

# Filtrado de URL y seguridad Web de Cascadia Labs

Resultados del verano de 2009

## Resumen ejecutivo

En verano de 2009 Cascadia Labs realizó varias pruebas de eficacia de cinco gateways de Internet seguros líderes en el mercado, incluidos tres appliances de perímetro de Blue Coat y McAfee, software de Websense y Trend Micro InterScan Web Security Virtual Appliance.

Cascadia Labs realizó las pruebas con URL que recopiló, clasificó y verificó de forma independiente usando sus propios sistemas (las URL no fueron suministradas ni eran conocidas

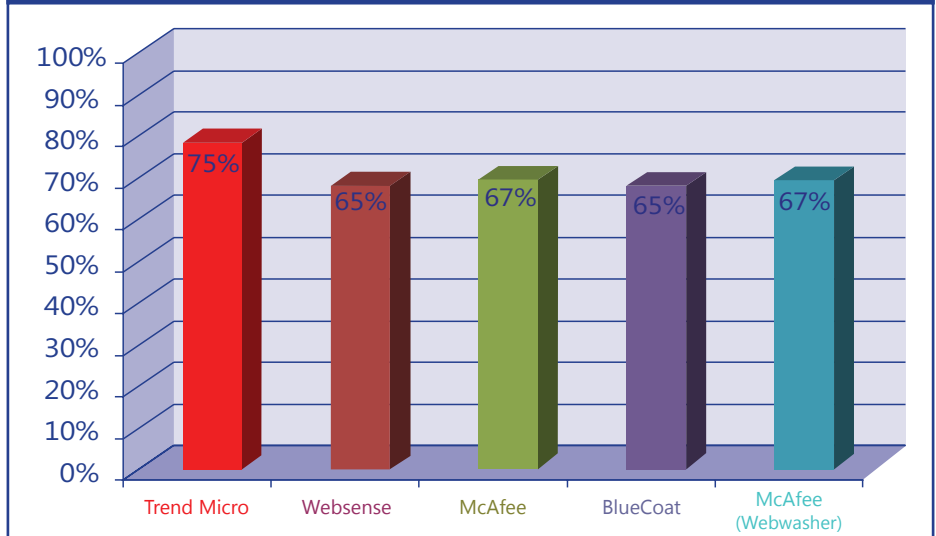
**Trend Micro se erigió como el claro vencedor, manteniendo el liderazgo obtenido en 2008.**

por parte de las empresas cuyos productos se probaron). Recopilamos y verificamos las URL de seguridad en los días inmediatamente anteriores a las pruebas para garantizar que representaban amenazas actuales, incluidos los posibles ataques de día cero que se produjeran.

En estas pruebas, Trend Micro se erigió como claro vencedor general, afianzando de este modo la posición líder que estableció en nuestras pruebas de finales de 2008.

Trend Micro también demostró una marcada ventaja frente a las amenazas de seguridad, con una contribución significativa de sus servicios de reputación Web. Trend Micro obtuvo la mejor puntuación en cada una de las categorías de seguridad (malware,

Gráfico 1 - Eficacia general del bloqueo (media ponderada)



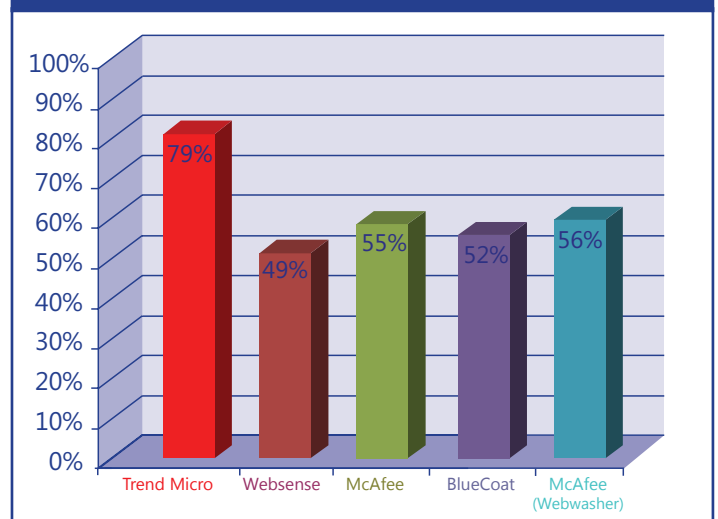
vulnerabilidades, phishing, proxys y aplicaciones potencialmente no deseadas). Con una eficacia general del bloqueo de las amenazas de seguridad de casi un 80%, Trend Micro IWSVA Secure Web Gateway es una solución que destaca claramente del resto de los productos, con unas puntuaciones medias de entre el 49 y el 55%.

## Introducción general

Los gateways de Internet seguros poseen una nutrida gama de capacidades para gestionar, bloquear y controlar el contenido Web en el perímetro. Las empresas confían en estos productos para proteger a sus empleados,

equipos informáticos y redes frente al contenido peligroso, inapropiado y no deseado que circula por la red. Además de aplicar políticas de uso para las páginas Web que contienen contenido sexual explícito, violento o ilegal, estos productos también desempeñan una función vital en la seguridad de

Gráfico 2 - Eficacia del bloqueo de seguridad general



las redes corporativas frente a amenazas Web, incluidas las descargas automáticas, el malware y los ataques de phishing.

A medida que estas amenazas de seguridad de Internet aumentan en frecuencia, volumen y sofisticación, resulta más evidente la necesidad de agregar capas adicionales de protección a una estrategia de seguridad con defensa exhaustiva. Mientras que el filtrado de los sitios para adultos y no productivos tiene carácter prioritario, existen grandes variaciones en cuanto a la eficacia de los productos a la hora de combinar funciones como bases de datos de URL y servicios de reputación Web para bloquear las amenazas de seguridad.

En verano de 2009 Cascadia Labs sometió a distintas pruebas cinco gateways de Internet seguros líderes del mercado: appliances de perímetro de Blue Coat y McAfee (incluido un producto anterior, Webwasher), software Websense y el appliance virtual de Trend Micro. Trend Micro se erigió como claro vencedor general, con una marcada ventaja frente a las amenazas de seguridad.

Como se muestra en el Gráfico 1, Trend Micro InterScan Web Security Virtual Appliance (IWSVA) obtuvo una puntuación general ponderada del 75%. Los dos productos de McAfee consiguieron el segundo puesto, con un 67% cada uno. Además de conseguir la mayor puntuación general, Trend Micro también destacó en el bloqueo de URL que conducían a amenazas de seguridad, con una puntuación dominante del 79%, en comparación con las puntuaciones del resto de productos de aproximadamente un 50%.

Dejando a un lado la seguridad, los productos de filtrado de URL también realizan una función importante en la aplicación de políticas de uso en las redes de las empresas. Según las pruebas realizadas, podemos afirmar que todos ellos bloquean la gran mayoría de URL de las categorías de adultos y productividad y ocio, y que

todos ellos funcionan adecuadamente, aunque con margen para mejorar, en los grupos de uso de ancho de banda, comunicaciones y responsabilidad legal.

### Productos probados

Cascadia Labs probó los cinco productos siguientes durante agosto de 2009:

- **Trend Micro InterScan Web Security Virtual Appliance v5**
- **Websense Security Suite v7.1**
- **McAfee Email and Web Security Appliance 3000**
- **Blue Coat Proxy SG 210A v5.4.1.12**
- **McAfee Web Gateway WW500E (anteriormente Webwasher) v6.8**

IronPort no nos permitió comprar su software para la realización de estas pruebas.

Se debe recordar que Websense ha cambiado el nombre del producto a "Websense Web Security".

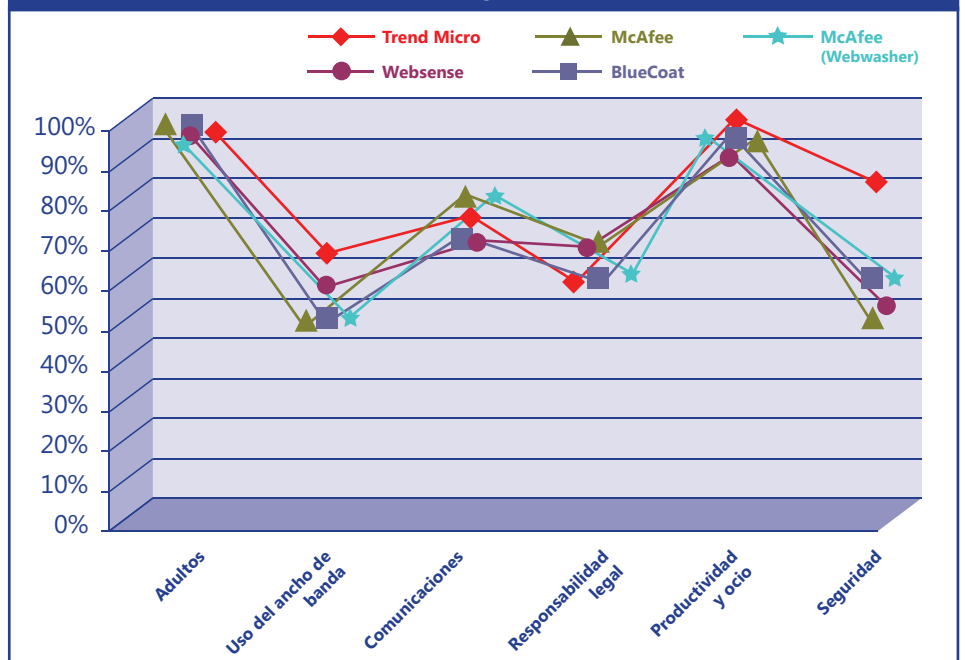
A lo largo del presente informe, Cascadia Labs se centra exclusivamente en la eficacia del bloqueo de las bases de datos de URL y la reputación Web de los productos.

### Resultados y análisis

Trend Micro IWSVA, que incluye funciones de valoración remota y reputación Web, se mantuvo de forma constante en la posición principal o muy cerca de ella en cuanto a la eficacia de bloqueo de cada uno de los tipos de contenido (Gráfico 3).

En los últimos años, las funciones de valoración remota y reputación Web han permitido que muchos productos de gateways de Internet seguros tengan una mejor respuesta al complejo y variable entorno Web. En vez de solo consultar una copia local de una base de datos de URL, los productos con valoración remota pueden realizar consultas a servidores remotos para ofrecer la información más actualizada. De forma similar, los productos con funciones de reputación Web pueden usar tecnología heurística para detectar patrones poco comunes detrás de los evidentes en el contenido de la página. Aunque nosotros analizamos la contribución de estos distintos enfoques, en última instancia son los clientes los que se preocupan por la capacidad del producto para bloquear URL no deseadas independientemente de la tecnología implicada, motivo por

Gráfico 3 - Eficacia del bloqueo (por grupo)



el que los informes que publicamos solo muestran los resultados más destacados de la eficacia del bloqueo.

El gran reto para esos productos sigue siendo las amenazas a la seguridad. Las tasas medias de bloqueo se sitúan en un 58%, relativamente bajas si se comparan con otras categorías, aunque la media ha mejorado en el último año. En esta área, Trend Micro ha mostrado una ventaja clara sobre el resto de los productos probados.

En las categorías no relacionadas con la seguridad, las variaciones en la eficacia fueron escasas. Los productos bloquearon las URL relacionadas con la responsabilidad legal en una media del 59%, sin que destacara ningún producto en concreto. El bloqueo del uso del ancho de banda fue menos eficaz en general, con un porcentaje del 47%. Los productos bloquearon las URL de comunicaciones, incluida la omnipresente categoría de medios sociales, con una media del 69%. Como en trimestres anteriores, los grupos de adultos y productividad y ocio son gestionados eficazmente por todos los productos sin diferencias reseñables.

### Seguridad

La media de bloqueo de Trend Micro del 79% en todas las categorías de seguridad lo situó radicalmente por encima del resto de productos, los

cuales variaron en eficacia entre un 49 y un 55%. Su capacidad de bloqueo de cuatro de cada cinco amenazas, incluso sin activar la exploración del perímetro, demuestra el valor que puede añadir un gateway de Internet seguro como parte de una estrategia de seguridad con defensa exhaustiva.

### Malware

Trend Micro bloqueó tres cuartos de todas las URL de malware, seguido de McAfee 3000 con un 62%. El resto de productos obtuvo un porcentaje de bloqueo de entre un 53 y un 55%. Definimos "URL de malware" como las URL que redireccionan directamente a archivos binarios maliciosos (que suelen usar trampas de la ingeniería social para confundir a los usuarios para que los descarguen e instalen involuntariamente) y las URL con rutinas maliciosas introducidas durante las descargas automáticas.

El bloqueo de URL de malware es una alternativa con escasa latencia a la búsqueda de binarios en el perímetro. Para centrarnos en las capacidades de bloqueo de URL de los productos, Cascadia Labs no realizó ninguna búsqueda de malware para estas pruebas.

### Vulnerabilidades de seguridad

Trend Micro bloqueó cerca del 80% de las URL que se aprovechan de vulnerabilidades mientras que el resto

de productos lo hizo solo en un 48-58%. Las vulnerabilidades de seguridad, o las descargas automáticas, son amenazas muy molestas que pueden explotar los puntos débiles de los exploradores y las aplicaciones de otros fabricantes cuando los usuarios visitan una página Web. Es especialmente importante que los gateways de Internet seguros bloqueen estas amenazas puesto que son invisibles y que pueden contenerlas incluso sitios de confianza muy visitados, generalmente como resultado de un ataque SQL Injection de un hacker o por contenido generado por los usuarios.

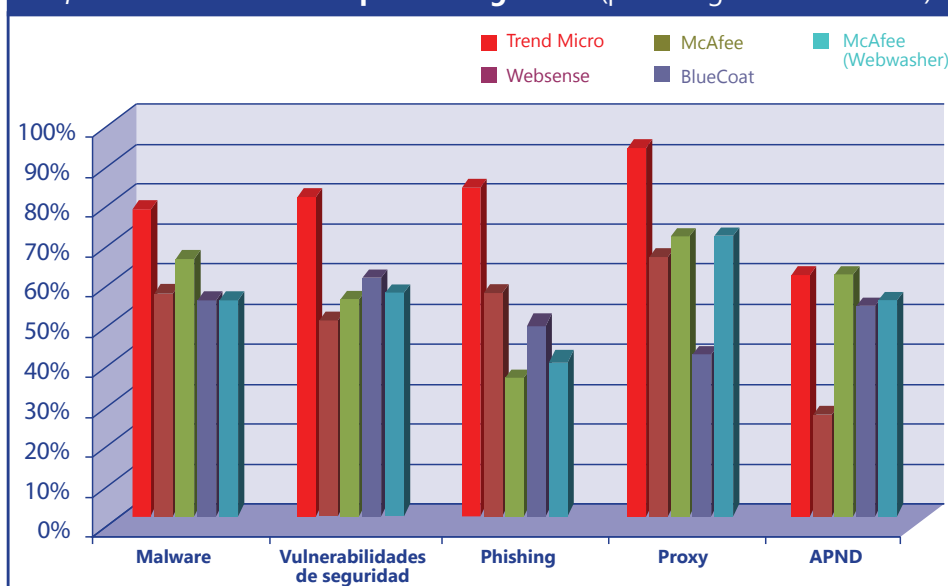
### Phishing

Trend Micro consiguió bloquear más de un 80% de las URL de phishing. Websense y Blue Coat bloquearon un 55% y un 47%, respectivamente, mientras que la tasa de bloqueo de los productos de McAfee no alcanzó el 40%. El phishing es un problema ya familiar, y mientras que los productos de seguridad del correo electrónico pueden eliminar muchos de estos mensajes, los productos de gateways de Internet seguros ofrecen una capa adicional de protección al bloquear el enlace a la URL de phishing peligrosa en los mensajes de correo electrónico que no se filtran de otro modo o a los que los usuarios acceden mediante otro proveedor de correo electrónico sin protección.

### Proxys anónimos

Como en el resto de categorías de seguridad, Trend Micro obtuvo la mejor puntuación: un bloqueo del 91% de los proxys. A continuación le siguen los dos productos de McAfee y Websense, con un bloqueo superior al 60%; Blue Coat quedó en último lugar con una eficacia inferior al 40%. Los proxys anónimos no son peligrosos en sí mismos, si bien permiten a los usuarios burlar las políticas de uso y acceder a contenido no deseado o potencialmente peligroso. Las URL que probamos en este informe son de proxys basados en Internet donde los usuarios introducen una URL en el campo de un formulario.

Gráfico 4 - Eficacia del bloqueo de seguridad (por categoría de amenaza)



### *Aplicaciones potencialmente no deseadas*

Trend Micro y McAfee 3000 bloquearon un 59% de estas URL; las tasas de Blue Coat y McAfee Webwasher fueron también superiores al 50%. Websense solo pudo bloquear un 23% de estas URL. Nuestra definición de "aplicaciones potencialmente no deseadas" incluye herramientas con algunos usos legítimos pero que muchas empresas prefieren bloquear, como es el caso de algunas utilidades del sistema, herramientas de sondeo de la red y el adware.

### **Adultos**

Como suele ocurrir con este grupo, todos los productos obtuvieron un rendimiento superior al 90% de eficacia que esperaba Cascadia Labs. A este grupo pertenece contenido sexual explícito y prendas de ropa interior/ de baño que se pueden considerar inapropiadas para el lugar de trabajo.

### **Uso del ancho de banda**

Al grupo de uso del ancho de banda pertenecen las descargas, las aplicaciones P2P y las URL de streaming, además de sitios Torrent y contenido de vídeo en la red. SurfControl fue el vencedor en esta categoría por un amplio margen con un 75% frente a la media del 59%. IronPort y Trend Micro fueron los siguientes, con un 62 y un 59% respectivamente, siendo la menor puntuación de un 47%. Se debe recordar que nuestras pruebas de uso del ancho de banda comprueban la habilidad de los productos para bloquear URL según la propia URL en vez de un protocolo o tipo de archivo, enfoques complementarios que también pueden adoptar las empresas.

### **Comunicaciones**

El producto Webwasher de McAfee encabezó los resultados de este grupo con un bloqueo cercano a los tres cuartos de todas las URL. El resto de los productos bloquearon entre el 62 y el 69%. Este grupo abarca los sitios de medios sociales, los blogs y las comunicaciones y foros personales.

### **Responsabilidad legal**

McAfee 3000 obtuvo la mejor puntuación, un 63%, seguido de cerca por Websense con un 61%. El resto de productos bloqueó solo la mitad del contenido de este grupo, el cual incluye actividad delictiva, odio y violencia, drogas ilegales y contenido ofensivo. Como ocurre con las categorías de adultos, las empresas suelen bloquear estas categorías para ofrecer un

---

**Las URL de seguridad representan las amenazas actuales y no son suministradas, ni conocidas, por parte de ninguna de las empresas cuyos productos participaron en las pruebas.**

---

entorno laboral más cómodo libre de contenido inadecuado o que pueda desembocar en procesos judiciales.

### **Productividad y ocio**

Como ocurre en el grupo de adultos, hay muy poca diferencia entre los productos en lo que se refiere a las categorías de productividad y ocio; todos los productos bloquearon alrededor del 90% de las URL. Estas categorías incluyen posibles sitios no productivos como sitios de ocio, juegos, noticias y compras.

### **Clasificaciones, corpus y metodología**

---

#### **Puntuación y clasificaciones**

Para calcular los resultados generales hemos aplicado ponderaciones a los resultados de bloqueo brutos que representan lo que creemos que son las prioridades relativas para el cliente empresarial medio. Cascadia Labs vuelve a evaluar esta ponderación trimestralmente, y en los últimos años, la seguridad ha continuado ganando importancia; para este informe, el grupo de seguridad supone un 30% de nuestras puntuaciones generales. El grupo de adultos representa el 20%; el uso del ancho de banda, un

15%; responsabilidad legal, un 15%; comunicaciones, un 10%; y, por último, productividad y ocio, un 10%. Aunque esta ponderación refleja la creciente importancia de los gateways de Internet seguros como componentes de una estrategia de seguridad con defensa en profundidad, también reconoce la necesidad continua de las empresas de bloquear el contenido visible como el de páginas Web de medios sociales u ofensivas.

Se debe tener en cuenta que estas clasificaciones no consideran el rendimiento, la escalabilidad, la interfaz de usuario, las características ni la funcionalidad, únicamente la eficacia del bloqueo frente a nuestro corpus del verano de 2009.

### **Corpus**

Creamos nuestro corpus de URL independiente para atender a los requisitos del mercado empresarial, con especial énfasis en la seguridad. El corpus contiene 22 categorías únicas organizadas en seis grupos con más de 1.600.000 de URL de unos 100.000 dominios únicos, de interés principalmente para los usuarios de habla inglesa.

Nuestro corpus incluye amenazas de seguridad de cinco categorías distintas: malware, vulnerabilidades, phishing, proxy y aplicaciones potencialmente no deseadas (APND). Recopilamos y verificamos las URL de seguridad en los días inmediatamente anteriores a las pruebas para garantizar que representan amenazas actuales, incluidos los posibles ataques de día cero que se produzcan. Esta precisión temporal es crucial para diferenciar la capacidad de los productos para gestionar amenazas Web realistas y efímeras.

Para este informe, Cascadia Labs probó más de 2.000 URL de seguridad que incluían aproximadamente 250 casos de malware, 1.100 vulnerabilidades, 200 phishing, 400 evasiones de proxy y más de 200 URL de aplicaciones potencialmente no deseadas.

Las URL que Cascadia Labs usa para las pruebas se recopilan de sitios en libre circulación, con nuestras propias técnicas de detección, análisis y verificación. Ninguna URL es suministrada, ni conocida, por parte de las empresas cuyos productos van a someterse a prueba.

### **Metodología de las pruebas**

Configuramos los productos sometidos a las pruebas como proxys. En el caso de Websense, usamos la integración con Microsoft ISA Server.

Durante todas las pruebas, permitimos que todos los productos usaran cualquier capacidad de valoración remota disponible y que se actualizaran.

Puesto que cada proveedor usa su propio conjunto de categorías para clasificar las URL, creamos correspondencias de categorías entre nuestras categorías y las de los proveedores para garantizar que

usamos configuraciones de bloqueo comparables para cada producto. Configuramos los productos para que bloquearan un grupo completo (definido para contener categorías similares), a fin de que no hubiera interferencias en los resultados de bloqueo de nuestras pruebas a causa de las pequeñas diferencias entre las categorías de los distintos proveedores.

Puesto que la reputación Web suele tener como objetivo las URL de seguridad, solo activamos esta característica para las pruebas de ese grupo.

Con el objeto de aislar las capacidades de filtrado de URL de cada producto, Cascadia Labs no activó el filtrado de protocolos ni las exploraciones de malware en ninguno de los productos. El filtrado de protocolos puede ser una medida adicional eficaz para bloquear la mensajería instantánea y otros servicios no deseados, aunque, por supuesto, el filtrado de protocolos

no es práctico para el protocolo HTTP (y las URL que probamos) dada la importancia de Internet. La búsqueda de binarios en el perímetro ofrece otra capa de protección, aunque puede introducir una latencia adicional para los usuarios, por lo que decidimos no incluirla como parte de las pruebas del presente informe.

Para poder probar las capacidades de valoración en tiempo real y remota sin poner en peligro la integridad de nuestro corpus de URL, Cascadia Labs usa una muestra de 1.000 URL seleccionadas aleatoriamente en cada categoría (y 2.000 para todo el conjunto de categorías de seguridad), lo que nos permite establecer resultados de bloqueo en las principales categorías con un intervalo de confianza de  $\pm 3\%$  (en el nivel de confianza del 95%). Después de usarlas, estas URL se desechan a excepción de las URL de sitios de tráfico elevado, para evitar conceder ventaja a un producto en las pruebas posteriores. ▲



Independent evaluations of technology products

Contacto: [info@cascadialabs.com](mailto:info@cascadialabs.com)  
[www.cascadialabs.com](http://www.cascadialabs.com)



*Esta reseña comparativa, realizada de forma independiente por Cascadia Labs en el verano de 2009, ha sido patrocinada por Trend Micro. El objetivo de Cascadia Labs es ofrecer un análisis objetivo e imparcial de cada producto según pruebas prácticas en su laboratorio de seguridad.*