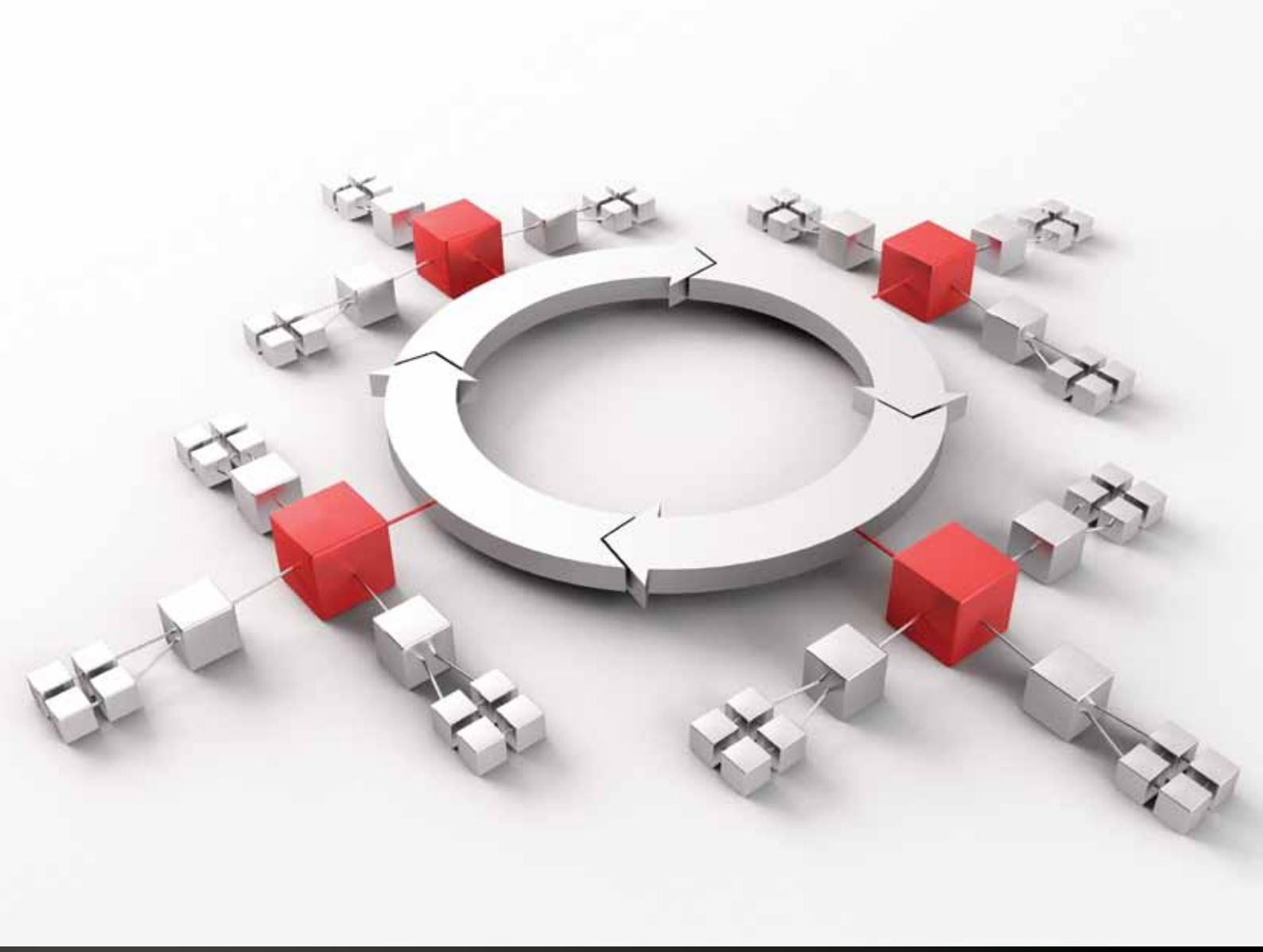

radware

COMPARTIR ESTE FOLLETO

Solución para mitigación de ataques

Solución para mitigación de ataques

Protege las empresas contra los ciberataques con detección y mitigación permanentes de ataques DDoS.

La mitigación de ataques de Radware es una solución híbrida que integra la detección y la mitigación en las instalaciones con la depuración de ataques volumétricos en la nube y el soporte 24x7 del Equipo de Respuesta a Emergencias (ERT).

Las organizaciones se enfrentan al desafío de un panorama de amenazas en permanente evolución que reduce sus ganancias, aumenta sus gastos y afecta negativamente su reputación. Los cibercriminales usan actualmente métodos sofisticados (con frecuencia vectores de ataque múltiples en la misma campaña de ataque) para destruir la presencia en la web de los centros de datos y de las organizaciones. La simplicidad con la que se lanzan estos ciberataques y la variedad de herramientas de ataque disponibles son algunos de los motivos por los cuales más organizaciones sufren más ataques, como DDoS.

La era de la solución híbrida integrada

Actualmente, las tecnologías de defensa estándar, incluida la protección DDoS, el análisis de comportamiento y anomalías, IPS, la protección SSL y los firewalls de aplicaciones web (WAF) se brindan generalmente en determinadas soluciones. Estos sistemas casi nunca se encuentran integrados y exigen recursos dedicados en términos de expertos en seguridad y gerentes de TI que deben mantenerlos y sincronizarlos.

La solución de mitigación híbrida de ataques de Radware combina las tecnologías requeridas para que las empresas logren ser resilientes a los ciberataques con sistemas instalados en el perímetro y con la capacidad de utilizar bajo demanda un servicio de depuración basado en la nube.

Solución para mitigación de ataques

Al proteger a las empresas en tiempo real contra las amenazas que surgen para las aplicaciones y la red, el abordaje en capas de Radware está diseñado para ayudar a las organizaciones a mitigar los ataques que se pueden detectar y ofrecer una solución de seguridad que combine herramientas de detección y mitigación de un único proveedor. La solución de Radware ofrece la máxima cobertura, la detección más precisa y el tiempo más breve para lograr la protección.

La solución de mitigación de ataques de Radware ofrece mitigación y detección de ataques de distintos vectores, y protege contra los ataques basados en el servidor y en las capas de la red, la propagación del software y las actividades de intrusión. Esta solución se completa con análisis del comportamiento de la red, antiDoS, defensa SSL, IPS, WAF y mitigación de DoS en la nube, todo en un único sistema integrado. La solución cuenta con hardware dedicado especialmente a combatir distintos vectores de ataque de forma simultánea.

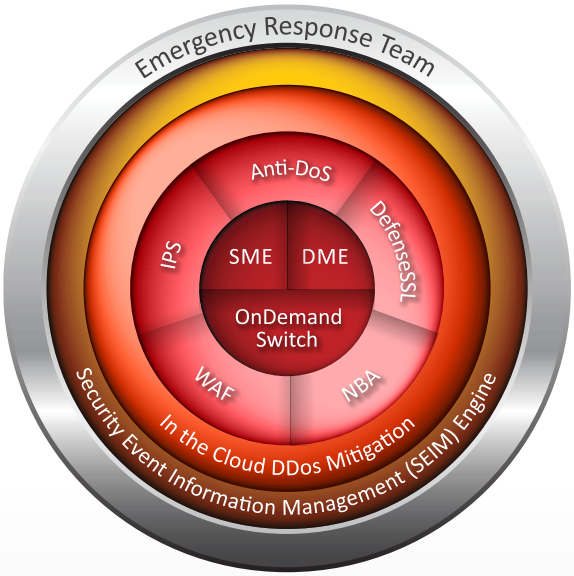

Figura 1: Sistema de mitigación de ataques de Radware

Para mitigar los ataques en la red que amenazan con saturar la conexión a Internet, la solución de mitigación de ataques de Radware incluye un servicio de depuración de DDoS basado en la nube que funciona de forma sincronizada con los dispositivos de mitigación de ataques en las instalaciones.

Optimizada con un sistema central de monitoreo y generación de informes, la solución ofrece conocimiento unificado e información permanente de la salud de la red y las aplicaciones usando un solo motor de gestión de la información sobre los eventos de seguridad (SEIM) para todos los componentes.

Durante las campañas de ataques de larga duración en los que el sistema no puede mitigar todos los vectores de ataques fuera de lo establecido (“out-of-the-box”), Radware ofrece el soporte de su Equipo de Respuesta a Emergencias (ERT), un equipo de expertos en seguridad que ofrece un servicio en tiempo real 24x7 para ayudar a los clientes a restaurar el estado operativo afectado por el ataque.

Protección permanente contra DDoS con óptima mitigación de ataques

El dispositivo de mitigación de ataques en las instalaciones de Radware garantiza que el centro de datos se encuentre constantemente protegido brindando detección en tiempo real y mitigación de ataques DDoS de distintos vectores, lo que no es posible usando solamente una solución para DDoS basada en la nube.

Únicamente en casos de ataques volumétricos, en los que la conexión a Internet de la organización se encuentra a punto de saturarse, el tráfico se desvía hacia el centro de depuración basado en la nube de Radware, donde el tráfico del ataque se depura antes de que llegue a afectar la conexión a Internet de la compañía. Esto permite una transición sin complicaciones entre las opciones de mitigación y garantiza la protección inmediata sin trastornos y sin que se sume la latencia del centro de depuración.

Solo el 15 % de los ataques DDoS manejados por el ERT de Radware saturaron la conexión a Internet[1]. Estas capacidades de protección híbrida garantizan que el tráfico no se desvíe a menos que esto sea absolutamente necesario. Como resultado, la organización se encuentra completamente protegida y el tiempo de mitigación se puede medir en segundos.

⚠ Vectores de ataque

Se detectan y mitigan más de 100 vectores de ataque en las capas de la aplicación y la red, entre otros:

Ataques de grandes volúmenes en la red
Desbordamientos SYN
Low and slow
Desbordamientos HTTP
Cifrado SSL
Fuerza bruta
Ataques BGP
Ataques de sesión
Escaneos invasivos

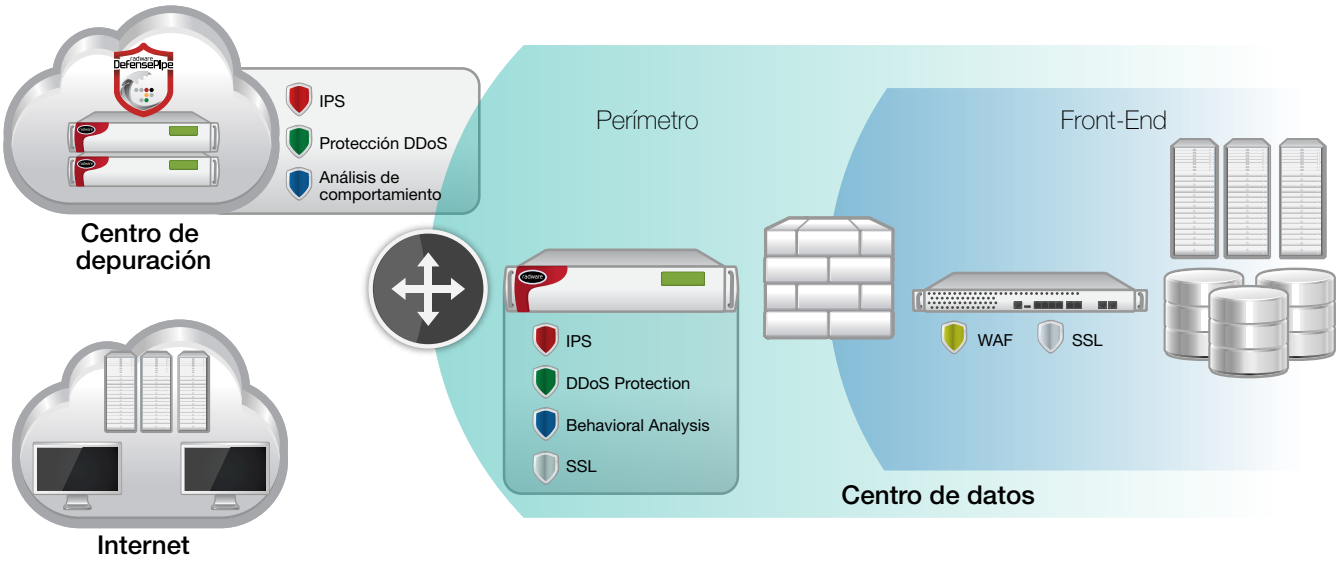

Figura 2: Solución híbrida de mitigación de ataques de Radware

Monitorear. Analizar. Informar.

La solución de mitigación de ataques de Radware incluye monitoreo activo y comprobaciones de la salud del sistema en el servicio o la aplicación protegidos. Además, el sistema realiza un monitoreo de saturación de la conexión y se notifica a los clientes cuando existe el riesgo de saturación y se requiere algún tipo de acción.

Los informes continuos acerca de todos los ataques que fueron mitigados por el sistema (invocados o mitigados automáticamente) se encuentran disponibles para su visualización en un portal de servicio basado en la web. Cuando el ERT de Radware se involucra en la mitigación de un ataque, se le proporciona al cliente un informe completo de análisis posterior al ataque.

Punto único de contacto para mitigación de ataques DDoS

La solución de Radware incluye soporte del ERT a toda hora, todos los días del año, para obtener asistencia en la mitigación de ataques desde un punto único de contacto. El ERT ofrece el conocimiento necesario durante ataques prolongados de distintos vectores. Esto implica trabajar de cerca con los clientes para decidir el desvío del tráfico durante los ataques volumétricos, proveer asistencia en la captura de archivos, el análisis de la situación y garantizar la implementación de las mejores opciones mitigación. La experiencia del ERT en la lucha contra los ataques más conocidos en la industria brinda los mejores modos de abordaje basados en la práctica para combatir todos y cada uno de los ataques.

[1] *Fuente: Equipo de Respuesta a Emergencias de Radware (ERT)*

Figura 3: Portal del servicio híbrido de protección contra ataques DDoS en la nube

"La solución para mitigación de ataques de Radware mitiga tanto las formas de ataques nuevas como las conocidas y, al mismo tiempo, permite el manejo normal del tráfico comercial legítimo para preservar la continuidad de las actividades comerciales de los clientes en la nube aun cuando estas sufran un ataque".

Nathaniel Kemberling, Director técnico, Brinkster

"La solución para mitigación de ataques de Radware se combina a la perfección con nuestra arquitectura de hosting seguro en la nube. La capacidad de detener una gran variedad de ataques a distintos niveles en los límites de nuestras redes en Norteamérica y Europa le permite a FireHost brindar la mejor protección en la industria".

Chris Drake, Director ejecutivo, FireHost

Aplicaciones web: Detectar. Señalar. Bloquear.

El firewall de aplicaciones web (WAF) de Radware brinda protección completa contra: ataques a la aplicación web, ataques a aplicaciones web, ataques a aplicaciones web detrás de CDN, ataques HTTP avanzados (desbordamientos dinámicos, ataques *slowloris*), ataques de fuerza bruta en páginas de inicio de sesión, y mucho más.

Un mecanismo de envío de mensajes le permite al WAF de Radware informar al dispositivo de mitigación de ataques en el perímetro de Radware cuando se detecta un ataque a la aplicación web y es necesario bloquearlo en el perímetro para proteger el resto de la red.

Dado que las organizaciones migran las aplicaciones a la nube, Radware ofrece un servicio WAF basado en la nube. El WAF basado en la nube híbrida de Radware ofrece un WAF de nivel empresarial completamente gestionado que protege tanto las aplicaciones en las instalaciones como las basadas en la nube usando una única solución tecnológica.

Mitigar la amenaza de SSL

La solución de mitigación de SSL de Radware es única en la industria. Mitiga ataques cifrados de desbordamiento en el perímetro de la red. La solución mitiga los ataques basados en SSL usando técnicas de mitigación de desafío-respuesta y descifrado de SSL, y los mecanismos de desafío-respuesta se refuerzan únicamente cuando el tráfico es sospechoso. El resultado es una solución de mitigación de SSL con la latencia más baja en la industria, ya que el tráfico legítimo no se ve afectado por los esfuerzos de mitigación realizados.

Beneficios

- Solución híbrida con la más amplia cobertura de seguridad y el tiempo de mitigación más breve: mitigación inmediata en las instalaciones y desviación del tráfico únicamente en casos de saturación de la conexión
- Único punto de contacto: El ERT combate el ataque durante toda la campaña, sin involucrar a otros proveedores
- Sistema integrado de generación de informes incluido en las instalaciones y en los informes de mitigación basados en la nube
- Disponible como servicio completamente administrado con modelos de pago flexibles (suscripción basada en CAPEX o OPEX)

Acerca de Radware

Radware (NASDAQ: RDWR), es un líder global de entrega de aplicaciones y soluciones de seguridad cibernética para centros de datos virtuales, de nube y definidos por software. Su galardonada cartera de soluciones ofrece garantía de nivel de servicio para aplicaciones críticas para el negocio, al tiempo que maximiza la eficiencia de TI.

Las soluciones de Radware permiten que más de 10.000 clientes empresariales y operadores en el mundo se adapten rápidamente a los desafíos del mercado, mantengan la continuidad del negocio y alcancen su productividad máxima, minimizando, al mismo tiempo, sus costos. Para obtener más información, visite www.radware.com.

Radware le recomienda que se una a nuestra comunidad y nos siga en: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, la app para iPhone Radware Connect y nuestro centro de seguridad DDoSWarriors.com que proporciona un análisis completo sobre las herramientas, tendencias y amenazas DDoS.

Soporte de seguridad

Radware ofrece soporte técnico para todos sus productos a través del *Certainty Support Program*. Cada nivel del Programa de soporte de seguridad consta de cuatro elementos: soporte telefónico, actualizaciones de software, mantenimiento de hardware y asistencia en el sitio. Radware también cuenta con personal de ingeniería que se dedica especialmente a brindar asistencia a clientes en cuestión de servicios profesionales para implementaciones de proyectos avanzados.

Más información

Para descubrir cómo las soluciones integradas de provisión y seguridad de aplicaciones de Radware pueden ayudarlo a aprovechar al máximo sus inversiones informáticas y comerciales, envíenos un correo electrónico a info@radware.com o visite www.radware.com.

PRD-AMS-BR-05-2016/05 – A4