

Reducir la complejidad de la seguridad en la nube

No son sólo los atacantes los que ponen en peligro sus aplicaciones y su negocio.

La nube híbrida añade un extra de complejidad para sus equipos de seguridad y TI.

Los proveedores de la nube suelen tener sus propias herramientas y procesos, lo que supone un aumento exponencial del esfuerzo de gestión de los entornos de nube híbrida. Esta complejidad, combinada con sofisticadas amenazas a la seguridad, dificulta la protección de su organización.

Principales retos de la nube¹

1 Gestionar la complejidad de numerosas herramientas y API

2 Aplicación de políticas de seguridad coherentes

Principales riesgos de seguridad en la UE²

1 Ransomware

2 Ataques DDoS, que se están especializando en la capa de aplicación

Con el 98% de las organizaciones utilizando o planteándose utilizar la cloud híbrida,³ el riesgo y la complejidad resultantes son motivo de preocupación en, prácticamente, todos los sectores. Estos problemas se ven agravados por la escasez de casi 4 millones de trabajadores de ciberseguridad en todo el mundo.⁴

Cómo superar la complejidad de la cloud híbrida

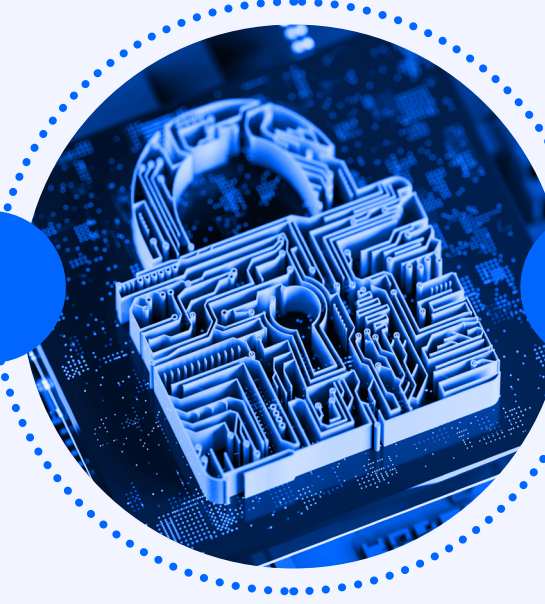
Para abordar la complejidad de la cloud híbrida, la clave es una solución que integre diversos entornos de manera uniforme y que reúna las siguientes características:

Escalabilidad



Capaz de gestionar grandes volúmenes de tráfico y datos sin necesidad de añadir infraestructura.

Cumplimiento



Se ajusta a las regulaciones y normas de seguridad locales y del sector.

Compatibilidad



Fácil y rápida de implantar sin cambiar el código de la aplicación.

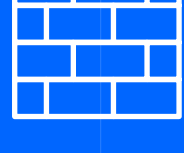
Rentabilidad



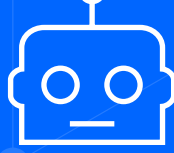
Menor uso de recursos debido a la ausencia de hardware y al mínimo esfuerzo de gestión.

Proteja las aplicaciones web y las API en cualquier lugar

Telefónica Tech Web Application Defense (WAD) es un servicio de seguridad gestionado diseñado para proteger las aplicaciones empresariales y las API frente a ciberamenazas que van desde el Top 10 de OWASP hasta ataques automatizados de bots. La solución de Web Application and API Protection (WAAP) proporciona una seguridad robusta con gestión centralizada y visibilidad respaldada por el soporte 24x7 del Security Operations Center (SOC) de Telefónica Tech.



Web Application Firewall (WAF) protege las aplicaciones en nubes, centros de datos privados, redes locales y edge clouds con una gestión unificada y políticas coherentes.



Bot Defense utiliza expertos y aprendizaje automático para detectar el tráfico de bots maliciosos al tiempo que permite usuarios legítimos y bots útiles.



DDoS Mitigation protege contra ataques volumétricos y de capa de aplicación en todos los entornos para reducir los costes operativos y la afectación al servicio.



API Security descubre automáticamente los endpoints de API asignados a sus aplicaciones, controla las conexiones y supervisa los comportamientos anómalos.

WAAP

Telefónica Tech WAD le permite:



Mejorar la postura de seguridad

Mantenga la continuidad del negocio, protéjase contra amenazas y fraudes, y cumpla con la normativa.



Reducir la complejidad

Simplifique la seguridad con una gestión experta y reoriente los recursos cualificados hacia otras tareas.



Mejorar la experiencia del usuario

Aumente la satisfacción del cliente con aplicaciones seguras que estén siempre disponibles.

Responda a las necesidades empresariales específicas de los clientes de cualquier sector con WAD



Los bancos son uno de los principales objetivos de los ataques DDoS,⁵ y deben cumplir requisitos normativos como PCI-DSS y GDPR. WAD puede identificar amenazas ocultas en canales cifrados para mejorar la seguridad. Asimismo, ofrece capacidades de informes y visibilidad para ayudar a demostrar el cumplimiento.

Las compañías de seguros manejan grandes cantidades de datos personales y son objetivos frecuentes de ciberataques y fraudes. WAD protege las aplicaciones y APIs frente a las amenazas que podrían exponer datos confidenciales mediante diversas técnicas de IA y aprendizaje automático.



Los negocios al por menor a menudo luchan para evitar que los bots acaparen el inventario o se apoderen de cuentas de usuarios legítimos, legítimos. Sin embargo, muchas soluciones de seguridad añaden fricciones que pueden ahuyentar a los clientes. WAD puede identificar y bloquear bots maliciosos incluso cuando éstos se reconfiguran, proporcionando una protección eficaz sin afectar a los clientes.

Reduzca la complejidad de la seguridad con WAD

Como parte de las soluciones gestionadas de Telefónica Tech Next Defense, WAD ayuda a proteger su viaje hacia la nube y a defenderse de los ataques especializados a aplicaciones con un servicio gestionado por expertos que es fácil de implantar y utilizar. Nuestro equipo de técnicos cualificados aporta una gran experiencia y un amplio y sólido conocimiento del sector, lo que garantiza soluciones personalizadas para cada desafío. Su enfoque proactivo y su asistencia 24x7 garantiza una protección óptima y permiten que sus aplicaciones empresariales funcionen sin problemas.

Más información en telefonicatech.com