INFINYT

YubiKey 5 FIPS Series:
La certificación FIPS 140-2 garantiza seguridad sólida y cumplimiento

Depender únicamente de la seguridad del nombre de usuario y la contraseña pone en riesgo los datos de la empresa

Los titulares de los principales medios del mundo informan diariamente de catastróficos ataques de seguridad. Se espera que el costo del delito cibernético global sea de $ 6 billones en 2021, un aumento de $.

3 billones en 20151, y el 81% de los ataques son causados por contraseñas robadas o débiles.2 Como resultado, las organizaciones de TI no pueden confiar exclusivamente en contraseñas para proteger el acceso a datos corporativos. Deben adoptar una autenticación más sólida de empleados y proveedores, o corren el riesgo de convertirse en el próximo objetivo

La Familia YubiKey 5 FIPS elimina el robo de cuentas

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

- Ofrece múltiples protocolos de autenticación y criptográficos, incluidos FIDO2 / WebAuthn, FIDO U2F, Smart Card compatible con verificación de identidad personal (PIV) y contraseña de un solo uso (OTP) de Yubico para proteger el acceso de los empleados a computadoras, redes y servicios en línea con solo un toque.
- Admite inicio de sesión seguro sin contraseña con tarjeta inteligente y autenticación FIDO2 / WebAuthn.
- Funciona en los principales sistemas operativos, incluidos Microsoft Windows, macOS, Android y Linux, así como en los principales navegadores.
- Disponible en una selección de seis formatos que permiten a los usuarios conectarse a través de USB-A, USB-C, NFC y Lightning.

La YubiKey 5 FIPS es la primera línea de autenticadores multiprotocolo FIDO2 / WebAuthn validados por 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

Google, Facebook y Salesforce confían en Yubikey desde 2012

Ofrece una sólida autenticación multifactor:
La YubiKey combina la autenticación basada en hardware y la criptografía de clave pública para garantizar una autenticación sólida y eliminar el robo de cuentas. Las capacidades incluyen FIDO2 / WebAuthn y FIDO U2F, estándares de autenticación abiertos compatibles con FIDO Alliance, así como funcionalidad de Smart Card basada en la interfaz PIV especificada en NIST SP 800-73.

Reduce los costos de TI:
Después de 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 confiabilidad del dispositivo redujeron los incidentes de soporte de contraseñas en un 92%. Esto le ahorra a la empresa miles de horas al año en costos de soporte.3

Proporciona seguridad fácil, rápida y confiable para los empleados:
El hardware de YubiKey es confiable porque no requiere batería ni conectividad de red, por lo que siempre está encendido y accesible. La autenticación es rápida con un simple toque que es cuatro veces más rápido que la autenticación de dos factores por SMS y móvil.

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

- Cero robo de cuentas
- Inicio de sesion 4 veces más rápido
- Reducción de llamadas de soporte de 92%

YubiKeys instalados en:

- **4 de los principales 10 bancos de USA**
- **9 de las 10 principales empresas de tecnología**
- **2 de los 3 principales minoristas globales**

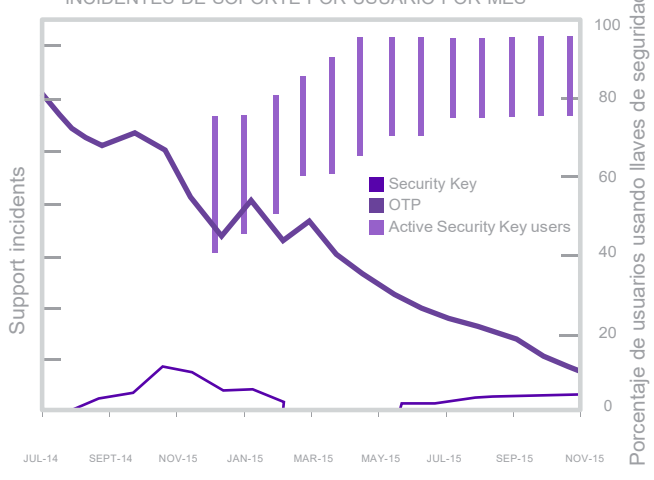
YubiKey: Seguridad probada y fácil de usar en la que confían las empresas líderes del mundo

Defensa contra el phishing para una autenticación segura

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

Reduce los costos de TI

La YubiKey reduce drásticamente el principal costo de soporte de TI (restablecimiento de contraseñas) que le cuesta a Microsoft más de $ 12 millones por mes.4
Al cambiar de OTP móviles a YubiKeys, Google redujo los incidentes de soporte de contraseñas en un 92% porque las YubiKeys son más confiables, más rápidas y más fáciles de usar.



Este gráfico ilustra la rapidez con la que Google redujo los incidentes de soporte de contraseñas después de cambiar de OTP a YubiKey[5]

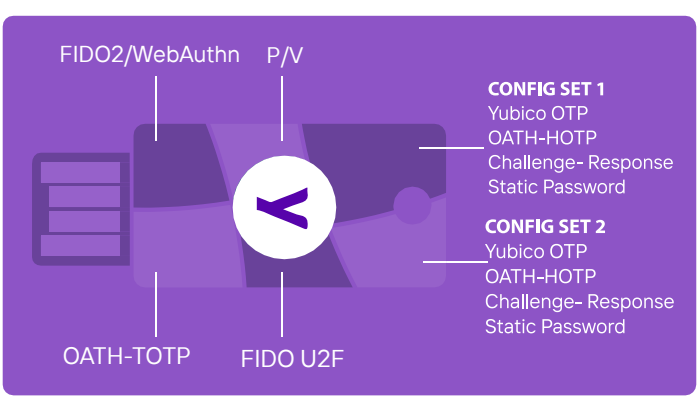
Fácil de usar , Rápido y Confiable

Los usuarios no necesitan instalar nada; los clientes o empleados simplemente registran su propia YubiKey, ingresan su nombre de usuario y contraseña como de costumbre, y conectan y presionan YubiKey cuando se les solicite.

La YubiKey 5 NFC FIPS, YubiKey 5C NFC FIPS, YubiKey 5Ci FIPS y YubiKey 5C FIPS entran cómodamente en un llavero, mientras que las YubiKey 5 Nano FIPS y YubiKey 5C Nano FIPS están diseñadas para permanecer en el puerto USB. Esto asegura que cada YubiKey sea de fácil acceso y proporcione el mismo nivel de seguridad digital. Las YubiKey 5 NFC FIPS / 5 Nano FIPS son resistentes a golpes y al agua.

Fácil de Implementar

TI puede implementar YubiKeys en días, no en meses. Una sola llave puede acceder a varios sistemas modernos o heredados, lo que elimina la necesidad de llaves separadas o trabajo de integración adicional.



Líder de autenticación confiable

Yubico es uno de los inventores del estándar de autenticación U2F adoptado por la alianza FIDO y fue la primera empresa en producir una llave de seguridad U2F.
Las YubiKeys se implementan en nueve de las 10 principales empresas de tecnología mundial, cuatro de los 10 principales bancos de EE. UU. Y dos de los tres principales minoristas mundiales.

Las YubiKeys se fabrican en nuestras plantes de EE. UU. Y Suecia, manteniendo la seguridad y el control de calidad durante todo el proceso de fabricación.

Certificación FIPS 140-2
Proteja su organización con FIPS 140-2 niveles generales 1 y 2 y la versión validada de seguridad física nivel 3 de la solución de autenticación multifactor líder en la industria, YubiKey. La familia Yubikey 5 FIPS permite que las agencias gubernamentales y las industrias reguladas cumplan con los requisitos más altos de seguridad del autenticador de nivel 3 (AAL3) de la nueva guía NIST SP800-63B.

INFINYT

Seguridad Inteligente

+ 52 (81) 2474 5555
info@infinyt.mx
INFINYT.MX