Motivos Principales para Comprar WatchGuard Identity Security

AuthPoint Identity Security incluye autenticación multifactor (MFA), capacidades avanzadas de generación de contraseñas y bóvedas de contraseñas seguras. AuthPoint brinda a las empresas las herramientas que necesitan para mantenerse seguras en un mundo cada vez más digital. Además, nuestra función de supervisión de dark web ayuda a las empresas a mantenerse a la vanguardia en la detección de credenciales comprometidas antes de que puedan usarse de forma maliciosa.

Características y Beneficios Clave de AuthPoint Identity Security

Desbloquee capacidades avanzadas de generación de contraseñas y seguimiento de dark web para ayudar a proteger las credenciales corporativas

Servicio de MFA Premiado

La MFA de AuthPoint, que se implementa a través de WatchGuard Cloud, facilita a los usuarios la autenticación con métodos de verificación fuera de línea y en línea y políticas de acceso a través de endpoints, VPN y aplicaciones web. El acceso eficaz y seguro a los recursos de la nube también está disponible con los portales de aplicaciones de inicio de sesión único (SSO).

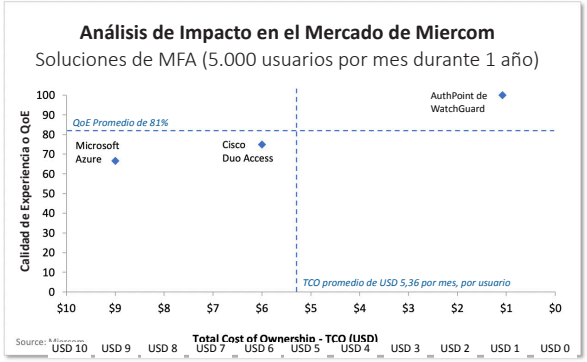
Servicio de Supervisión de Dark Web

El servicio de Supervisión de Dark Web de AuthPoint notifica de forma proactiva a los clientes cuando se encuentran credenciales comprometidas de hasta tres dominios supervisados en bases de datos de vulneración de credenciales recién adquiridas. Las alertas se envían a los administradores y usuarios finales afectados para que puedan generar nuevas contraseñas rápidamente y antes de la adquisición de la cuenta.

Administrador de Contraseñas

Creado con casos de uso empresarial en mente, el administrador de contraseñas de AuthPoint brinda a las organizaciones un estándar más alto de contraseñas seguras y puede reducir las solicitudes de restablecimiento generando contraseñas que no necesitan ser recordadas. Además, nuestro administrador de contraseñas ofrece:

- **Bóveda Corporativa** : agregue credenciales y genere contraseñas seguras para las aplicaciones de uso común en el lugar de trabajo, en las que no tenga habilitado el inicio de sesión único (SSO). Además, los administradores pueden compartir credenciales para el uso común de aplicaciones y herramientas de TI.
- **Bóveda Privada** : agregue credenciales y genere contraseñas seguras para las aplicaciones personales y sociales. Si el empleado abandona la organización, estas credenciales personales se pueden exportar y usar dentro de otro administrador de contraseñas.



Fuente: Miercom

Los cuadrantes se forman en función de los valores promedio. WatchGuard estaba en el cuadrante superior derecho, lo que demuestra que tenía la QoE más alta que los proveedores de la competencia, al costo más bajo. Cisco y Microsoft no ofrecen las mismas cantidad de funcionalidades, facilidad de uso o intuitiva interfaz que WatchGuard.

¿Por qué las Organizaciones Eligen MFA de AuthPoint?

Seguridad en el Trabajo Híbrido Más Sencilla

Simplifique el uso de contraseñas con las configuraciones de inicio de sesión único (SSO), que permiten el trabajo remoto con un inicio de sesión y acceso a las aplicaciones seguros.

Experiencia de Usuario Fluida

La validación independiente del producto muestra a AuthPoint como la mejor opción para los usuarios primerizos gracias a su interfaz intuitiva, las guías útiles y las configuraciones de un solo clic, en comparación con otras soluciones en el mercado.

ADN Móvil para una Migración Segura

La solución MFA de WatchGuard incluye una funcionalidad de ADN de dispositivo móvil que coincide automáticamente con el teléfono del usuario autorizado antes de otorgar acceso. Cualquier atacante que clone el dispositivo de un usuario para acceder a sistemas protegidos se bloquea inmediatamente.

Valor y Rendimiento de Inversión (ROI) Altos

En comparación con otras soluciones, WatchGuard ofrece un amplio conjunto de funciones nativas, cientos de integraciones y atención al cliente dedicada, todo por un precio fijo por usuario y por mes.

Camino de Adopción de Zero Trust con Políticas de Autenticación

Las políticas y los controles adaptativos de AuthPoint permiten la administración de acceso unificado, un paso clave para la adopción de seguridad de Zero Trust.

Características Clave de Seguridad de Identidad

Aplicación de Autenticación Móvil de AuthPoint

TIPOS DE AUTENTICADOR
Notificación push con activador de antisuplantación de identidad (modo en línea)
Generador de código QR (modo sin conexión)
Código de acceso de un solo uso basado en el tiempo (modo sin conexión)
FUNCIONALIDADES DE SEGURIDAD
Jailbreak y detección de raíz
Protección contra intercambio de ADN/SIM del dispositivo móvil
Activación en línea con generación dinámica de claves
Protección de la aplicación: PIN, huella digital y reconocimiento de rostro
Migración autoservicio segura a otro dispositivo
Soporte de terceros y de varios tokens
Personalización del nombre y el ícono del token
PLATAFORMAS COMPATIBLES
Android 7.0 o superior
iOS 12.5.7 o superior

Administración de AuthPoint en la Nube

FUNCIONALIDADES DE ADMINISTRACIÓN
Administración, configuración y administración con WatchGuard Cloud
Recursos de autenticación configurables
Autenticación personalizable y políticas de riesgo (red, tiempo, geovalla y geocinética)
Análisis de dark web de hasta 3 dominios
Supervisión de credenciales en la dark web de hasta 3 dominios por licencia
Widgets del panel de control para autenticaciones, usuarios, dispositivos y suscripciones
Implementación sencilla con guías y asistentes de integración
Sincronización con Active Directory, Azure AD y LDAP
Herencia de usuarios para proveedores de servicios
GATEWAY DE AUTHPOINT
Conexión saliente segura desde la red hasta WatchGuard Cloud
Sincronización de Active Directory y LDAP
Servidor RADIUS

AGENTES E INSTALADORES DE AUTHPOINT
Inicio de sesión en macOS El Capitan (10.11) o superior
Inicio de sesión en Windows v8.1 o superior
Inicio de sesión en Windows Hello for Business
Active Directory Federation Server 2012 y versiones posteriores (SSO)
Inicio de sesión en Windows Server 2012 y versiones posteriores
Acceso web a escritorio remoto de Windows
Agente de gateway de WatchGuard AuthPoint
TOKEN DE HARDWARE
Token de hardware de WatchGuard sin exposición de valores de inicialización
Tokens de hardware de Tercero con contraseña de un solo uso basada en tiempo (TOTP)

ESTÁNDARES COMPATIBLES
OATH Algoritmo de contraseña de un solo uso basada en tiempo (TOTP) - RFC 6238
OATH Algoritmos de desafío/respuesta (OCRA) - RFC 6287
OATH Protocolos de aprovisionamiento dinámico de claves simétricas (DSKPP) - RFC 6063
Protocolo RADIUS (IETF)
Perfil SAML 2.0 (OASIS)
Argon 2id (código abierto)

INTEGRACIONES DE AUTHPOINT MFA con Inicio de Sesión Único
SAAS: Atlassian, BlueJeans, Box, Citrix, Confluence, Dropbox, Evernote, Github, Google Workspace, Go-to-Meeting, Jira, Lucid Charts, Microsoft 365, Salesforce, ServiceNow, Slack, Tableau, Zoom, WebEx y más…
IAAS: Adobe Cloud, Amazon Web Services, Google Cloud Platform, Microsoft Azure, Salesforce Cloud, Oracle Cloud y más…
Seguridad y Administración: Akamai, BMC, Cisco, ConnectWise, CyberArk Fortinet, ITGlue, JAMF, ManageEngine, MobileIron, PagerDuty, Thycotic, VMWare, WatchGuard Firebox, WatchGuard VPN y más…

Pero No se Quede Solamente con Lo Que Decimos

TrustRadius ★★★★½

"Una autenticación de dos factores confiable y rentable para nuestros clientes. Se utiliza principalmente para el acceso MFA a VPN para que los usuarios autenticados trabajen de forma remota. Antes de usar AuthPoint de WatchGuard, no teníamos una buena solución para todos nuestros clientes que usaban MFA para conectarse a la VPN".

– Robbie Matthew, Ingeniero Senior de Redes
Invision Technologies, LLC (Telecomunicaciones, 51-200 empleados)

VENTAS EN MÉXICO: +52 55 5347-6063 VENTAS ESPAÑA: +34 911 410 918 WEB: www.watchguard.com/es WatchGuard Technologies, Inc.