yubico

Serie YubiKey 5 FIPS: La validación de FIPS 140-2 garantiza una seguridad robusta y conformidad normativa

La serie YubiKey 5 FIPS es la primera línea de autenticadores FIDO2/WebAuthn y multiprotocolo con validación FIPS. De izquierda a derecha: YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS y YubiKey 5C Nano FIPS.

Confiar únicamente en la seguridad de los nombres de usuario y las contraseñas pone en peligro los datos de la empresa

Las graves vulneraciones de seguridad son noticia en los titulares de todo el mundo cada día, y por una buena razón. El coste del cibercrimen global se espera que sea de $6 trillones en 2021, un incremento significativo de los $3 trilliones en 2015[1] y el 81 % de las vulneraciones son debidas a robos o a la debilidad de las contraseñas.[2] Como resultado, las organizaciones de TI no pueden confiar exclusivamente en las contraseñas para proteger el acceso a los datos corporativos. Tienen que adoptar una autenticación de empleados y proveedores más robusta o arriesgarse a convertirse en el próximo objetivo.

La serie YubiKey 5 FIPS elimina las suplantaciones de cuentas

La YubiKey FIPS facilita la implementación de una autenticación sólida y escalable que elimina la suplantación de cuentas en los ataques de phishing. La YubiKey es una solución basada en hardware que:

- Ofrece varios protocolos de autenticación y criptográficos, incluido FIDO2/WebAuthn, FIDO U2F, tarjeta inteligente compatible con la verificación de identidad personal (PIV) y la contraseña de un solo uso (OTP) de Yubico para proteger el acceso de los empleados a los ordenadores, redes y servicios en línea con un solo toque.
- Soporte para inicio de sesión seguro sin contraseña con autenticacion de tarjeta inteligente y FIDO2/WebAuthn
- Funciona en los principales sistemas operativos, incluido Microsoft Windows, macOS, iOS, Android y Linux, así como en los principales navegadores.
- Disponible en seis factores de forma que permiten a los usuarios conectarse a través de USB-A, USB-C, NFC y Lightning.

YubiKey ha sido la elección de confianza de Google, Facebook y Salesforce desde 2012

Ofrece una autenticación multifactor sólida: la YubiKey combina la autenticación basada en hardware y la criptografía de clave pública para garantizar una autenticación sólida y eliminar la suplantación de cuentas. Sus capacidades incluyen FIDO2/WebAuthn y FIDO U2F, estándares abiertos de autenticación adoptados por la FIDO Alliance, así como la funcionalidad de tarjeta inteligente basada en la interfaz PIV especificada en el NIST SP 800-73.

Reduce los costes de TI: tras evaluar los datos recopilados de una implementación de más de 50.000 YubiKeys en 70 países, Google descubrió que la facilidad de uso y la fiabilidad del dispositivo redujeron las incidencias de asistencia técnica sobre contraseñas en un 92 %. Esto permite ahorrar a la empresa miles de horas al año en costes de asistencia técnica.[3]

Proporciona una seguridad fácil, rápida y fiable para los empleados: el hardware de la YubiKey es fiable porque no requiere batería ni conectividad de red, por lo que siempre está disponible y accesible. La autenticación es rápida con un simple toque, que es cuatro veces más rápida que la autenticación de dos factores de los SMS y notificaciones push los móviles.

Desde la implementación de YubiKey en 2010, Google ha experimentado:

- Cero suplantaciones de cuentas
- Inicios de sesión 4 veces más rápidos
- Un 92 % menos de llamadas de soporte de TI

[1] Cybersecurity Ventures

[2] 2017 Data Breach Investigations Report 10th Edition, (Informe de investigaciones sobre la infracción de datos en 2017), 10.ª edición, Verizon

[3] Security Keys: Practical Cryptographic Second Factors for the Modern Web (Claves de seguridad: segundos factores criptográficos prácticos para la web moderna) de Google Inc.

Las YubiKeys ya se han implementado en:

9 de las 10 principales empresas tecnológicas internacionales

4 de los 10 principales bancos de EE. UU.

2 de los 3 principales minoristas internacionales

YubiKey: seguridad probada y fácil de usar en la que confían las principales empresas del mundo

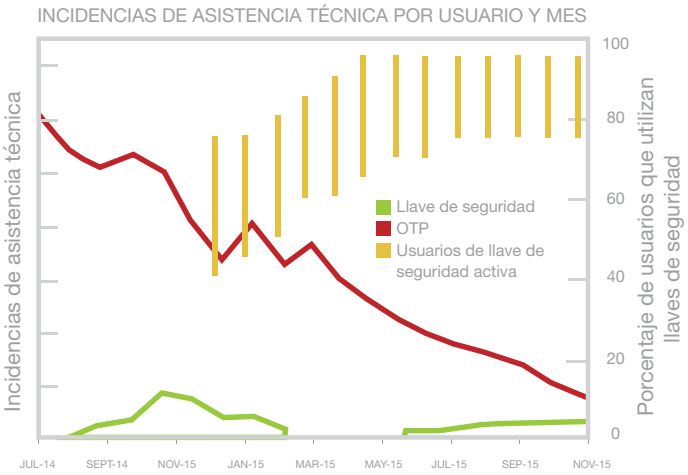
Defensa contra el phishing para una autenticación empresarial segura

La YubiKey almacena el secreto de autenticación en un chip de hardware seguro. Este secreto nunca abandona la YubiKey y, por tanto, no se puede copiar ni robar.

Reduce los costes operativos de TI

La YubiKey reduce significativamente el coste del principal caso de asistencia de TI, el restablecimiento de contraseñas, que le cuesta a Microsoft más de 12 millones de dólares al mes.[4]

Al cambiar de las contraseñas OTP para móviles a las YubiKey, Google redujo las incidencias de asistencia técnica sobre contraseñas en un 92 %, ya que las YubiKey resultaron más fiables, rápidas y fáciles de usar.



Este gráfico ilustra la rapidez con la que Google redujo las incidencias de asistencia técnica sobre contraseñas tras pasar de OTP a YubiKey.[5]

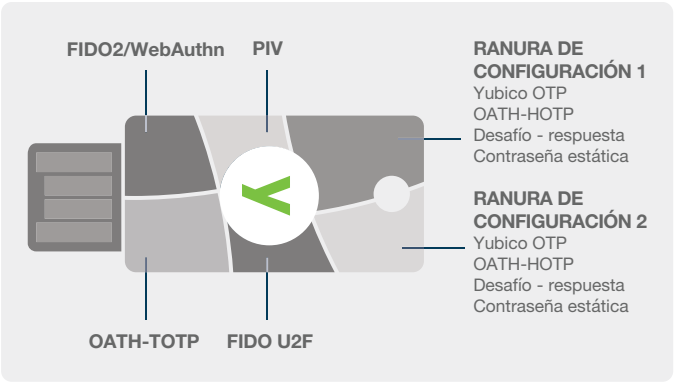
Fácil de usar, rápida y fiable

Los usuarios no necesitan instalar nada: los clientes o empleados simplemente registran su YubiKey, introducen su nombre de usuario y contraseña como de costumbre, conectan la YubiKey y la tocan cuando se les indica.

Las YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS y YubiKey 5C FIPS se pueden llevar cómodamente en un llavero, mientras que la YubiKey 5 Nano FIPS y la YubiKey 5C Nano FIPS se han diseñado para permanecer en el puerto USB. Esto garantiza que se puede acceder fácilmente a todas las YubiKey y que se proporciona el mismo nivel de seguridad digital. Las YubiKey 5 NFC FIPS / 5 Nano FIPS son resistentes al aplastamiento y al agua.

Fácil de implementar

El departamento de TI puede implementar YubiKeys en cuestión de días, no en meses. Una sola llave puede acceder a varios sistemas tanto modernos como heredados, lo que elimina la necesidad de llaves diferenciadas o de un trabajo de integración adicional.



Capacidades de la YubiKey: estas funcionalidades están incluidas en las llaves de seguridad YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS, YubiKey 5C FIPS, YubiKey 5 Nano FIPS y YubiKey 5C Nano FIPS. Las especificaciones técnicas están disponibles en yubico.com.

Líder de confianza en autenticación

Yubico es el principal inventor del estándar de autenticación U2F adoptado por la alianza FIDO y es la primera empresa en fabricar la llave de seguridad U2F.

Las YubiKey se han implementado en 9 de las 10 principales empresas tecnológicas mundiales, 4 de los 10 principales bancos de EE. UU. y 2 de los 3 principales minoristas mundiales.

La YubiKey se fabrica en nuestras oficinas de EE. UU. y Suecia, por lo que mantenemos la seguridad y el control de calidad en todo el proceso de fabricación.

FIPS 140-2 validada

Proteja su empresa con la versión validada FIPS 140-2 (nivel general 1 y 2, nivel 3 de seguridad física) de YubiKey; lasolución de autenticación multifactor líder del sector. La serie YubiKey FIPS permite a las agencias gubernamentales y a los sectores regulados cumplir con los más altos requisitos del nivel 3 de garantía de autenticidad (AAL3) de la nueva directriz NIST SP800-63B.

[4] "Saying Goodbye to Passwords" (Adiós a las contraseñas) de Alex Simons y Manini Roy, Microsoft Ignite 2017

[5] Security Keys: Practical Cryptographic Second Factors for the Modern Web (Claves de seguridad: segundos factores criptográficos prácticos para la web moderna) de Google Inc.

Acerca de Yubico Yubico establece nuevos estándares globales para el acceso fácil y seguro a ordenadores, servidores y cuentas de internet. Fundada en 2007, Yubico es una empresa privada con oficinas en Alemania, Australia, Estados Unidos, Reino Unido, Singapur y Suecia. Descubra por qué 9 de las 10 principales marcas de internet y millones de usuarios en más de 160 países utilizan nuestra tecnología en www.yubico.com

Yubico AB
Kungsgatan 44
2 ° piso
SE-111 35 Estocolmo
Suecia

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (número gratuito)
650-285-0088