CLOUDFLARE®

Securing the Web Perimeter – WordPress

How unpatched WordPress installs can increase the risk of security breaches

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV: 190408

TABLE OF CONTENTS

Executive Summary

The Equifax and Yahoo breaches have highlighted just how vulnerable enterprises are to cyber attacks that aim to exfiltrate data by exploiting web application vulnerabilities. Content Management Systems (CMS) are among the most popular platforms on the world wide web - over 30% of the websites in the Alexa top 1 million use WordPress- a popular CMS[1].

Exploits of WordPress have soared in recent times[2]. Securing a combination of legacy environments and newer stacks, keeping up with the latest security patches, and reducing response times to zero-day vulnerabilities all remain challenges for organizations using WordPress.

This white paper outlines some common causes of WordPress vulnerabilities and offers guidelines on securing WordPress installations.

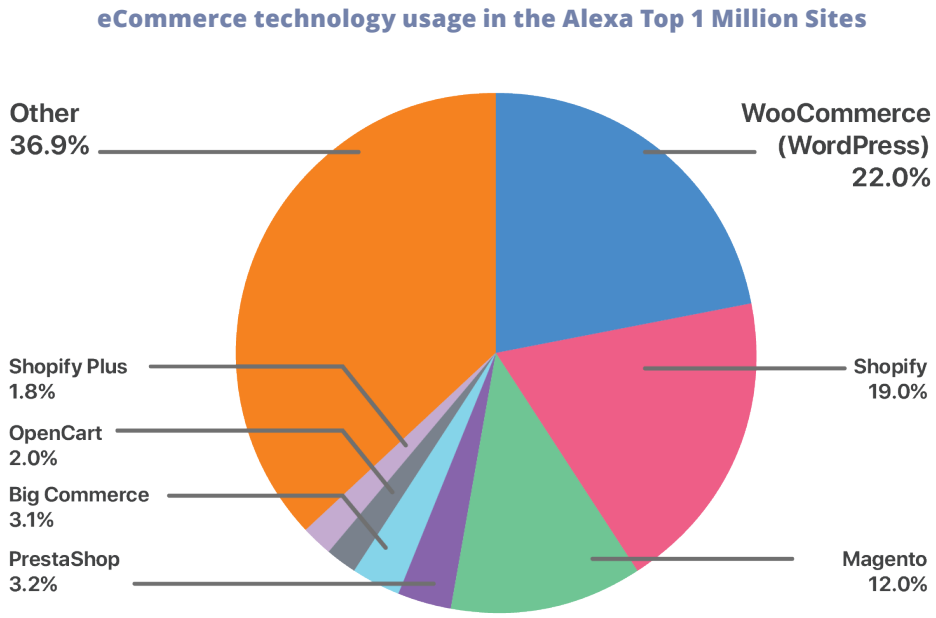
Part 1 of this three part white paper offers insights on why WordPress is commonly targeted by attackers and guidance on choosing security solutions that can help enterprises reduce the risk of security breaches.

1 Usage of Content Management Systems: https://w3techs.com/technologies/overview/content_management/all

2 Thousands of WordPress sites backdoored with malicious code: https://www.zdnet.com/article/thousands-of-wordpress-sites-backdoored-with-malicious-code/

WordPress dominates market share but also leads in vulnerabilities

WordPress powers 30.9% of the Alexa top 10 million websites[3], which roughly translates to 30% of the Internet as we know it. WordPress is also the web's most popular e-commerce platform; according to data from BuiltWith, WooCommerce, a popular open source e-commerce WordPress plugin, powers around 22% of the e-commerce stores in the Alexa top 1 million sites.

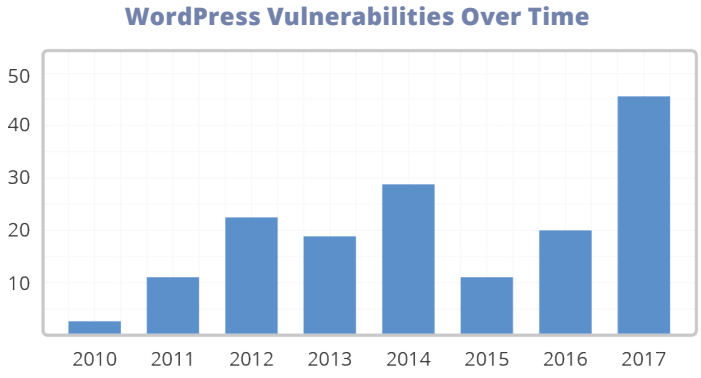


Source: https://trends.builtwith.com/shop

The popularity of WordPress and plugins such as WooCommerce have made this CMS a prime target for bad actors looking to infect websites with malware and exfiltrate data or gain control over a site's operations. In November 2018, researchers at RIPS tech uncovered a serious vulnerability in WooCommerce that allowed bad actors to perform a complete account takeover and gain control over web shops[4].

WordPress Vulnerabilities Have Surged

WordPress adoption, along with an increase in security research worldwide, has led to a surge in WordPress Common Vulnerability and Exposures[5] (CVEs) being announced in recent years.



Source: https://www.cvedetails.com/product/4096/Wordpress-Wordpress.html?vendor_id=2337

3 Usage statistics and market share of WordPress for websites: https://w3techs.com/technologies/details/cm-wordpress/all/all

4 WordPress Design Flaw + WooCommerce Vulnerability Leads to Site Takeover: https://www.bleepingcomputer.com/news/security/wordpress-design-flaw-woocommerce-vulnerability-leads-to-site-takeover/

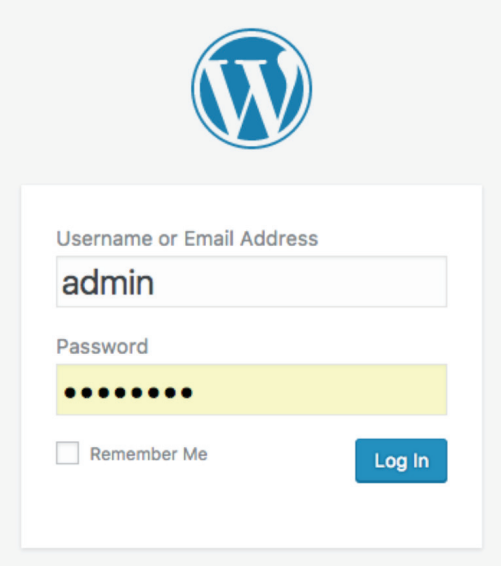
5 The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures: https://cve.mitre.org/

Why WordPress is so 'hackable'

From a threat actor's perspective, hacking into a popular platform such as WordPress is more appealing than hacking into a proprietary platform for several reasons:

- Security vulnerabilities are well-publicized and most users are slow to update or install publicly available patches
- Readily available (and hackable) third-party plugins and themes make it easier to find and exploit security holes

One example of a relatively unsophisticated attack is when a bad actor visits a WordPress site administrator login page at /wp-admin and tries logging in with a simple script that generates combinations of commonly used usernames and passwords. Such an attack is an example of a 'dictionary attack' in which a bad actor uses brute force methods to try and gain access.



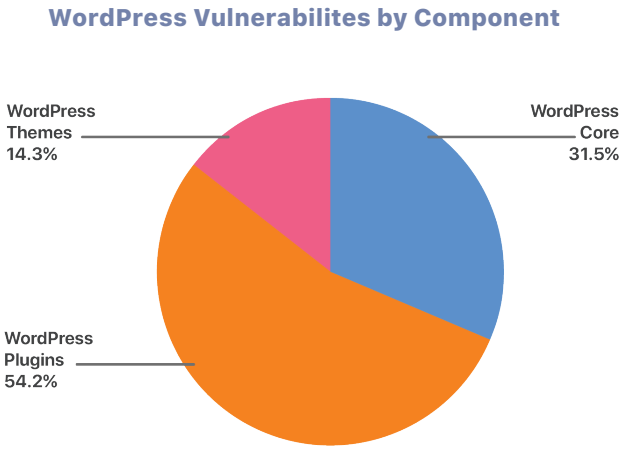
Administrators Struggle To Patch Well Publicized WordPress Vulnerabilities

Furthermore, WordPress security vulnerabilities are well-publicized. Even though these vulnerabilities are publicly disclosed and patched quickly, many administrators struggle to keep up with the latest patches that address these vulnerabilities. In February 2017, bad actors defaced 1.5 million pages on over 39,000 WordPress domains by exploiting a flaw in the WordPress REST API on sites running WordPress versions 4.7.0 and 4.7.1[6] and by carrying out content injection. This flaw had already been patched in version 4.7.2, but the defaced sites had failed to download and install the security patch.

A recent survey by Hashed Out reported that **49% of WordPress sites in the Quantcast Top 10,000 are not running the latest, most secure version, and 33% are multiple updates behind[7].**

Plugins and Themes Are Common Targets

Additionally, the sheer extensibility of WordPress, in terms of the ability for administrators to install numerous plugins, themes, and extensions written by third-party developers, also makes it more open to security vulnerabilities. According to WPScan, the most popular black box WordPress vulnerability scanner[8], **plugins and extensions are the biggest source of vulnerabilities, with 1,305 vulnerabilities (54% of the global WordPress vulnerabilities count)**. These are followed by 344 (14.3%) theme vulnerabilities and 758 (31.5%) core vulnerabilities.



Source: https://wpvulndb.com/statistics

6 Attacks on WordPress Sites Intensify as Hackers Deface Over 1.5 Million Pages https://www.bleepingcomputer.com/news/security/attacks-on-wordpress-sites-intensify-as-hackers-deface-over-1-5-million-pages/

7 33% of WordPress websites are at least two versions behind: https://www.thesslstore.com/blog/33-percent-top-wordpress-sites-are-at-least-two-versions-behind/

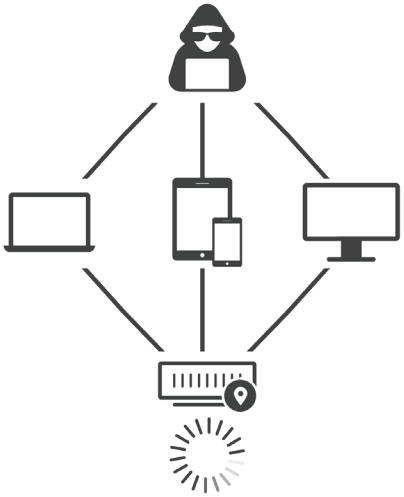
8 https://wpscan.org/

Common WordPress attack types

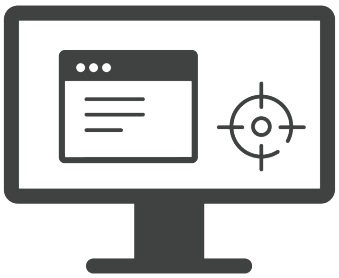
APART FROM TARGETING UNPATCHED CORE, PLUGIN, OR THEME VULNERABILITIES, THREAT ACTORS CAN PERFORM SEVERAL OTHER ATTACKS:

DDoS and Malware Attacks:

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. From a high level, a DDoS attack is like a traffic jam clogging up the highway, preventing regular traffic from arriving at its desired destination.



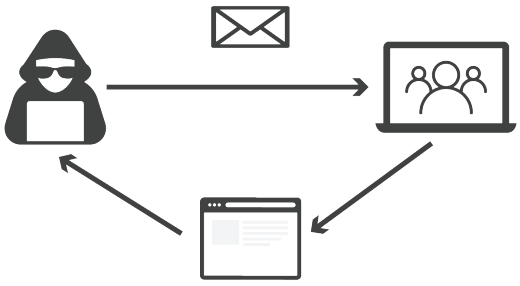
DDoS attacks do this by utilizing multiple compromised computer systems as sources of attack traffic, or by using 'botnets' - groups of devices that have been infected by malware and are under the control of a malicious actor. Exploited machines can include computers and other networked resources such as IoT devices. DDoS botnet malware can have different levels of visibility; some malware is designed to take total control of a device, while other malware runs silently as a background process while waiting silently for instructions from the attacker or "bot herder."



Injection Attacks and Cross-Site Scripting:

Content injection is an attack targeting weaknesses in applications that do not properly handle user-supplied data. One example of this is Structured Query Language (SQL) Injection - a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database, the destruction of sensitive data, alterations to existing data, modifications of transactions and balances, or other malicious actions.

Cross-site scripting (XSS) is an exploit where the attacker attaches malicious code onto a legitimate website. This code executes when the victim loads the website. That malicious code can be inserted in several ways. Most popularly, it is either added to the end of a URL or posted directly onto a page that displays user-generated content. In more technical terms, cross-site scripting is a client-side code injection attack.



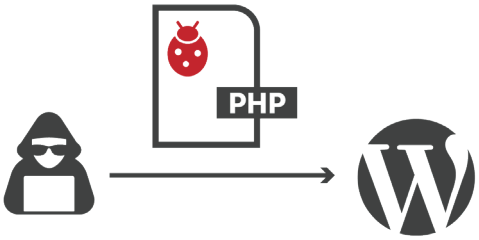
File Inclusion and Remote Code Execution[9]:

Many WordPress plugins support file inclusion so as to 'include' (or refer to) files on or outside of the website's server.

Remote and Local File Inclusion is an attack technique used to exploit dynamic file include mechanisms in WordPress plugins. When plugins take user input (URL, parameter value, etc.) and pass them into file include commands, the web application might be tricked into including local or remote files with malicious code.

1. The attacker scans for vulnerable Wordpress plugins

2. The attacker uploads infected/ malicious files to WordPress



FILE INCLUSION IS USUALLY A PRECURSOR TO REMOTE CODE EXECUTION. ATTACKERS CAN:

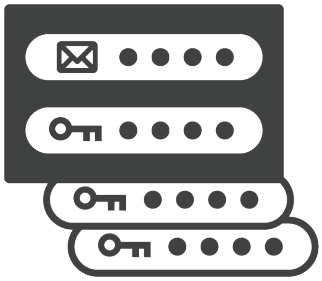
Run malicious code on the server: Any code in the included malicious files will be run by the server. If the file include is not executed using some wrapper, code in include files is executed in the context of the server user. This could lead to a complete system compromise.

Run malicious code on clients: The attacker's malicious code can manipulate the content of the response sent to the client. The attacker can embed malicious code in the response that will be run by the client (for example, JavaScript to steal the client session cookies).

Brute Force Attacks:

A brute force attack is a trial-and-error method used to decode sensitive data. The most common applications for brute force attacks are cracking passwords and cracking encryption keys.

One example of such an attack is 'credential stuffing.' Generally this is an automated bot attack that tries to successfully log in to WordPress using brute force 'dictionary attacks' on the login page, entering well-known credential combinations or cycling through previously stolen credentials. These attacks usually take advantage of user tendencies to rely on default usernames and passwords such as 'admin' and 'password12345' or to reuse login credentials across several sites.



9 Remote File Inclusion: http://projects.webappsec.org/w/page/13246955/Remote%20File%20Inclusion

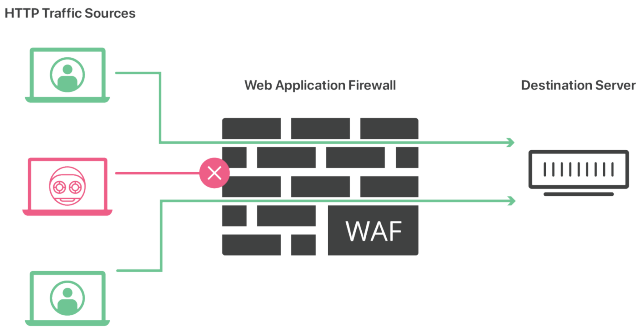
Protecting WordPress Sites from Known and Zero Day Vulnerabilities

Web Application Firewall (WAF)

A great way of protecting WordPress and other web applications is investing in a Web Application Firewall (WAF). A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks such as **cross-site-scripting (XSS), file inclusion, and SQL injection,** among others. A WAF is a protocol layer 7 defense (in the OSI model), and is not designed to defend against all types of attacks.

This method of attack mitigation is usually part of a suite of tools that together create a holistic defense against a range of attack vectors, including the **OWASP top 10** - a list of the 10 most critical security risks to web applications as identified by security experts from around the world[10].

How WAFs Work



By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy server protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules, often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policies can be modified, allowing for faster response to varying attack vectors. During a DDoS attack, for instance, administrators can quickly implement rate limiting by modifying WAF policies.

WAF IMPLEMENTATION TYPES:

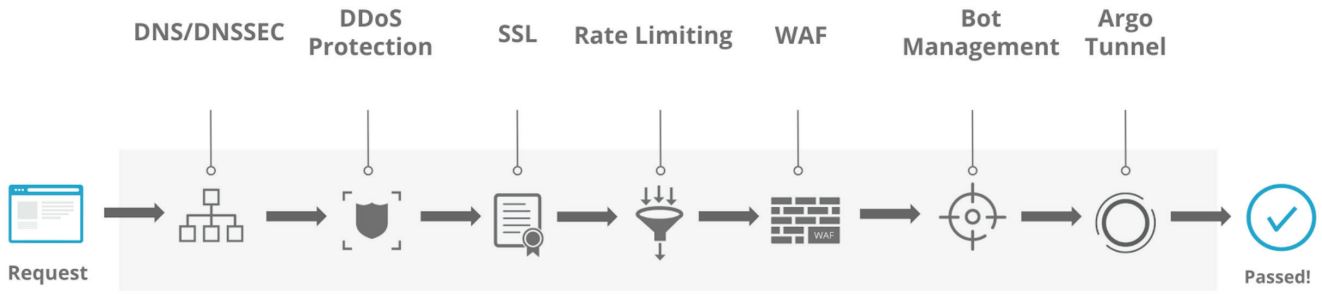
A network-based WAF is generally hardware-based. Since they are installed locally they minimize latency, but network-based WAFs are the most expensive option and also require the storage and maintenance of physical equipment.

A host-based WAF may be fully integrated into an application's software. This solution is less expensive than a network-based WAF and offers more customizability. The downside of a host-based WAF is the consumption of local server resources, implementation complexity, and maintenance costs. These components typically require engineering time, and may be costly.

Cloud-based WAFs offer an affordable option that is very easy to implement; they usually offer a turnkey installation that is as simple as a change in DNS to redirect traffic. Cloud-based WAFs also have a minimal upfront cost, as users pay monthly or annually for security as a service. Cloud-based WAFs can also offer a solution that is consistently updated to protect against the newest threats without any additional work or cost on the user's end. The drawback of a cloud-based WAF is that users hand over the responsibility to a third-party, therefore some features of the WAF may be a black box to them.

10 OWASP Top Ten Project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

The Cloudflare Solution



Cloudflare offers an enterprise-class cloud WAF as part of an integrated security solution differentiated by its depth of integration. The WAF spans DNS security, DDoS protection, SSL/TLS encryption, rate limiting (for protecting against brute force attacks), bot management, and Argo Tunnel for origin server protection.

The Cloudflare WAF protects WordPress installations from common attack types like SQL injection attacks, cross-site scripting, and DDoS or botnet attacks, with no changes to existing infrastructure. **It not only supports the OWASP ModSecurity Core Rule Set by default, but it also includes application-specific rule sets and custom rule sets.**

The Cloudflare Difference

Cloudflare offers an enterprise-class cloud WAF as part of an integrated security solution differentiated by its depth of integration. The WAF spans DNS security, DDoS protection, SSL/TLS encryption, rate limiting (for protecting against brute force attacks

Shared Intelligence at Scale

Cloudflare protects 13 million web properties and processes 400B requests per day. The WAF leverages the data gathered from this traffic and:

- Protects against emerging threats
- Identifies and blocks repeat offenders proactively using machine learning
- Reduces risk of data loss and exposure
- Defends against DDoS and Layer 7 attacks

Integration with Related Security Features

The WAF integrates with other Cloudflare services to address the ever-widening scope of threats:

- **Cloudflare Workers** enables customers to create custom security logic at the edge
- **Cloudflare Access** authenticates web application access with leading identity providers like G Suite and Okta

Performance Gains

Security should not be at the expense of performance. Cloudflare performance capabilities include:

- Accelerated origin traffic through **Argo Smart Routing**
- SSL termination close to the customer from 165+ data centers
- Compression and content caching to reduce latency

Conclusion

To manage the threats of an ever-growing attack surface, newer ways of exploiting zero-day vulnerabilities in popular platforms such as WordPress, increases in authentication and access control exploits, and vulnerabilities in TLS, websites and applications **require the resilience and intelligence of a scalable network that uses a single control plane for ease of use.**

Cloudflare security services protect enterprises from threats without degrading performance caused by security-induced latencies. Distinguished by easy-to-configure controls to eliminate misconfigurations, and powered by a global Anycast network with 165+ data centers and 25 Tbps capacity, Cloudflare proactively safeguards enterprises by learning from attacks targeting 13 million web properties on its network and helps enterprises mitigate the risk of security breaches.

';--have i been pwned?

"As someone who deals with post-data breach analysis on an almost daily basis, I love Cloudflare for its ease of use and quality of security offerings such as SSL/TLS for all and the Web Application Firewall.

Whether you're a blogger just trying to get SSL/TLS on your personal site or an enterprise looking to enhance your risk mitigation model, Cloudflare is a great step to getting world-class breach protection while handling massive performance demands."

-Troy Hunt

Troy Hunt is a Microsoft Regional Director and Most Valuable Professional award winner for Developer Security. He is also an international speaker on web security and the author of many top-rated security courses for web developers on Pluralsight.

"As the value of data increases, the number of breaches will rise. Given this new reality, we partnered with Cloudflare to develop a solution for our customers that secures their WordPress digital experiences, protects data, safeguards operations and keeps threats far away via the global edge network."

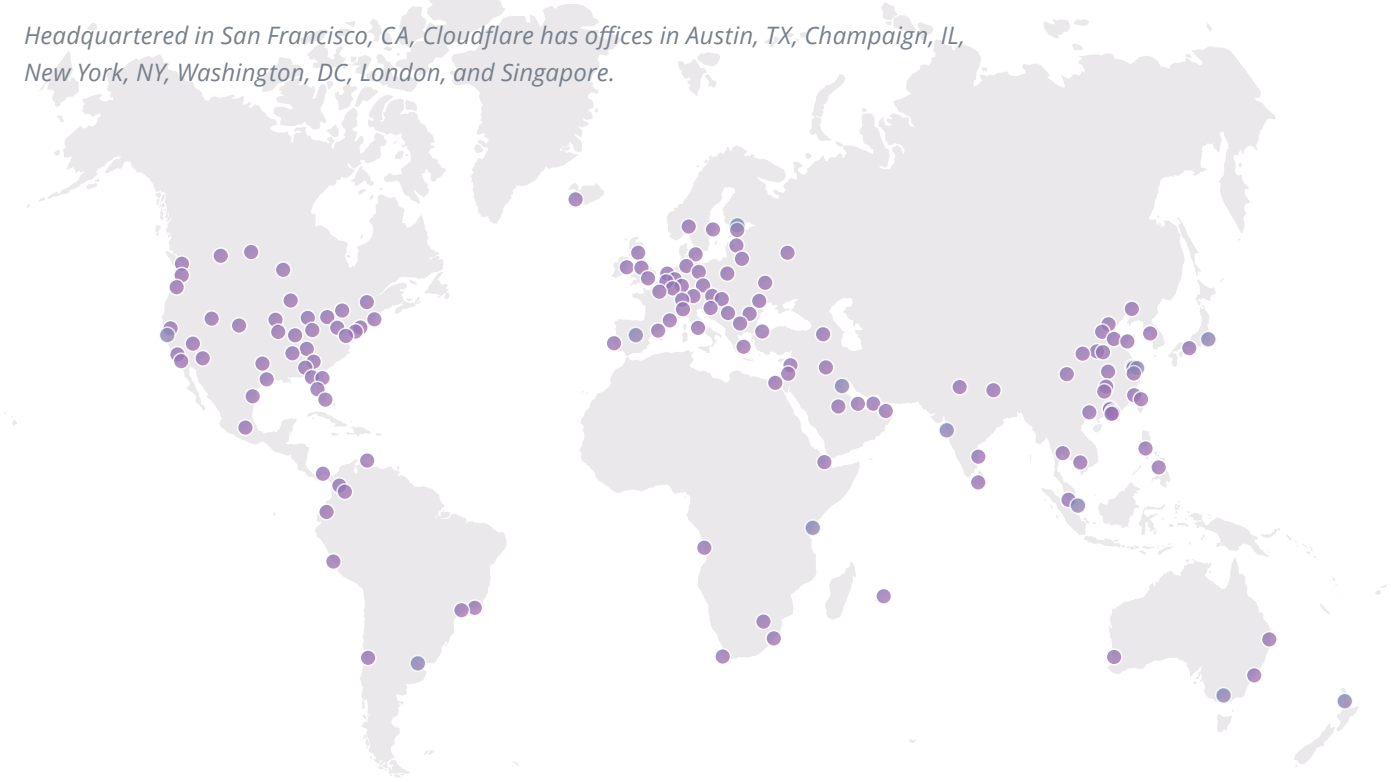
-Lee McClendon, Senior Vice President of Research and Development, WP Engine

WP Engine provides managed WordPress hosting for mission critical sites around the world.

About Cloudflare

Cloudflare, Inc. (www.cloudflare.com / @cloudflare) is on a mission to help build a better Internet. Today the company runs one of the world's largest networks that powers more than 10 trillion requests per month, which is nearly 10 percent of all Internet requests for more than 2.8 billion people worldwide. Cloudflare protects and accelerates any Internet application online without adding hardware, installing software, or changing a line of code.

Headquartered in San Francisco, CA, Cloudflare has offices in Austin, TX, Champaign, IL, New York, NY, Washington, DC, London, and Singapore.



Forrester Wave for Web Application Firewalls: Cloudflare is a CONTENDER

Cloudflare was recognized as a Leader for the second consecutive year, by Forrester Research Inc.:.

https://www.forrester.com/report/The+Forrester+Wave+Web+Application+Firewalls+Q2+2018/-/E-RES141629

Gartner Magic Quadrant for Web Application Firewalls, 2018: Cloudflare is a CHALLENGER

Cloudflare was named a Challenger by Gartner for the second year, in the "Gartner Magic Quadrant for Web Application Firewalls, 2018".

https://www.cloudflare.com/gartner-mq-waf-2018/

Cloudflare World Headquarters

San Francisco
101 Townsend St
San Francisco, CA 94107

+1 (888) 99 FLARE

For specific country offices and contact numbers, please visit our website.

https://www.cloudflare.com/

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com