yubico

YubiKey 5 FIPS-Series:

Der Multiprotokoll-Sicherheitsschlüssel, der eine passwortlose Authentifizierung ermöglicht

Sicherheitsmaßnahmen, die lediglich auf Benutzernamen und Kennwörtern basieren, setzen Unternehmensdaten Risiken aus

Nahezu jeden Tag liest man in den Schlagzeilen von neuentdeckten, katastrophalen Datenlecks und Sicherheitsvorfällen. Und das aus gutem Grund: es wird erwartet, dass die weltweiten Kosten für Cyberkriminalität in den nächsten Jahren um 15 Prozent pro Jahr steigen und bis 2025[1] jährlich 10,5 Billionen US-Dollar erreichen werden.

Hauptgrund für die meisten Sicherheitsvorfälle: Passwörter. 82% der Datenschutzverletzungen werden durch gestohlene oder schwache Passwörter verursacht.[2] IT-Organisationen sollten sich daher nicht ausschließlich auf Passwörter verlassen, um Zugang zu Unternehmensdaten zu schützen. Sie müssen stärkere Authentifizierungsmaßnahmen für Mitarbeiter und externe Dienstleister einführen – oder sie riskieren, das nächste Angriffsziel zu werden.

Die YubiKey 5 FIPS Series bietet starke Phishing-resistente MFA

Die YubiKey 5 FIPS Series macht eine starke, skalierbare Authentifizierung einfach, die die Übernahme von Kontenübernahme durch Phishing-Angriffen verhindert. Der YubiKey ist eine hardwarebasierte Lösung mit den folgenden Funktionen und Eigenschaften:

- Unterstützung mehrerer Authentifizierungs- und Kryptografieprotokolle, darunter FIDO2/WebAuthn, FIDO U2F, PIV-kompatible Smartcards und Yubico One-Time Password (OTP) zum Schutz des Mitarbeiterzugriffs auf Computer, Netzwerke und Onlineservices per Fingertipp
- Unterstützt passwortlose sichere Anmeldung mit Smartcard und FIDO2/WebAuthn-Authentifizierung
- Kompatibel mit allen gängigen Betriebssystemen, darunter Microsoft Windows, macOS, Android und Linux, sowie mit den führenden Browsern
- Erhältlich in sechs Formfaktoren, die es Nutzern ermöglichen Verbindungen über USB-A, USB-C, NFC und Lightning herzustellen

[1] Cybersecurity Ventures, Cybercrime To Cost The World $10.5 Trillion Annually By 2025
[2] Verizon, 2022 Data Breach Investigations Report
[3] Google Research, Security Keys: Practical Cryptographic Second Factors for the Modern Web

Die YubiKey 5 FIPS-Series ist die erste mit FIPS-validierte Multiprotokoll-Support inklusive FIDO2/WebAuthn Serie. Von links nach rechts: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS.

Seit 2010 schützen YubiKeys Google-Mitarbeiter

0	92%	4x	0
Konto-übernahmen	weniger Supportanfragen	schnellerer Lolgin	Konto-sperrungen

Google, Meta und Salesforce verlassen sich seit 2012 auf den YubiKey

Liefert sichere Multifaktor-Authentifizierung

Der YubiKey sorgt dank einer Kombination aus hardwarebasierter Authentifizierung und Public-Key-Kryptografie für sichere Authentifizierung und unterbindet Kontoübernahmen. Zu den Funktionen gehören FIDO2/WebAuthn und FIDO U2F, offene Authentifizierungs- standards, die von der FIDO Alliance unterstützt werden, sowie Smartcard-Funktionalität basierend auf der in NIST SP 800-73 spezifizierten PIV-Schnittstelle.

Senkt IT-Kosten

Nach der Auswertung der Daten, die durch den Einsatz von YubiKey gesammelt worden sind, stellte Google fest, dass die Benutzerfreundlichkeit und Zuverlässigkeit des Geräts die Supportfälle bezüglich Kennwörtern um 92 % reduziert hatte. So spart das Unternehmen jährlich tausende Stunden an Supportkosten.[3]

Liefert einfache, schnelle und zuverlässige Sicherheit für Mitarbeiter

YubiKey-Hardware ist zuverlässig, da sie keine Batterie oder Netzwerkverbindung erfordert. Sie ist also immer einsatzfähig und verfügbar. Die Authentifizierung erfolgt schnell mit einer einfachen Berührung. Somit ist diese Art der Authentifizierung bis zu viermal schneller, als die mobile Zwei-Faktor- und die SMS-Authentifizierung.

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 weltweit führende Unternehmen vertrauen

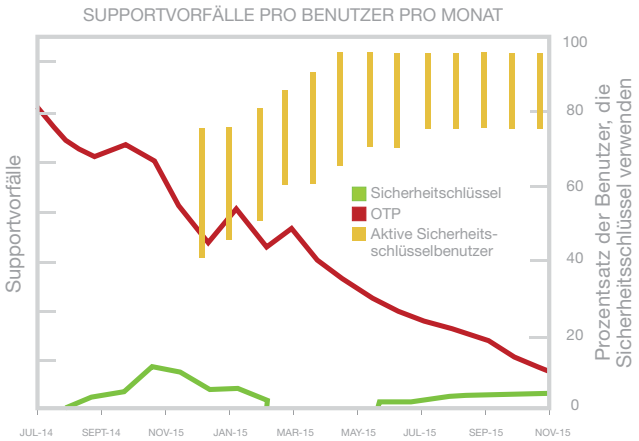
Schutz vor Phishing für die sichere Unternehmensauthentifizierung

Der YubiKey speichert das Authentifizierungs-Secret in einem sicheren Hardwarechip. Dieses Secret wird nie übertragen und kann daher nicht kopiert oder gestohlen werden.

Senkt IT-Kosten

Der YubiKey trägt zu einer wesentlichen Reduzierung der IT-Supportkosten bei. Diese sind größtenteils auf Kennwortrücksetzungen zurückzuführen, die z. B. Microsoft mehr als 12 Millionen US-Dollar monatlich kosten.[4]

Durch den Wechsel von mobilen Einmalkennwörtern zu YubiKeys konnte Google die Supportfälle bezüglich Kennwörtern um 92 % reduzieren, da YubiKeys zuverlässiger, schneller und benutzerfreundlicher sind.



Dieses Diagramm veranschaulicht, wie schnell Google Supportvorfälle bezüglich Kennwörtern nach dem Wechsel von Einmalkennwörtern zu YubiKey reduzieren konnte.[5]

Benutzerfreundlich, schnell und zuverlässig

Benutzer müssen nichts installieren – Kunden oder Mitarbeiter registrieren ihren YubiKey einfach, geben ihren Benutzernamen und ihr Kennwort ein, setzen den YubiKey ein und tippen darauf, wenn sie dazu aufgefordert werden.

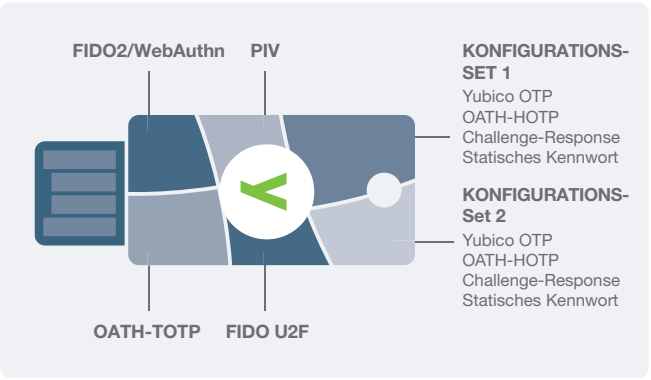
YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS und YubiKey 5C FIPS lassen sich ganz einfach an einem Schlüsselbund befestigen, während YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS im USB-Anschluss verbleiben können. So ist jeder YubiKey stets zugänglich und bietet die gleiche digitale Sicherheit. Der YubiKey 5 NFC FIPS/5 Nano FIPS ist dabei sehr robust und wasserfest.

[4] "Saying Goodbye to Passwords," Alex Simons, Manini Roy, Microsoft Ignite 2017

[5] Google Research, Security Keys: Practical Cryptographic Second Factors for the Modern Web

Einfach bereitzustellen

Die IT-Abteilung kann YubiKeys innerhalb von Tagen anstatt Monaten bereitstellen. Sie können so mit einem einzelnen Schlüssel auf die unterschiedlichsten, egal ob moderner und älterer, Systeme zugreifen, ohne dass separate Hardware oder zusätzlicher Integrationsaufwand erforderlich ist.



YubiKey Fähigkeiten: Diese Funktionen sind in den Sicherheitsschlüsseln YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS und YubiKey 5C Nano FIPS enthalten. Technische Daten finden Sie auf yubico.com.

Vertrauenswürdiger führender Authentifizierungsanbieter

Yubico ist der Hauptentwickler des Authentifizierungsstandards U2F, der von der FIDO Alliance übernommen wurde, und das erste Unternehmen, das den U2F-Sicherheitsschlüssel hergestellt hat.

YubiKeys werden in unseren Niederlassungen in den USA und Schweden hergestellt, unter Einhaltung strenger Sicherheits- und Qualitätskontrollen während des gesamten Fertigungsprozesses.

FIPS 140-2-geprüft

Schützen Sie Ihr Unternehmen mit der nach FIPS 140-2 geprüften Version (Gesamtstufe 1 und 2, Physische Sicherheitsstufe 3) der branchenführenden YubiKey-Lösung für Multifaktor-Authentifizierung. Mit der YubiKey 5 FIPS-Series können Regierungsbehörden und regulierte Branchen die Anforderungen der höchsten Sicherheitsstufe für Authentifikatoren (Authenticator Assurance Level 3, AAL3) aus den neuen NIST SP800-63B-Empfehlungen erfüllen.

Kontaktieren Sie uns
yubi.co/kontakt

Erfahren Sie mehr
yubi.co/fips-de

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.