

Entrega Continua sin Vulnerabilidad Continua

El desarrollo de aplicaciones web es cada vez más complejo, rápido y más vulnerable que nunca. El servicio WAF de Radware Cloud proporciona la mejor seguridad de aplicaciones web del sector mediante el uso de un modelo de seguridad positivo basado en tecnologías de aprendizaje automático para brindar una cobertura de protección integral contra las 10 principales amenazas de OWASP y otras vulnerabilidades. El servicio Cloud WAF de Radware proporciona políticas de seguridad dinámicas con corrección automática de falsos positivos, protección DDoS incorporada, mitigación de bots integrada y muchas otras características para ayudar a proteger a las organizaciones contra el riesgo de pérdida de datos.



PROTECCION COMPLETA

La mejor protección de aplicaciones web de la industria basada en un modelo de seguridad positivo para una cobertura completa contra las amenazas TOP 10 de OWASP y más.

RÁPIDO DESPLIEGUE

Las tecnologías avanzadas de automatización de Radware detectan instantáneamente ataques, responden de forma inmediata y reducen la exposición.



SOBRECOSTO REDUCIDO

Las defensas WAF automáticas de Radware y los servicios administrados por expertos alivian la carga de los equipos de TI y brindan una mejor seguridad con menor sobrecosto.

CONSOLA UNIFICADA

Radware ofrece una solución de seguridad integrada que brinda protección de aplicaciones web multivectoriales con administración e informes centralizados.



Cómo Radware le Mantiene Ágil y Seguro

Aprendizaje Automático de Tráfico

Radware utiliza algoritmos avanzados de aprendizaje automático que analizan el tráfico, aprenden lo que constituye un comportamiento legítimo y bloquean automáticamente la actividad maliciosa.

Mapeo de aplicaciones

Radware mapea automáticamente las aplicaciones protegidas, detecta cambios en el código cada vez que se agregan o modifican nuevas funciones e identifica vulnerabilidades potenciales.

Políticas Adaptativas

Radware adapta continuamente las políticas de seguridad para optimizar la cobertura al perfil de amenazas de las aplicaciones para maximizar la cobertura de seguridad y reducir los falsos positivos.

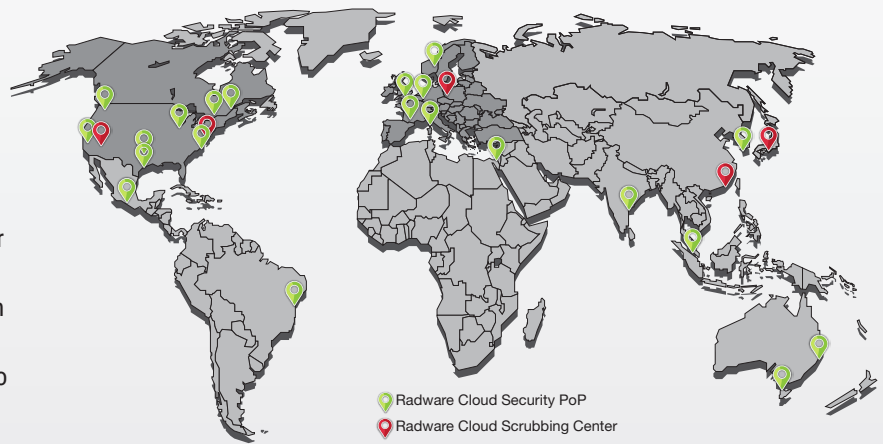
Cloud WAF con Cumplimiento PCI Completo

Radware Cloud WAF Service es el único servicio WAF en la nube que implementa completamente los 10 mecanismos de seguridad recomendados de la Regulación 6.6 de PCI-DSS, incluido el cumplimiento de un Modelo de Seguridad Positivo y la implementación de controles de Prevención de Fuga de Datos (DLP). El Cloud WAF de Radware también está certificado por PCI-DSS y se basa en la tecnología certificada de NSS Labs e ICSA Labs, lo que significa que los clientes pueden implementar el Servicio Cloud WAF de Radware con total confianza para un cumplimiento máximo.



Presencia global, Justo al lado de su Servidor de Origen

El servicio WAF en la nube de Radware se basa en una red global de puntos de presencia (PoP) WAF distribuidos, asegurándose de que siempre esté protegido desde el punto más cercano a su servidor de origen. Los PoPs Cloud WAF de Radware se encuentran en los principales centros de tráfico con conexiones a ISP de Nivel 1, lo que garantiza una baja latencia y un impacto mínimo en el rendimiento de las aplicaciones web.



Características de servicio del servicio Radware Cloud WAF

Protección completa contra las amenazas TOP 10 de OWASP

- ▶ Basado en un modelo de seguridad positivo que utiliza tecnologías avanzadas de análisis de comportamiento para detectar amenazas
- ▶ Protección DDoS incorporada para detener ataques DDoS en la aplicación
- ▶ Mitigación de bots mediante el uso de huellas dactilares avanzadas para identificar bots maliciosos basados en características únicas del dispositivo.
- ▶ Mecanismos de prevención de fuga de datos para enmascarar automáticamente datos confidenciales del usuario, como información de identificación personal (PII)

Mayor agilidad para la Entrega Continua de Aplicaciones

- ▶ Servicio de seguridad completamente administrado por el experto y experimentado Equipo de Respuesta de Emergencia de Radware (ERT)
- ▶ Gerente de cuenta técnico dedicado (TAM) que sirve como punto focal para todos los problemas, incluida la configuración, integración, actualizaciones y mitigación de ataques
- ▶ Políticas de adaptación continua que mapean automáticamente las aplicaciones, detectan cambios en ellas e implementan dinámicamente la política de seguridad óptima
- ▶ Corrección automática de falsos positivos utilizando potentes algoritmos de aprendizaje automático que identifican el comportamiento legítimo de la aplicación



Flexibilidad en el despliegue

- ▶ Compatibilidad con tráfico SSL de alta capacidad para garantizar la disponibilidad total desde el PoP más cercano, incluso en horas pico
- ▶ El servicio global de CDN se basa en un enrutamiento basado en anycast y una capacidad masiva de 30+ Tbps en más de 100 PoPs
- ▶ Capacidades avanzadas de balanceo de carga, que incluyen balanceo de carga de sitio (GSLB) local y global, conmutación por error del sitio, alta disponibilidad y monitoreo de estado
- ▶ Amplias capacidades de cumplimiento y certificaciones, incluidas las certificaciones específicas de la industria como PCI y HIPAA, así como estándares de seguridad en la nube como ISO 27001, ISO 27017, ISO 27018, ISO 27032 y otros.

Fácil gestión y control

- ▶ Panel de gestión centralizado para mostrar amenazas y administrar la configuración.
- ▶ Capacidades de alerta granular para asegurarse de que usted es el primero en saber si algo sucede
- ▶ Informes ejecutivos fáciles de leer con detalles concisos del incidente
- ▶ Informes centralizados para protección WAF y DDoS

