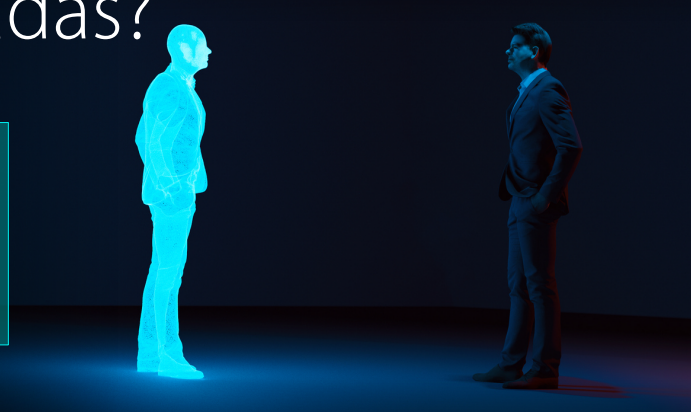
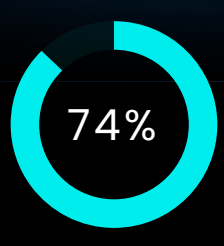
¿Sus Prácticas de Seguridad de la Identidad están actualizadas?



La CISA (Agencia de Seguridad de Infraestructura y Ciberseguridad) incluye autenticación de un solo factor en su lista de Malas Prácticas de Ciberseguridad.[1]

¿POR QUÉ?

El 74% de las vulneraciones de 2022, incluidas las credenciales robadas, involucraron el elemento humano, según el Data Breach Investigations Report de Verizon de 2023.[2]



¿CÓMO DEBE RESPONDER?

Las autoridades de ciberseguridad de los EE. UU., Nueva Zelanda, Canadá, los Países Bajos y el Reino Unido dicen que utilizar una MFA y políticas de contraseñas sólidas para fortalecer las credenciales son las mejores prácticas contra el crecimiento de los ciberataques.[3]

★ Beneficio adicional: Implementar prácticas de seguridad de la identidad sólidas lo ayudará a calificar para las mejores tarifas de seguro de ciberseguridad.

[1] https://www.cisa.gov/BadPractices
[2] https://www.verizon.com/business/resources/reports/dbir/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa22-137a

Cinco Preguntas que lo Ayudarán a Elegir la Solución de Seguridad de la Identidad Adecuada

1. ¿La solución de MFA utiliza la verificación basada en SMS como la opción de autenticación principal o predeterminada?

   La verificación basada en SMS es menos segura que otros métodos porque es vulnerable al secuestro.

2. ¿Es compatible con la autenticación sin conexión?

   Los empleados necesitan acceder a sus computadoras portátiles sin conexión a Internet (ya sea mientras están en un avión, cuando se conectan a la red de un hotel o a un Wi-Fi público, o cuando una conexión a Internet es irregular) y, para ello, se requiere la autenticación sin conexión.

3. ¿Brinda un inicio de sesión único en la Web seguro (SSO)?

   El inicio de sesión único en la Web no solo facilita la solución, sino que también la hace más segura. El inicio de sesión único en la Web permite a su empresa implementar diversas aplicaciones en la nube y que los usuarios solo inicien sesión una vez para acceder a ellas, lo cual reduce la cantidad de contraseñas, restablecimientos y llamadas al servicio de asistencia, y aumenta la felicidad de los empleados.

4. ¿Incluye herramientas de administración de credenciales, como un administrador de contraseñas y supervisión de dark web?

   Gracias a la amplia adopción de contraseñas que se debe a más de 20 años de desarrollo de sistemas y aplicaciones, las contraseñas llegaron para quedarse… y son uno de los factores en la MFA. Los servicios de administración de credenciales mejoran la seguridad mediante herramientas para aumentar la protección contra los riesgos inherentes del manejo de contraseñas poco seguras.

5. ¿Cuánto cuesta la solución?

   Los productos gratuitos y de bajo costo para el consumidor pueden ser tentadores, y los precios pueden estar ocultos en grandes paquetes de software de SO; por eso, es importante evaluar los costos directos e indirectos con el objetivo de obtener un panorama completo. ¿Está incluido el soporte, tanto técnico como de administración de suscripciones? ¿Hay software adicional para el cual se necesitará licencia? ¿Tiene una interfaz de administración que permite la administración corporativa, la generación de reportes y la visibilidad, o está agobiando a su equipo de seguridad de TI con pasos y costos adicionales? ¿Están aumentando los costos del servicio de asistencia debido a los déficits de facilidad de uso?

Comience a usar hoy mismo AuthPoint Total Identity Security de WatchGuard

- Administrador de Contraseñas Corporativas
- Supervisor de Dark Web
- Autenticación Multifactor

Una Respuesta Para Mantener la Verdadera Identidad

Para obtener más información, hable con su distribuidor autorizado de WatchGuard o visite https://www.watchguard.com/es/wgrd-products/authpoint

ACERCA DE WATCHGUARD

WatchGuard® Technologies, Inc. es un líder mundial en ciberseguridad unificada. Nuestra Unified Security Platform® está diseñada exclusivamente para que los proveedores de servicios administrados brinden una seguridad de primer nivel que permita aumentar la escala y la velocidad de su negocio y, al mismo tiempo, mejorar la eficiencia operativa. Los productos y servicios galardonados de la empresa, elegidos por más de 17.000 revendedores de seguridad y proveedores de servicios para proteger a más de 250.000 clientes, abarcan seguridad e inteligencia de red, protección avanzada de endpoints, autenticación multifactor y Wi-Fi seguro. Juntos, ofrecen cinco elementos que son vitales en una plataforma de seguridad: seguridad integral, conocimiento compartido, claridad y control, alineación operativa y automatización. La empresa tiene su oficina central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, Asia-Pacífico y Latinoamérica. Para obtener más información, visite **WatchGuard.com/es.**

N.º de pieza WGCE67607_092122