheitsschlüssel, die Smartcard-Lesegeräte überflüssig machen.

Passkey

Wenn Sie bereits auf eine Cloud-First-Umgebung wie Microsoft Entra ID umgestiegen sind, können Sie Passkeys einfach implementieren, um Office 365 und andere verbundene Unternehmensanwendungen zu nutzen.

Hybrid

In einer hybriden Umgebung ist es möglich, sowohl eine Smartcard-Lösung als auch einen Passkey zu implementieren, je nach geschäftlichem Anwendungsfall.

Welcher Passkey-Authentifikator ist der richtige für Sie?

Passkeys sind eine attraktive Option, um die Benutzerauthentifizierung in modernen Arbeitsumgebungen zu sichern und zu vereinfachen. Passkeys erschweren die Ausnutzung von Zugangsdaten und machen unbefugten Zugriff dank der Verwendung von Public-Key-Kryptografie deutlich unwahrscheinlicher. Sie werden in den Ökosystemen von Apple, Microsoft und Google immer häufiger eingesetzt.

Während in der Passkey-Definition angegeben ist, dass anstelle von Passwörtern kryptografische Schlüssel für die Anmeldung verwendet werden, gibt es erhebliche Unterschiede zwischen synchronisierten Passkeys und gerätegebundenen Passkeys – und darüber hinaus zwischen gerätegebundenen Passkeys auf Allzweckgeräten, wie z. B. solchen, die auf einer Windows-Plattform erstellt und in einem Trusted Platform Module (TPM) unter Verwendung von Windows Hello gespeichert wurden, und solchen auf zweckgebundenen Sicherheitsschlüsseln wie dem YubiKey.

Die Wahl des Authentifikators bestimmt, wie gut Sie den Passkey kontrollieren können:

- **Sicherheitsschlüssel** erstellen Passkeys auf dedizierten portablen Authentifikatoren, so dass Sie Ihren Passkey von Arbeitsplatz zu Arbeitsplatz und auf Ihre mobilen Geräte mitnehmen können, um sich nahtlos auf jeder Plattform anzumelden. Sicherheitsschlüssel bieten die größte Sicherheit, dass die privaten Schlüssel erstellt werden und immer auf dem Authentifikator verbleiben, auf dem sie erstellt wurden. Sicherheitsschlüssel, die sowohl FIDO2 als auch Smartcard unterstützen, bilden eine wichtige Brücke zu passwortlosen Umgebungen und unterstützen sowohl ältere als auch moderne Umgebungen.
- **Plattform-Authentifikatoren** werden von sicheren Enklaven unterstützt, die in die Geräte integriert sind, die Sie bereits zur Produktivitätssteigerung verwenden, und häufig mit den auf dem Gerät verfügbaren biometrischen Sensoren verwendet werden. Die Passkeys, die Sie auf der Plattform erstellen, können je nach verwendeter Plattform synchronisierbar oder gerätegebunden sein.
- **Drittanbieter von Passkeys** sind Software-Authentifikator-Apps und Passwortmanager, die Passkeys erstellen und in den vom Drittanbieter verwalteten Tresoren speichern können. Die meisten Drittanbieter von Passkeys nutzen synchronisierbare Passkeys, aber neue Optionen werden auch in der Lage sein, gerätegebundene Passkeys zu speichern.

Der Authentifikator muss sicherstellen, dass die von ihm ausgeführten Prozesse sicher sind und Schlüsselmaterial nicht vom Gerät kopiert werden kann. Ansonsten könnte ein geklonter Authentifikator entwickelt und zur Authentifizierung verwendet werden.

Darüber hinaus klassifizieren **Authentifizierungs-Sicherheitsstufen (AALs)** die Stärke von Authentifikatoren. Ein Authentifikator mit AAL1 (z. B. ein Passwort) bietet nur geringes Vertrauen. Ein Authentifikator mit AAL3 bietet hingegen ein sehr hohes Vertrauen, da die anmeldende Person durch Besitz nachweisen kann, dass sie ist, wer sie vorgibt zu sein. Dadurch sinkt die Gefahr von Kompromittierungen und Angriffen durch Phishing.

Um die Sicherheitseigenschaften eines Authentifikators zu verstehen, sollten sich vertrauende Parteien die Gerätebescheinigungserklärungen ansehen. Die **Bescheinigung** ermöglicht es jeder vertrauenden Partei, eine kryptografisch verifizierte Vertrauenskette des Geräteherstellers zu verwenden, sodass Zugriffsentscheidungen auf der Grundlage eines Risikoprofils getroffen werden können. Die Informationen zu den Bescheinigungen sollten erfasst werden, damit aktuelle und zukünftige Entscheidungen getroffen werden können, bis hin zur Sperrung, falls Probleme auftreten. Die Bescheinigungsschlüssel werden bei der Herstellung festgelegt und können nicht geändert oder exportiert werden. **Nur gerätegebundene Passkeys bieten Bescheinigungsfunktionen für Unternehmen**.

	Synchronisiert (mehr auf Benutzerfreundlichkeit ausgerichtet; weniger Sicherheit)	**Geräte-/hardwaregebunden** (höhere Sicherheitsgarantie; nicht alle sind gleichwertig)	
Plattform	iOS OS X android	Windows Hello	**Sicherheits-schlüssel**
Anwendungen von Drittanbietern	DASHLANE 1Password	Microsoft Authenticator	YubiKey

> Der einzige effektive Ansatz, um Phishing aus der Bedrohungslandschaft eines Unternehmens zu entfernen, besteht darin, sicherzustellen, dass jeder Benutzer und jeder Prozess innerhalb des Unternehmens Phishing-resistent wird.“
>
> **Derek Hanson** | VP Solutions Architecture and Alliances | Yubico

So machen Sie Ihre Benutzer Phishing-resistent

Überlegungen zum Konto-Lebenszyklusmanagement

Bei allen passwortlosen Lösungen müssen Unternehmen eine Beziehung herstellen, die die Smartcard oder den Passkey registriert, um sicherzustellen, dass der Benutzer derjenige ist, für den er sich ausgibt. Die meisten Organisationen stellen Smartcard-Beziehungen persönlich her, aber dies ist bei Passkeys, die in der Regel auf Selbstbedienungsregistrierung basieren, schwieriger. Viele Implementierungen greifen in dieser Phase des Authentifizierungslebenszyklus auf Passwörter oder veraltete MFA zurück, was die Bemühungen um Zero Trust untergräbt.

Sichere passwortlose Implementierungen berücksichtigen den gesamten Authentifizierungslebenszyklus und nicht nur die **Phishing-resistente Authentifizierung**, sondern auch **Phishing-resistente Benutzer**. Diese Verlagerung beinhaltet eine umfassendere Berücksichtigung einer starken Authentifizierung, die mit dem Benutzer mitwandert und Lücken im Zusammenhang mit dem Onboarding, dem Bootstrapping, der ersten Anmeldung oder der Authentifizierung bei Altsystemen schließt.

Onboarding Passkey-Drittanbieter; gerätegebundene Passkeys auf Allzweckgeräten

Ein Tag im Leben eines neuen Mitarbeiters, dessen Onboarding mithilfe von gerätegebundenen Passkeys erfolgt, die sich in einem Allzweckgerät wie einem Smartphone befinden.

1. Der Mitarbeiter verwendet eine PIN oder biometrische Daten, um sich am mobilen Gerät anzumelden.

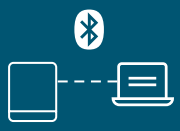
2. Der Mitarbeiter installiert und konfiguriert die Authentifikator-App als Passkey-Anbieter.

3. Der Mitarbeiter meldet sich mit seinem Phishing-anfälligen Geheimcode an.

Schwachstelle! Phishing-Resistenz unterbrochen

4. Der Mitarbeiter schließt das Verfahren ab und registriert einen von über die App verwalteten Passkey. Der Passkey kann für die Anmeldung bei Apps auf demselben mobilen Gerät verwendet werden.

5. Um den Passkey an anderen Arbeitsplätzen zu verwenden, muss der Mitarbeiter einen QR-Code mit der Kamera scannen und das Telefon mit Bluetooth verbinden, ein Anmeldeverfahren durchführen und das Telefon optional mit dem Arbeitsplatz verknüpfen.*



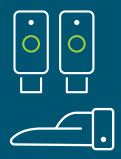
6. Der Mitarbeiter kann sich nun mit dem Passkey auf dem Mobilgerät bei jedem seiner anderen Geräte anmelden.

7. Der Mitarbeiter kann einen gerätegebundenen Passkey zur Optimierung der Anmeldung direkt über den Arbeitsplatz registrieren.*

*sofern dies vom Gerät und Anwendungsfall unterstützt wird

Onboarding Sicherheitsschlüssel; gerätegebundene Passkeys auf Authentifikatoren, die für Sicherheit entwickelt wurden

Ein Tag im Leben eines neuen Mitarbeiters, dessen Onboarding mit YubiKeys erfolgt



Option 1

Für Mitarbeiter im Büro

Der Mitarbeiter beginnt an Tag 1 und erhält 2 vom Administrator bereitgestellte Sicherheitsschlüssel, für die gerätegebundene Passkeys auf den Benutzer registriert sind.

Option 2

Für Remote-Mitarbeiter

Der Mitarbeiter beginnt an Tag 1 und erhält 2 Hardware-Sicherheitsschlüssel mit vorregistrierten gerätegebundenen Passkeys per Post.

Option 3

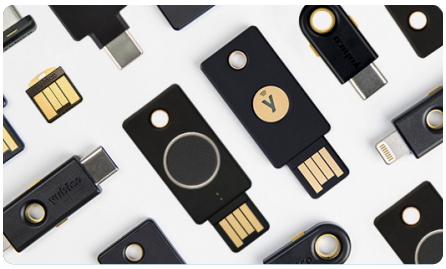
Es gibt auch andere, hier nicht dargestellte Selbstbedienungsvarianten, die eine Phishing-resistente Autorisierung unterstützen. Dabei könnte ein Administrator Smartcard-Zugangsdaten auf einem YubiKey bereitstellen, bevor er ihn an einen Benutzer weitergibt, damit dieser sich anmelden und dann einen Passkey auf demselben YubiKey registrieren kann.

Der Benutzer kann sich jetzt mit den Sicherheitsschlüsseln auf jedem seiner Geräte anmelden.

Innerhalb von FIDO2 stellt die Benutzerverifizierung sicher, dass die Person, die sich bei einem Dienst authentifiziert, tatsächlich die Person ist, die sie vorgibt zu sein, und dass sie die Kontrolle über den privaten Schlüssel hat. Der Benutzer ist berechtigt, seine Identität durch Eingabe einer PIN oder eines biometrischen Merkmals, wie z. B. eines Fingerabdrucks, über eine Eingabeaufforderung im Client zu verifizieren. Der Authentifikator führt die Benutzerverifizierung durch und antwortet der vertrauenden Partei, dass die Verifizierung erfolgreich war, und zwar auf eine kryptografisch überprüfbare Weise. Wenn ein FIDO2-Zertifikat für den passwortlosen Ablauf verwendet wird, muss die Benutzerüberprüfung auf „ERFORDERLICH“ festgelegt werden und der IDP muss dies überprüfen und durchsetzen.

Durch die Schaffung von Phishing-resistenten Benutzern wird sichergestellt, dass der Benutzer für jede Authentifizierungsaufgabe eine Phishing-resistente MFA-Lösung verwendet. Die meisten Lösungen und Umgebungen unterstützen nur Phishing-anfällige Authentifizierungsmechanismen für das Bootstrapping eines Passkey-Anbieters, es sei denn, Sie verfügen zudem über eine **portable Vertrauensbasis**, wie einen Sicherheitsschlüssel.

Sicherheitsschlüssel sind wie keine andere Lösung in der Lage, diese Anforderung zu erfüllen. Sicherheitsschlüssel sind tragbar und hochsicher und unterstützen sowohl Smartcard als auch WebAuthn in einem hochgradig portablen Format, wodurch sie äußerst nützlich für das Bootstrapping anderer Arten von Authentifikatoren sind, um andere Tools zu unterstützen und zu sichern. Auf diese Weise können Unternehmen einen Phishing-resistenten Benutzer einrichten.



> „Der größte Vorteil, den Hyatt durch die Bereitstellung von YubiKeys erhält, besteht darin, Passwörter aus der Unternehmensumgebung auszuschließen. Was nicht da ist, kann keinen Schaden anrichten."
>
> **Art Chernobrov** | Director of Identity, Access, and Endpoints | Hyatt Hotels Corporation

Erste Schritte auf Ihrem Weg zur Passwortlosigkeit mit Yubico FIDO Pre-Reg

Um Unternehmen dabei zu helfen, mit dem YubiKey passwortlose Bereitstellungen sicher und skalierbar zu beschleunigen, bietet Yubico einen innovativen Service namens FIDO Pre-Reg an, der eine schlüsselfertige FIDO-Aktivierung für YubiKeys ermöglicht. FIDO Pre-Reg setzt neue Maßstäbe für die Sicherheit, indem es die Abhängigkeit von weniger sicheren Prozessen für den Erstzugriff oder Wiederherstellungsszenarien beseitigt und so dazu beiträgt, das Risiko von Kontoübernahmen zu eliminieren. Sie erfordert nur minimale Einstellungen durch einen IT-Administrator und standardisiert und optimiert die YubiKey-Onboarding- und Kontowieder-herstellungsprozesse, wodurch der IT-Administrationsaufwand reduziert und gleichzeitig die User Experience verbessert wird.

YubiKey ist Ihre Brücke zur passwortlosen Authentifizierung

Der Weg zur Passwortlosigkeit lässt sich nicht über Nacht bewältigen. Yubico steht Ihnen jedoch bei jedem Schritt zur Seite.

Yubico hat den **YubiKey** entwickelt, einen Hardware-Sicherheitsschlüssel, der gerätegebundene Passkeys enthält und eine **Phishing-resistente MFA und passwortlose Authentifizierung in großem Maßstab mit einer optimierten User Experience** unterstützt.

Der YubiKey ist ein Multiprotokoll-Sicherheitsschlüssel, der eine Reihe von Authentifizierungsprotokollen unterstützt, darunter passwortlose Authentifizierung über Smartcard/PIV und Passkey (FIDO2/WebAuthn) sowie OTP und OpenPGP. Er lässt sich nahtlos in bestehende lokale und moderne Cloud-Umgebungen integrieren und unterstützt Unternehmen so bei der Umstellung auf eine passwortlose Zukunft.

YubiKeys funktionieren mit über 1000 Produkten, Services und Anwendungen, darunter führende Identitäts- und Zugriffsverwaltungsplattformen (IAM), Lösungen für die Verwaltung privilegierter Zugriffe (PAM) und Cloud-Services. Der YubiKey **reduziert nachweislich das Risiko um 99,9 %** und bietet großen Unternehmen einen erheblichen geschäftlichen Nutzen mit einem ROI von 203 %[13]. Gleichzeitig ermöglicht er eine reibungslose User Experience, sodass sich Benutzer schnell und sicher mit einem einzigen Tastendruck oder einer Berührung anmelden können.

Einzelfaktor (passwortlos): Authentifikator + Berühren/Tippen

Ersetzt schwache Passwörter durch einen Hardware-Authentifikator für eine starke Einzelfaktor-Authentifizierung.

Multi-Faktor (passwortlos): Authentifikator + Berühren/Tippen + PIN

Multi-Faktor mit Kombination aus Hardware-Authentifikator mit Benutzereingabe und PIN, um hohe Sicherheitsanforderungen für beispielsweise finanzielle Transaktionen oder das Einreichen von Rezepten zu gewährleisten.

Im Gegensatz zu synchronisierten Passkeys, die sich auf Geräten befinden, die nicht speziell für Sicherheitszwecke entwickelt wurden, und die sich einfach kopieren und teilen lassen, was ein Risiko für das Unternehmen darstellt, können gerätegebundene Passkeys, die sich in YubiKeys befinden, nicht geteilt oder kopiert werden. Dadurch kann das Unternehmen die FIDO-Zugangsdaten besser nachverfolgen und ihnen vertrauen, was für die Einhaltung von Vorschriften und für Audits von entscheidender Bedeutung ist. Passkey-Anmeldeinformationen, die auf dem YubiKey gespeichert sind, stellen sicher, dass Benutzer nahtlos und sicher auf einer Reihe von Plattformen und Geräten sowie in verschiedenen Ökosystemen (z. B. Apple, Google, Microsoft) arbeiten können. Außerdem dienen sie als wertvolle Vertrauensbasis zur Unterstützung anderer Authentifikatoren (z. B. Windows Hello for Business, Okta FastPass).

Gerätegebundene Passkeys ermöglichen Unternehmen die Implementierung passwortloser Systeme und die Erfüllung der strengsten Sicherheits- und Compliance-Anforderungen mit NIST AAL3-Unterstützung – eine gängige Anforderung in regulierten Branchen. Alle anderen heute verfügbaren Passkeys unterstützen nur bis zu AAL2.

Fazit

Unternehmen müssen sich von Passwörtern und veralteten Authentifizierungsmethoden verabschieden, um sich vor der wachsenden Zahl von Cyberbedrohungen zu schützen und zukunftssicher zu sein.

Die Lösungen von Yubico sind so konzipiert, dass sie Sie auf Ihrem Weg zur Passwortlosigkeit unterstützen. Sie bieten eine sichere, eigenständige, passwortlose Lösung zur Unterstützung von Passkey-, Smartcard- oder Hybrid-Implementierungen und eine portable Vertrauensbasis, um andere Authentifikatoren zu bootstrappen und so die kritischen Lücken in der Authentifizierung während des Lebenszyklus zu schließen, die Zero Trust untergraben können.

Der YubiKey bietet einen hochsicheren Weg zur passwortlosen Authentifizierung in großem Maßstab für eine Vielzahl komplexer Authentifizierungsszenarien. Wir bieten einen einfachen 6-Schritte-Bereitstellungsleitfaden mit Best Practices für den Einstieg in die passwortlose Nutzung von gerätegebundenen Passkeys.

Planung

Sicherstellung der Bereitschaft und Klärung von Anwendungsfällen und Benutzergruppen

Validierung

Bestätigung des Prozesses mit einer kleinen Gruppe von Benutzern vor der allgemeinen Umsetzung

Integration

Sicherstellung, dass die wichtigsten Apps und Services YubiKey-fähig sind

Einführung

Verteilung der Schlüssel an Benutzer per Komplettbereitstellungsservice oder Vertriebspartner

Akzeptanz

Förderung der Akzeptanz durch bewährte Schulungen und Unterstützung

Messung

Berichterstattung zu Auswirkungen auf Sicherheit und Geschäftswert

> „Wenn Sie passwortlose Systeme und Zero Trust betrachten, wird Ihnen klar, dass all Ihre Maßnahmen zur gleichen Sicherheit beitragen. Ich werde einfach weiter meine Kreise ziehen, die Passwortlosigkeit expandieren und über den Tellerrand hinausschauen, um meine Festung zu schützen."
>
> **Jason Rucker** | Director of IT | City of Southgate, MI

Um das Rätselraten bei Planung, Einkauf und Lieferung zu beseitigen, bietet Yubico YubiKey as a Service an – ein servicebasiertes und erschwingliches Modell, das die Beschaffung, Aktualisierung und Unterstützung von YubiKeys durch Unternehmen vereinfacht und eine optimierte globale Verteilung an entfernte und innerbetriebliche Standorte über YubiEnterprise Delivery und vertrauenswürdige Vertriebspartner ermöglicht.

Wenn Sie eine engere Partnerschaft bei einem der sechs Schritte dieses Plans wünschen, steht Ihnen das Professional Services Team von Yubico gerne zur Verfügung.

Kontaktieren Sie uns
yubi.co/Kontakt

Erfahren Sie mehr
yubi.co/passwordless

Quellen

1. Verizon, 2024 Data Breach Investigations Report
2. Google Cloud, August 2023 Threat Horizons Report, (August 2023)
3. S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
4. David Jones, Microsoft, Apple and Google double down on FIDO passwordless standard, (5. Mai 2022)
5. S&P Global Market Intelligence, With Security Breaches Mounting, Now Is the Time To Move From Legacy MFA to Modern, Phishing-Resistant MFA, 2023
6. Forrester Research, Inc, Optimize User Experience With Passwordless Authentication, (2. März 2020)
7. IBM, 2024 Cost of Data Breach Report
8. Kurt Thomas und Angelika Moscicki, New research: how effective is basic account hygiene at preventing hijacking, (17. Mai 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. CISA, Zero Trust Maturity Model v 2.0, (April 2023)
11. David Jones, Microsoft, Apple and Google double down on FIDO passwordless standard, (5. Mai 2022)
12. NIST, NIST SP 800-63-4 Digital Identity Guidelines, (Dezember 2022)
13. Forrester, The Total Economic Impact of Yubico YubiKeys, (September 2022)

yubico

Über Yubico

Yubico (Nasdaq Stockholm: YUBICO) ist der Erfinder des YubiKey, einem Hardware-Sicherheitsschlüssel, der den Goldstandard für eine Phishing-resistente Multi-Faktor-Authentifizierung (MFA) darstellt. Die Lösungen von Yubico bieten Unternehmen und Benutzern Anwendungsexpertise und betriebliche Flexibilität, da YubiKeys mit Hunderten von Verbraucher- und Unternehmensanwendungen und -diensten funktionieren.

Yubico hat wesentlich zur Entwicklung der offenen Authentifizierungsstandards FIDO2/Passkey, WebAuthn und FIDO Universal 2nd Factor (U2F) beigetragen. Das Unternehmen ist ein Pionier bei der Bereitstellung einer hardwarebasierten passwortlosen Authentifizierung in Form von hochsicheren Passkeys für Kunden in über 160 Ländern.

Weitere Informationen finden Sie unter: www.yubico.com.