Seguridad Diseñada para su Empresa

WatchGuard®

INTRODUCCIÓN

Su día comienza con una taza de café (o tal vez una bebida energética, si no le gusta el café) y una larga lista de notificaciones que debe atender de inmediato. Hace todo lo posible por terminar de revisar todas las alertas de la noche anterior antes de que los demás lleguen y lo bombardeen con las novedades del día.

¿Y qué sucede con el proyecto que está tratando de terminar hace tres semanas? Al parecer, tendrá que postergarlo un día más. ¿No sería fantástico contar con soluciones de seguridad que mantuvieran a salvo su organización, le proporcionaran la visibilidad necesaria de la red y le permitieran retomar la lista de tareas pendientes?

Vea algunas de las amenazas de seguridad más comunes a las cuales se enfrenta, las mejores prácticas que puede aplicar para que no interfieran en su lista de tareas pendientes y la ayuda que puede brindarle WatchGuard.

Contraseñas Poco Seguras o Reutilizadas

El 81 % de las infracciones relacionadas con los ataques informáticos aprovechan contraseñas robadas o poco seguras.[1] Anotar las contraseñas en notas adhesivas o usar Contraseña123 son prácticas que ya no se utilizan.

Los empleados necesitan contraseñas seguras que sean realmente fáciles de administrar. ¿De qué manera garantiza que las contraseñas no dejen a la empresa vulnerable ante una infracción?

1 http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Mejores Prácticas Relacionadas con las Contraseñas

Sea INTELIGENTE con sus contraseñas:

Incluya símbolos, letras y números.

Use más de 12 caracteres.

Evite usar información personal.

No reutilice contraseñas anteriores.

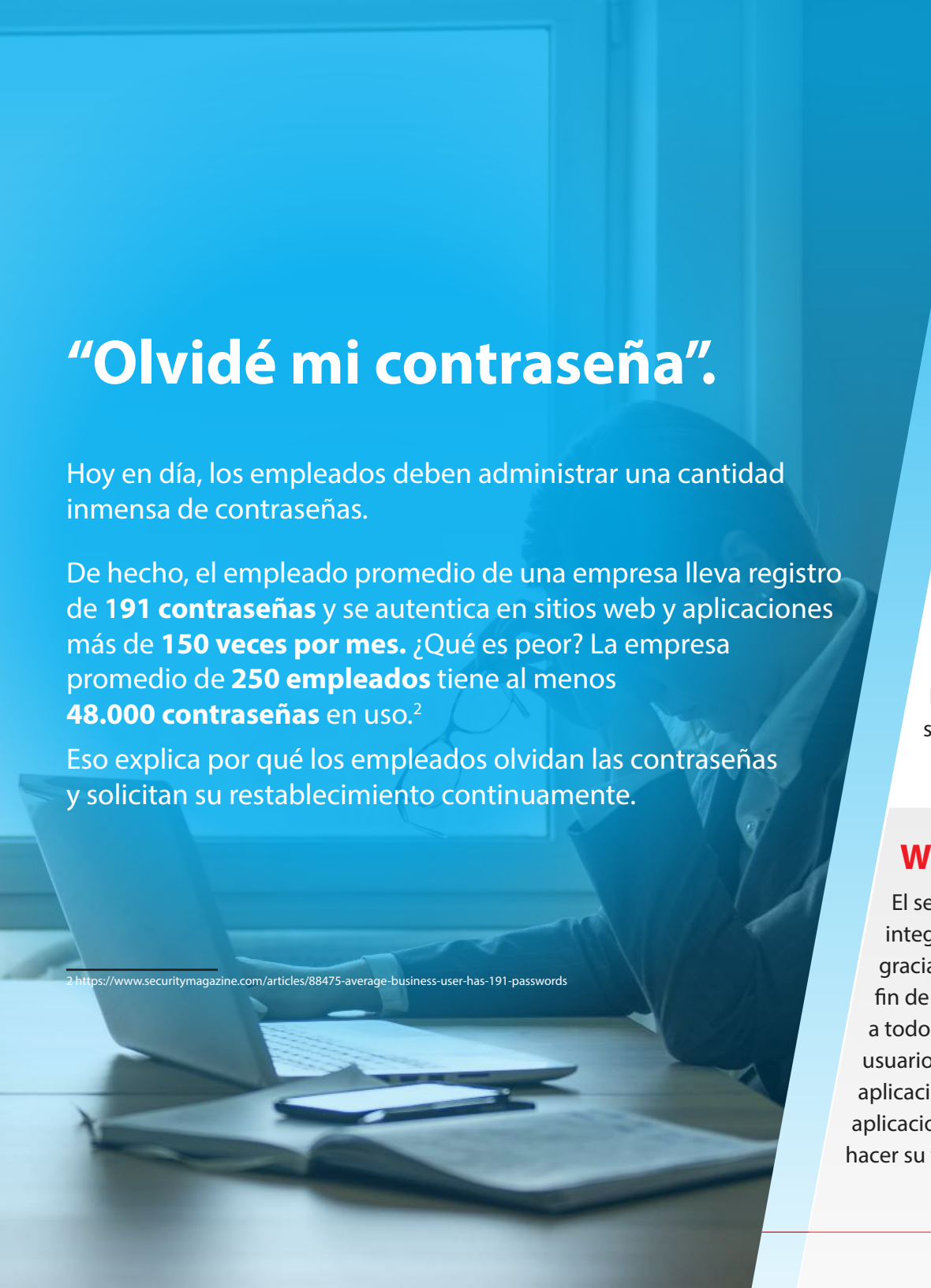
Confíe en las herramientas de administración de contraseñas.

Autenticación Multifactor (MFA)

Las herramientas de MFA proporcionan otras pruebas de identificación, además de simples contraseñas. No solo solicitan a los usuarios que se autentiquen con datos (como una contraseña), sino también con alguna pertenencia o algún rasgo personal. De ese modo, limitan las posibilidades de que un cibercriminal use credenciales robadas para acceder a sus cuentas.

WatchGuard AuthPoint

Nuestra exclusiva solución de autenticación multifactor ayuda a los clientes a reducir la probabilidad de que se produzcan interrupciones en la red y pérdidas de datos a raíz del robo o la pérdida de credenciales. Además, se ofrece completamente desde la nube para facilitar la instalación y la administración incluso con personal limitado. AuthPoint va un paso más allá de la autenticación de dos factores (2FA) tradicional, ya que ofrece nuevas maneras de identificar a los usuarios de manera fehaciente, por ejemplo, mediante el ADN de dispositivo móvil. Asimismo, nuestro gran ecosistema de integraciones con terceros implica que los clientes pueden implementar la protección constante de AuthPoint para acceder a la red, las VPN, las aplicaciones en la nube y donde sea necesario.



“Olvidé mi contraseña”.

Hoy en día, los empleados deben administrar una cantidad inmensa de contraseñas.

De hecho, el empleado promedio de una empresa lleva registro de **191 contraseñas** y se autentica en sitios web y aplicaciones más de **150 veces por mes.** ¿Qué es peor? La empresa promedio de **250 empleados** tiene al menos **48.000 contraseñas** en uso.[2]

Eso explica por qué los empleados olvidan las contraseñas y solicitan su restablecimiento continuamente.

2 https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

Herramientas de Almacenamiento de Contraseñas

Las herramientas de administración y almacenamiento de contraseñas permiten a los usuarios utilizar contraseñas seguras sin la necesidad de recordarlas. Además, permiten configurar recordatorios para el momento en que se necesite modificar las contraseñas.

Autenticación multifactor

Las herramientas de MFA proporcionan otras pruebas de identificación, además de simples contraseñas. No solo solicitan a los usuarios que se autentiquen con datos (como una contraseña), sino también con alguna pertenencia o algún rasgo personal. De ese modo, limitan las posibilidades de que un cibercriminal use credenciales robadas para acceder a sus cuentas.

Al incorporar soluciones de MFA a todos los recursos digitales y ofrecer a los usuarios fácil acceso a un portal de identidad, ellos solo deben iniciar sesión una vez y ya no es necesario que recuerden miles de contraseñas.

WatchGuard AuthPoint

El servicio WatchGuard AuthPoint admite muchas integraciones con terceros y pronto admitirá más, gracias a nuestro eficaz y creciente ecosistema, con el fin de que pueda agregar protección mediante MFA a todos sus valiosos recursos. Lo que es mejor aún, los usuarios de AuthPoint solo se autentican una vez en las aplicaciones en la nube, y se les otorga acceso a todas las aplicaciones y los recursos en la nube que necesitan para hacer su trabajo.

Usuarios Desprevenidos

El 90 % de los ataques comienzan con un correo electrónico de suplantación de identidad (phishing).[3]

Mientras en las organizaciones haya usuarios desprevenidos que hagan clic en el enlace, los hackers seguirán aprovechando este método para distribuir malware.

La educación sobre la suplantación de identidad es una forma importante de garantizar que todos los empleados reconozcan los signos de advertencia de un intento de suplantación de identidad. De todos modos, también es necesario contar con protección contra la suplantación de identidad.

¿No sería fantástico tener una solución que, además de ofrecer protección, permita repasar la capacitación?

3 https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing

Educación sobre la Suplantación de Identidad (phishing)

La educación es fundamental para que los usuarios conozcan los riesgos que corren de recibir mensajes de correo electrónico de suplantación de identidad y los signos de advertencia a los cuales deben prestar atención. El objetivo es garantizar que los empleados estén preparados para defenderse contra cualquier ataque que reciban en sus casillas de correo.

Supervisión y Bloqueo de DNS

A pesar de la importancia de la educación, esta no garantiza la protección total de los empleados. Dado que los mensajes de correo electrónico de suplantación de identidad son cada vez más personalizados y dirigidos, las probabilidades de hacer clic en un enlace indebido son cada vez mayores. Por eso, es necesario contar con una solución que supervise el tráfico de DNS y bloquee el acceso a sitios maliciosos.

DNSWatch

WatchGuard DNSWatch detecta las solicitudes de DNS maliciosas y bloquea el acceso a los sitios. El usuario es redirigido a una página segura donde se muestran los signos de riesgo y las advertencias de un ataque de suplantación de identidad. Estos son momentos de aprendizaje para los empleados y una forma muy eficaz de concientizar a todos sobre los riesgos que se corren al hacer clic en enlaces de suplantación de identidad.

Descarga Desmedida de Archivos

Al igual que los enlaces maliciosos enviados por correo electrónico, otro medio muy común por el cual los hackers realizan sus ataques es el envío de archivos adjuntos maliciosos.

Este método requiere que los hackers desarrollen un archivo adjunto que atraiga al usuario para que lo descargue.

Los señuelos que más comúnmente se envían como archivos adjuntos son los siguientes:

- Facturas
- Documentos escaneados
- Mensajes de error de entrega
- Confirmaciones de pedidos y pagos
- Confirmaciones de vuelos específicos

¿Se puede proteger a los usuarios de los ataques de descargas maliciosas?

Protección contra Amenazas Basada en Firmas

Realizar un análisis de archivos maliciosos conocidos antes de abrir un archivo brinda un nivel necesario de detección que permite prevenir este método de ataque.

Sandbox en la Nube para la Detonación de Archivos

El sandbox en la nube es una forma segura de abrir amenazas y detonar archivos potencialmente maliciosos. Al abrirlos en un entorno virtual que refleja el sistema de forma exacta, se puede identificar perfectamente cualquier intento malicioso sin poner en riesgo el dispositivo real.

GAV y APT Blocker

Total Security Suite de WatchGuard incluye Gateway AntiVirus (GAV) y APT Blocker, que ofrecen defensas en capas contra los archivos adjuntos maliciosos de los ataques de suplantación de identidad.

GAV utiliza una base de datos de firmas que se actualiza constantemente para bloquear extensiones de archivos maliciosos de modo que estos no se abran.

Las amenazas desconocidas y los ataques de malware de día cero implican una serie de desafíos nuevos para la defensa de la organización. Sin embargo, con WatchGuard APT Blocker, se pueden detonar estos archivos en un entorno virtual seguro para determinar si son maliciosos. Si lo son, el archivo entra en cuarentena para garantizar que no se abra.

Empleados remotos = objetivos fáciles

Ante el crecimiento continuo de las empresas, los empleados están cada vez menos protegidos por la burbuja que proporciona la seguridad de la red.

La falta de actualización de los componentes de software, los complementos y los navegadores, además de la carencia de parches y de protección de los sistemas, deja a los empleados remotos aún más vulnerables a los ataques.

¿Cuenta con alguna solución para proteger a los empleados remotos que quedan fuera de la red?

Análisis Profundo de Amenazas

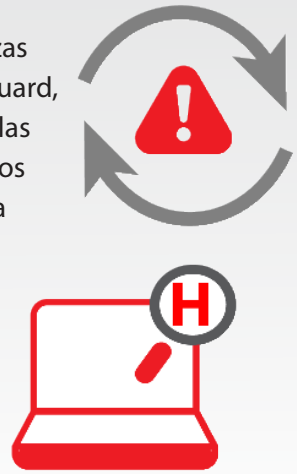
Las amenazas avanzadas y evasivas requieren la implementación de soluciones de protección realmente potentes para defenderse de ellas. Uno de los recursos para protegerse de estas amenazas son las herramientas de análisis profundo de amenazas, como el sandbox de la red y del host. Al detonar amenazas maliciosas y supuestas en entornos virtuales seguros, se puede determinar el objetivo real de una amenaza antes de que afecte a los usuarios.

Visibilidad del Endpoint

No es posible detener lo que no se puede ver. Es decir que, en el caso de los empleados remotos, es necesario asegurarse de tener buena visibilidad de sus endpoints, aun cuando no están conectados a la red.

TDR y Sensor de Host

La función Detección y Respuesta ante Amenazas (TDR), que incluye el Sensor de Host de WatchGuard, permite visualizar detalladamente los eventos y las actividades amenazantes para los endpoints de los usuarios, incluso cuando no están conectados a la red. Además, la función TDR permite detonar las supuestas amenazas del endpoint en un entorno virtual para determinar si son maliciosas. Si se determina que la amenaza es maliciosa, se puede reparar rápidamente antes de que produzca daños.



Empleados Navegando y Tráfico Lento

Las visitas a sitios que hacen perder el tiempo o resultan inapropiados pueden afectar en gran medida la productividad de una empresa.

De hecho, el empleado promedio puede perder más de 8 horas semanales en actividades no relacionadas a su trabajo. Eso equivale a un día entero.[4]

Por otro lado, un rendimiento lento puede significar que una oficina atestada trabaje a la velocidad de un caracol. ¿Será que Karen, del área de contabilidad, está viendo demasiados videos de gatos en YouTube? ¿O tal vez Patrick, del área de ventas, está viendo el partido al cual no pudo asistir?

¿Cómo es posible garantizar que los empleados maximicen su productividad durante las horas de trabajo y, lo que es aún más importante, que no visiten sitios web peligrosos o inapropiados en el trabajo?

4 https://nypost.com/2017/07/29/this-is-how-much-time-employees-spend-slacking-off/

Visibilidad de la Actividad Web

Los empleados necesitan tener acceso a la Web para llevar a cabo su trabajo, pero esto también puede causar estragos en el rendimiento de la red. Es necesario tener visibilidad de los sitios web que visitan los usuarios para determinar si el problema yace en que los sitios son una pérdida de tiempo.

Filtrado de URL

Es necesario tener la posibilidad de proteger la red contra contenidos web peligrosos, actividades maliciosas e, incluso, sitios web que hacen perder el tiempo. El filtrado web permite aplicar la política corporativa para garantizar la supervisión y la aprobación del acceso a cualquiera de estos sitios.

WebBlocker

WebBlocker de WatchGuard ofrece una solución eficaz y fácil de usar para controlar y supervisar las actividades web que se realizan en toda la organización. Asimismo, permite bloquear o limitar las actividades web que se llevan a cabo fuera del horario laboral para garantizar que haya suficiente ancho de banda disponible en todo momento.

Dimension

WatchGuard Dimension permite ver la actividad de red en tiempo real presentada en paneles e informes intuitivos e interactivos. Esto permite ver quién consume más ancho de banda, si hay patrones de tráfico inusuales y cuáles son los sitios web más visitados.

¿Cuál Será la Siguiente Gran Amenaza?

No cuenta con el tiempo (o tal vez la energía) para mantenerse actualizado con respecto a las tendencias de las amenazas y los ataques de malware más recientes de la actualidad.

Sin embargo, las amenazas siguen evolucionando, y los hackers atacan a su empresa desde todos los ángulos.

¿Cuenta con alguna solución que le brinde protección contra las amenazas de malware conocidas, desconocidas y evasivas?

Acceso a la Investigación de Amenazas de una Forma Fácil de Consumir

Es necesario contar con una forma de mantenerse actualizado con respecto a las tendencias y las predicciones de amenazas. Si no cuenta con el ancho de banda necesario, asegúrese de trabajar con equipos que puedan brindarle esta información.

Seguridad en Capas que Brinda Protección en Todos los Niveles

Los ataques de hoy en día y las amenazas del futuro requieren un enfoque en capas para las soluciones de seguridad. Es necesario tener las capacidades necesarias para defenderse contra todo tipo de ataques en todas las capas.

Total Security Suite

Total Security Suite de WatchGuard brinda protección contra amenazas avanzadas en todas las capas. Desde servicios fundamentales, como Gateway antivirus y el Servicio de prevención de intrusiones, hasta servicios más avanzados, como el sandbox en la nube y la prevención de pérdida de datos, WatchGuard cuenta con soluciones que brindan protección contra ataques conocidos, desconocidos e, incluso, evasivos.

Panorama de Amenazas

Nuestro equipo de investigación de amenazas tiene un objetivo principal: mantenerse actualizado con respecto a las tendencias de las amenazas y los ataques más recientes para que usted no tenga que hacerlo. Nos esforzamos para proporcionarle las tendencias y las sugerencias para mantenerse seguro ante las amenazas más recientes.

¿Se pasa la vida lidiando con alertas constantes?

¿Evita ir a la sala de descanso porque no quiere toparse con una cantidad enorme de gente?

¿Se estremece un poco cada vez que su teléfono suena los fines de semana por miedo a que haya ocurrido algún accidente en la oficina?

Proteger la oficina no significa no tener vida. Solo es necesario contar con las soluciones de seguridad adecuadas.

Es necesario contar con una solución de seguridad que proteja a su empresa desde todos los ángulos.

Proteger a su empresa es un trabajo de 24 horas al día, todos los días del año. Pero eso no significa que no pueda hacer nada más.

Debe tener la posibilidad de ver las actividades de red y los eventos de amenazas y, al mismo tiempo, tener la confianza de que su solución de seguridad brinda la protección necesaria contra todos los ataques en todas las capas de la red.

WatchGuard

WatchGuard ofrece a los clientes una solución de seguridad inteligente de una forma sencilla y fácil de administrar. Total Security Suite de WatchGuard brinda protección contra las amenazas conocidas, desconocidas y evasivas en una sola solución fácil de usar. Con un dispositivo y una licencia, se pueden obtener todos los servicios de seguridad necesarios al precio deseado.

La versión estándar de WatchGuard Dimension incluye nuestros dispositivos y brinda un conjunto de herramientas de generación de informes y visibilidad de big data que identifica y extrae tendencias, problemas y amenazas de seguridad de red clave.

Busque el dispositivo de WatchGuard que más se adecue a su empresa.
Visite https://www.watchguard.com/compare para obtener más información

PROTEJA SU EMPRESA • PROTEJA SUS ACTIVOS • PROTEJA A SU GENTE

La seguridad informática es más importante que nunca. La cantidad de ataques informáticos en todo el mundo ha llegado a un récord histórico y no hay señales de que vaya en descenso, mientras las pequeñas y medianas empresas siguen siendo víctimas de graves impactos en las operaciones comerciales y en su continuidad. WatchGuard llegó para proporcionar la protección en capas que usted necesita para enfrentar los tipos más avanzados de malware de un modo fácil de mantener. Usted enfrenta las mismas amenazas que las organizaciones empresariales, ¿no debería entonces tener el mismo nivel de seguridad?

Oficina Central Internacional
Estados Unidos
Tel.: +1.800.734.9905
Correo electrónico: sales@watchguard.com

Oficina central de Europa
Países Bajos
Tel.: +31(0)70.711.20.85
Correo electrónico: sales-benelux@watchguard.com

Oficina central de Asia, el Pacífico
y el Sudeste Asiático
Singapur
Tel.: +65.3163.3992
Correo electrónico: inquiry.sea@watchguard.com

WatchGuard®