AuthPoint

MFA Poderosamente Sencilla

En vistas del panorama de seguridad actual, la táctica principal que utilizan los hackers para vulnerar recursos de red es el robo de credenciales. De hecho, las contraseñas robadas o poco seguras son la causa principal del 80% de los casos de vulneración de datos*. La autenticación multifactor es la única mejora de seguridad que necesita para proteger su negocio.

La solución de autenticación multifactor (MFA) de WatchGuard no solo protege identidades y reduce las interrupciones de red y la vulneración de datos debido a credenciales poco seguras o robadas, sino que también proporciona esta funcionalidad importante íntegramente desde la nube a fin de lograr una configuración y una administración sencillas. La tecnología de ADN móvil exclusiva de AuthPoint deja atrás la autenticación de dos factores tradicional (2FA) gracias a la incorporación de maneras innovadoras de identificación y protección. Con nuestro gran ecosistema de más de 130 integraciones de terceros, se implementa una protección sólida de manera constante en toda la red, las VPN y las aplicaciones en la nube; donde se necesite. Incluso los usuarios no técnicos consideran que la aplicación móvil AuthPoint es cómoda y fácil de usar. En última instancia, WatchGuard AuthPoint es la solución correcta en el momento adecuado a fin de convertir en realidad la MFA para las empresas con la necesidad urgente de bloquear ataques.

Autenticación de Riesgos para la Adopción del Modelo de Confianza Cero

La adopción del modelo de confianza cero no puede realizarse sin la protección de identidad y, gracias a que la autenticación basada en riesgos es un elemento central de la MFA, AuthPoint se convierte en la solución clave para cumplir el criterio "nunca confíe, siempre corrobore". Si no cuenta con políticas de riesgos, la empresa deberá activar el método de autenticación más seguro para todos los usuarios en todo momento, lo que posiblemente ocasione el desacuerdo de los usuarios en algunas áreas. Con AuthPoint, tendrá acceso a las funciones de riesgos sin costo adicional. Estas incluyen ubicaciones de red, programación de tiempo, funciones de ubicación geográfica y el exclusivo ADN móvil que previene la clonación de tokens móviles.

Un Servicio Basado en la Nube con un bajo Costo Total de Propiedad (TCO)

Las empresas con personal de TI limitado y pocos conocimientos de seguridad se benefician con la protección de la MFA que se implementa y se administra fácilmente desde la nube. AuthPoint se ejecuta en la plataforma de WatchGuard Cloud y está disponible dondequiera que esté. No hay necesidad de instalar software, programar actualizaciones ni administrar revisiones. Además, la plataforma adapta cómodamente la vista de una cuenta global única o de muchas cuentas independientes, de modo que las empresas distribuidas y los proveedores de servicios administrados puedan visualizar solo los datos relevantes para el rol de una persona.

Amplia Cobertura con SSO en la Web

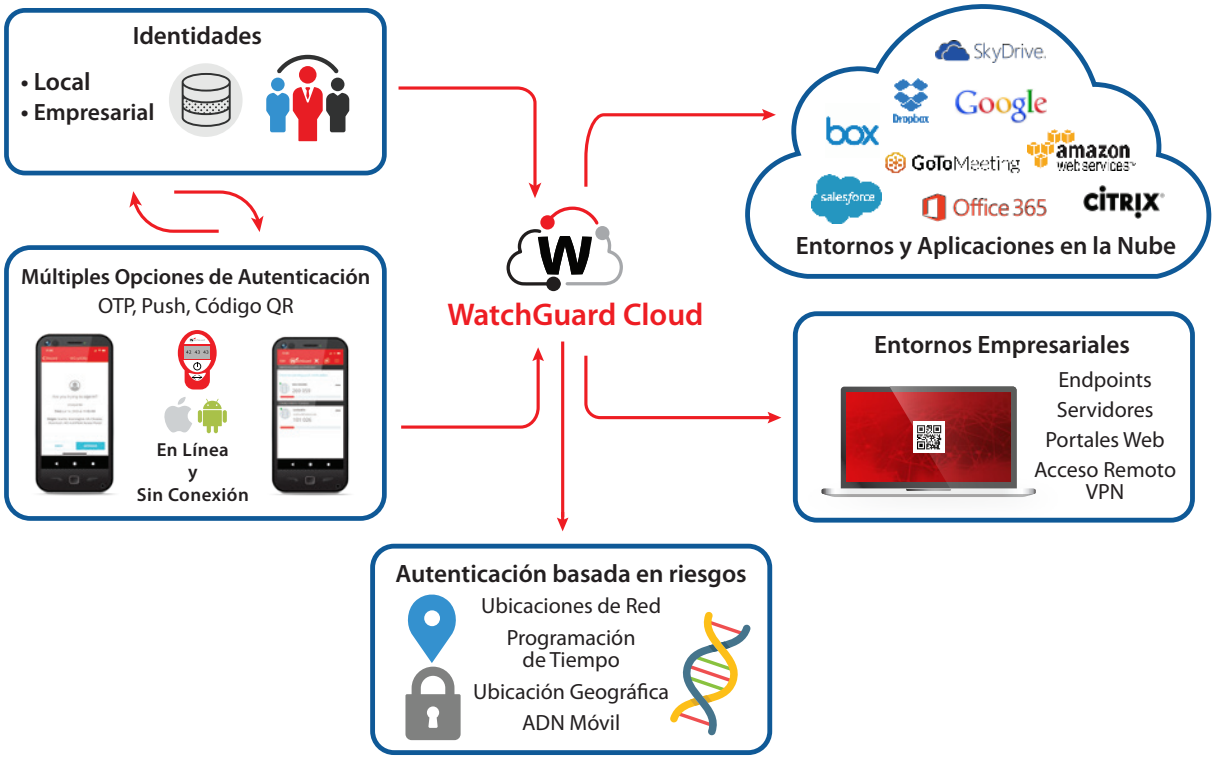
Ya no necesita preocuparse por recordar innumerables contraseñas complejas. Gracias al inicio de sesión único (SSO) seguro de AuthPoint, resulta más sencillo para los usuarios acceder a múltiples aplicaciones en la nube, VPN y redes con un solo conjunto de credenciales. Esto supera a los desafíos que presenta la fatiga de contraseñas y reduce el riesgo de vulnerabilidad de seguridad a causa de contraseñas poco seguras y los costos relacionados con el restablecimiento de contraseñas. AuthPoint cuenta con el protocolo estándar de lenguaje de marcado para confirmaciones de seguridad (SAML), lo que permite que los usuarios se registren una vez y accedan a una gran variedad de aplicaciones y servicios. Nuestra función de inicio de sesión seguro también permite la autenticación en línea y sin conexión para dispositivos Windows y Mac mediante la aplicación AuthPoint o un token de hardware.

Aplicación Móvil Optimizada y Fácil de Usar

Instale y active la aplicación AuthPoint de WatchGuard en solo unos segundos para realizar la autenticación desde su teléfono inteligente. La aplicación no solo brinda una autenticación push rápida, sino que también ofrece la función de autenticación pull para mejores uso y seguridad. También incluye la autenticación sin conexión a través de códigos QR que lee la cámara del teléfono celular. La aplicación está disponible en13 idiomas y mediante descargas gratuitas desde App Store y Google Play.

**Informe de 2020 sobre las investigaciones de pérdida de datos de Verizon*

Mantenga a los Impostores fuera de las Redes, las VPN, los Recursos en la Nube y más



Plataforma de WatchGuard Cloud

- Administración basada 100% en la nube en tres zonas
- Administración sólida de políticas basadas en riesgos
- Registros y reportes
- Acceso basado en roles de auditoría
- Interfaz de usuario intuitiva y atractiva

Aplicación Móvil AuthPoint

- Tres métodos de autenticación en uno:
  1. Mensajes push con entrega garantizada
  2. Contraseñas de un solo uso
  3. Códigos QR de desafío/respuesta
- Autenticador móvil, sin necesidad de transportar hardware adicional
- 13 idiomas
- Soporte multi-tokens
- iOS y Android: descarga gratuita
- Protección biométrica y con PIN (en algunos equipos)
- ADN de dispositivo móvil: factor de autenticación adicional
- Autoservicio de migración de token móvil a dispositivos nuevos
- Compatibilidad con tokens de terceros para proteger cuentas personales (Gmail, redes sociales, etc.)

Gateway de AuthPoint

- Gateway de red corporativa
- Sincronización y autenticación de usuarios AD y LDAP
- Proxy RADIUS

Agentes de AuthPoint

- Integración con aplicaciones de terceros sin compatibilidad nativa con la MFA
- Protección del inicio de sesión en línea, sin conexión y de protocolo de escritorio remoto (RDP) para Windows y macOS
- Agente para web de escritorio remoto y servicios de federación de Active Directory (ADFS)

Ecosistema de AuthPoint

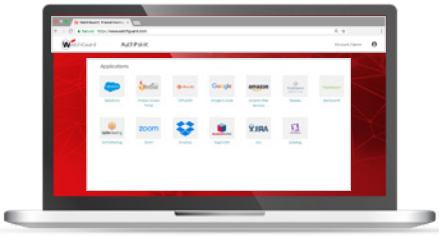
- Adicione MFA a los recursos de la nube, bases de datos, aplicaciones y recursos en la nube
- Compatibilidad con estándares SAML y RADIUS
- Más de 130 guías de integración de terceros, incluidas soluciones de administración de relaciones con el cliente (CRM) y de videoconferencias
- Integración directa de Firebox con AuthPoint para una configuración rápida de VPN
- Token de hardware de AuthPoint sin exposición de valores de inicialización de token y compatibilidad para tokens de hardware de terceros (OATH y TOTP)

Casos de Uso Recomendados

VPN/Acceso Remoto

La misma experiencia de usuario que con el nombre de usuario y la contraseña, PERO más segura y con confirmación mediante un solo clic. Se integra con cualquier firewall, pero, en especial, con las aplicaciones de uso inmediato de Firebox.

1. Solicite la conexión con el nombre de usuario y la contraseña
2. Confirme la conexión VPN solicitada mediante la aplicación AuthPoint



Aplicaciones en la Nube: SSO en la Web

1. Acceda al portal de identidad (IdP)
2. Realice la autenticación mediante OTP, push o un código QR
3. Acceda a todas las aplicaciones que tenga asignadas con una sola contraseña. No necesita volver a autenticarlas

Inicio de Sesión en PC o Conexión RDP

1. Inicie sesión en Windows/Mac con un nombre de usuario y una contraseña
2. Elija el método de autenticación que prefiera (push, código QR u OTP)
3. Autorice desde su celular para completar el inicio de sesión

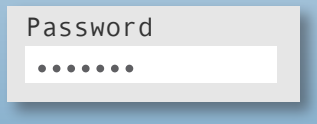
Inicio de Sesión en PC: Autenticación sin Conexión

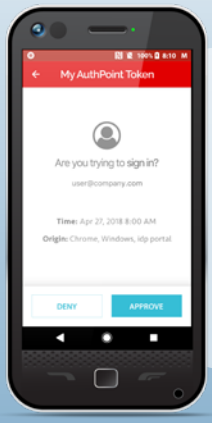
1. Inicie sesión en Windows/Mac con un nombre de usuario y una contraseña
2. Escanee el código QR (u OTP) a través de la aplicación AuthPoint
3. En este ejemplo, escribiría la respuesta 717960

¿Qué es la Autenticación Multifactor (MFA)?

Uso de 2 o más factores de autenticación, entre los siguientes:

- **Algo que conoce** (contraseña, PIN)
- **Algo que tiene** (token, teléfono móvil)
- **Una parte de su cuerpo** (huella digital, rostro)





Factores de AuthPoint:

1. **Su contraseña**
2. **Aprobación de su autenticador móvil**
3. **ADN de teléfono móvil correcto**
4. **Huella digital para acceder** (en ciertos modelos de teléfonos)

AuthPoint cumple la promesa de la MFA al limitar los riesgos empresariales asociados con las contraseñas deficientes sin resignar facilidad de uso para los empleados y el personal de TI por igual.

Todo está en el servicio en la nube, sin hardware para instalar ni software para mantener. Ahora, la MFA se considera una protección esencial, y WatchGuard la ofrece sin complicaciones.

Tom Ruffolo
CEO, eSecurity Solutions

Reduzca los Riesgos con MFA

Las contraseñas poco seguras son un enorme riesgo para su empresa. **El usuario promedio tiene casi 100 cuentas en línea**, y muchas de ellas tienen sus propios requisitos de contraseña. El uso de numerosas contraseñas es un verdadero problema y pone a su empresa en riesgo. Basta con una contraseña poco segura o que haya sido descifrada para que un criminal cibernético logre acceder a todos sus datos y sus cuentas.

¿Está seguro de que todos sus empleados utilizan las mejores prácticas para definir contraseñas?

- Se roban cerca de 250.000 contraseñas por día[1]
- Solo uno de cada cinco usuarios utiliza una única contraseña para todas sus cuentas[2]
- El 3% de las personas utilizan la contraseña 1234563[3]

> Durante 2021, las empresas que amplíen el acceso remoto con rapidez sin implementar MFA experimentarán incidentes de adquisición de cuentas cinco veces más que aquellas que utilicen MFA.
>
> Gartner, Inc., Mejorar la Seguridad de Acceso Remoto con Autenticación Multifactor y Administración de Acceso
>
> Ant Allan, Rob Smith, Michael Kelley, 6 de mayo de 2020

Una vulneración de datos puede tener un costo lo suficientemente alto como para llevar su empresa a la quiebra. El costo promedio de una vulneración de datos es de USD 148 por registro con datos relacionados a la información confidencial, lo que suma 1,38 millones de dólares si se considera que una vulneración promedio contiene 9.350 registros. Esto no incluye los costos indirectos como el daño a la reputación de la empresa, la pérdida de confianza por parte del cliente y el tiempo de trabajo perdido.

La buena noticia es que puede reducir el riesgo cibernético y aumentar el rendimiento de la inversión en seguridad fácilmente. Ofrecer protección mensual de MFA a cada uno de sus empleados cuesta menos que un desayuno en Starbucks. Use AuthPoint y elimine el principal riesgo para su empresa.

¿Quiere probarlo? Visite watchguard.com/TryAuthPoint o comuníquese con uno de nuestros especialistas designados para realizar una prueba gratuita de 30 días.

1 https://breachalarm.com/
2 https://www.statista.com/statistics/763091/us-use-of-same-online- passwords/
3 https://www.techspot.com/news/77864-worst-passwords-2018-revealed-123456-retains- top-spot.html

LA UNIFIED SECURITY PLATFORM™ DE WATCHGUARD

Seguridad de Red

Las soluciones de Seguridad de Red de WatchGuard están diseñadas desde el inicio para ser fáciles de implementar, usar y administrar, además de brindar la mayor seguridad posible. Nuestra propuesta única para la seguridad de redes se centra en brindar la mejor seguridad de tipo empresarial de su clase a cualquier organización, independientemente de su magnitud o capacidad técnica.

Autenticación Multifactor

WatchGuard AuthPoint® es la solución correcta para abordar la brecha de seguridad basada en contraseñas con la autenticación multifactor en una plataforma de nube fácil de usar. El enfoque exclusivo de WatchGuard agrega el "ADN del teléfono móvil" como factor de identificación para garantizar que solo las personas correctas tengan acceso a las redes confidenciales y a las aplicaciones en la nube.

Wi-Fi Seguro en la Nube

La solución Secure Wi-Fi de WatchGuard, una verdadera innovación en el mercado actual, está diseñada para proporcionar un espacio aéreo seguro y protegido para los entornos de Wi-Fi, a la vez que elimina los problemas administrativos y reduce los costos en gran medida. Cuenta con herramientas de interacción amplias y visibilidad de análisis empresarial, y proporciona la ventaja competitiva que su empresa necesita para tener éxito.

Seguridad de Endpoints

La Seguridad de Endpoints de WatchGuard es un portafolio avanzado de seguridad de endpoints, nativo de la nube, que protege a las empresas contra cualquier tipo de ataque cibernético presente y futuro. Su principal solución, WatchGuard EPDR, impulsada por la inteligencia artificial, mejora de inmediato la posición de seguridad de las organizaciones. Combina las capacidades de protección de endpoints (EPP) y detección y respuesta de endpoints (EDR) con el servicio de confianza cero de aplicaciones y el de búsqueda de amenazas.

Más información

Para conocer más detalles, comuníquese con un revendedor autorizado de WatchGuard o visite **www.watchguard.com**.

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de red, seguridad de endpoint, Wi-Fi seguro, autenticación multifactor y servicios de inteligencia de red. Más de 18.000 revendedores de seguridad y proveedores de servicios de todo el mundo confían en los productos y los premiados servicios de la empresa para proteger a más de 250.000 clientes. La misión de WatchGuard es lograr que empresas de todos los tipos y tamaños accedan de manera sencilla a una seguridad de calidad empresarial. Por ello, WatchGuard es una solución ideal para las medianas empresas y para empresas distribuidas. La empresa tiene su sede central en Seattle, Washington, y posee oficinas en Norteamérica, Europa, el Pacífico y Latinoamérica. Para obtener más información, visite WatchGuard.com/es.