

SEGURIDAD

BUSINESS INTELLIGENCE

ESCÁNERES Y BOTS

PRIORIZA LA SEGURIDAD DE TUS APPS

# CÓMO ESCOGER EL WAF ADECUADO

GUÍA PRÁCTICA

EFICIENCIA

FRAUDE DE CLICS

NAVEGADORES HEADLESS



WE MAKE APPS  SAFER

# INTRODUCCIÓN

Pese a los esfuerzos del sector tecnológico por desarrollar aplicaciones seguras, la mitad de las aplicaciones actuales siguen siendo vulnerables a los ataques

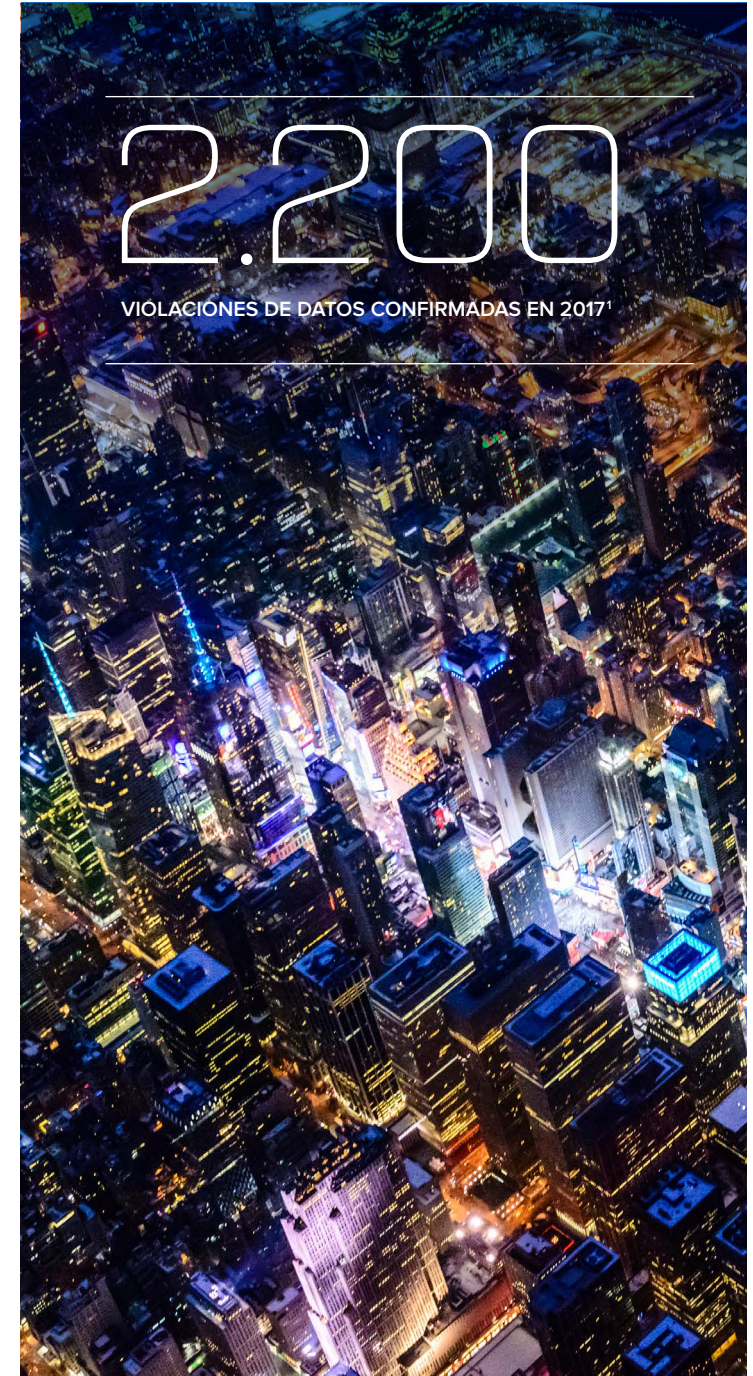
Según el informe Verizon 2018 sobre violaciones de datos (DBIR), en 2017 se perpetraron más de 2.200 violaciones de seguridad (y esas son solo las conocidas).<sup>1</sup> Pese a los esfuerzos del sector tecnológico por desarrollar aplicaciones seguras, la mitad de las aplicaciones actuales siguen siendo vulnerables a los ataques. Y es que diseñar aplicaciones seguras no es una tarea fácil.<sup>2</sup>

La buena noticia es que existen herramientas para ayudarte a proteger tus aplicaciones frente a eventuales violaciones de datos, mitigando sus vulnerabilidades y deteniendo los ataques: son los cortafuegos de aplicaciones web (WAF). Los WAF inspeccionan el tráfico entrante y saliente para identificar y bloquear escáneres, hackers y bots, preservando y acelerando al mismo tiempo el uso legítimo de las aplicaciones. Ya sea desplegada localmente, en el cloud o como servicio, la tecnología WAF puede ayudarte a defender a tu empresa de los ataques contra sus aplicaciones web, que son el principal punto de entrada a las violaciones de datos.<sup>3</sup>

<sup>1</sup> [https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_execsummary\\_en\\_xq.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xq.pdf)

<sup>2</sup> <https://www.whitehatsec.com/news/half-of-corporate-web-apps-contain-flaws-that-are-at-least-a-year-old/>

<sup>3</sup> <https://www.f5.com/labs/articles/threat-intelligence/lessons-learned-from-a-decade-of-data-breaches-29035>



## ¿NECESITAS UN WAF? DEPENDE DE VARIOS FACTORES

- ¿Tienes una web abierta al público?
- ¿Procesa datos altamente sensibles?
- ¿Trata con bots y tráfico automatizado no deseado?
- ¿Está sujeta al cumplimiento de obligaciones legales?
- ¿Tienes mucho software difícil de actualizar?
- ¿Aprovechas las aplicaciones web heredadas?
- ¿Necesitas un respiro de los ataques de día cero?
- ¿Quieres reducir el time-to-market?

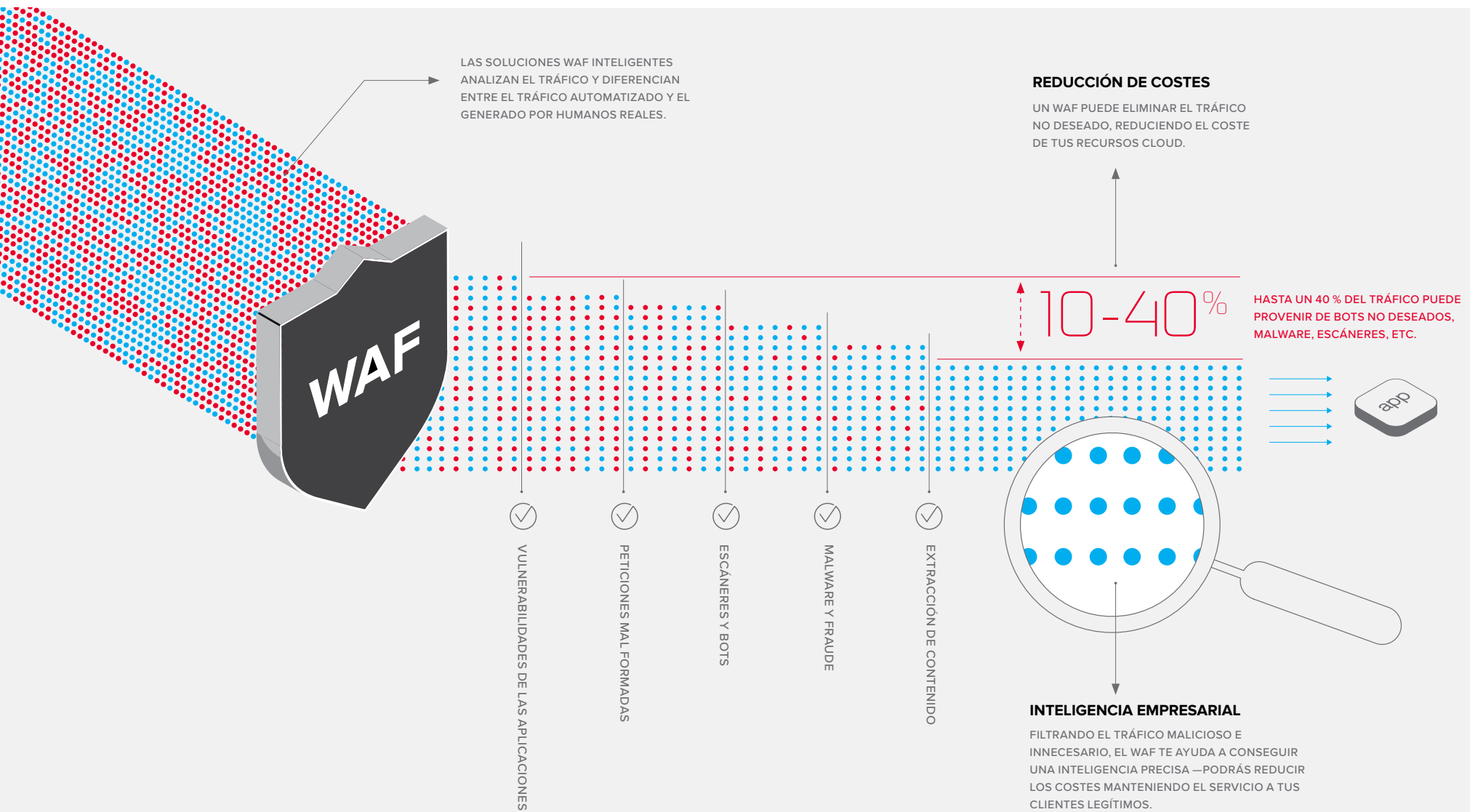
Si respondiste que sí a alguna de estas preguntas, deberías empezar a pensar en la tecnología WAF para proteger las aplicaciones, los datos y la actividad de tu empresa ante eventuales ataques a aplicaciones web y violaciones de datos.

Al igual que sucede con cualquier buena herramienta, dispones de múltiples opciones —se trata de escoger la mejor para cada situación. Sigue leyendo para saber cómo escoger el modelo WAF más adecuado para tu empresa.



50%

DE LAS APLICACIONES CORPORATIVAS TIENEN  
FALLOS DESDE HACE AL MENOS UN AÑO.



## UN WAF PUEDE REDUCIR LOS COSTES CLOUD Y MEJORAR LA INTELIGENCIA DE TU EMPRESA.

La implementación de un WAF al frente de una aplicación basada en la nube puede ahorrarte dinero y, a la vez, facilitar el acceso a los datos que necesita la empresa.

# 1 ¿PUEDEN LAS HERRAMIENTAS DE SEGURIDAD INTELIGENTES AÑADIR VALOR AL NEGOCIO?

Los gastos en soluciones de seguridad pueden ser difíciles de justificar. Por supuesto, todos somos conscientes de que *deberíamos* contar con potentes medidas defensivas y confiamos en estar protegidos en caso de ataque. Pero nunca se sabe cuando una empresa va a ser atacada y mucho menos si su firewall o IPS será capaz de proteger su red de manera efectiva en caso de que ocurra. La seguridad suele verse como un mal necesario con un retorno de la inversión incuantificable, pero esto no siempre tiene que ser así.

En el mundo de la nube y el big data, una buena solución de seguridad puede ayudarte a ahorrar dinero, ya que optimiza tus aplicaciones y sitios web, al tiempo que protege a tu

empresa de los ataques. Las soluciones WAF inteligentes pueden filtrar el tráfico de tu web, ayudándote a diferenciar mejor entre bots automatizados y humanos reales. Esto es importante porque, a medida que aumentan los servicios que se facturan a través de la nube, el tráfico de bots puede aumentar tus gastos sin proporcionarte valor comercial real.

Si utilizas un WAF para eliminar gran parte de ese tráfico inútil o malicioso, optimizarás las propiedades de tu web de cara a tus destinatarios, obteniendo un ahorro de costes significativo. Podrás estar seguro de que solo estás atendiendo a tus clientes reales y potenciales, lo que significa que tus herramientas de seguridad te están proporcionando un valor

## EN EL MUNDO DE LA NUBE Y EL BIG DATA, UNA BUENA SOLUCIÓN DE SEGURIDAD PUEDE AYUDARTE A AHORRAR DINERO

real al ayudarte a controlar tus costes en la nube. Además, los datos de interacción con el cliente se definirán aún más, obteniendo una inteligencia empresarial más sólida. Cuando cuentas con datos sólidos, procesables y fiables, estarás en una mejor posición para promocionarte de manera efectiva entre tus clientes reales.

### OPCIONES A TENER EN CUENTA:



#### WAF LOCAL AVANZADO (DISPOSITIVO VIRTUAL O DE HARDWARE)

Añade valor comercial real, además de actuar como póliza de seguridad en caso de violación. Con una defensa proactiva contra bots, protección avanzada de aplicaciones, inteligencia de amenazas y aprendizaje automático, este tipo de WAF puede ayudarte a reducir costes en la nube y afinar tu inteligencia empresarial.



#### WAF BASADO EN LA NUBE + AUTOADMINISTRADO

Te permite reducir costes, afinar tu inteligencia empresarial y obtener un gran valor comercial. Además de las mismas funciones de un WAF local, el WAF autoadministrado basado en la nube te ofrece una defensa proactiva contra bots, protección avanzada de aplicaciones, inteligencia de amenazas y aprendizaje automático.

## 2 ¿QUÉ QUIERES GESTIONAR, TU NEGOCIO O TUS SOLUCIONES DE SEGURIDAD?

Según el informe [State of Application Delivery Report 2018 de F5 \(SOAD\)](#), el número de violaciones de seguridad se ha disparado durante el año pasado. Conforme aumentan las violaciones, menor es la confianza depositada en las soluciones de seguridad a la hora de salvaguardar los datos confidenciales que las empresas tratan y almacenan.<sup>4</sup> El problema es que, a menos que seas un CISO dedicado en exclusiva a proteger los datos de tu empresa, no podrás estar todo tu tiempo gestionando las minucias de los muchos riesgos de seguridad de tus aplicaciones web.

Necesitas una solución de seguridad que sencillamente funcione y te permita dedicarte a desarrollar e implementar las aplicaciones importantes para tu empresa, manteniéndolas en línea y disponibles. Afortunadamente, existen varias

opciones de WAF que te permitirán hacerlo. Y no solo eso: según la misma edición del informe SOAD, la utilización de un WAF tiene un efecto significativo en la confianza de los encuestados en relación a la protección de sus aplicaciones. De las empresas que despiertan muy poca confianza en la protección de sus aplicaciones locales, solo el 6 % utilizaban un WAF. Sin embargo, de aquellas con un nivel de confianza muy alta, el 37 % utilizaban un WAF.<sup>5</sup> Está claro que la implementación de un WAF puede ayudar a proteger tus aplicaciones, pero la elección de las diferentes formas de implementación depende de las necesidades de cada empresa.

<sup>4</sup> [https://interact.f5.com/2018\\_SOAD.html](https://interact.f5.com/2018_SOAD.html)

<sup>5</sup> [https://interact.f5.com/2018\\_SOAD.html](https://interact.f5.com/2018_SOAD.html)

SI BUSCAS UNA SOLUCIÓN DE SEGURIDAD QUE SENCILLAMENTE FUNCIONE, EXISTEN VARIAS OPCIONES QUE TE PERMITIRÁN HACERLO

### OPCIONES A TENER EN CUENTA:



#### WAF BASADO EN LA NUBE + COMPLETAMENTE GESTIONADO COMO SERVICIO

Protege tus aplicaciones web y datos de las nuevas amenazas, al tiempo que ofrece asistencia 24/7. Aumenta (o sustituye) tus recursos internos con un servicio completamente configurado, implementado y mantenido por expertos certificados que trabajan en un centro de operaciones de seguridad (SOC).



#### WAF BASADO EN LA NUBE + AUTOAPROVISIONADO

Te ofrece el mismo nivel de control y personalización que un centro de datos privado, a la vez que permite responder rápidamente a las amenazas contra aplicaciones en la nube.



#### WAF LOCAL AVANZADO (DISPOSITIVO VIRTUAL O DE HARDWARE)

Ofrece niveles de control accesibles que pueden satisfacer tus necesidades de protección y visibilidad del tráfico de las aplicaciones sin necesidad de una administración a tiempo completo.

### 3 ¿QUIERES HACER ALGO MÁS QUE CUMPLIR LA NORMATIVA BÁSICA?

Muchas empresas están satisfechas con su actual estrategia de seguridad y aún así se plantean la tecnología WAF para adaptarse a la normativa o por las conclusiones de su auditoría. Varios WAF de distintos niveles de entrada pueden ayudarte a cumplir con los requisitos más básicos, pero las empresas que implementan solo lo básico a menudo descubren que eso tiene un coste.

Los WAF básicos pueden ayudarte a superar la auditoría, pero a menudo no tienen en cuenta la capacidad operativa y causan más problemas de los que ayudan a solucionar. Además, al no ofrecer la funcionalidad completa de un WAF potente, puedes acabar descubriendo que, pese a la gran inversión realizada, no estás tan protegido como esperabas.

Existe una solución mejor. Si necesitas un WAF para cumplir con los requisitos legales o de auditoría, ¿por qué no adquirir uno que ofrezca algo más que una protección mínima? Un buen WAF te permite cumplir con las exigencias legales al tiempo que te ofrece la visibilidad adicional que necesitas para valorar adecuadamente tu riesgo real con respecto al riesgo percibido. Y dado que en 2017 el 44 % de las empresas denunció al menos una violación de seguridad, los resultados podrían llegar a sorprenderte.<sup>6</sup>

<sup>6</sup> <https://betanews.com/2018/06/05/organization-data-breaches/>

UN BUEN WAF TE PERMITE CUMPLIR LOS REQUISITOS NORMATIVOS, ADEMÁS DE OFRECERTE LA SEGURIDAD Y VISIBILIDAD ADICIONAL QUE NECESITAS

#### OPCIONES A TENER EN CUENTA:



##### PRODUCTO BÁSICO

Puede ayudarte a pasar la auditoría, pero no ofrece niveles altos de protección —a menos que tengas conocimientos elevados en materia de configuración y realices un mantenimiento continuo, y puede que ni siquiera entonces.



##### WAF LOCAL AVANZADO (DISPOSITIVO VIRTUAL O DE HARDWARE)

Ofrece una mejor protección y análisis más precisos. No solo te ayuda a pasar auditorías, sino que aumenta realmente la estrategia de seguridad de tu empresa.



##### WAF BASADO EN LA NUBE + AUTOADMINISTRADO

Un WAF avanzado basado en la nube y autoadministrado ofrece una protección similar a la de un WAF local, con una protección robusta y análisis precisos que reforzarán tu estrategia de seguridad general.

## 4 ¿QUIERES CONTROLAR EL TRÁFICO DE BOTS SIN DEJAR DE CENTRARTE EN TUS CLIENTES?

Incluso disponiendo de un proceso de desarrollo de aplicaciones potente y seguro, y confiando en la seguridad de las aplicaciones que estás usando, es posible que te encuentres con otro problema: un gran porcentaje del tráfico que se dirige a tu sitio o servicio web proviene probablemente de programas autónomos o bots. Si bien este tráfico puede parecer real a primera vista, los clics de los bots no son iguales a los clics de humanos. El tráfico no deseado ni rentable puede sesgar tus analíticas y distorsionar tu inteligencia de mercado, inundando tus sistemas con datos adulterados.

Además, los hackers utilizan sistemas automatizados para escanear tus aplicaciones en busca de vulnerabilidades, atacar las credenciales de las cuentas o perpetrar ataques DoS. Utilizando un WAF avanzado, equipado con defensas proactivas contra bots, podrás detener los ataques automatizados y, usando una combinación de técnicas basadas en desafíos y comportamientos, podrás identificar y filtrar el tráfico de bots. Es sin duda una buena noticia para las empresas con problemas para administrar la actividad creciente de bots en sus propiedades digitales. La tecnología WAF adaptable puede liberarte de esta pesada carga para que puedas centrarte en atender a tus clientes reales.

LA TECNOLOGÍA WAF ADAPTABLE PUEDE MITIGAR LOS EFECTOS DEL TRÁFICO BOT NO DESEADO

### OPCIONES A TENER EN CUENTA:



#### WAF LOCAL AVANZADO (DISPOSITIVO VIRTUAL O DE HARDWARE)

Ofrece protección proactiva contra bots para defender tus aplicaciones frente a ataques DoS de capa 7, extracción de contenido web y ataques de fuerza bruta, antes de que puedan dañar a tu sitio.



#### WAF BASADO EN LA NUBE + AUTOADMINISTRADO

Un WAF basado en la nube y autoadministrado también puede ofrecer el mismo nivel de protección proactiva contra bots y así proteger tus aplicaciones contra la extracción de contenido web y los ataques DoS de capa 7 y fuerza bruta.



#### WAF BASADO EN LA NUBE + COMPLETAMENTE GESTIONADO COMO SERVICIO

Protege tus aplicaciones web de las amenazas basadas en bots, al tiempo que ofrece asistencia 24/7. Identificando los bots maliciosos omitidos por los métodos de detección estándar, las soluciones basadas en la nube también pueden mitigar las amenazas antes de que causen daños.





SIGUIENTES PASOS:

## ESCOGIENDO EL WAF ADECUADO PARA TU EMPRESA

La primera pregunta que debes hacerte al elegir un WAF es qué grado de implicación deseas para su utilización y administración.





Un WAF no debería ser difícil de utilizar y gestionar pero, como cualquier otra herramienta, cuanto más completo, más provecho sacarás de él. Además, ciertos vectores de amenazas (como los ataques contra empresas concretas o propiedades digitales) pueden ser difíciles de manejar.

Finalmente, la visibilidad que obtienes usando un WAF avanzado puede ayudarte a tomar decisiones, tanto en materia

de seguridad de aplicaciones como de cara a los objetivos generales del negocio —siempre que la empresa esté preparada para aprovechar estos datos.

Exploremos los distintos tipos de WAF, con sus ventajas e inconvenientes.

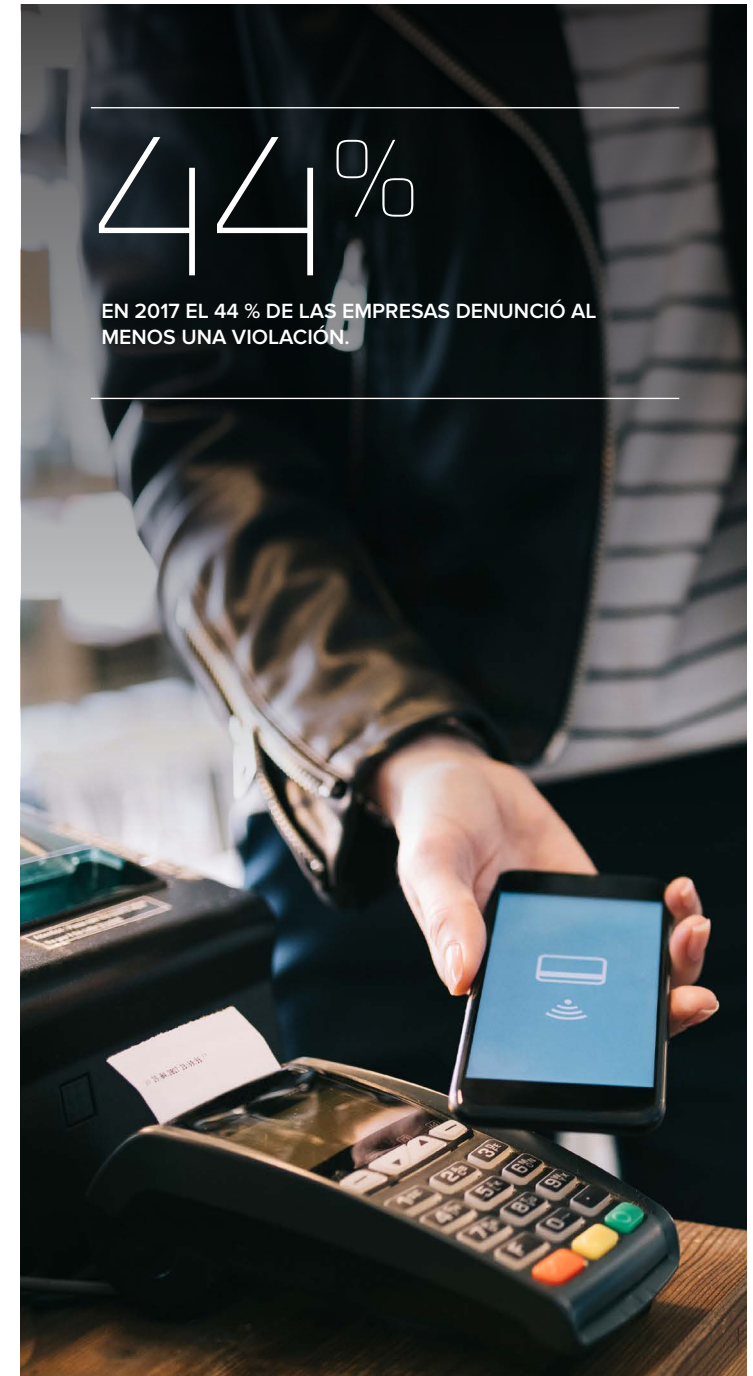
# TIPOS DE WAF DISPONIBLES

	VENTAJAS	INCONVENIENTES	PRODUCTOS F5
 <p><b>WAF BASADO EN LA NUBE + COMPLETAMENTE GESTIONADO COMO SERVICIO</b></p>	<p>Escoge esta opción si buscas la forma más rápida y sencilla de obtener un WAF (y mitigar DDoS) para proteger tus aplicaciones.</p>	<p>Aunque las opciones como servicio enteramente gestionadas pueden estar disponibles más rápidamente que con otros modelos, pueden no ofrecer mucha flexibilidad estructural. Algunos productos podrían no darte control directo sobre tus políticas de seguridad, desde el punto de vista administrativo.</p>	<p><a href="#">F5 Silverline WAF</a></p>
 <p><b>WAF BASADO EN LA NUBE + AUTOADMINISTRADO</b></p>	<p>Toda la flexibilidad y portabilidad de la nube, manteniendo el control de la administración del tráfico y los ajustes de tu política de seguridad.</p>	<p>Al ser autoadministrado, este modelo precisa un cierto grado de implicación por parte de tu equipo de seguridad y los propietarios de la aplicación para implementar y crear las políticas de seguridad de las aplicaciones.</p>	<p><a href="#">F5 Advanced WAF</a></p> <p><a href="#">F5 BIG-IP Cloud Edition</a></p>
 <p><b>WAF BASADO EN LA NUBE + AUTOAPROVISIONADO</b></p>	<p>Esta es una de las maneras más fáciles de usar un WAF en la nube. El autoaprovisionamiento te permite implementar una política de seguridad adaptada a tus necesidades de una manera sencilla y económica.</p>	<p>Según la arquitectura de tu aplicación, este modelo puede no proporcionarte tanta flexibilidad como otros.</p>	<p><a href="#">F5 WAF for Azure Security Center</a></p> <p><a href="#">F5 Silverline WAF Express</a></p>
 <p><b>WAF LOCAL AVANZADO (DISPOSITIVO VIRTUAL O DE HARDWARE)</b></p>	<p>Un WAF local (virtual o de hardware) puede ayudarte en las funciones más exigentes, cuando la flexibilidad arquitectónica, el rendimiento y la seguridad avanzada son básicas.</p>	<p>Este modelo puede requerir más inversión inicial en términos de adquisición y uso que otros modelos, pero dicha inversión se traducirá en beneficios para aquellas empresas que necesitan la flexibilidad que proporciona.</p>	<p><a href="#">F5 Advanced WAF</a></p>
 <p><b>PRODUCTO BÁSICO</b></p>	<p>Un WAF low-cost te proporciona protección básica para algunos de los vectores de ataque conocidos y puede ayudarte a cumplir con los requisitos normativos.</p>	<p>Los WAF básicos pueden no ofrecer la flexibilidad y resiliencia que necesitan las empresas para defenderse contra los nuevos vectores de amenazas que no dejan de evolucionar. Este tipo de WAF probablemente no te protegerá de vulnerabilidades de las aplicaciones como los bots y el fraude.</p>	<p><a href="#">F5 Rules for AWS WAF</a></p>

## CONCLUSIÓN

Aunque la elección puede parecer difícil, lo cierto es que nunca ha habido mejor momento para adquirir un WAF. La tecnología WAF es actualmente más accesible, asequible y fácil de administrar —una excelente noticia ahora que las empresas necesitan más que nunca la protección de un WAF.

Para obtener más información sobre cómo escoger el WAF adecuado para tu empresa, visita [f5.com/security](https://f5.com/security).



## PRIORIZA LA SEGURIDAD DE TUS APPS

Las aplicaciones activas y conectadas de forma permanente pueden ayudar a impulsar y transformar tu negocio. Sin embargo, también pueden ser una puerta de entrada a tus datos más preciados y quedar fuera de la protección de tus firewalls. Dado que la mayoría de ataques tienen lugar a nivel de las aplicaciones, proteger las capacidades que impulsan tu empresa pasa por proteger las aplicaciones que las hacen posible.

