

Web Application Firewall

Protect your website against SQL injections, cross-site scripting attacks and more

Cloudflare's Web Application Firewall (WAF) protects your website from SQL injection, cross-site scripting (XSS) and zero-day attacks, including OWASP-identified vulnerabilities and threats targeting the application layer. Customers include the Alexa-ranked Top 50, financial institutions, ecommerce companies and major enterprises. Fully-integrated with our DDoS protection, our WAF blocks millions of attacks daily, automatically learning from each new threat.

A robust rules engine to customize to your needs

Our WAF runs ModSecurity rule sets out of the box, protecting you against the most critical web application security flaws as identified by OWASP. It can also handle your existing rule sets and custom rules. Rules become effective in under 30 seconds.

Cloud deployment plus DDoS mitigation and CDN

As a cloud-based service, Cloudflare's WAF requires no hardware or software to install and maintain. Deploy the WAF with a single click, customizing it to meet your needs.

Its integration into the overall Cloudflare service means you get additional functionality for free. You can secure your website against DDoS attacks and use our global content delivery network to make it run faster.

Cloudflare Image optimization Web Mobile Visitor & APIs

Highlights:

- · Automatic protection from diverse threats, with strong default rule sets and extensive customization providing Layer 7 protection that is fully integrated with DDoS mitigation
- · Lightning-fast 0.3 ms processing times, with instant global updates
- · Compliance for PCI DSS requirement 6.6 — Cloudflare's WAF enables you to cost-effectively fulfill PCI compliance
- Real-time reporting robust logging lets you see what's happening instantaneously
- · Cloud deployment with no hardware, software or tuning required

Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/ exclude specific subdomains for WAF protection to test domains or include/ exclude specific subdomains. Allows full stack protection against DDoS — no extra implementation required Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Protection to the strain intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Protect against backers from specific IPs and the supdates. Restrict by IP or geolocation Can blocklist/whitelist traffic from specific IPs addresses or countries to protect against backers from specific IPs or countries. Low false positive Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation. Rule sets Automatic learning paired with eccurate against zero-day vulnerabilities or new threats with patches automatically deployed by our security to a protect of the protect	Key features	Benefit
SQL injection, cross site scripting attacks and thousands more SSL Terminate SSL connections without any overhead or additional latency. Apply your Wiff policy to SSL encrypred traffic without having to upload certificates or invest in costly hardware solutions. Cover's range of HTTP/S traffic URL-specific custom rule sets I Allows you to include/exclude specific uRLs or subdomains for WAF protection to test domains in include/exclude specific uRLs or subdomains. DOS mitigation integration Allows full-stack protection against DDoS — no extra implementation required Preputation database integration Real-time intelligence on over 1 billion unique IPs used to block malidious traffic — no extra implementation required Wirtual patching Fixes a widnerability before you patch your server or update your code, allowing you more time to patch and test updates. Restrict by IP or geolocation Can blackfirst/whitelist traffic from specific IPs addresses or countries to protect against hackers from specific IPs or countries. Coveral IT-SOM fixes positive traffic from specific IPs addresses or countries to protect against hackers from specific IPs or countries. Coveral IT-SOM fixes positive traffic from specific IPs addresses or countries to protect against hackers from specific IPs or countries. Coveral IT-SOM fixes positive traffic from specific IPs addresses or countries to protect against hackers from specific IPs or countries. Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rules sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against zero-day uninerabilities or new threats with patches automatically deployed by our security ream Allows you to easily import existing rule sets to maintain existing protection Allows you to easily import existing rule sets to maintain existing protection Allows you to assily import existing rule sets to m	Security	
WAF policy to SSE, encrypted traffic without having to upload certificates or invest in costly hardware solutions. Covers range of HTTP/S traffic Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/exclude specific subdomains. Dos mitigation integration Allows full-stack protection against DDoS — no extra implementation required Preputation database integration Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Privated patching Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates. Restrict by IP or geolocation Can blacklist Arkhitelist traffic from specific IPs addresses or countries to protect against nackers from specific IPs or countries Overall 1/50M false positive are ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required authomatic learning paired with generated with generated and the supplication of the patch and test updates. Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against DWASP vulnerabilities, the most critical flaws as identified by the Open Web Application Security Project (OWASP)—included as default with no extra fees Paterom-specific rule sets for major CMS and eCommerce platforms Core of Sundanes Security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Cover situations unique to your web application included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Cover situations unique to your web application included as default with no extra fees Platform-specific pulse sets for major CMS and eCommerce platforms Cover situations unique to your web a		
Allows you to include/exclude specific URLs or subdomains for WAF protection to test domains or include/ exclude specific subdomains. Allows full stack protection against DDOS — no extra implementation required Resl-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Resl-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Restrict by IP or geolocation Restrict by IP or geolocation Restrict by IP or geolocation Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries Low false positive Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with geologied by our security team Compatibility with Modsecurity logic and format Core OWASP ModSecurity rule sets Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Custom rules Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Customizable block pages Customizable block pages Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Availability to help you fine-tune the WAF Access to rave log files Achallenge page avisable substor	SSL	WAF policy to SSL encrypted traffic without having to upload certificates or invest in
to test domains or include/exclude specific subdomains DDoS mitigation integration Allows full-stack protection against DDoS — no extra implementation required Real-time intelligence on over 1 billion unique IPs used to block malicious traffic — no extra implementation required Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates. Restrict by IP or geolocation Gan blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries Low false positive Overall 1/50M false positive from specific IP addresses or countries to protect against hackers from specific IPs or countries Low false positive Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security ream to represent the protect of the pr	For GET and POST HTTP/S requests	Covers range of HTTP/S traffic
Real-time intelligence on over 1 billion unique IPs used to block malicious traffic— no extra implementation required Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates. Restrict by IP or geolocation Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries. Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities or new threats with patches automatically deployed by our security team Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP)—included as default with no extra fees Zero-day Cloudflare rule sets Rely on Cloudflare's security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major Wordfleres, Jonnal, Plone, Drupal, Magneto, Ils, etc. Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Block Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF A	URL-specific custom rule sets	
Nirtual patching Fixes a vulnerability before you patch your server or update your code, allowing you more time to patch and test updates. Restrict by IP or geolocation Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries Low false positive Overall I/SOM false positive rate ensures legitimate traffic reaches you Full integration with CDN service, offering outbound content transformation Rules sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against DWASP vulnerabilities or new threats with patches automatically deployed by our security team Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP)—included as default with no extra fees Rely on Cloudflare's security tream to protect you against threats identified across our customer base—included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms WordPress, Joonala, Plone, Drupal, Magneto, IIS, etc. Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Block Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Castomize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduc	DDoS mitigation integration	Allows full-stack protection against DDoS — no extra implementation required
you more time to patch and test updates. Restrict by IP or geolocation Can blacklist/whitelist traffic from specific IP addresses or countries to protect against hackers from specific IPs or countries Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees Rely on Cloudflare security seam to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees for platforms such as WordPress, Joomila, Plone, Drupal, Magneto, IIS, etc. Custom rules Receive protection out of the box with no extra fees for platforms such as WordPress, Joomila, Plone, Drupal, Magneto, IIS, etc. Custom rules Block Block Blocking an attack will stop any action before it is posted to your website. The set for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customizable block pages Real-time logging Gain visibility to help you fine-tune the WAF Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simp	IP reputation database integration	
Low false positive Low false positive Overall 1/50M false positive rate ensures legitimate traffic reaches you Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against zero-day vulnerabilities or new threats with patches automatically deployed by our security team Allows you to easily import existing rule sets to maintain existing protection Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees Rey on Cloudflarer sets our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, Ils, etc. Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Set rules to trigger more or less depending on sensitivity Customizable block pages Customizable block pages Gain visibility to help you fine-tune the WAF Access to raw log files Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Virtual patching	
Reduces web latency for your site visitors — no extra implementation required outbound content transformation Rule sets Automatic learning paired with security deployed by our security team Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities or new threats with patches automatically deployed by our security team Allows you to easily import existing rule sets to maintain existing protection Allows you to easily import existing rule sets to maintain existing protection Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees Rely on Cloudflare's security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Wordflerss, Joonila, Plone, Drupal, Magneto, Ils, etc. Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Restrict by IP or geolocation	
Rule sets Automatic learning paired with security-driven research deployed by our security team Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP) — included as default with no extra fees Zero-day Cloudflare rule sets Rely on Cloudflare's security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc. Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customizable block pages Customizable block pages Gain visibility to help you fine-tune the WAF Access to raw log files Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Low false positive	
Automatic learning paired with security-driven research Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by The Open Web Application Security Project (OWASP)—included as default with no extra fees Zero-day Cloudflare rule sets Rely on Cloudflare's security team to protect you against threats identified across our customer base—included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Administration High availability — built on service Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS		Reduces web latency for your site visitors — no extra implementation required
deployed by our security team Compatibility with ModSecurity logic and format Core OWASP ModSecurity rule sets Protects against OWASP vulnerabilities, the most critical flaws as identified by. The Open Web Application Security Project (OWASP) — included as default with no extra fees Rely on Cloudflare's security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Custom rules Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc. Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customizable block pages Customizable for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Rule sets	
Achallenge A challenge A challenge Block Simulate Challenge A challenge page ask visitors to submit a CAPTCHA to continue to your website. Set rules to findlenge A challenge pages Customizable block pages Customizable block pages Block Simulate Challenge A challenge page ask visitors to submit a CAPTCHA to continue to your website. Set rules to rigger more or less depending on sensitivity Customizable block pages Customizable block pages Block Simulate Biorking an attack will stop any action before it is posted to your website. Set rules to rigger more or less depending on sensitivity Customizable block pages Bl	Automatic learning paired with security-driven research	
The Open Web Application Security Project (OWASP) — included as default with no extra fees Rely on Cloudflare's security team to protect you against threats identified across our customer base — included as default with no extra fees Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc. Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS		Allows you to easily import existing rule sets to maintain existing protection
Platform-specific rule sets for major CMS and eCommerce platforms Receive protection out of the box with no extra fees for platforms such as WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc. Custom rules Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. Simulate To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Core OWASP ModSecurity rule sets	The Open Web Application Security Project (OWASP) — included as default with
CMS and eCommerce platforms WordPress, Joomla, Plone, Drupal, Magneto, IIS, etc. Cover situations unique to your web application included as default with no extra fees for Business and Enterprise customers WAF settings Block Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Zero-day Cloudflare rule sets	
WAF settings Block Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS		
Blocking an attack will stop any action before it is posted to your website. To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Custom rules	
To test for false positives, set the WAF to Simulate mode, which will record the response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs Sign up with a simple change in DNS	WAF settings	
response to possible attacks without challenging or blocking. Challenge A challenge page asks visitors to submit a CAPTCHA to continue to your website. Threshold / sensitivity setting Set rules to trigger more or less depending on sensitivity Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Block	Blocking an attack will stop any action before it is posted to your website.
Threshold / sensitivity setting Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Set rules to trigger more or less depending on sensitivity Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Bain visibility to help you fine-tune the WAF Enterprise customers can conduct in-depth analysis covering all WAF requests Administration Susiness and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Simulate	
Customizable block pages Customize the page a visitor sees when they're blocked, e.g. "Call this telephone number for help." Available for Enterprise customers. Reporting Real-time logging Gain visibility to help you fine-tune the WAF Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Sign up with a simple change in DNS	Challenge	A challenge page asks visitors to submit a CAPTCHA to continue to your website.
number for help." Available for Enterprise customers. Reporting Real-time logging Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required number for help." Available for Enterprise customers. Bair visibility to help you fine-tune the WAF Enterprise customers can conduct in-depth analysis covering all WAF requests Administration Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Threshold / sensitivity setting	Set rules to trigger more or less depending on sensitivity
Real-time logging Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Gain visibility to help you fine-tune the WAF Enterprise customers can conduct in-depth analysis covering all WAF requests Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Customizable block pages	
Access to raw log files Enterprise customers can conduct in-depth analysis covering all WAF requests Administration High availability — built on service offering SLAs No hardware, software or tuning required Enterprise customers can conduct in-depth analysis covering all WAF requests Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Reporting	
Administration High availability — built on service offering SLAs No hardware, software or tuning required Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Real-time logging	Gain visibility to help you fine-tune the WAF
High availability — built on service offering SLAs Business and Enterprise customers enjoy 100% uptime guarantee and financial penalties if not met Sign up with a simple change in DNS	Access to raw log files	Enterprise customers can conduct in-depth analysis covering all WAF requests
offering SLAs penalties if not met No hardware, software or tuning required Sign up with a simple change in DNS	Administration	
	High availability — built on service offering SLAs	
PCI certification Cloudflare's service has received Level 1 service provider certification	No hardware, software or tuning required	Sign up with a simple change in DNS
	PCI certification	Cloudflare's service has received Level 1 service provider certification