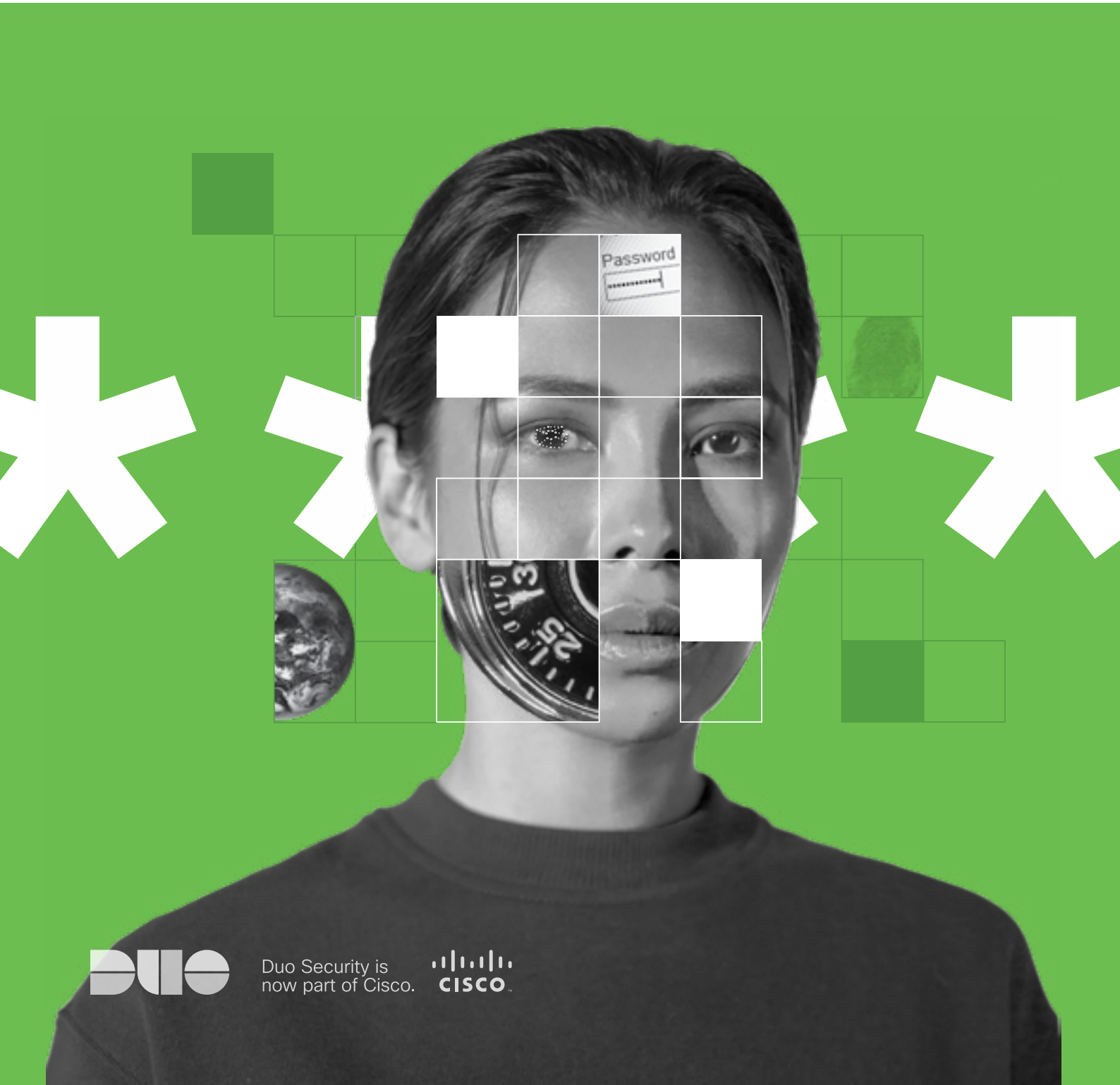
Passwordless

Die Zukunft der Authentifizierung



Duo Security is
now part of Cisco.

Passwordless

Die Zukunft der Authentifizierung

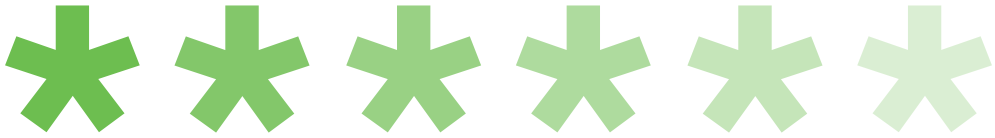
Table of Contents

Sicherheit und Benutzerfreundlichkeit für Digitale Transformation

Um transformative Geschäftsziele zu erreichen, wettbewerbsfähig zu bleiben und die Erwartungen der Benutzer zu erfüllen, unterziehen Unternehmen eine digitale Transformation. Was auch als Modernisierung bezeichnet wird.

Unternehmen migrieren von Legacy-Systemen in die Cloud, was zu hybriden Umgebungen führt. Die Verbrauchermärkte treiben den Drang nach nutzbarer mobiler Technologie die stets bereit, immer verfügbaren Cloud und webbasierten Anwendungen voran. Diese Umstellung auf die Cloud umfasst sowohl Kunden als auch alle Arten von Unternehmensbenutzern - einschließlich Mitarbeiter, Auftragnehmer, Lieferanten, Partner usw.

Diese Umstellung auf ein dezentrales, identitätsorientiertes Betriebsmodell hat dafür gesorgt, dass der sichere Zugriff für Benutzer immer wichtiger wird. Die Zukunft der Authentifizierung erfordert sowohl eine sichere als auch eine nutzbare Methode, um Benutzer sowohl für Cloud- als auch für lokale Systeme zu autorisieren.



Die Umschaltung der Authentifizierung auf Passwordless

Laut **Computer History** and **Wired** stammte das Passwort Mitte der 1960er Jahre am Massachusetts Institute of Technology (MIT) mit der Entwicklung des Compatible Time-Sharing-Systems (CTSS). Hunderte von Benutzern konnten den Computer mit einem gemeinsamen Mainframe teilen. Das Kennwort wurde als Buchhaltungstool entwickelt, um Benutzern für einen bestimmten Zeitraum den Zugriff auf ihre spezifischen Ressourcen zu ermöglichen.

Im Laufe der Zeit teilten einige Benutzer ihre Passwörter mit und andere forderten eine bessere Sicherheit, und der Schwerpunkt verlagerte sich auf die Authentifizierung. In den 1980er Jahren patentierte Security Dynamics Technologies eine „Methode und einen Apparat zur positiven Identifizierung einer Person“ und ebnete den Weg für zusätzliche Authentifizierungsfaktoren. In den letzten 20 Jahren hat sich die Multi-Faktor Authentifizierung (MFA) zu einer sekundären Authentifizierung entwickelt, die der primären Kennwortauthentifizierung eine zusätzliche Sicherheitsebene bietet.

Mit zunehmender Routine von Datendumps und Kennwortdiebstahl wurden die primäre Kennwortauthentifizierung und die sekundäre MFA-Authentifizierung unerlässlich. Das 60 Jahre alte Einzelfaktor-Passwort hat den Test der Zeit einfach nicht bestanden. Im Jahr 2019 veröffentlichte ein anonymer Ersteller 2,2 Milliarden Benutzernamen und Passwörter frei in einem Angreiferforum, das zu dieser Zeit als die größte Sammlung von Sicherheitsverletzungen bekannt war (**Wired**).

Fortschritte bei sekundären Faktoren, von der Verbreitung von Smartphones bis zur Konsumierung biometrischer Daten, haben viele dazu veranlasst, die Notwendigkeit und Verwendung des Passworts überhaupt in Frage zu stellen. Wenn eine starke Authentifizierung auf mehreren Faktoren basiert und Kennwörter der am stärksten gefährdeten Faktor sind, warum sollten sie dann überhaupt benötigt werden? Diese Erkenntnis hat die Branche dazu veranlasst, Passwörter durch sicherere, vereinfachte Authentifizierungsmethoden zu ersetzen.

Tech- und Sicherheitsanalysten sagen voraus, dass Unternehmen die Passwordless Authentifizierung für ihre Benutzer implementieren werden, um diese moderne digitale Transformation zu ermöglichen.

> “Bis 2022 werden 60% der großen und globalen Unternehmen und 90% der mittelständischen Unternehmen (MSEs) in mehr als 50% der Anwendungsfälle kennwortlose Methoden implementieren, was einer Steigerung von heute weniger als 5% entspricht.”
>
> – **Gartner Market Guide für die Benutzerauthentifizierung**

2.0

Das Problem mit Passwörtern

Passwörter sind mit Problemen behaftet, die sie zu einem unsicheren Faktor für die Identitätsprüfung machen. Darüber hinaus verursachen Passwörter viel Reibung und Frustration beim Benutzer.

Die Verwaltung von Passwörtern ist teuer und zeitaufwändig.

Passwörter beanspruchen jedes Jahr viel IT- und Helpdesk-Support - laut **Forrester** so sehr, dass viele große US-amerikanische Unternehmen jährlich über 1 Million US-Dollar für passwortbezogene Supportkosten bereitgestellt haben.

Laut **The Gartner Group** sind jedes Jahr 20% bis 50% aller IT-Helpdesk-Tickets für das Zurücksetzen von Passwörtern bestimmt. Diese Zeit könnte sonst für neue IT-Initiativen aufgewendet werden.

Abgelaufene Passwörter kosten ein großes, globales Technologie- und Sicherheitsunternehmen insgesamt 30 US-Dollar pro Mitarbeiterfall Unterstützung von über 500.000 USD und Produktivitätsverlust pro Jahr.

Passwörter verursachen schlechte Benutzererfahrungen.

Eine von der International Data Group (IDG), gesponsert von MobileIron, durchgeführte Umfrage unter 200 IT-Sicherheitsmanagern ergab, dass 62 Prozent der Befragten extreme Frustration unter den Benutzern angaben, wenn Passwörter gesperrt wurden. Das ist keine Überraschung. Sperren beeinträchtigen die Produktivität und tragen zu einer schlechten Benutzeranmeldung bei.

Zusätzlich zu Kennwortsperrungen hat die Anzahl der Cloud-Dienste und Kennwörter, bei denen sich ein Benutzer anmelden muss, um seine Arbeit zu erledigen, im Laufe der Jahre zugenommen. Ein durchschnittliches Unternehmen nutzt derzeit 1.400 verschiedene Cloud-Dienste, während sich der durchschnittliche Geschäftsbenutzer laut **SkyHigh Networks** and **Security Magazine** mit bis zu 190 Passwörtern anmelden muss.

Passwörter können leicht kompromittiert werden.

Es gibt auch eine Reihe anderer kennwortbezogener Bedrohungen und Angriffe, die häufig von Angreifern verwendet werden, hauptsächlich weil sie einfach sind und funktionieren. Einige Beispiele sind das Füllen von Anmeldeinformationen (umfangreiche automatisierte Anmeldeversuche mit gestohlenen Anmeldeinformationen). Phishing (ein Versuch, Benutzer zu täuschen und vertrauliche Informationen wie Passwörter illegal zu erhalten); Brute-Force-Angriffe (Erraten von Passwörtern); usw.

Passwörter sind für Gegner von Natur aus leicht zu untergraben. Aufgrund der Ermüdung der Passwörter wählen Benutzer häufig schwache Passwörter. Außerdem werden alte Passwörter häufig für verschiedene Konten wiederverwendet oder nur geringfügig geändert. Eine **akademische Studie von Virginia Tech aus dem Jahr 2018** ergab, dass bei 52% aller Benutzer eine Wiederverwendung von Passwörtern beobachtet wurde.

Infolgedessen betreffen 81% der Verstöße gestohlene oder schwache Anmeldeinformationen, während 29% aller Verstöße die Verwendung gestohlener Anmeldeinformationen betreffen, wie aus dem **Untersuchungsbericht zu Datenverletzungen von Verizon 2020 hervorgeht**.

Was ist echte Passwordless Authentifizierung?

Eine echte kennwortlose Authentifizierung stellt eine starke Sicherheit der Identität eines Benutzers sicher, ohne sich auf Kennwörter verlassen zu müssen, und ermöglicht es Benutzern, sich mithilfe von Biometrie, Sicherheitsschlüsseln oder einem mobilen Gerät zu authentifizieren. Es bietet sicheren Zugriff für jeden Unternehmensanwendungsfall (Hybrid-, Cloud-, lokale und Legacy-Apps).

Durch Technologiepartnerschaften ist Duo auf dem Weg zu einer echten kennwortlosen Zukunft, die Benutzerfreundlichkeit mit einer stärkeren Authentifizierung in Einklang bringt. Passwordless bietet Benutzern ein reibungsloses Anmeldeerlebnis und reduziert gleichzeitig den Verwaltungsaufwand und die allgemeinen Sicherheitsrisiken für das Unternehmen.

Geschäftsvorteile von Passwordless

Die kennwortlose Authentifizierung bietet eine einzige, starke Sicherheit der Benutzeridentität, um das Vertrauen der Benutzer zu erreichen. Dadurch können Unternehmen folgende Vorteile erzielen:

Bessere Benutzererfahrung
Durch die Beseitigung der Kennwortabhängigkeit profitieren Benutzer von weniger Müdigkeit und Frustration beim Anmelden und einer höheren Benutzerproduktivität.

Reduzierte IT-Zeit und -Kosten
In ähnlicher Weise können Administratoren und Unternehmen durch passwortbezogene Helpdesk-Tickets und das Zurücksetzen von Passwörtern von einer geringeren Belastung profitieren.

Stärkere Sicherheitslage
Das Eliminieren der Passwortabhängigkeit kann dazu führen, dass verwandte Bedrohungen und Schwachstellen wie Phishing, gestohlene oder schwache Passwörter, Wiederverwendung von Passwörtern, Brute-Force-Angriffe usw. beseitigt werden.

> "In an effort to combat hackers who target passwords to access cloud-based applications, passwordless methods that associate users to their devices offer increased security and usability, which is a rare win/win for security,"

Peter Firstbrook
Gartner Research Vice President, **Gartner Security & Risk Management Summit 2019**

DIE HERAUSFORDERUNG:

Ein aufstrebender Markt

Heutzutage können viele kennwortlose Anbieter nur einen Anwendungsfall lösen, indem sie Benutzern weniger Kennwörter oder eine Kennwort-Lite-Erfahrung durch Single Sign-On (SSO) zur Verfügung stellen, die Reihenfolge der Faktoren und das Sitzungsmanagement ändern. Sie beheben jedoch nicht die inhärente Sicherheitsanfälligkeit von Kennwörtern.

Moderne Unternehmen können heute nicht alle Anwendungsfälle für den Zugriff mit einer einzigen kennwortlosen Lösung abdecken.

Es sind zusätzliche geschäftliche Herausforderungen zu berücksichtigen:

Komplexe und Hybride IT Umgebungen

Die Suche nach einer Lösung, die sowohl Legacy- als auch Cloud Anwendungen unterstützt und eine konsistente, vereinfachte Benutzererfahrung bietet. Der Cloud Verbund ist nur für Cloud Anwendungen kennwortlos. Benutzer können sich anmelden und ihre Identität mithilfe von Biometrie oder einem Sicherheitsschlüssel überprüfen. In der Realität müssen moderne Unternehmen jedoch den Zugriff auf eine hybride Mischung aus Cloud- und lokalen Anwendungen schützen.

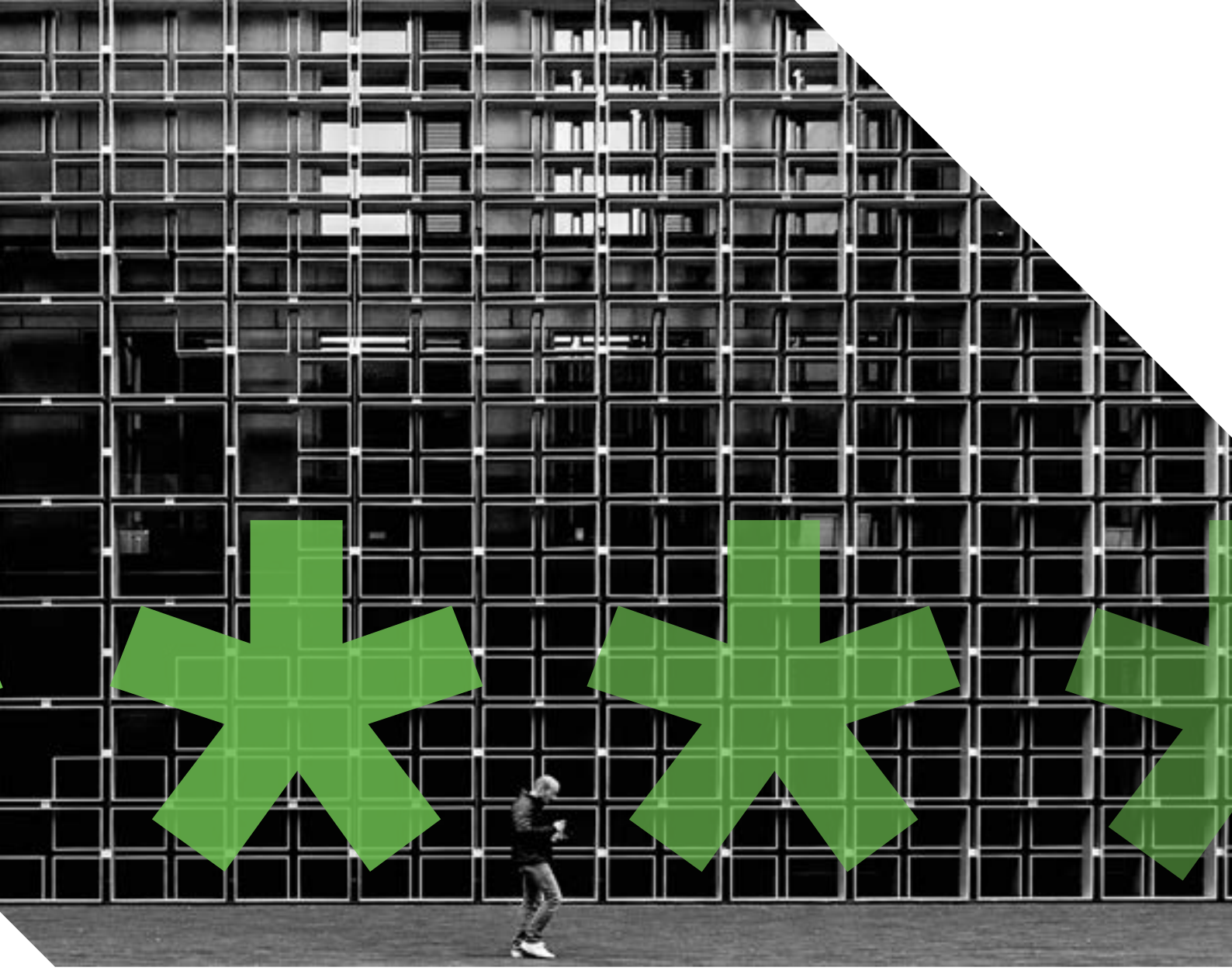
Anwendung und Verwaltungskosten

Die Unterstützung für kennwortlose Technologie kann kostspielige Sicherheitshardware und Geräteverwaltung umfassen.

Kosten für Sicherheitsschlüssel und biometrische Authentifizierung können ein Hindernis für den Zugriff sein, um verschiedene Benutzertypen in einer Organisation zu unterstützen.

Compliance-Anforderungen

Viele Unternehmen oder Partnerunternehmen der Lieferkette, die Compliance-Standards für die Datenregulierung erfüllen müssen, haben ihre Richtlinien an Kennwörter gebunden, was es schwierig macht, auf stärkere Authentifizierungsmethoden umzusteigen. Bundesstandards wie **NIST 800-63** enthalten weitere Richtlinien für Kennwörter, MFA und alternative Authentifizierungsmethoden sowie **neuere Anleitungen** zum Löschen von Kennwortablauf- und Komplexitätsanforderungen.



PROBLEMPOSITION

Kennwortlose Punktlösungen lösen nicht mehr jede gängige Anwendung in modernen Unternehmen, was zu kritischen Lücken in der Zugriffssicherheit führt.

PASSWORDLESS HERAUSFORDERUNG

Richten Sie eine Basis für das Vertrauen in die Benutzeridentität ein, die nicht auf Kennwörtern basiert - unabhängig davon, wohin der Benutzer geht oder auf was er zugreifen möchte.

UNSERE LÖSUNG:

Der Pfad zu Passwordless

Wir empfehlen einen schrittweisen Ansatz zur Bereitstellung eines sicheren Zugangs für die Belegschaft, der Sie mit jedem Schritt einer völlig kennwortlosen Zukunft näher bringt:

1.

Identifizieren Sie Anwendungsfälle ohne Kennwort und aktivieren Sie eine starke Authentifizierung.

Reduzieren Sie Ihre Abhängigkeit von Kennwörtern und verringern Sie das Risiko des Diebstahls von Anmeldeinformationen, indem Sie bestimmte Anwendungsfälle für Unternehmen identifizieren und auswählen. Ordnen Sie die Anwendungsfälle nach Benutzererfahrung, IT-Zeit und -Kosten sowie Sicherheits- und Compliance-Risiken. Gruppieren Sie die Anwendungsfälle nach anwendbaren kennwortlosen Lösungen, um nicht zu einer Reihe von Punktlösungen zu gelangen. Erstellen Sie Implementierungspläne für Bereiche mit der größten Auswirkung und der kürzesten Wertschöpfungszeit.

Starke Authentifizierung für alle Apps
Reduzieren Sie Ihre Abhängigkeit von Kennwörtern als einzige Form der Benutzerauthentifizierung und eröffnen Sie zusätzliche Faktoren, um später die primäre Authentifizierung bereitzustellen. Schützen Sie Cloud- und lokale Anwendungen mit MFA von Duo. Auf diese Weise können Sie das Risiko eines Diebstahls von Anmeldeinformationen verringern, indem Sie eine zweite Methode zur Identitätsprüfung benötigen, die von einem Angreifer nicht einfach aus der Ferne gestohlen werden kann.

2.

Die Optimierung und Konsolidierung von Authentifizerungsworkflows.

Minimieren Sie Kennwörter für Cloud- und gehostete Apps
Rationalisieren Sie die Authentifizierung für eine Reihe von Anwendungsfällen als Teil des Implementierungsplans. Erzielen Sie bei Cloud-Apps weniger Kennwörter, indem Sie SSO für SAML-basierte Anwendungen verwenden. Integrieren Sie für lokale Dienste die Workflows mithilfe von Zugriffsproxys und Authentifizierungsproxys.

Mit MFA und einer erweiterten Anmeldeerfahrung können Sie Kennwortrichtlinien ändern, für die strenge und komplexe Kennwortzeichen erforderlich sind, sowie Richtlinien zum Zurücksetzen von Kennwörtern. Dies verringert die Frustration der Benutzer mit der Kennwortsicherheit und verringert ihre Abhängigkeit von der Kennwortkomplexität als primäre Authentifizierung.

3.

Das Vertrauen in Authentifizierung erhöhen.

Steigern Sie das Vertrauen mit adaptiven Richtlinien
Eine häufig geäußerte Sorge um kennwortlos ist das Potenzial, das Sicherheitsrisiko zu erhöhen, wenn die Schritte zur Authentifizierung reduziert werden. Beheben Sie dieses Problem, indem Sie die Kontrolle basierend auf dem Kontext der Benutzerauthentifizierung erhöhen.

Kommt die Authentifizierung von einem vertrauenswürdigen Gerät? Entspricht die Sicherheitslage des Zugriffsgeräts den Sicherheitshygienestandards des Unternehmens? Überprüfen Sie abschließend, ob verdächtiges Verhalten wie ungewöhnliche Authentifizierungsfaktoren, ungewöhnliche Orte, ungewöhnliche Tageszeiten oder Zugriffsversuche von Benutzern mit hohem Risiko oder gegen Anwendungen mit hohem Risiko vorliegen. Wenden Sie adaptive Zugriffsrichtlinien an, die auf dem Kontext des Benutzers, des Geräts, des Standorts, des Verhaltens usw. basieren, um sicherzustellen, dass die Authentifizierung vertrauenswürdig ist.

4.

Ein Passwordless Erlebnis anbieten.

Wenn MFA ein Kennwort mit einem oder mehreren Authentifizierungsfaktoren ist, wird kennwortlos am besten als ein oder mehrere Authentifizierungsfaktoren ohne Kennwörter beschrieben. Benutzer können sich mit einem einzigen biometrischen Authentifikator (oder Sicherheitsschlüssel) anmelden, um auf Anwendungen zuzugreifen. Implementieren Sie in diesem Schritt die Standardtechnologie, um Kennwörter als primären Authentifizierungsfaktor für die Anwendungsfälle und Bereiche zu entfernen, die den größten Einfluss auf Benutzererfahrung, Kosten und Sicherheit haben.

Erwägen Sie beispielsweise bei Cloud-Apps die Verwendung von WebAuthn, um sich mit integrierten biometrischen Authentifikatoren auf Laptops und Smartphones, z. B. einem Touch ID-Fingerabdruckleser auf MacOS-Laptops, sicher bei Konten anzumelden. WebAuthn ist ein offener Standard, der eine starke Kryptografie mit öffentlichen Schlüsseln ermöglicht, um die Benutzerpräsenz zum Zeitpunkt der Authentifizierung sicherzustellen. Es erfordert einen unterstützten Webbrowser, ein Betriebssystem und einen integrierten Authentifikator wie Touch ID oder USB-basierte Sicherheitsschlüssel.

5.

Das Passwordless Toolset optimieren

Erzielen Sie für alle Anwendungsfälle eine echte Kennwortlosigkeit, einschließlich für ältere Tools ohne Kennwort, die ältere Protokolle zusammen mit Cloud-basierten Anwendungen verwenden. Der Weg zu Passwordless ist ein iterativer Ansatz zum Auswählen, Optimieren und Sichern der Authentifizierung. Der letzte Schritt auf dem Weg ist die Integration der Technologie und die kontinuierliche Verbesserung. Mit True Passwordless müssen Sie sich bei jedem Anmelde-Workflow weder hinter den Kulissen noch während der gesamten Benutzererfahrung auf Kennwörter verlassen.

Dies ist die Herausforderung auf dem heutigen Markt, die Anbieter von kennwortlosen Technologieplattformen lösen müssen. Duo arbeitet mit Industrie- und Technologiepartnern zusammen, um ein umfassendes Ökosystem zu schaffen, das echte Passwörter in jedem Geschäftsanwendungsfall unterstützt.

Was kann man heute tunen?

Die Kombination von kennwortloser Technologie mit starker MFA zum Schutz des Zugriffs über die Cloud und vor Ort ist eine praktische Möglichkeit, um heute die umfassendste Sicherheitsabdeckung bereitzustellen. Mit MFA können Sie die Abhängigkeit von Kennwörtern verringern und Kennwortrichtlinien so ändern, dass weniger häufige Zurücksetzungen erforderlich sind, wodurch die Belastung des Helpdesks verringert und die Frustration der Benutzer verringert wird.

Duo empfiehlt die Verwendung des offenen W3C-Standards WebAuthn und des Cloud-basierten SSO, um Kennwörter für Cloud-Anwendungen zu entfernen. Dadurch werden Kennwörter nicht vollständig entfernt, es wird jedoch das Ziel erreicht, die Kennwortabhängigkeit zu verringern.

Passwordless ermöglicht Zero Trust

Die Authentifizierung - oder der sichere Zugriff - ermöglicht die Umstellung auf ein mobiles und Cloud-First-Unternehmen, sodass Benutzer remote arbeiten können, die Produktivität steigern und die geschäftliche Flexibilität steigern können.

Mit der Identität als neuem Perimeter müssen Unternehmen die Belegschaft sichern: die Benutzer und Geräte, die auf Anwendungen zugreifen. Die kennwortlose Authentifizierung ist ein wichtiger Baustein für die Gewährleistung einer vertrauenswürdigen Sicherheit für die Belegschaft.

Eine Kombination aus **Benutzer-** und **Gerätevertrauen**, die durch **adaptive Richtlinien** gesteuert wird, stellt sicher, dass der Zugriff auf Anwendungen und Daten gesichert ist.

Die kennwortlose Authentifizierung verbessert die Erfahrung der Mitarbeiter und stärkt gleichzeitig unser Vertrauen in die Authentifizierung - ein entscheidender Schritt beim Aufbau einer "Zero Trust" -Architektur.

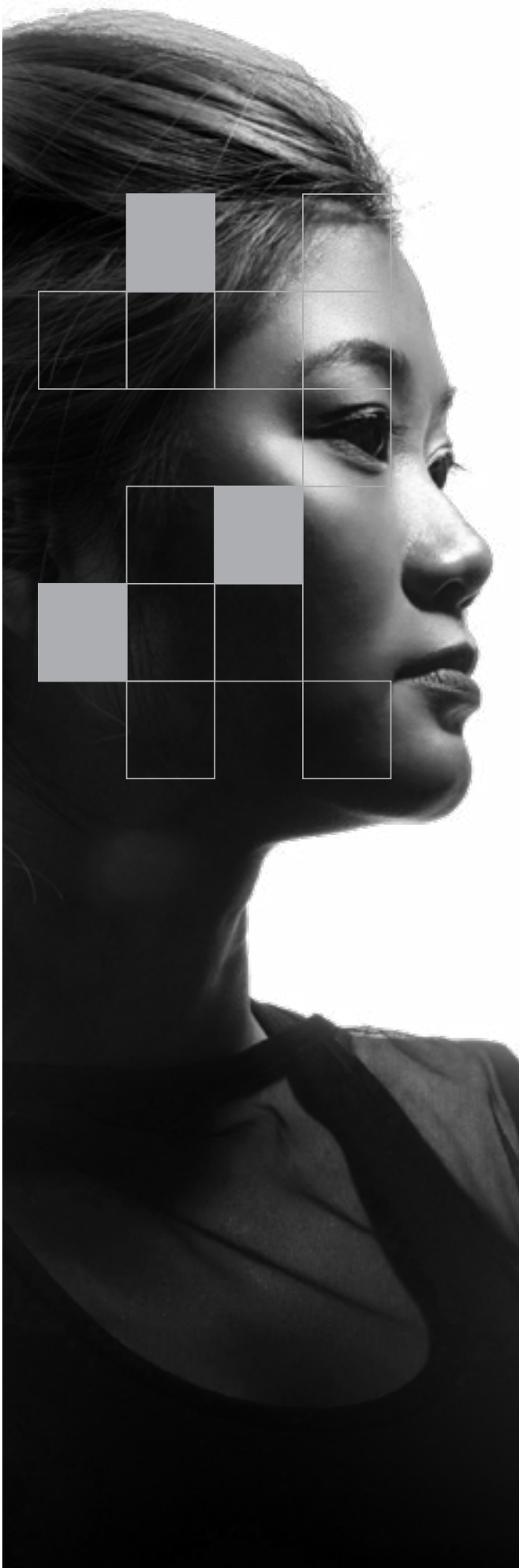
In seinen 10 Prinzipien der Zero-Trust Architektur verweist das National Cyber Security Center (NCSC) auf Passwordless als Teil der "**Schaffung einer einzigen starken Benutzeridentität**."

"In order to remove trust from the network, you need to instead gain confidence in the authentication, verification and authorization of users and services. This is achieved by **building trust into the user's identity** (user authentication), their devices (device verification), and the services they access (service authorisation).

For this model to be effective, each connection to a service should be authenticated and the device and connection authorised against a policy, regardless of where the connection request comes from."

– **UK NCSC Zero Trust Architecture**

Passwordless ist ein Baustein für Unternehmen auf einer Reise zu "Zero Trust". Dies ist der Schlüssel zur Schaffung einer einzigen, starken Benutzeridentität und eines starken Vertrauens.



Durch Partnerschaft für eine Passwordless Zukunft sorgen

Duo arbeitet mit Anbietern von Technologieplattformen und Branchenorganisationen zusammen um eine vollständig kennwortlose Zukunft in einen für das Unternehmen nutzbaren Zustand zu bringen.

Kennwortlose Technologieplattformen wie Windows Hello, Touch ID, Face ID und Fingerabdruck-APIs sind erforderlich, um mit hardwarebasierten biometrischen Authentifikatoren zu arbeiten, die von offenen Standards wie WebAuthn und CTAP unterstützt werden.

Diese Technologien ebnen den Weg in eine kennwortlose Zukunft und wir arbeiten eng mit ihnen zusammen, um Herausforderungen zu lösen, indem wir:

+ Partnerschaft mit Microsoft als erstem Softwarepartner für Windows Hello for Business, das Vertrauen für die biometrische Authentifizierung von Geräten und Webdiensten schafft
+ Unterstützung von **WebAuthn-Sicherheitsschlüsseln** für wichtige Browser
+ Duo-Experten in der **WebAuthn-Arbeitsgruppe**, **W3C** and **FIDO Alliance** setzen sich für Unternehmensfunktionen ein
+ Bereitstellung von Entwicklertools mit **WebAuthn.io** und **WebAuthn.guide**

Zusätzliche Ressourcen

Erfahren Sie mehr über Duo und was wir tunen, um eine Zukunft ohne Passwörter zu ermöglichen indem Sie daran arbeiten kennwortlose Technologien und Standards für die breitere Community offen, zugänglich und einfach zu machen:

What is WebAuthn?

Web Authentication: What It Is and What It Means for Passwords

WebAuthn.guide

WebAuthn.io

VIDEO: **A Technical How-To Guide for WebAuthn 2019**

Introducing the WebAuthn Authenticator Open-Source Library

Duo.com