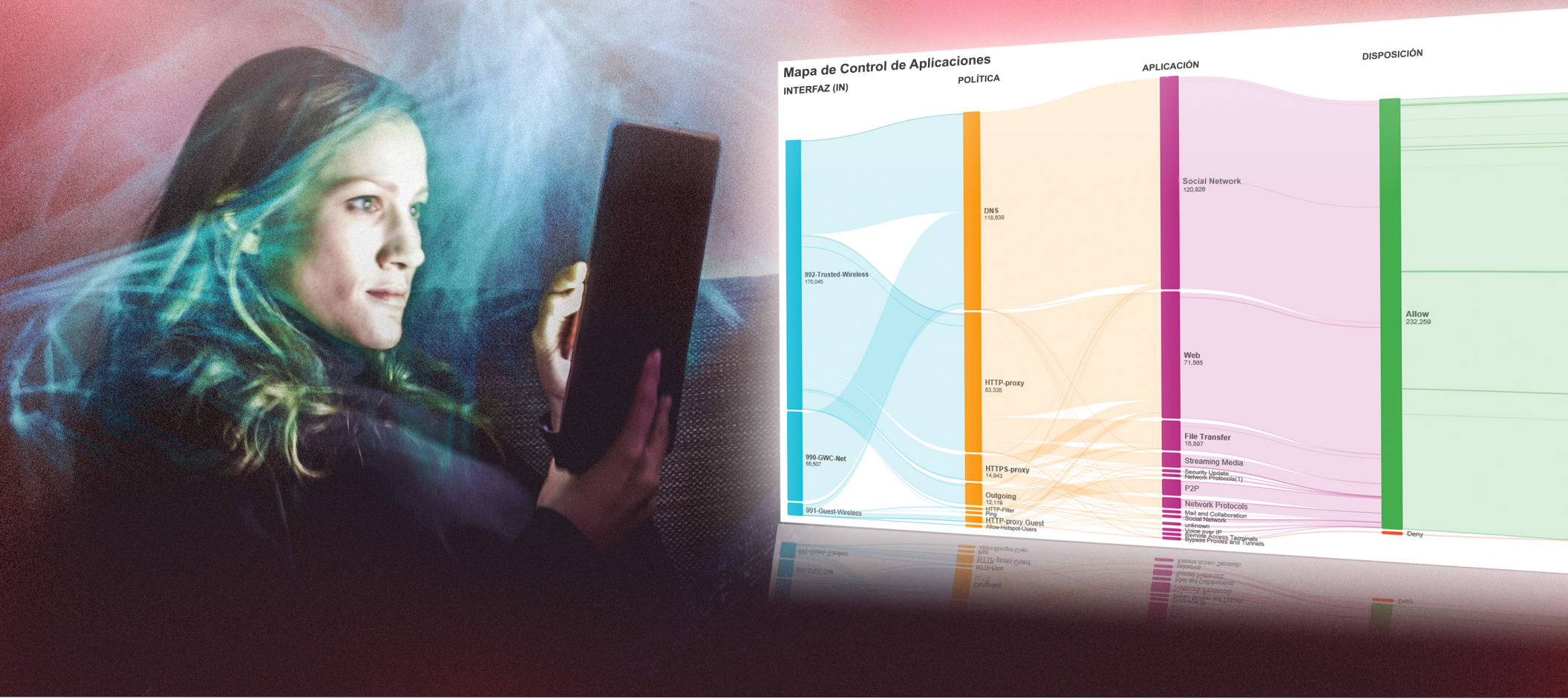
Elimine los Puntos Ciegos de su Red con Visibilidad Completa



Índice

Un Panorama de Amenazas en Evolución

La cantidad de ciberataques mundiales se encuentra en constante crecimiento y no parece que vaya a disminuir. La capacidad de los administradores de TI de detectar incidentes cada vez demora más a medida que se ahogan en una cantidad cada vez mayor de datos de registro. Lo que es peor, los cibercriminales se han enfocado en pequeñas y medianas empresas (SMB), ya que las consideran un blanco fácil con sistemas de seguridad inadecuados. Las grandes corporaciones están al tanto de esta creciente amenaza y dedican equipos de profesionales especializados de seguridad a monitorear continuamente cada rincón de la red en busca de actividad maliciosa. ¿Qué les queda a las organizaciones más pequeñas que no pueden afrontar el costo de un personal de seguridad de TI dedicado? ¿Qué pueden hacer las SMB para mantenerse competitivas en cuanto a la rápida evolución de robo de datos cuando no cuentan con una persona para monitorear e investigar regularmente el trafico sospechoso? ¿Existe una solución al alcance de las SMB que cuentan con un presupuesto pequeño y experiencia limitada?

La solución a este importante desafío es la Visibilidad. Una de las estrategias más importantes para proteger una organización es proporcionar visibilidad completa de la actividad de red. Solamente cuando pueda ver claramente todo el tráfico de red, los dispositivos conectados y los usuarios en tiempo real, podrá adelantarse constantemente a las potenciales amenazas. Toda organización necesita una perspectiva clara e integral sobre lo que sucede dentro de su red.



> Los datos en sí mismos no son valiosos en absoluto. El valor radica en los análisis de esos datos y cómo los datos se convierten en información...
>
> *~ Mark van Rijmenam, Estratega de Grandes Datos*

Las Infracciones de Seguridad Son Cada Vez Más Difíciles de Detectar

Las amenazas son cada vez más difíciles de detectar a medida que el malware es más sofisticado. Además, los profesionales de TI se ahogan en océanos de datos de registro.

97 % de las organizaciones **recolecta registros**[1]

44 % de estas organizaciones dice que **revisan** sus **registros regularmente**[1]

14 % Solo este porcentaje se siente seguro sobre su **capacidad** de **analizar grandes conjuntos de datos** para identificar **tendencias de seguridad**[1]

80 días En **2013**, la cantidad de tiempo promedio que tomaba detectar una amenaza era **80 días**[2]

6 meses Para el **2014**, el promedio había crecido a **6 meses**[2]

8,5 meses Para el **2015**, el promedió creció hasta un aún más peligroso número de **8,5 meses**[2]

¿Quién Detectó la Infracción?

El personal interno rara vez detecta las infracciones de seguridad.
Generalmente, las detecta una agencia de terceros u organismos de seguridad.

67 %

Un Tercero

16 %

Organismos de Seguridad

1 %

Personal Interno

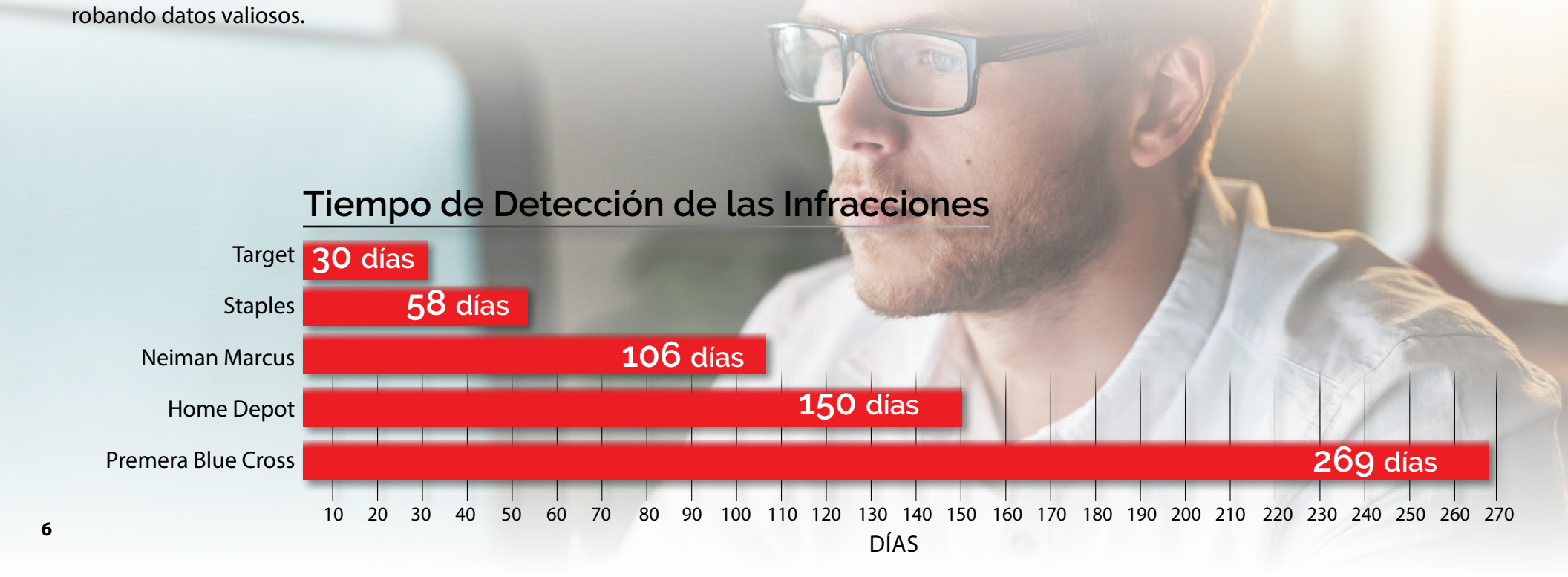
Tres Áreas Claves de Visibilidad

La Visibilidad Causa Avances en la Seguridad, Productividad y Eficacia

Si no puede identificar la fuente del problema, es imposible resolverlo. Una deficiente visibilidad de red es un gran riesgo para la seguridad de una organización y, además, amenaza la productividad de los empleados y dificulta la gestión de las molestias diarias como el tiempo sin actividad y los cuellos de botella en la red. Las empresas también necesitan una visibilidad de red completa para medir con precisión el retorno de la inversión de su infraestructura de TI.

1. Amenazas de Seguridad

Las redes enfrentan constantes amenazas y las infracciones son cada año más difíciles de detectar en un entorno de amenazas cada vez más difícil de predecir. El malware, las puertas traseras y la pérdida de datos pueden pasar desapercibidos rutinariamente durante meses, y, en algunos casos, hasta años a la vez. Cuando finalmente se descubre la infracción, generalmente lo informa un tercero externo y rara vez se descubre a través de una revisión interna. Las tecnologías y los procesos no pueden identificar las amenazas de una manera que permita tomar medidas y, hasta que las organizaciones puedan vincular los eventos de seguridad con los usuarios en tiempo real, los criminales continuarán robando datos valiosos.



2. Productividad de los Empleados

Algunos empleados desperdician mucho tiempo y recursos en descargar medios y explorar la Web e ignoran sus tareas diarias. La ciberpereza seguirá creciendo si no se tiene una visibilidad adecuada de la actividad del usuario. Con la introducción de tecnologías que monitoreen el uso de aplicaciones, las empresas pueden usar la limitación y modelación de tráfico para asegurarse de que las aplicaciones críticas del negocio cuenten con la adecuada cantidad de ancho de banda mientras que mantienen a sus empleados enfocados en lo que importa.

3. Eficacia de Red

Las empresas pueden experimentar velocidades de conexión lentas en el mismo horario todos los días. Estos cuellos de botella ocurren generalmente cuando las demandas de recursos se encuentran en su pico diario. Esto puede frustrar a los usuarios y hacer que las operaciones sean realmente lentas. Sin una visibilidad completa del diseño físico de su red, no puede identificar la fuente del cuello de botella y los problemas continuarán.

Problemas que Comparten las Industrias Principales

Los Cibercriminales No Discriminan

A la hora de robar datos valiosos, los cibercriminales no discriminan. Mientras exista un mercado negro lucrativo, las organizaciones de todas las industrias pueden sufrir ciberataques. Entre los sectores más atacados encontramos a **Educación, Ventas al por Menor, Atención médica** y **Hotelería**. Es fundamental para las empresas tener una visibilidad completa de las tendencias y amenazas más comunes que impactan en su organización.

Educación

Atención Médica

Hotelería

Ventas al por Menor

Educación

En el sector de educación, los maestros y el personal son responsables de proteger la red de amenazas externas, pero también son responsables de proteger a los estudiantes del contenido inapropiado y malicioso. Los dispositivos móviles reemplazan a los libros de textos en las escuelas de todo el mundo. Esta tendencia abrió la puerta a la diseminación de malware en todos los predios escolares, lo que deja a los sistemas de red críticos en una posición vulnerable. Para proteger a los estudiantes y a las redes de las que dependen, las escuelas tienen que monitorear y filtrar el tipo de contenido al que acceden los estudiantes.

> Con la plataforma de WatchGuard, hemos observado que tenemos una mayor visibilidad de los tipos de datos que se envían, lo que nos permite tomar decisiones más informadas, mantener nuestro cumplimiento y proporcionarle a nuestra escuela un mayor nivel de protección ante las amenazas inadvertidas.
>
> *~ Aaron Anderson, Vicepresidente, Tecnología de la Información, Anthem College*

Director

Es un imperativo de mi escuela proporcionales a mis estudiantes y al personal un acceso a Internet seguro, consistente y rápido. Comprendemos que el acceso a Internet es esencial para las investigaciones de proyectos y como una emergente ayuda de aprendizaje. Pero también comprendemos que los estudiantes pueden visitar sitios ilegales o inapropiados si no se los monitorea.

Ventas al por Menor

Los minoristas intercambian datos de clientes con sus sedes centrales y, generalmente, ofrecen Wifi para invitados para fomentar visitas más largas y repetidas. Cuando finalmente ocurre una infracción, el limitado personal de TI del minorista necesita una notificación clara e inmediata para poder tomar las medidas necesarias para mitigar el problema. Y mientras el Wifi para invitados ciertamente tiene sus beneficios, presenta un potencial punto ciego en la red. Los clientes que transmiten medios o usan otras aplicaciones que requieren un intensivo ancho de banda pueden fácilmente causar una disminución en la velocidad de transacciones en el sistema de POS. Los profesionales de TI necesitan visualizar los entornos de los invitados para poder asegurar que los sistemas de POS tengan suficiente ancho de banda para procesar rápidamente las transacciones.

> Con una combinación de las soluciones de Dimension y Gestión Unificada de Amenazas (UTM) de WatchGuard, mi equipo puede observar la salud de la red completa en tiempo real, investigar las obstrucciones e implementar políticas para resolver el problema. Todo esto se puede realizar en menos de una hora.
>
> *~ Tony Sim, Gerente de TI, EpiCentre*

Propietaria de la Empresa

El Wifi para invitados es de gran valor para mi empresa, pero no puedo permitir que afecte un aspecto fundamental de mi empresa: las transacciones de punto de venta (POS). Necesito una solución interna que sea fácil de gestionar y que le proporcione a mi pequeño equipo de TI el conocimiento necesario para mantener las operaciones empresariales en marcha y a mis clientes felices.

Hotelería

Un sistema de gestión de propiedades (PMS) es una aplicación de software que utilizan los hoteles para automatizar y coordinar diversas funciones empresariales que incluyen desde operaciones de atención al cliente hasta operaciones administrativas, como la gestión de la información de las tarjetas de crédito. Además, los sistemas PMS comúnmente se integran a los POS y a los sistemas de reservas, lo cual constituye un objetivo muy valioso para los criminales cibernéticos. Muchas cadenas de hoteles importantes han sido víctimas de infracciones en los sistemas PMS o POS, lo cual les significó multas, demandas y daños a su reputación. Sin la visibilidad de las redes de invitados y las corporativas, las empresas del sector de hotelería no pueden responder ante las infracciones y el tiempo sin actividad en la red.

> Ahora tenemos la visibilidad necesaria para detectar muy rápidamente dónde está el trafico excesivo, por punto de acceso (AP), usuario de Wifi, usuario cableado, por protocolo o puerto. Además, fue muy sencillo hacer que el inicio de sesión y la visualización con Dimension sean operacionales sin tener que retocar o personalizar el proceso, como generalmente sucede con los sistemas de generación de informes.
>
> *~ Fahyaz Khan, Gerente de TI, Kensington Close Hotel*

Gerente General

Necesito que todos los procesos diarios funcionen sin problemas. El tiempo sin actividad de red puede significar pérdidas en los ingresos y clientes insatisfechos, lo que, en esta época de Yelp, se traduce en malas críticas y pérdidas de ingresos. Una infracción de datos es aún peor ya que la prensa hará que clientes potenciales busquen en otros lugares alojamiento y salas.

Atención Médica

La industria de atención médica se enfrenta a una serie de desafíos de seguridad únicos que surgen de la naturaleza altamente confidencial y valiosa de los datos que se intercambian en la red. La HIPAA, junto con estándares globales similares, exige que las organizaciones que procesan datos de pacientes cumplan con una serie de estrictas prácticas de seguridad. Diversos tipos de tecnologías médicas han evolucionado para intercambiar datos de manera inalámbrica, lo cual abre una nueva ventana de vulnerabilidad. Las organizaciones de atención médica necesitan tener una visibilidad completa de la salud de sus pacientes y de sus recursos de red para garantizar el mejor cuidado posible a la vez que se cumple con los estándares de protección de datos en evolución.

> Ahora contamos con una solución líder mundial en la que podemos confiar un rendimiento seguro y, sobre todo, confiar el acceso seguro a la información confidencial del paciente, ya sea desde un dispositivo portátil o PC.
>
> *~ Paul Freear, Jefe de Servicios al Cliente de TI de Northern Lincolnshire*

Administrador de Red

Al ser responsable de una vasta cantidad de dispositivos conectados en mi red, necesito visibilidad total de cada conexión y de cada vulnerabilidad potencial que se presente. Son esenciales las herramientas de generación de informes e inicio de sesión integrales y precisas para mantener el cumplimiento de la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), un requisito ineludible para mi organización de atención médica.

La Visibilidad de Red Impacta en una Amplia Variedad de Funciones

La necesidad de contar con una visibilidad de red completa se extiende más allá de la oficina de TI. Con implicaciones que van desde cumplimiento hasta productividad, las ganancias de visibilidad pueden beneficiar a las funciones en todo tipo de organizaciones.

Propietarios de Empresas

Los propietarios de empresas tienen que asegurarse de que sus inversiones en tecnología les están brindando valor a sus negocios. Los paneles de control muestran la cantidad de tráfico analizado y los virus bloqueados, así como también los informes de uso que proporcionan conocimientos de alto nivel para el valor de los sistemas de TI.

Administradores de Red de TI/ Directores de TI

Los administradores de TI son generalmente responsables de la gestión de múltiples tecnologías empresariales a través de una gestión intuitiva y de recursos de visibilidad altamente valiosos. Como las primeras personas que responden ante los eventos de seguridad, los administradores dependen de las alertas en tiempo real y detalles pormenorizados para rápidamente diagnosticar y mitigar las amenazas.

Los Directores de Finanzas (CFO)/ Oficiales de Cumplimiento

Los Directores de Finanzas (CFO) evalúan constantemente el gobierno, los riesgos y el cumplimiento en toda la organización. Con escaso tiempo para sumergirse en los resúmenes de los paneles de control, estos individuos dependen de los informes de resumen diseñados para los estándares de cumplimiento específicos de su organización, lo que incluye la HIPAA y las normas de la Industria de Tarjetas de Pago (PCI).

Oficiales de Seguridad de Información Central

El liderazgo ejecutivo desea una revisión de alto nivel de toda la actividad de red para desarrollar e implementar estrategias de seguridad y también monitorear y aplicar las políticas corporativas. Los informes de resumen automatizados les proporcionan los conocimientos que necesitan para mantenerse al día en las amenazas de seguridad que enfrenta su organización.

Supervisores

Los empleados generalmente usan computadoras portátiles, tabletas y otros dispositivos conectados para completar sus tareas diarias. A pesar de que esta tecnología proporciona grandes ganancias en productividad, su uso inapropiado puede causar el desperdicio de muchas horas. Los gerentes dependen de una visibilidad completa, lo que incluye informes de resumen y panel de control para monitorear la actividad de red.

Elimine los Puntos Ciegos de su Red

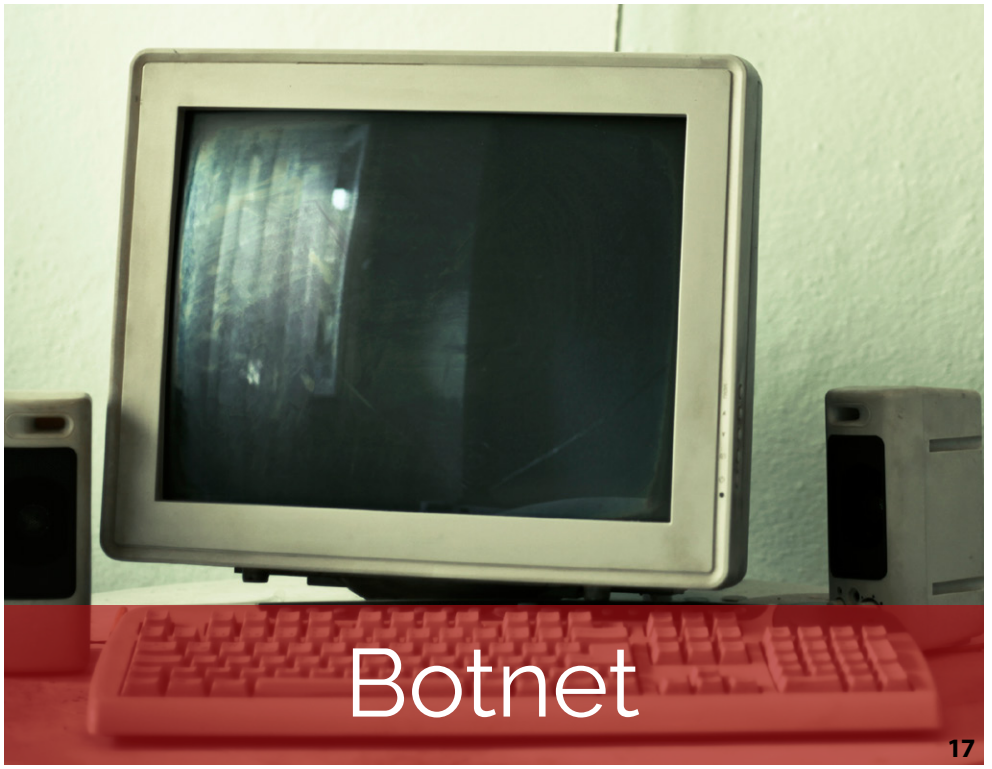
WatchGuard está adelantado años luz dentro de la industria de seguridad de red con un caudal de tecnologías que detectan amenazas, identifican tendencias y detienen las actividades potencialmente peligrosas antes de que impacten en sus operaciones diarias.

Cuatro Puntos Ciegos Comunes

Actividad de Red

Dispositivos Conectados

Dispositivos Móviles



Botnet

Punto Ciego: Actividad de Red

Solución: WatchGuard Dimension

WatchGuard Dimension® es una solución de seguridad apta para funcionar en la nube que brinda visibilidad completa de toda la actividad de red. Extraiga información rápidamente con vistas e informes detallados de su actividad de red mientras identifica inmediatamente amenazas de seguridad, problemas y tendencias antes de que se conviertan en problemas masivos.

Dimension ofrece más de 100 informes y paneles de control de seguridad integrales. Desde un nivel superior, los administradores pueden ver quién consume más ancho de banda, patrones de tráfico inusuales y los sitios web más visitados. Luego, puede explorar en profundidad los datos de registros individuales para obtener detalles pormenorizados.

Ya sea que usted ocupe un cargo ejecutivo de alto nivel, sea director de TI, oficial de cumplimiento o propietario de una pequeña empresa, los informes se pueden diseñar según sus necesidades para obtener una visibilidad de red completa.

Punto Ciego: Actividad de Red

Solución: WatchGuard Dimension

Panel de Control Ejecutivo

Esta vista de alto nivel le brinda un panorama del tráfico permitido en la red, lo que incluye dominios, aplicaciones y los tipos de sitios web. A partir de allí, los administradores pueden explorar en profundidad y ver los datos en un nivel pormenorizado.

Panel de Control de Seguridad

El Panel de Control de Seguridad le muestra todo el tráfico bloqueado, lo que incluye ataques de malware y clientes y protocolos denegados. También rastrea la actividad de IPS y le muestra a los administradores las últimas amenazas detectadas rápidamente. Las direcciones de IP asociadas, los nombres de dominio y las aplicaciones se pueden agregar a la lista de Sitios Bloqueados para obtener protección automática en el futuro.

FireWatch

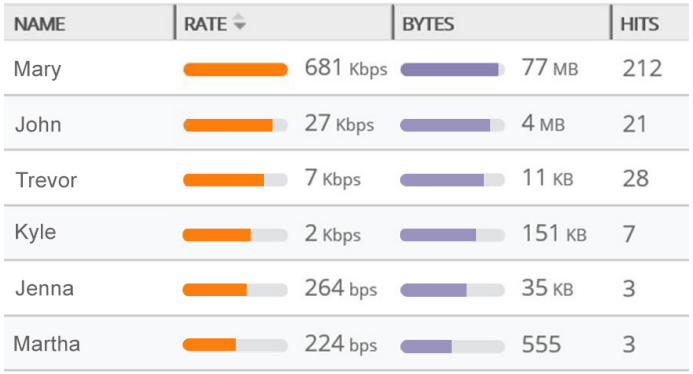
FireWatch es un panel de control interactivo en tiempo real que filtra el tráfico en una forma que trae a la superficie instantáneamente la información más fundamental sobre los usuarios activos y conexiones. FireWatch le permite ver qué está consumiendo el mayor ancho de banda y qué sitios y aplicaciones son los más populares.

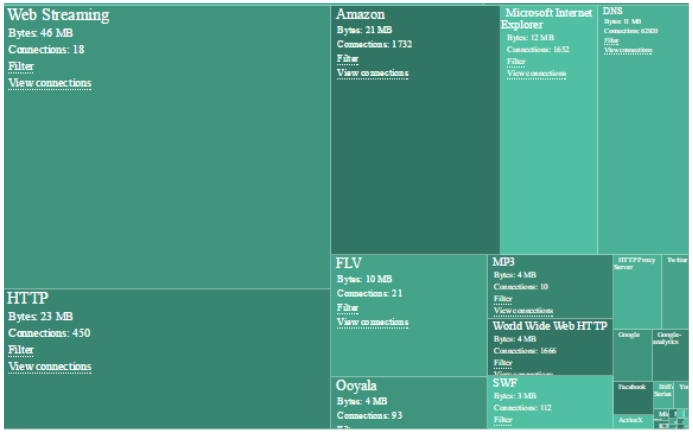
Informes de Salud

Como recurso de prevención, los Informes de salud le permiten identificar problemas potenciales antes de que se conviertan en verdaderos problemas. El uso de interfaz física, memoria y CPU son factores críticos para lograr el máximo tiempo de operación. Sin la visibilidad de estas estadísticas de salud, las organizaciones corren el riesgo de sobrecargar y desactivar inadvertidamente los equipos de red.

Mapa de Políticas

El Mapa de políticas muestra el impacto de las políticas en toda la red, lo que simplifica la identificación de configuraciones incorrectas. El Mapa de políticas también muestra el flujo general del tráfico de red y permite que los administradores filtren y dinamicen los datos para revelar detalles más valiosos.



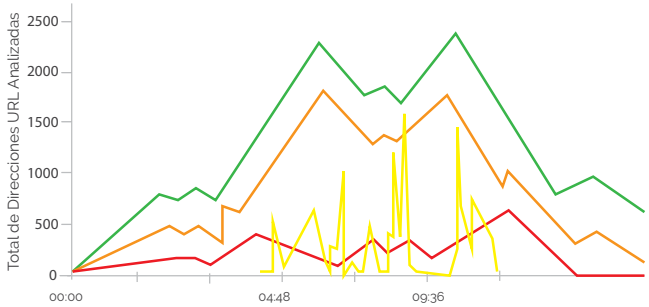


Punto Ciego: Actividad de Red

Solución: WatchGuard Dimension

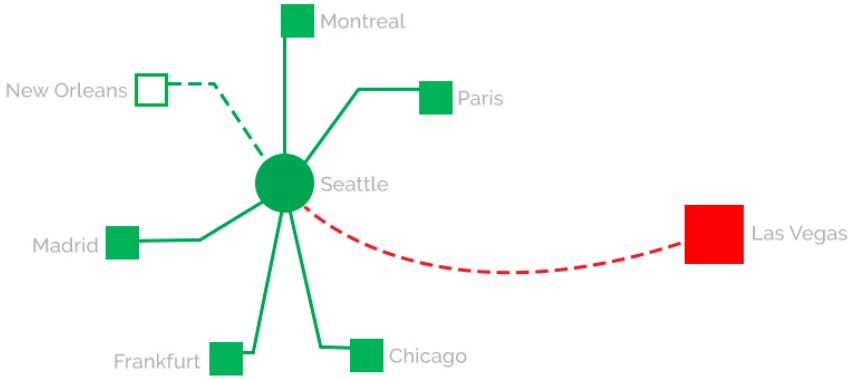
Panel de Control de Servicios de Suscripción

El Panel de control de Servicios de Suscripción le brinda un resumen de rendimiento integral con estadísticas que muestran los resultados del análisis de Firebox®. También le permite brindar información en un formato fácil de entender para los usuarios no técnicos.



Informe de Uso de Políticas

El Informe de Uso de Políticas proporciona perspectivas valiosas acerca de la frecuencia de uso de las políticas. Este informe le permite mantener las políticas de firewall actualizadas y elimina aquellas que no son necesarias. Las políticas que no se usan presentan una falla de seguridad ya que los hackers puede aprovecharse de ellas para infiltrarse en la red.

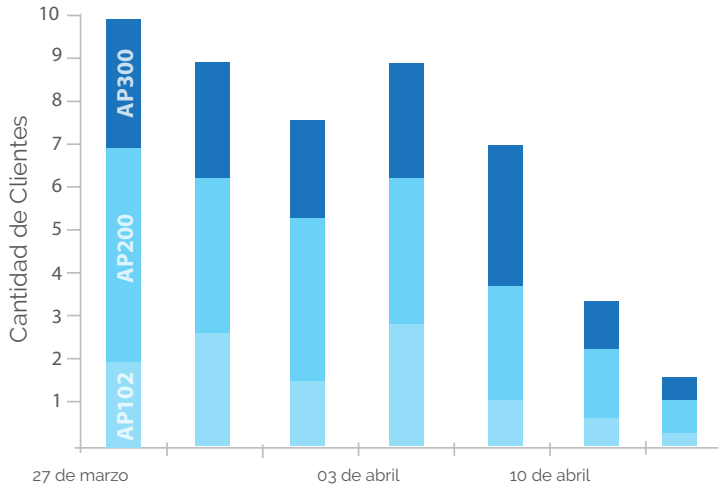


Centro y VPN Spoke

Nunca ha sido más simple monitorear el estado de las conexiones seguras de las oficinas sucursales. Las organizaciones pueden establecer y gestionar los túneles de VPN de forma rápida y fácil dentro del Centro de Dimension y el Generador VPN Spoke.

Panel de Control del Punto de Acceso

Uno de los más comunes puntos ciegos de seguridad dentro de una organización proviene de sus redes inalámbricas. El Panel de control de AP muestra información valiosa para los puntos de acceso conectados, lo que incluye una tabla con las opciones de dinamización y período para ver la cantidad de bytes o de clientes en un dispositivo AP.



Punto Ciego: Dispositivos Conectados

Solución: Network Discovery de WatchGuard

El análisis de su red para detectar los dispositivos no autorizados es un paso fundamental para verdaderamente comprender su red. El servicio de suscripción Network Discovery de WatchGuard realiza un análisis completo de red que genera un mapa visual de todos los dispositivos conectados. Esto proporciona una visibilidad total de todas las conexiones. Con Network Discovery, las organizaciones pueden garantizar que solo los dispositivos autorizados estén conectados a la vez que se detectan todos los protocolos y los puertos abiertos.

Punto Ciego: Dispositivos Móviles

Solución: Mobile Security de WatchGuard

El servicio de suscripción de Mobile Security de WatchGuard ofrece un nivel adicional de visibilidad de red ya que le permite a los administradores identificar y realizar auditorías de los dispositivos móviles que se intentan conectar a su red. Prevenga el acceso por parte de dispositivos descifrados o descodificados y bloquee aquellos dispositivos que descargan aplicaciones desde fuentes no autorizadas.

Punto Ciego: Botnet

Solución: Reputation Enabled Defense (RED) de WatchGuard

Las redes o computadoras infectadas, comúnmente denominadas botnet, las usan los cibercriminales para atacar o infiltrarse en un objetivo específico. Los empleados desprevenidos se unen inadvertidamente a las botnet luego de ser víctimas de sitios web (drive-by download) o de un ingeniosamente diseñado correo de suplantación de identidad. Cuando el código malicioso ingresa en la computadora del empleado, el experto en botnet puede usar el dispositivo comprometido como un soldado adicional de su corrupto régimen. Sin la visibilidad de estos sitios web o máquinas víctimas, está respaldando, sin saberlo, a los soldados de una campaña de terror. Con la integración de WatchGuard de la Detección de botnet en el servicio de Reputation Enabled Defense, las organizaciones obtienen visibilidad en tiempo real de los clientes infectados y de los sitios que los conducen hacia el lado oscuro.

“Nos referimos a la visibilidad como la capa faltante de la seguridad de información, pero, en realidad, es más bien como unos lentes de visión nocturna. Le permite observar áreas que antes eran solo un vacío sombrío. No importa cuán buena sea su seguridad, el panorama de amenazas continuará evolucionando. Ya que no puede detener todos los ataques, necesita mecanismos que lo ayuden a ver, analizar y responder frente a ellos antes de que sea demasiado tarde”.

Corey Nachreiner, Director Tecnológico de WatchGuard

WatchGuard® Technologies, Inc. es líder mundial de soluciones de seguridad comercial multifuncionales e integradas que de manera inteligente combinan el estándar de la industria en hardware, características de seguridad de primer nivel y herramientas de gestión basadas en políticas. WatchGuard brinda una protección fácil de usar, pero de grado empresarial para miles de negocios en todo el mundo. Para obtener más información, visite **WatchGuard.com/visibility**.

1. SANS Institute, “Ninth Log Management Survey Report” (Noveno informe de la encuesta de gestión de informes), octubre de 2014

2. Ponemon Institute, “The Post Breach Boom” (La explosión posterior a la infracción)

3. Ponemon Institute, “2014: A Year of Mega Breaches" (2014: un año de grandes infracciones)

4. Ponemon Institute, “2015 Cost of Data Breach Study: Global Analysis” (Estudio de 2015 sobre el costo de la infracción de datos: un análisis global)

5. Verizon, “2014 Data Breach Investigations Report” (Informe de 2014 sobre las investigaciones de infracciones de datos)