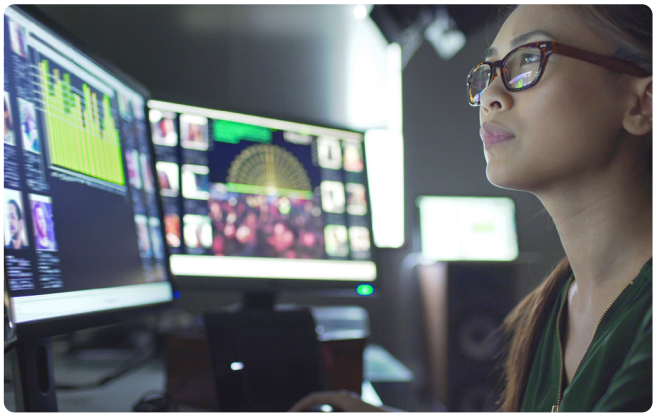
yubico

Cómo proteger mejor su entorno con restricciones para móviles



¿Qué es un entorno con restricciones para móviles y qué requisitos únicos plantea?

El término “con restricciones para móviles” describe cualquier entorno en el que los dispositivos móviles no se permiten, no son fiables o deben limitarse por cuestiones de seguridad. Casi todas las organizaciones tienen algún caso de uso en el que los dispositivos móviles no están permitidos o no se pueden usar. Además, el flujo constante de ciberdelitos que aparecen en las noticias recientemente han llevado a los equipos de seguridad a pensar de manera más estratégica en la forma de proteger estos espacios de trabajo confidenciales.

Los entornos con restricciones para móviles se pueden encontrar en una amplia variedad de sectores e industrias que cuentan con estos entornos, donde los teléfonos móviles están restringidos por motivos de seguridad. Estos entornos se pueden encontrar en sectores como los servicios financieros, la fabricación, el comercio minorista y la hostelería, además de en entornos laborales específicos que existen en cada sector, como los centros de llamadas. El concepto de “con restricciones para móviles” también se puede aplicar a cualquier entorno en el que los problemas de conectividad puedan dificultar la colaboración o la productividad, como en el sector de la energía y los recursos naturales, en el que el trabajo se puede llevar a cabo en ubicaciones sin conectividad móvil. En todas estas situaciones, la autenticación de los usuarios mediante autenticación de múltiples factores (MFA) heredada, como la autenticación móvil, simplemente no es una opción viable. Por lo tanto, las organizaciones deben buscar formas modernas y eficaces de autenticar de forma segura a los usuarios antes de darles acceso a los recursos confidenciales.

Consideraciones clave a la hora de elegir la solución de MFA ideal

Jualquier solución de autenticación para un entorno con restricciones para móviles debe equilibrar los dos polos de seguridad y facilidad de uso. Dónde reside este equilibrio depende de las condiciones sobre el terreno, las necesidades de acceso de los usuarios y los requisitos y estándares del sector en concreto. No obstante, una buena regla general es preguntar qué nivel de “factor agobio” pueden soportar sus usuarios antes de empezar a no cumplir los procedimientos o empezar a buscar atajos.

Utilice la siguiente información como lista de comprobación para ver si la solución de autenticación que está considerando cumple los requisitos críticos de una situación con restricciones para móviles.

Adaptable para estaciones de trabajo compartidas

Los entornos con restricciones para móviles a menudo incluyen estaciones de trabajo compartidas y dichas estaciones pueden tener requisitos de inicio y cierre de sesión específicos. En el pasado, las empresas empleaban procedimientos de seguridad físicos en estos entornos, pero para disfrutar de una seguridad más sólida, los protocolos físicos se deben complementar con autenticación a prueba de phishing también en las estaciones de trabajo.

Ofrezca dispositivos reforzados que no requieren conectividad móvil

En los lugares de trabajo al aire libre o remotos, los dispositivos de seguridad deberán soportar los impactos físicos y las condiciones climáticas. Incluso un entorno de oficina habitual puede ser duro para los dispositivos, ya que los usuarios pueden dejarlos caer o derramar bebidas sobre ellos. Los dispositivos reforzados deben ser capaces de funcionar en cualquier situación, sin conectividad móvil, y proteger una variedad de ordenadores y otros puntos finales que funcionan sin conexión o en la red.

Ofrezca una experiencia de usuario fácil

A menudo se suele ignorar a los usuarios a la hora de buscar una solución. Asegúrese de revisar los comentarios de las encuestas a usuarios y encuentre a un buen escritor y comunicador en su equipo de implementación interno para preparar a los usuarios para el cambio con antelación. Hacer que este sistema sea útil debe ser tan importante como hacer que sea seguro, ya que una cosa no se puede conseguir sin la otra.

Compatibilidad con entornos complejos

No existe una solución que sirva para la mayoría de las ubicaciones. Se deben considerar diferentes protocolos si la

Se han implementado YubiKeys en:

9 de las 10 empresas tecnológicas mundiales

4 de los 10 principales bancos de EE. UU

5 de los 10 principales minoristas internacionales

solución se debe adaptar fácilmente a lo que ya existe. Las organizaciones que quieren modernizar la seguridad en sus entornos con restricciones para móviles y que utilizan principalmente una infraestructura local podrían optar por un enfoque de seguridad basado en tarjetas inteligentes, mientras que aquellas que utilizan principalmente un entorno basado en la nube pueden plantearse un enfoque basado en FIDO. Si las organizaciones quieren cambiar a la autenticación sin contraseña, deberían optar por una solución que permita ambas situaciones (sin contraseña mediante tarjeta inteligente o sin contraseña mediante FIDO) como estrategia de seguridad preparada para el futuro.

Ofrezca una seguridad sólida

La solución debe garantizar una alta confianza del mecanismo de autenticación en sí. La alta confianza se consigue asegurándose de que el proveedor tenga un proceso de fabricación y cadena de suministro seguro. Si el equipo de seguridad del proveedor puede demostrar una seguridad sólida en toda su cadena de suministro y sigue los protocolos adecuados de firma de código, puede estar un poco más tranquilo. Además, es importante habilitar redes de seguridad contra la mayor sofisticación, ya que los atacantes son cada vez más audaces e idean sistemas que se aprovechan de los errores humanos. Una solución debe ir por delante de la innovación maliciosa, empleando políticas contra el phishing o autenticación para ofrecer una barrera contra cualquier ataque de ransomware o malware

Capaz de garantizar el cumplimiento de las normativas en el futuro

Los futuros requisitos de cumplimiento son algo que los líderes deben vigilar siempre de cerca. De cara al futuro, las mayores normativas de cumplimiento dictarán que las organizaciones avancen hacia enfoques de MFA resistente al phishing, en todos los entornos, incluidos los entornos con restricciones para móviles. Se pasará de los enfoques basados en OTP, que son vulnerables al phishing, a los enfoques basados en PIV (tarjetas inteligentes) y FIDO2/WebAuthn, que son muy resistentes al phishing.

Por qué las YubiKeys son una solución ideal para los entornos con restricciones para móviles

Las YubiKeys no requieren la instalación de software de cliente y no necesitan baterías. Alguien que trabaja en un entorno con restricciones para móviles solo tiene que conectarla a un puerto USB y tocar el botón o “tocar y listo” mediante NFC para una autenticación segura. Las YubiKeys no tienen pantallas que se puedan romper, no necesitan conexión móvil y son resistentes al agua y al aplastamiento (índice de protección IP68). Todas estas cualidades son útiles en un entorno con restricciones para móviles que puede presentar algunos peligros físicos (por ejemplo, las instalaciones de trabajo de una fábrica o una ubicación al aire libre).

Al permitir varios protocolos de autenticación en una sola YubiKey, como OTP y OpenPGP, y protocolos de autenticación sólidos como tarjetas inteligentes, FIDO U2F y FIDO2/WebAuthn, una YubiKey ofrece a las organizaciones la flexibilidad para implementar una autenticación sólida utilizando una única llave en una variedad de infraestructuras heredadas y modernas, para ayudar a las organizaciones sin importar en qué parte de su proceso para dejar de usar contraseñas se encuentren.

Cuando la autenticación móvil no es una opción, la versatilidad de una YubiKey permite trabajar perfectamente en una amplia variedad de entornos de trabajo confidenciales y remotos, donde la autenticación siempre activa es indispensable.

Una YubiKey ofrece la comodidad necesaria para ayudar a los empleados que en la actualidad trabajan en persona, a distancia o de forma híbrida. Es cómoda de usar en áreas con y sin restricciones para móviles, y ofrece un enfoque de MFA resistente al phishing coherente y sólido en todos los entornos.

Resumen

Para lograr el equilibrio adecuado en un espacio con restricciones para móviles, Yubico recomienda conocer primero las necesidades únicas de ese espacio, establecer un amplio equipo interno para revisar los requisitos (además de la experiencia y los comentarios de los usuarios), y luego trabajar con un proveedor de confianza para instalar una solución en ambos polos: productividad y seguridad.

Es bien sabido que los métodos de MFA tradicionales, como OTP y los tokens digitales, tienen brechas notables en las que se pueden iniciar ataques. La autenticación móvil no es una solución superior en cualquier entorno, con o sin restricciones para móviles. Las llaves de seguridad basadas en hardware pueden ofrecer la mejor solución en un entorno con restricciones para móviles.

Las YubiKeys llevan protegiendo a los empleados de Google desde 2009

0	92%	4x	0
apropiaciones de cuentas	menos de incidentes de asistencia	más rapidez para iniciar sesión	bloqueos de cuentas[1]

Contacto
yubi.co/contactar

Leer más
yubi.co/yk5-es

[1] Yubico, Google defends against account takeovers and reduces IT costs