yubico

YubiKey 5 CSPN-Serie

Gewährleistung von Sicherheit und Compliance

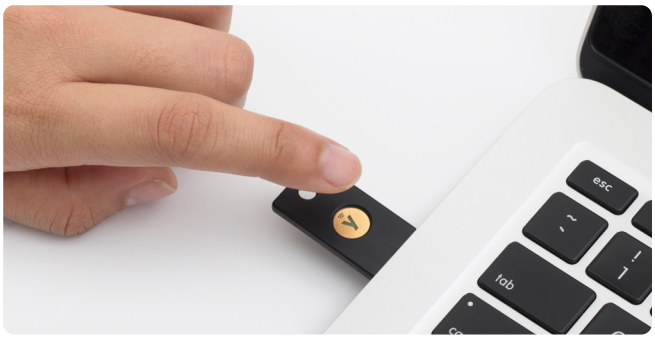
Die YubiKey 5 CSPN-Serie ist die erste CSPN-zertifizierte FIDO2/WebAuthn, Multi-Protokoll-Authentifikator-Reihe. Von links nach rechts: YubiKey 5 NFC CSPN, YubiKey 5C NFC CSPN, YubiKey 5Ci CSPN, YubiKey 5C CSPN, YubiKey 5 Nano CSPN und YubiKey 5C Nano CSPN.

Die ausschließliche Verwendung von Benutzernamen und Passwörtern gefährdet die Unternehmensdaten

Katastrophale Sicherheitsverletzungen machen täglich Schlagzeilen, und das aus gutem Grund. Ein einziger Sicherheitsverstoß in einem Unternehmen kostet durchschnittlich 4,35 Millionen Dollar,[1] und 61 % der Sicherheitsverstöße werden durch gestohlene oder schwache Passwörter verursacht.[2] Daher können sich IT-Organisationen beim Schutz des Zugriffs auf Unternehmensdaten nicht ausschließlich auf Passwörter verlassen. Sie müssen eine stärkere Authentifizierung von Mitarbeitern und Lieferanten einführen – oder sie riskieren, das nächste Ziel zu werden.

Die YubiKey 5 CSPN-Serie verhindert die Übernahme von Konten und macht es einfach, eine starke, skalierbare Authentifizierung zu implementieren und schützt Unternehmen vor Phishing-Angriffen. Der YubiKey ist eine hardwarebasierte Lösung und bietet:

- Mehrere Authentifizierungs- und Verschlüsselungsprotokolle, einschließlich FIDO2/WebAuthn, FIDO U2F, Personal Identity Verification-kompatible (PIV) Smart Card und Yubico One-Time Password (OTP) zum Schutz des Mitarbeiterzugangs zu Computern, Netzwerken und Online-Diensten – mit nur einer Berührung
- Unterstützung passwortloser sicherer Anmeldung mit Smartcard und FIDO2/WebAuthn-Authentifizierung
- Unterstützung aller gängigen Betriebssysteme, darunter Microsoft Windows, macOS, Android und Linux sowie der führenden Browser
- Erhältlich in einer Auswahl von sechs Formfaktoren, die es Nutzern ermöglichen, Verbindungen über USB-A, USB-C, NFC und Lightning herzustellen



YubiKeys haben Google-Mitarbeiter seit 2009 geschützt

0	92 %	4x	0
Konto-übernahmen	Weniger Supportfälle	schnellere Anmeldung	Konto-sperrungen

YubiKey ist seit 2012 die vertrauenswürdige Wahl von Google, Facebook und Salesforce

Bieten einer starken Multi-Faktor-Authentifizierung: Der YubiKey kombiniert hardwarebasierte Authentifizierung und Public-Key-Kryptografie, um eine starke Authentifizierung zu gewährleisten und die Übernahme von Konten zu verhindern. Zu den Funktionen gehören FIDO2/WebAuthn und FIDO U2F, offene Authentifizierungsstandards, die von der FIDO Alliance unterstützt werden, sowie Smartcard-Funktionen, die auf der in NIST SP 800-73 spezifizierten PIV-Schnittstelle basieren.

Reduzieren der IT-Kosten: Nach der Auswertung der Daten von mehr als 50.000 YubiKeys in 70 Ländern stellte Google fest, dass die Benutzerfreundlichkeit und Zuverlässigkeit des Geräts die Zahl der Vorfälle beim Passwort-Support um 92 % reduziert hat. Dadurch spart das Unternehmen Tausende von Stunden pro Jahr an Supportkosten.[3]

Bieten einfacher, schneller und zuverlässiger Sicherheit für Mitarbeiter: Die YubiKey-Hardware ist zuverlässig, da sie weder eine Batterie noch eine Netzwerkverbindung benötigt, sodass sie immer eingeschaltet und zugänglich ist. Die Authentifizierung erfolgt schnell durch eine einfache Berührung und ist viermal schneller als SMS und mobile Zwei-Faktor-Authentifizierung.

Phishing-Abwehr für sichere Unternehmensauthentifizierung

Der YubiKey speichert das Authentifizierungsgeheimnis auf einem Hardware-Chip mit sicherem Element. Dieses Geheimnis wird niemals übermittelt und kann daher weder kopiert noch gestohlen werden.

YubiKeys werden genutzt in:

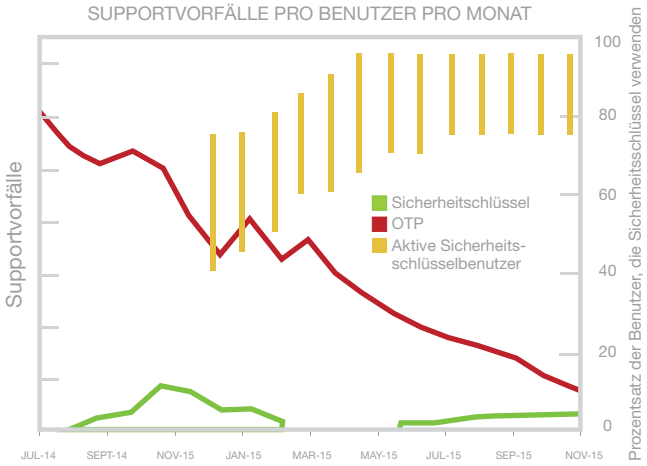
- **9 der 10 führenden** Technologieunternehmen weltweit
- **4 der 10 führenden** US-Banken
- **5 der 10 führenden** globalen Handelsunternehmen

YubiKey: Bewährte, benutzerfreundliche Sicherheit, der die führenden Unternehmen der Welt vertrauen

Reduziert IT-Kosten

Der YubiKey reduziert drastisch die wichtigsten IT-Supportkosten – Passwortrücksetzungen – die Microsoft über 12 Millionen Dollar pro Monat kosten.[4]

Durch die Umstellung von mobilen OTPs auf YubiKeys konnte Google die Zahl der Vorfälle beim Passwort-Support um 92% reduzieren, da YubiKeys zuverlässiger, schneller und einfacher zu verwenden sind.



Diese Grafik veranschaulicht, wie schnell Google die Zahl der Vorfälle beim Passwort-Support nach dem Wechsel von OTP zu YubiKey reduziert hat.[5]

Einfach zu bedienen, schnell und zuverlässig

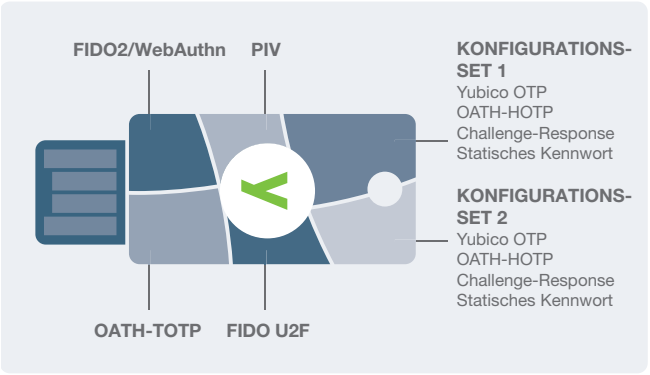
Die Benutzer müssen nichts installieren – Kunden oder Mitarbeiter registrieren einfach ihren eigenen YubiKey, geben wie gewohnt ihren Benutzernamen und ihr Passwort ein, schließen den YubiKey an und tippen ihn an, wenn sie dazu aufgefordert werden.

Der YubiKey 5 NFC CSPN, der YubiKey 5C NFC CSPN, der YubiKey 5Ci CSPN und der YubiKey 5C CSPN passen bequem an einen Schlüsselbund, während der YubiKey 5 Nano CSPN und der YubiKey 5C Nano CSPN so konzipiert sind, dass sie im USB-Anschluss bleiben. Dadurch wird sichergestellt, dass jeder YubiKey leicht zugänglich ist und das gleiche Maß an digitaler Sicherheit bietet. Der YubiKey 5 NFC CSPN / 5 Nano CSPN ist stoßfest und wasserbeständig.

Einfacher Einsatz

Die IT-Abteilung kann YubiKeys innerhalb von Tagen, nicht Monaten, einsetzen. Ein einziger Schlüssel kann auf mehrere moderne und ältere Systeme zugreifen, wodurch die Notwendigkeit separater Schlüssel oder zusätzlicher Integrationsarbeit entfällt.

[1] 2022 Cost of Data Breach Report, IBM
[2] Verizon, 2021 Data Breach Investigations Report
[3] Security Keys: Practical Cryptographic Second Factors for the Modern Web, Google Inc.
[4] "Saying Goodbye to Passwords", Alex Simons, Manini Roy, Microsoft Ignite 2017
[5] Security Keys: Practical Cryptographic Second Factors for the Modern Web, Google Inc.



YubiKey-Fähigkeiten: Diese Funktionen sind in den Sicherheitsschlüsseln YubiKey 5 NFC CSPN, YubiKey 5C NFC CSPN, YubiKey 5Ci CSPN, YubiKey 5C CSPN, YubiKey 5 Nano CSPN und YubiKaey 5C Nano CSPN enthalten.

Führend im Bereich der vertrauenswürdigen Authentifizierung

Yubico ist der Haupterfinder des von der FIDO-Allianz angenommenen U2F-Authentifizierungsstandards und war das erste Unternehmen, das den U2F-Sicherheitsschlüssel herstellte.

YubiKeys werden in neun der zehn weltweit führenden Technologieunternehmen, in vier der zehn führenden US-Banken und in fünf der zehn führenden globalen Handelsunternehmen eingesetzt.

First Level Security Certification (CSPN) von ANSII, und anerkannt vom BSI.

Schützen Sie Ihr Unternehmen mit der CSPN-zertifizierten Version der branchenführenden Multi-Faktor-Authentifizierungslösung YubiKey. Die YubiKey 5 CSPN-Serie ermöglicht es französischen/europäischen Behörden und regulierten Industrien, die strengen Sicherheits- und Authentifizierungsstandards gemäß den Richtlinien der französischen Agentur für Netzwerk- und Informationssicherheit (ANSSI) zu erfüllen.

Dieses Lineup ist auch vom BSI, der Bundesbehörde für Cybersicherheit in Deutschland, anerkannt. Das BSI erkennt die CSPN-Zertifizierung als Erfüllung seiner strengen Sicherheitsstandards an und entspricht damit der BSZ-Zertifizierung.

Um mehr zu erfahren, kontaktieren Sie bitte unsere Yubico Experten.

Über Yubico Als Erfinder des YubiKey macht Yubico sicheres Login mit Phishing-resistenter MFA-Technologie sehr einfach. Yubico setzt globale Standards für den plattformübergreifenden sicheren Zugang zu Anwendungen und Endgeräten und ist einer der Hauptentwickler und Mitgestalter von offenen Authentifizierungsstandards wie FIDO2 (WebAuthn) und FIDO U2F. Weitere Informationen finden Sie hier: www.yubico.com.

Yubico AB
Kungsgatan 44
2. Stock
SE-111 35 Stockholm
Schweden

Yubico Inc.
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054
USA