INFINYT

YubiKey FIPS Series:
La certificación FIPS 140-2 garantiza una seguridad robusta y cumplimiento

Confiar únicamente en la seguridadde nombre de usuario y contraseña pone en riesgo los datos de la empresa

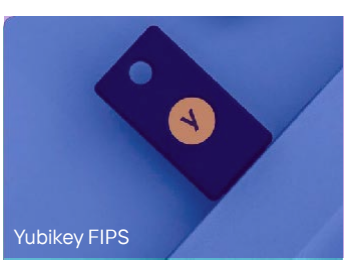
Violaciones importantes de seguridad son titulares en los periódicos cada día, y por buenas razones. Una sola violación de seguridad corporativa cuesta un promedio de $ 3.62M1, y el 81% de las violaciones son causadas por contraseñas robadas o débiles.2 Como resultado, las organizaciones de TI no pueden confiar exclusivamente en las contraseñas para proteger el acceso a los datos corporativos. Tienen que adoptar una autenticación más fuerte con empleados y proveedores, o arriesgarse a convertirse en el próximo objetivo.

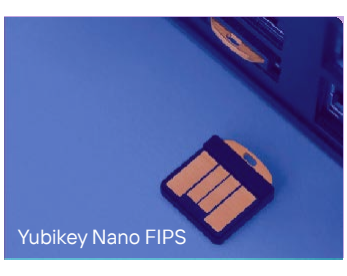
YubiKey elimina el robo de cuentas

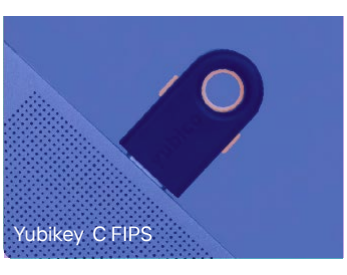
YubiKey facilita la implementación de una autenticación fuerte y escalable que elimina los robos de cuentas por ataques de phishing. YubiKey es una solución basada en hardware que:

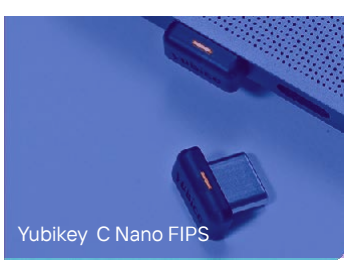
- Ofrece múltiples protocolos de autenticación criptográficos, incluidos FIDO Universal 2nd Factor (U2F), Smart Card compatible con verificación de identidad personal (PIV) y contraseña única de Yubico (OTP) para proteger el acceso de los empleados a computadoras, redes y servicios en línea con solo uno toque.
- Soporta inicio de sesión seguro sin contraseña con autenticación de Smart Card Funciona en los principales sistemas operativos, incluidos Microsoft Windows, macOS, Android y Linux, así como en los principales navegadores.
- Disponible en una selección de cuatro formas que permiten a los usuarios conectarse a través de USB

.


Yubikey FIPS


Yubikey Nano FIPS


Yubikey C FIPS


Yubikey C Nano FIPS

Google, Facebook y Salesforce confían en Yubikey desde 2012

Ofrece una sólida autenticación multifactor:

:La YubiKey combina autenticación basada en hardware y criptografía de clave pública para garantizar una autenticación sólida y eliminar los robos de cuentas. Las capacidades incluyen U2F, un estándar de autenticación abierto compatible con FIDO Alliance, así como la 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 compañía miles de horas por año en costos de soporte.3

Proporciona seguridad fácil, rápida y confiable para los empleados:

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

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**

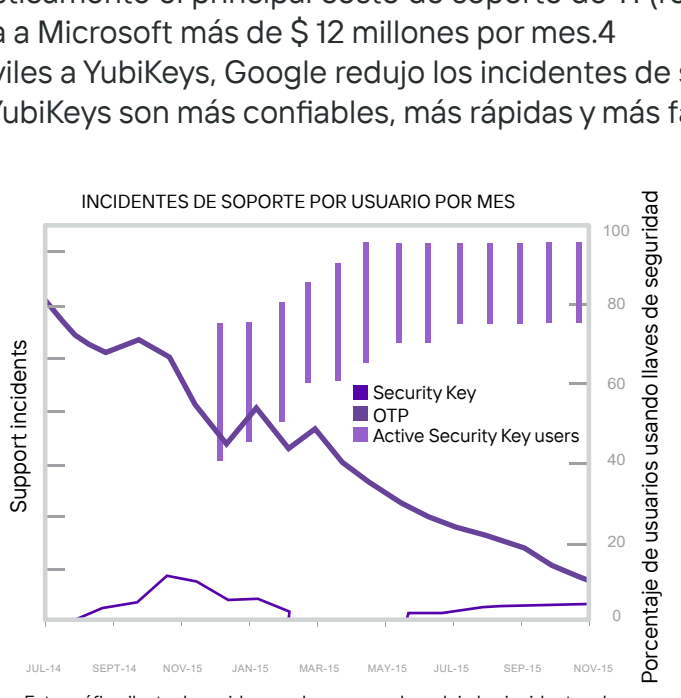
YubiKey: Seguridad probada y fácil de usar en la que confían las empresas líderes del mundo

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 contraseña después de cambiar de OTP a YubiKey[5]

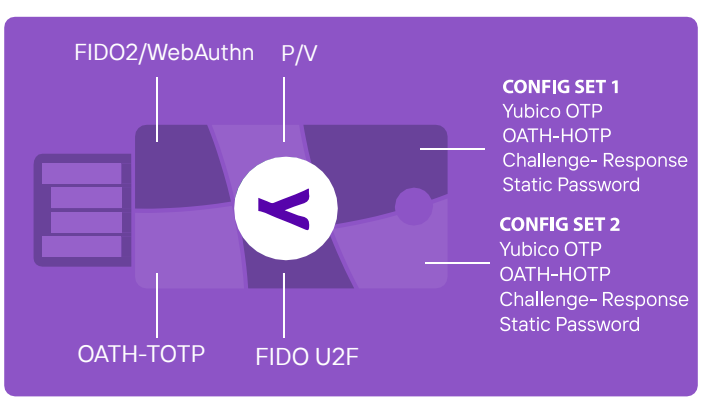
Fácil de usar , Rápido y Confiable

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, se conectan y tocan la YubiKey cuando se les solicita.

La YubiKey FIPS y la YubiKey C FIPS se ajustan convenientemente a un llavero, mientras que la YubiKey Nano FIPS y la YubiKey C Nano FIPS están diseñadas para permanecer en el puerto USB. Esto garantiza que cada YubiKey sea de fácil acceso y proporcione el mismo nivel de seguridad digital. Las YubiKey FIPS / Nano FIPS son resistentes a los 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 y 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 compañía en producir la llave de seguridad U2F.
Las YubiKeys se implementan en nueve de las 10 principales compañías tecnológicas mundiales, cuatro de los 10 principales bancos estadounidenses y dos de los tres principales minoristas mundiales.

.

Las YubiKeys se producen en nuestras oficinas en los EE. UU. Y Suecia, manteniendo la seguridad y el control de calidad en todo el proceso de fabricación.

Certificación FIPS 140-2
Proteja su organización con la versión certificada FIPS 140-2 (Nivel general 2, Nivel de seguridad física 3) de la solución de autenticación multifactor líder de la indutria YubiKey. La Yubikey FIPS Series permite que las agencias gubernamentales y las industrias reguladas cumplan con los requisitos más altos de garantía de autentificación nivel 3 (AAL3) de la nueva guía NIST SP800-63B.

INFINYT

Seguridad Inteligente

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