Derribar los Silos de Seguridad:

Lograr la Seguridad Mediante la Correlación

Ya sea que tenga una organización empresarial distribuida con 10 oficinas sucursales o una pequeña o mediana empresa con 10 empleados, distintas soluciones y entornos pueden causar brechas en la información de seguridad. Estos silos de seguridad presentan un gran problema para los equipos de TI que luchan por conectar la información en oficinas centrales y sucursales, o que lidian con soluciones de red y puntos finales de red incompatibles entre su red y de puntos finales de red.

Aquí le presentamos algunos “silos” comunes que puede encontrar en la actualidad.

1

A medida que las amenazas de seguridad contra las organizaciones de todos los tamaños siguen creciendo, hemos adoptado un enfoque de tipo «complementario» respecto de la seguridad. Esto incluye añadir a su infraestructura actual soluciones para problemas específicos, aún cuando no se comuniquen entre sí. Esto puede crear silos en su organización entre las soluciones de seguridad no relacionadas.

2

Las empresas distribuidas pueden encontrar discrepancias en la seguridad que se aplica en las oficinas centrales respecto de aquella de las oficinas sucursales. Contar con diferentes niveles de seguridad es razonable para estos tipos de organizaciones, pero puede crear un silo para que los equipos de TI administren varios sistemas de seguridad y ubicaciones.

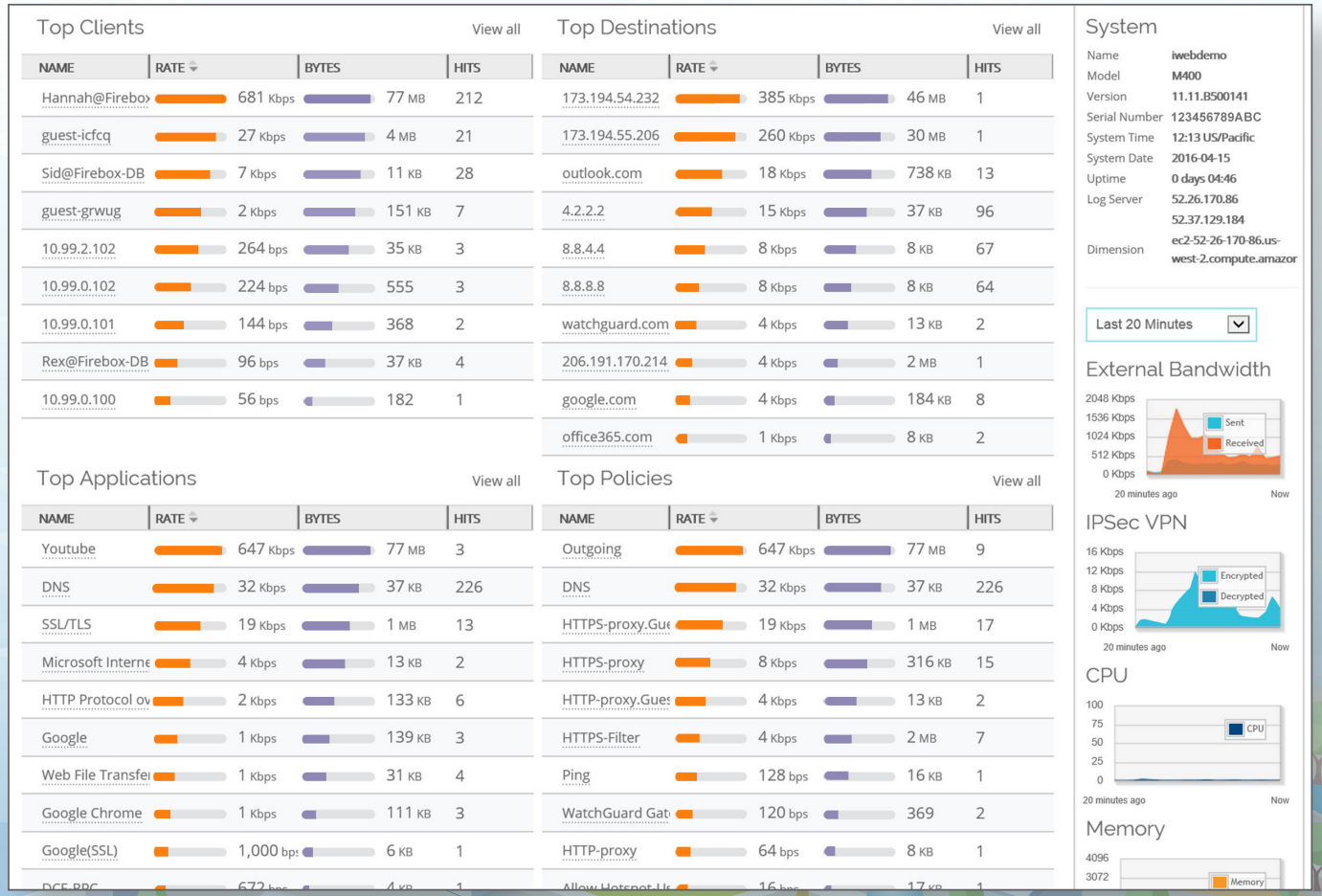
3

Los empleados remotos pueden ser especialmente susceptibles de amenazas, ya que rara vez se encuentran detrás del firewall. La falta de visibilidad completa de estos equipos remotos puede crear un vector vulnerable de ataque para hackers que buscan una entrada a su red.

Comenzar con la Red

La red contiene un tesoro escondido de información de seguridad. Contar con visibilidad de los patrones de tráfico bloqueados o inusuales, de las visitas a sitios web maliciosos o riesgosos y detectar botnets y otras amenazas es una medida fundamental para proteger su organización. También es importante saber qué equipos están conectados a su red, lo que garantiza que solo aquellas personas con privilegios y políticas de seguridad adecuadas tengan acceso.

Saber qué es lo que ocurre en su red también puede brindar información sobre la capacidad de proceso y los impactos en el rendimiento según el uso. Es fundamental obtener visibilidad sobre qué usuarios consumen más ancho de banda y saber para qué lo están usando, a fin de poder controlar la falta de rendimiento.



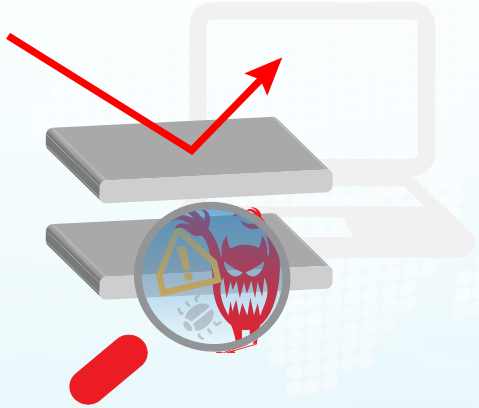
Red

Extremo

Moverse hacia el Extremo

La visibilidad de sus puntos finales comienza al conocer sus equipos y garantizar que se tomen las medidas de seguridad correspondientes para protegerlos. También es importante saber si algún usuario es particularmente susceptible de amenazas o si ya está infectado.

Existen **dos capas de visibilidad** para proteger el extremo:
bloquear lo que conoce y **averiguar lo que no conoce**.



Las soluciones de antivirus actuales que aprovechan firmas son una excelente forma de bloquear las amenazas que ya conocemos. Sin embargo, pueden existir brechas en esta capa de protección, ya que las actualizaciones de revisiones solo se hacen semanalmente o cuando son necesarias.

Detectar lo que usted no conoce puede ser un poco más complejo. Existen una variedad de soluciones que usan diferentes métodos para determinar si un evento es una amenaza. Ya sea que esté rastreando heurística, análisis de comportamiento o cambios en los archivos, procesos y registros, es fundamental contar con visibilidad del extremo. Sin esta información, las organizaciones pueden quedar excesivamente vulnerables a los ataques de malware y de ransomware.

Mejorar la Inteligencia ante Amenazas

Gartner define la inteligencia ante amenazas como «*conocimiento basado en la evidencia, incluido el contexto, mecanismos, indicadores, implicaciones y consejo accionable acerca de una amenaza existente o emergente o peligro para los bienes, que se puede usar para informar sobre decisiones relacionadas con la respuesta del sujeto a dicha amenaza o peligro*».

Lo sentimos... ¿Qué? Básicamente, la inteligencia ante amenazas recopila toda la información que conocemos sobre una amenaza existente o recientemente liberada para informar a las víctimas potenciales, con la esperanza de poder bloquear la amenaza mediante firmas. Eso suena tedioso y lento. Aunque no lo crea, existen proveedores que están dispuestos a hacerlo, cobrarle una GRAN cantidad de dinero y ofrecerlo principalmente a empresas.

Si bien existen varias fuentes de amenazas disponibles de forma gratuita, es importante recordar que lo barato sale caro. Las fuentes de inteligencia ante amenazas gratuitas por lo general no se actualizan con frecuencia, lo cual significa que se le podría escapar una amenaza detectada hoy o incluso esta semana. Además, las fuentes de inteligencia ante amenazas de nivel empresarial suelen funcionar mejor en conjunto, pero son muy costosas para las pequeñas y medianas empresas.

No obstante, la inteligencia ante amenazas es un elemento importante a la hora de defenderse contra la creciente cantidad de amenazas que enfrentan las pequeñas y medianas empresas. Estos sitios se actualizan casi en tiempo real y brindan la información más precisa sobre las amenazas conocidas que pueden causar un daño grave a una organización.

Crear un Conjunto con la Correlación

Contar con información sólida obtenida individualmente de la red, el extremo y las fuentes de inteligencia ante amenazas es fundamental para proteger su organización. Sin embargo, es difícil comprender realmente qué sucede mientras esta información sigue operando en silos. La magia ocurre realmente cuando se crea un conjunto mediante la correlación.

La correlación lleva la visibilidad de estas fuentes al siguiente nivel. Al combinar en un solo lugar todos los datos de eventos recolectados, las organizaciones pueden responder mejor mediante la perspectiva accionable. Analizar y priorizar esta información equipa mejor a los equipos de TI para que puedan responder con confianza a estas amenazas, que son las más peligrosas para la seguridad o para la productividad de la empresa. Esto se vuelve realmente importante para las organizaciones con tiempo y recursos limitados, ya que disminuye el tiempo de detección y permite una acción más eficiente y efectiva ante los ataques más graves.

Correlación

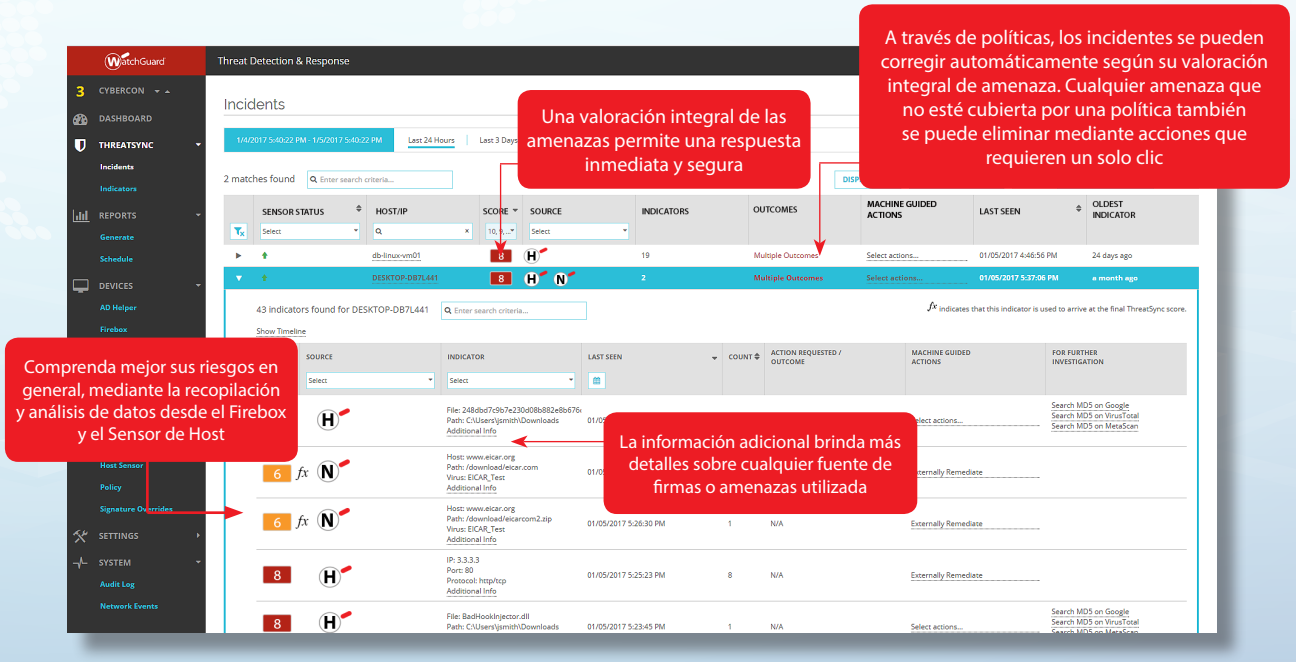
Correlacione, Priorice y Responda con WatchGuard

Si la correlación es tan buena, ¿por qué nunca antes oímos hablar de ella? Honestamente, es una muy buena pregunta. Y la respuesta simple es que no es algo fácil de hacer ni precisamente de automatizar.

Pero el nuevo servicio de seguridad de WatchGuard, Detección y Respuesta ante Amenazas (Threat Detection and Response, TDR), brinda capacidades de correlación de nivel empresarial para pequeñas y medianas empresas y empresas distribuidas.

ThreatSync, el componente de motor con correlación y valoración basado en la nube de TDR, analiza los datos de amenazas de Firebox, de los WatchGuard Host Sensor instalados en los endpoints y de las fuentes de inteligencia sobre amenazas de terceros. ThreatSync luego analiza estos datos para crear una valoración de amenazas integral según la gravedad para guiar la corrección. ¿Desea saber más sobre una posible amenaza? Los archivos sospechosos pueden enviarse para un análisis profundo a cargo de APT Blocker de WatchGuard, un espacio aislado de última generación en la nube.

Lo mejor de todo es que TDR viene con el conjunto de aplicaciones Total Security Suite e incluso recopila información de otros servicios de seguridad avanzada del conjunto, entre ellos, APT Blocker, WebBlocker y Reputation Enabled Defense (RED). WatchGuard es el único proveedor de servicios de Gestión Unificada de Amenazas (Unified Threat Management, UTM) que ofrece todos estos servicios de seguridad en un solo lugar, y el único que brinda capacidades sólidas de correlación para



Correlacione. Priorice. Responda.

El servicio de seguridad de WatchGuard, Threat Detection and Response, ofrece capacidades de correlación empresarial para pequeñas y medianas empresas y empresas distribuidas. No piense únicamente que puede haber un problema; sepa si existen soluciones líderes del sector que lo ayuden a iluminar su extremo, detectar y correlacionar amenazas y proteger sus bienes más importantes.

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