

- **Le provee una seguridad de red robusta y proactiva**
- **Lo protege de amenazas nuevas y desconocidas**
- **Cierra la ventana de vulnerabilidad**
- **Ofrece una opción mucho mejor que la de los productos que sólo se basan en firmas**



Tecnología amigable con la Tierra

## El Activo más Poderoso en su Sistema de Defensa de la Red

WatchGuard® provee una protección de Día Cero (Zero Day) verdadera a partir de las capacidades Intelligent Layered Security de sus dispositivos Firebox® X Unified Threat Management, dando de baja a una gran cantidad de nuevos ataques desconocidos sin la necesidad de una firma.

### Qué Significa el “Día Cero” (Zero Day)

Existe mucho murmullo en la industria de la seguridad sobre la protección de ataques del día cero, pero lo cierto es que la mayoría de los proveedores están sustancialmente lejos de ese concepto en su oferta.

- Las amenazas del Día Cero son ataques nuevos o desconocidos para los cuales aún no se escribió un parche ni una firma
- La protección de Día Cero, por lo tanto, significa estar protegido ante las amenazas nuevas y desconocidas antes de que la vulnerabilidad sea descubierta y la vulnerabilidad haya sido creada y lanzada

### La Arquitectura Firebox® Tiene Incorporada Protección Real para el Día Cero

Intelligent Layered Security de Firebox X combina capacidades clave de seguridad capaces de defender su red contra distintas clases de ataques y de protegerla ante nuevas variantes, aún antes de que se hagan conocidas. Entre estas capacidades se cuentan:

- **La detección de anomalía de protocolo**, que bloquea el tráfico malicioso que no se ajusta a lo establecido en los protocolos estándares
- **El matching de patrones** marca y remueve archivos de alto riesgo del sistema, tales como .exe y scripts, virus, spyware y trojanos, luego de inspeccionar el paquete completo
- **El análisis de comportamiento** identifica y detiene el tráfico proveniente de hosts que muestran un comportamiento sospechoso, incluyendo ataques DoS y DDoS, escaneos de puertos y escaneos de direcciones

### Qué Ofrecen las Firmas a una Solución de Seguridad

Algunos proveedores basan su discurso en el Día Cero, pero en realidad sus soluciones de seguridad están apoyadas sólo sobre escaneo basado en firmas. Las tecnologías de seguridad basadas en signatures

(firmas) individualizan cada nuevo ataque luego de que éste emerge, por lo que la protección recién llega cuando esta signature se agrega al sistema. Esto no es protección de Día Cero. Por su naturaleza, las signatures son reactivas: no pueden proteger ante un ataque nuevo o desconocido si no se hizo previamente una actualización.

El escaneo basado en signature provee una capa granular de protección contra el spyware, los virus, los gusanos, los trojanos y las amenazas combinadas a partir de la identificación de código malicioso dentro del tráfico y de los archivos críticos para el negocio. Pero esta técnica es tan solo un componente de una solución completa de Administración Unificada de Amenazas (Unified Threat Management).

*De los 30 virus más significativos lanzados entre 2003 y 2006 (incluyendo sus variantes), 22 fueron bloqueados por defecto sobre el Firebox®, con lo cual nuestros clientes estuvieron protegidos aún antes de que las signatures estuvieran disponibles\*.*

### La Ventana de Vulnerabilidad

Las soluciones basadas en firmas bloquean lo que ya ha sido identificado. Su red, entonces, aún está expuesta. Es que existe una ventana de vulnerabilidad que se da entre el momento en que se lanza una nueva vulnerabilidad y el instante en que se desarrolla y se despliega la signature o el parche que la detecta.

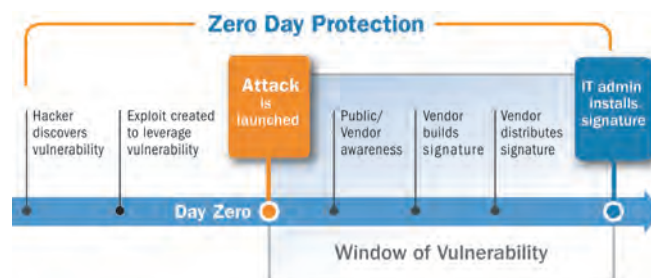
Considerando la velocidad y la capacidad destructiva de los ataques actuales, aún unos pocos minutos sin protección pueden ser devastadores. La realidad es que en ocasiones, esta ventana dura horas y hasta semanas, convirtiéndose en una verdadera pesadilla para los gerentes de IT.

### Protección Robusta de Verdad

En el corazón de nuestras soluciones de seguridad Firebox X reside una protección de Día Cero verdadera, que logra actuar antes de que la vulnerabilidad sea conocida. Póngala a trabajar para usted. Visite [www.watchguard.com](http://www.watchguard.com)

\*Based on most commonly used method of propagation (SMTP)

## Watchguard lo protege durante la ventana de vulnerabilidad



Protección de Día Cero (Zero Day) significa estar protegido contra las amenazas nuevas y desconocidas durante la ventana de vulnerabilidad, es decir, el período entre que se lanza un nuevo ataque y que el administrador de IT instala la firma que lo detecta.

- **Protección multifacética y completamente integrada**
- **Las más completa solución de seguridad en su clase**
- **Incluye prevención de ataques de Día Cero**
- **Las poderosas suscripciones de seguridad agregan aún más protección en áreas críticas de ataque**
- **Provee capacidades de administración unificada, monitoreo y registro**



Tecnología amigable con la Tierra

## Seguridad Completa con Protección Real de Día Cero (Zero Day)

Firebox® X Unified Threat Management de WatchGuard proveen la más amplia solución de seguridad de su clase, ofreciendo una protección de las amenazas que sufren las redes integradas y multifacéticas, entre las que se cuentan:

- ✓ Spyware
- ✓ Virus
- ✓ Inyecciones SQL
- ✓ Troyanos
- ✓ Spam
- ✓ Buffer overflows
- ✓ Worms
- ✓ Amenazas combinadas
- ✓ Ataques DoS/DDoS
- ✓ Bots
- ✓ Web-based exploits
- ✓ Violación de políticas

### ¿Qué es Unified Threat Management?

Unified Threat Management (UTM, Administración Unificada de Amenazas) es una tendencia emergente en el mercado de seguridad de redes. Los dispositivos UTM son una evolución de los tradicionales firewalls y VPNs y se convirtieron en una solución que tiene muchas capacidades adicionales, como filtro de URL, bloqueo de spam, protección contra spyware, prevención de intrusos y antivirus de gateway, así como la posibilidad de realizar una administración integrada, monitoreo y registro. Todas estas funciones eran antes logradas adquiriendo distintos sistemas específicos.

### La Esencia es una Protección de Día Cero Incorporada

El Intelligent Layered Security (ILS) en el dispositivo Firebox X brinda protección de Día Cero real. Asegura su red frente a amenazas nuevas y desconocidas antes de que la vulnerabilidad sea descubierta, creada y lanzada. Muchos proveedores sólo ofrecen protección basada en signatures. Estas soluciones reactivas dejan a sus usuarios expuestos a nuevos tipos de amenazas hasta que la vulnerabilidad se vuelve conocida, se escribe la signature correspondiente y se despliega la actualización para que los gerentes de IT la instalen.

### Poderosas Defensas Trabajan en Conjunto

A diferencia de muchos dispositivos UTM que están disponibles en el mercado en la actualidad, las capas de seguridad en el Firebox X con ILS trabajan en conjunto para fortalecer la seguridad general. Con capacidades de software combinadas, cada componente puede prestar soporte a la estructura de protección. Por ejemplo, cuando el Servicio de Prevención de Intrusiones (Intrusion Prevention Service) identifica un ataque, puede indicarle al firewall qué hacer con él. La comunicación cooperativa entre capas reduce el procesamiento requerido por las funciones de seguridad. Como resultado, usted logra proteger lo que necesita sin sacrificar desempeño.

### Suscripciones que Potencian Defensas

La flexibilidad de nuestras soluciones le permite agregar de manera sencilla cualquiera de nuestras suscripciones de seguridad, para mejorar la protección en áreas críticas de ataques. Todos los servicios que se incorporen pueden ser administrados desde una

única consola integrada. Entre las suscripciones de seguridad se cuentan:

- **spamBlocker:** Con una capacidad de bloqueo en tiempo real de hasta un 97 por ciento del correo electrónico no deseado en el momento de estallido del spam, es la mejor solución de la industria.
- **Gateway AV/IPS:** Protección robusta en el gateway basada en signature contra virus conocidos, spyware, troyanos y vulnerabilidades basadas en Web.
- **WebBlocker:** Incrementa la productividad y disminuye los riesgos de seguridad, ya que bloquea el acceso a contenido Web malicioso y administra la navegación Web de sus usuarios

### El rol de la Administración Integrada

No importa si usted es un experto de IT o un novato en seguridad. En las capacidades de administración integrada, monitoreo interactivo en tiempo real y registro de nuestras soluciones UTM, usted encontrará la facilidad de uso que necesite para poder configurar y manejar su seguridad sin mayores inconvenientes.

- Administre múltiples dispositivos desde una ubicación central
- Cree e implemente fácilmente políticas globales de seguridad, de forma tal que sea sencillo mantener una coherencia entre ella.
- Confíe en el monitoreo y registro interactivo en tiempo real
- Utilice sólo una única interfaz intuitiva para instalar y administrar todas sus capacidades de seguridad, incluyendo las suscripciones

### Ventajas en Costos y Escalabilidad

El hecho de correr múltiples softwares y de tener diversos dispositivos de seguridad hace que el presupuesto de IT y el tiempo de administración crezcan. Otras soluciones UTM pueden cobrar un costo de licencia por usuario, o solicitar que usted abone por las capacidades de registro y reporting centralizadas. Las soluciones WatchGuard UTM no tienen un costo por usuario ni precios adicionales por las herramientas de management. Y el usuario sólo tiene que aprender a manejar una única interfaz gráfica. Todas las capacidades de seguridad se administran centralmente y están integradas. Usted sólo está limitado por su capacidad de tráfico. Cuando usted alcanza esa capacidad, simplemente debe activar una clave de licencia de actualización para llegar a un modelo superior que habilita niveles adicionales de capacidad. Esta es la manera que menos trabajo requiere y la forma más efectiva de proteger sus inversiones en seguridad de la red.



Stronger Security, Simply Done™

DIRECCION: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · WEB: [www.watchguard.com](http://www.watchguard.com)

VENTAS U.S.A.: 1.800.734.9905 · VENTAS INTERNACIONALES: +1.206.613.0895

No se brindan garantías expresas o implícitas. Todas las especificaciones están sujetas a cambios imprevistos y los servicios y características ofrecidas actuales y futuras se proveerán si, y donde, estén disponibles. ©2007 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, El logo WatchGuard, Firebox, Firewall, LiveSecurity, Peak, Core, y Stronger Security, Simply Done son marcas registradas de WatchGuard Technologies, Inc. en los EE.UU. y en otros países. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. Part No. WGCE66355\_101707