HOJA DE DATOS

WATCHGUARD PASSPORT

PROTECCIÓN PERSISTENTE Y SIEMPRE ACTIVA QUE ACOMPAÑA A SU USUARIO

Las empresas deben poder hacer llegar las capacidades de seguridad a los usuarios y a los dispositivos, sin importar en qué lugar estén. Los empleados, los contratistas, los visitantes y sus dispositivos entran a su red y salen de ella en forma regular a medida que realizan sus tareas dentro y fuera de las instalaciones. Al mismo tiempo, un solo endpoint infectado o una contraseña robada podrían abrir las compuertas para un atacante. La solución Passport de WatchGuard es un paquete de servicios de seguridad centrados en el usuario que va dondequiera que van sus usuarios.

Con Passport Puede:

1. **Autenticar** a los usuarios e implementar una sólida autenticación multifactor en las VPN, las aplicaciones en la nube, los endpoints y más.
2. **Proteger** a los usuarios en Internet, bloquear intentos de suplantación de identidad y aplicar políticas de exploración de web en cualquier lugar, en cualquier momento y sin requerir una VPN.
3. **Responder** a través de la detección y eliminación de amenazas y malware, y la contención de ransomware y de canales de comando y control relacionados.

ADMINISTRACIÓN E IMPLEMENTACIÓN DESDE LA NUBE

Passport se administra en su totalidad desde la nube, de modo que no existe mantenimiento de software o implementación de hardware. Es posible ver reportes y alertas, configurar servicios, implementar clientes de endpoint y administrar tokens de autenticación, todo desde la nube. Y gracias a la integración con las principales herramientas de implementación de terceros, puede estar listo para trabajar con Passport de manera rápida y sencilla.

¿Qué incluye Passport?

Autenticación Multifactor

Con el aumento del malware de robo de credenciales y las nuevas vulneraciones de datos de nombres de usuario y contraseñas que quedan expuestos todos los días, la necesidad de una sólida autenticación nunca había sido tan grande. AuthPoint de WatchGuard aligera la carga para usted y sus clientes. AuthPoint utiliza mensajes push, códigos QR o contraseñas de un solo uso (OTP) en combinación con el ADN del dispositivo móvil del teléfono de cada usuario para identificar y autenticar usuarios.

Protección DNS

A medida que los usuarios se alejan de su red, pierde visibilidad de su actividad en Internet, lo cual genera un importante punto ciego en su seguridad y los deja vulnerables a la suplantación de identidad y los ataques de malware. Con DNSWatchGO obtiene visibilidad consolidada de los dispositivos protegidos, sin importar su ubicación. Cuando están fuera de la red, un cliente de host utiliza una lista agregada de dominios maliciosos para supervisar y correlacionar las solicitudes de DNS salientes. Los intentos de comunicarse con cualquiera de estos dominios se bloquearán y el tráfico se redireccionará a la nube de DNSWatchGO para mayor investigación.

Seguridad de Endpoints

Confiar solo en un antivirus basado en firmas para la protección contra el malware es una causa perdida. DNSWatchGO permite detectar y bloquear los canales de comunicación que utilizan los hackers para distribuir y controlar su malware. La detección y respuesta de endpoints administra los endpoints con protección de ransomware, aislamiento de dispositivos, correlación de amenazas y protecciones tradicionales de antivirus basados en firmas. La combinación de estas capacidades asegura que sus usuarios están protegidos contra todas las amenazas conocidas y desconocidas.

PASSPORT

Aplicación Móvil AuthPoint

FUNCIONES DE AUTENTICACIÓN
Autenticación basada en push (en línea)
Autenticación basada en código QR (sin conexión)
Contraseña de un solo uso basada en tiempo (sin conexión)
FUNCIONALIDADES DE SEGURIDAD
Firma de ADN de dispositivo
Activación en línea con generación dinámica de claves
Protección por autenticador • PIN • Huella digital (Samsung/Apple) • Reconocimiento facial (Apple)
Migración del autenticador segura y de auto servicio a otro dispositivo.
Jailbreak y detección de raíz
FUNCIONALIDADES DE COMODIDAD
Soporte de varios tokens
Soporte de tokens de redes sociales de terceros
Nombre e imagen de token personalizables
PLATAFORMAS COMPATIBLES
Android 4.4 o versión superior
iOS 9.0 o versión superior
ESTÁNDARES
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

DNSWatchGO

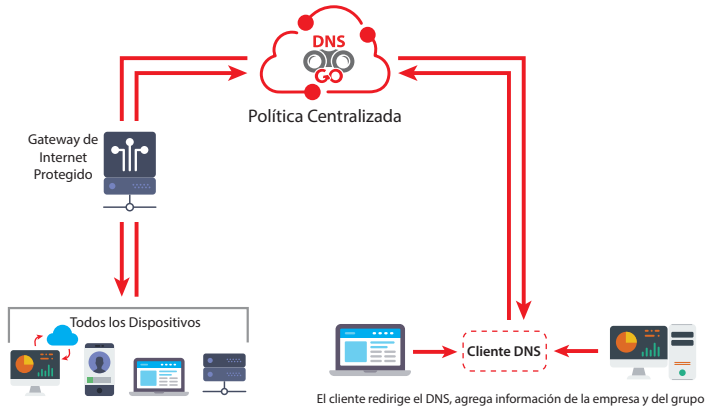
SOPORTE DE SISTEMA OPERATIVO
Windows 7, 8 y 10
FUNCIONES DE SEGURIDAD
Bloqueo de ataques de suplantación de identidad
Prevención de conexiones C2
Filtrado de contenido
Entrenamiento inmediato de conocimiento sobre seguridad
SOPORTE DE VPN
Totalmente compatible con los siguientes tipos de VPN móvil de WatchGuard: • IKEv2 • SSL/TLS • L2TP • IPSec

Detección y Respuesta de Endpoints

SOPORTE DE SISTEMA OPERATIVO
Windows 7, 8 y 10
macOS 10.13, 10.14 y 10.15
METODOLOGÍAS DE DETECCIÓN
Firmas
Análisis heurístico
Supervisión de comportamiento
Análisis de patrones de comportamiento
Análisis de código inactivo
Inteligencia artificial
CAPACIDADES DE RESPUESTA
Bloqueo
Contención del host
Clasificación del archivo
Destrucción del proceso
Cuarentena del archivo
Eliminación del registro

CÓMO FUNCIONA

WatchGuard DNSWatchGO supervisa las solicitudes de DNS salientes y las correlaciona con una lista completa de sitios maliciosos. Si se determina que una solicitud es maliciosa, se la bloquea y se redirige al usuario a un sitio seguro para reforzar su entrenamiento sobre suplantación de identidad.



EL PORTAFOLIO DE SEGURIDAD DE WATCHGUARD

Seguridad de red

Wi-Fi seguro

Autenticación multifactor

Para conocer más detalles, comuníquese con su revendedor autorizado de WatchGuard o visite el sitio web www.watchguard.com.

VENTAS EN EE. UU. 1.800.734.9905 VENTAS INTERNACIONALES +1.206.613.0895 SITIO WEB www.watchguard.com WatchGuard Technologies, Inc.