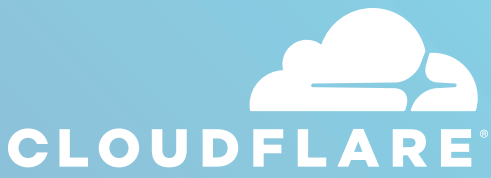


Securing the Web Perimeter

How WordPress, VPNs, outdated TLS, and Web Apps Built With Modern Stacks Can Increase The Risk Of Security Breaches

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

REV: 180628

TABLE OF CONTENTS

Executive Summary

The Equifax and Yahoo breaches have highlighted enterprise vulnerability to cyber attacks focusing on data exfiltration by exploiting web application vulnerabilities. As the global enterprise content management market size increases[1] and enterprises embrace remote workforces, adopt multi-clouds, expose new APIs, and shift server side functionality to the client, new security challenges emerge.

Securing a combination of legacy environments and newer stacks, keeping up with the latest security patches, and reducing response time to zero day vulnerabilities in order to safeguard from security breaches remains a challenge.

This white paper offers:

- Insights on why popular content management systems and platforms are commonly targeted by attackers
- Overlooked attack vectors and software engineering trends that adversely impact security postures
- Guidance on security frameworks that can help enterprises reduce the risk of security breaches while handling these new challenges

1 https://www.statista.com/statistics/506914/enterprise-content-management-market-size/

Incidents involving enterprise security breaches cause serious damage such as drops in valuation[2], loss of customer trust[3], decreased market cap, and changes in executive leadership[4].

Security breaches are widely discussed in the news but there are four considerations that are often overlooked:

- The growing popularity of content management platforms such as WordPress among small businesses and enterprises and failure to keep them patched makes them prime targets of attackers
- New software stacks expose new zero day vulnerabilities in the attack surface
- TLS encryption security might be much weaker than imagined
- Network perimeter security models that rely on VPNs used for securing access may actually weaken security postures

2 Verizon cuts Yahoo deal price by $350 million following data breach disclosure
http://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html

3 Equifax's massive data breach has cost them $ 4 billion in stock market value so far
http://time.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/

4 Equifax CEO Down After Epic Breach
https://www.nbcnews.com/business/consumer/equifax-ceo-richard-smith-retires-after-epic-breach-n80477

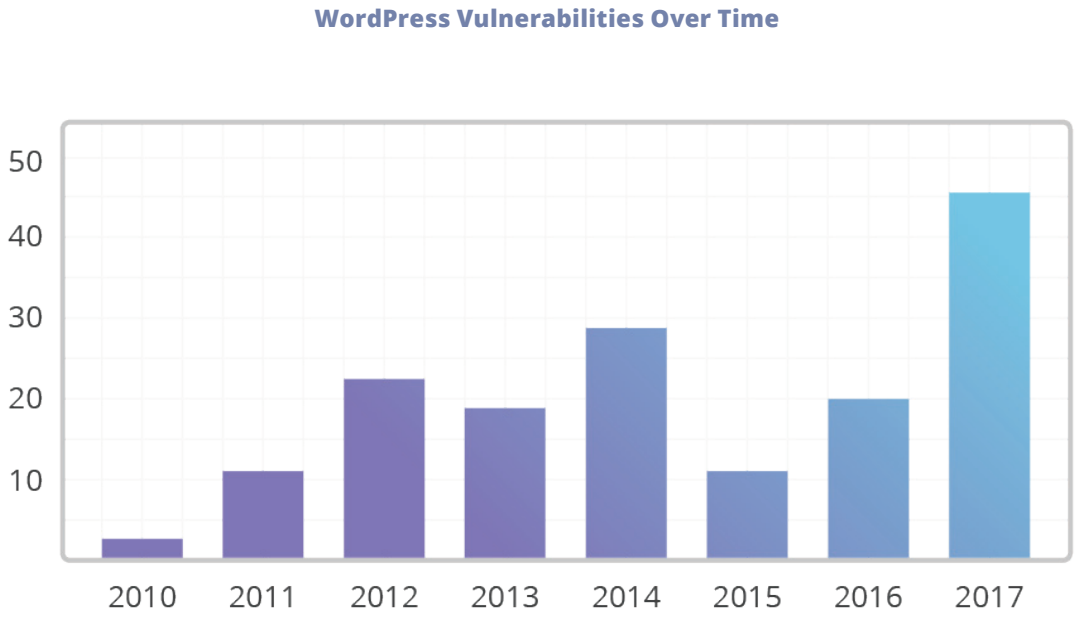
Sites Using WordPress are Prime Targets

WordPress dominates market share but also leads in vulnerabilities

WordPress powers 30.9% of the Alexa top 10 million websites, which for practical purposes, translates to 30% of the Internet[5]. WordPress is also the web's most popular e-commerce platform; according to data from BuiltWith[6], WooCommerce, a WordPress plugin, powers 42% of the e-commerce stores on the entire Internet.

The popularity of WordPress has made it a prime target for hackers looking to infect websites with malware and exfiltrate data or gain control over a site's operations.

WordPress adoption, along with an increase in security research worldwide, has created a surge of WordPress CVEs (Common Vulnerability and Exposures[7]) being announced in recent years.



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

Unsurprisingly WordPress also accounts for the highest rate of infected sites worldwide. According to a report from Sucuri, WordPress web sites accounted for 83% of all infected sites using a CMS.

5 https://w3techs.com/technologies/details/cm-wordpress/all/all

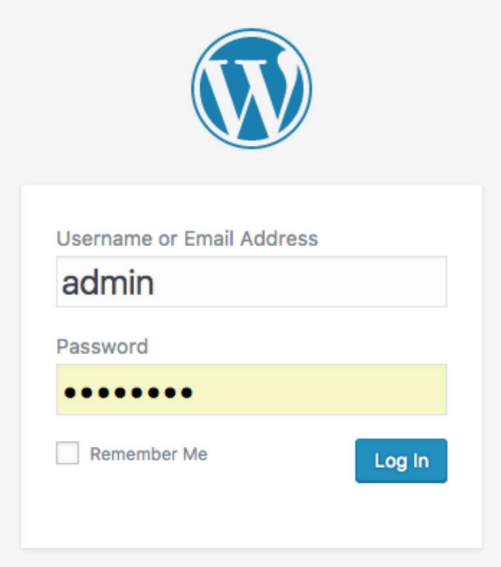
6 https://trends.builtwith.com/shop

7 The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures

Why WordPress is so 'hackable'

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

- Some attack types require low effort or sophistication
- Security vulnerabilities are well publicized and patches are publicly available yet many users do not install them
- Readily available (and hackable) third party plugins and themes make it easier to identify security holes and exploit them.



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

Furthermore WordPress security vulnerabilities are well publicized, and even after these vulnerabilities are publicly disclosed and patched, many sites struggle to keep up with the latest patches and do not run the required security updates that address these vulnerabilities. In February 2017, for example, 1.5 million pages over 39,000 WordPress domains were defaced by hackers who exploited a flaw in the WordPress REST API on sites running WordPress versions 4.7.0 and 4.7.1[8] and carried out content injection. This flaw had already been patched in version 4.7.2, however, the defaced sites had failed to download and install the security patch, and weren't using a security tool such as a web application firewall to reduce the risk of such vulnerabilities being exploited.

As of May 2018, **49% of WordPress sites in the Quantcast Top 10,000 are not running the latest, most secure version and 33% are multiple updates behind.[9]**

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.

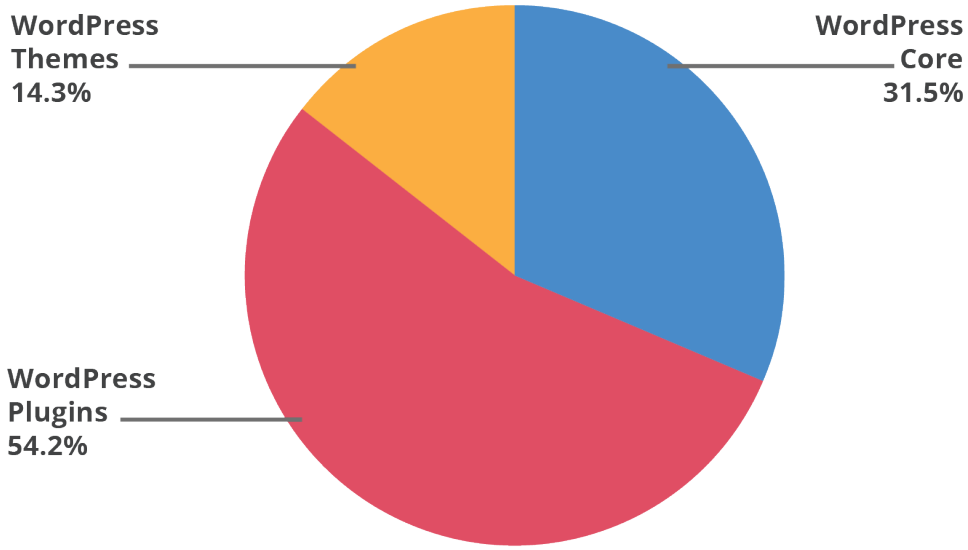
According to WPScan, the most popular black box WordPress vulnerability scanner[10], plugins are the biggest source of vulnerabilities with 1,305 vulnerabilities (54% of the global WordPress vulnerabilities count). These are followed by 344 (14.3%) theme vulnerabilities and 758 (31.5%) core vulnerabilities.

8 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/

9 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/

10 https://wpscan.org/

WordPress Vulnerabilites by Component



SECTION SUMMARY:

Hackers target WordPress because of its popularity and ease of hacking. Keeping WordPress updated, reducing the number of third party themes and plugins, and investing in security measures such as web application firewalls that can detect and prevent common injection attacks are some ways in which site administrators can reduce the risk of security breaches in WordPress.

New Trends in Web Application Development Using New Stacks Can Expose New Vulnerabilities

The MEAN Stack

Mongo DB
(database system)

Express
(back-end web framework)

Angular.js
(front-end framework)

Node.js
(back-end runtime environment)

To improve application performance and reduce development time, many companies are adopting modern development stacks such as the MEAN (MongoDB, Express.js, Angular.js and Node.js) and MERN (MongoDB, Express.js, React and Node.js) stacks. These stacks reduce server loads by moving functionality to the front-end. They also improve back-end performance and simplify business logic by handling large

volumes of unstructured data. Modern stacks can improve not only developer productivity, but also security by incorporating features such as context-aware encoding and CSRF protection.

However, in spite of inbuilt security improvements, these **stacks may mislead developers into believing their applications are safe while still exposing the business to risks of security breaches.**

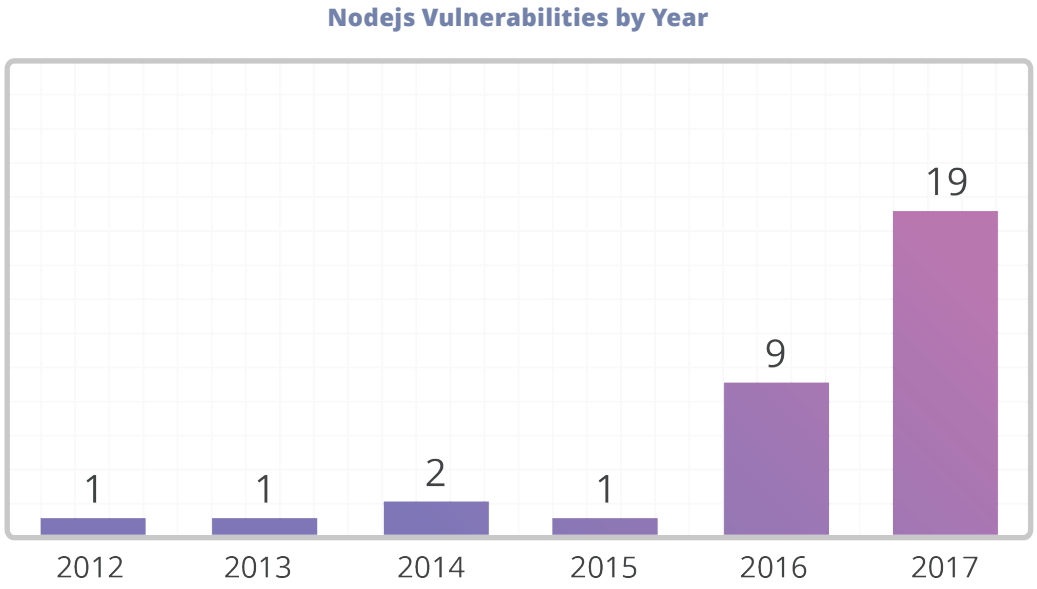
Sprint based development and lack of hardening - the price paid for novelty

As software developers adopt new stacks and move from a quarterly release cycle to sprint based release cycles they are pushed to deliver faster and with more frequency, which limits testing for security issues.

In some ways, the freshness of these new stacks makes them potentially less secure than the older solutions they intend to replace. Newer stacks, by having less time in the wild across different production environments and attack attempts, have also been less tested.

The legacy LAMP stack, for instance, has been used for almost two decades but the MEAN and MERN stacks are still relatively new.[11]

As newer development approaches and stacks continue to grow in popularity, new vulnerabilities are likely to surface explosively. This is illustrated by the spike in Node.js vulnerabilities in 2017 as seen by the CVE database.



Growing Codebases Expand The Attack Surface

As the number of new frameworks grow, both in terms of forks of popular versions as well as brand-new frameworks, developers get more choice. This choice, on the one hand, improves productivity and business value; but on the other, can result in increased code sprawl across an organization.

In exchange for speed, many developers expand the size of their code base since the frameworks do more of the logic and presentation "automagically." This increased number of lines of code also increases the attack surface. More code creates more potential areas of compromise.

11 https://www.upguard.com/blog/full-stack-blues-exploring-vulnerabilities-in-the-mean-stack

New stacks bring performance and development benefits along with added security features. While these features address known attack vectors, they may result in reduced vigilance by developers who place too much trust in them. Developers using them need to be aware of such vulnerabilities and implement best practice safeguards.

At the same time, because frameworks also encourage reuse, a vulnerability in one framework can expose multiple applications across an entire organization.

SECTION SUMMARY:

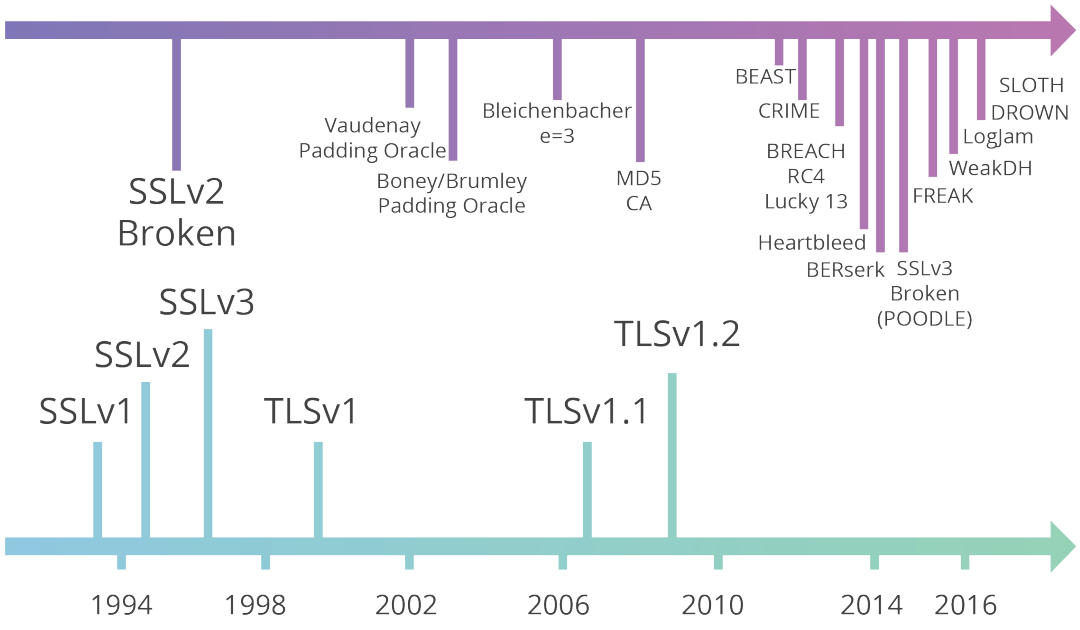
While new development approaches and stacks are helping companies to innovate and ship newer and better applications faster, they are also likely to result in more zero day exploits because:

- *Sprint based release cycles restrict developers' ability to battery test new code and apps in terms of security*
- *Modern stacks aren't as hardened or as well field-tested as older stacks*
- *Modern stacks increase the lines of code that could expand the attack surface*

TLS is Hard to Get Right and Enterprises Struggle to Manage and Adopt the Latest Version (TLS 1.3)

The Transport Layer Security (TLS) protocol is a replacement for the older Secure Sockets Layer (SSL). It encrypts internet traffic and facilitates secure communication and transactions, making it hard for attackers to snoop on data in transit. However, TLS has been shown to have numerous vulnerabilities in the past and has undergone successive upgrades to address them.

History of SSL/TLS vulnerabilities



The chart above shows a list of vulnerabilities that have been discovered in TLS since its inception. Some of these vulnerabilities such as FREAK had to do with the weak ciphers used and others related to the inherent architecture of the protocol itself.

TLS 1.2 came out back in 2008, with fairly minimal changes compared to TLS 1.1. Because it wasn't updated to TLS 1.3 for a long time, wrong assumptions about the protocol made by non-compliant middleboxes-network appliances designed to monitor and sometimes intercept HTTPS traffic - meant that some of the more invasive changes in TLS 1.3 broke those assumptions, and caused the middleboxes to misbehave. In the worst cases, these assumptions caused TLS connections passing through the middleboxes to break altogether.

Browser support for legacy versions weakens the most commonly used TLS version (1.2)

Most clients and servers support multiple versions of TLS simultaneously to ensure that some version of TLS can be used even if both do not support the latest version. To ensure future compatibility, TLS uses version negotiation - if a client sends a higher version than the server supports, the server should still be able to reply with whatever version the server supports.

However some servers implemented version negotiation incorrectly, causing them to disconnect rather than negotiating an earlier version when using TLS 1.2. This transferred the onus for version support to browsers who implemented a solution called an 'insecure downgrade' - they would keep trying to establish the connection with earlier versions all the way down to SSLv3.

The result was that TLS 1.2, which had added new, stronger encryption options to address vulnerabilities in TLS 1.1, ended up preserving all the legacy, weaker encryption schemes to prevent servers getting disconnected. Unfortunately this decision to support legacy versions led to a kind of a vulnerability called a downgrade vulnerability in which an attacker could downgrade connections to a weaker version of TLS such as TLS 1.0 or SSLv3 without the user being aware.

Once this downgrade was successfully performed, all the newer security measures of TLS 1.2 were rendered useless and attackers could exploit the same vulnerabilities (padding oracles, for instance) that they had exploited with earlier versions.

Earlier versions of TLS such as TLS 1.2 supports insecure cryptographic modes and key exchanges

While TLS 1.2 does have improved security, it still retains some serious vulnerabilities from the original design of SSL. These include support for insecure cryptographic modes such as cipher block chaining (CBC) and support for vulnerable public key exchange schemes.

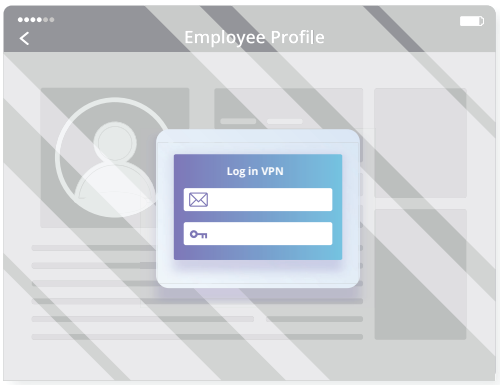
SECTION SUMMARY:

Not all versions of TLS are equal but enterprises tend to mistakenly assume that any version of TLS such as 1.1 or 1.2 is completely secure. This dangerous assumption along with the difficulty of deploying TLS correctly can lead companies into believing themselves safe from security breaches because they encrypt traffic from users, when in reality, their data encryption remains vulnerable.

The latest version of TLS (1.3) improves security by removing support for RSA key exchange and insecure CBC mode ciphers and addresses the shortcomings mentioned above. However, adoption has been slow because of version negotiation issues and lack of browser and middlebox support.

Authentication and Access Control Systems Exploits are on the Rise

Broken authentication and application access control displaced other attack vectors in the OWASP 2017 top 10[12]. This suggests that attackers are switching their attack tactics and are initially targeting users instead of applications to acquire authentication credentials.



The prevalence of broken authentication is due to the design and implementation of most identity and access controls that contain security vulnerabilities such as apps using plain text, or weakly hashed passwords. The LinkedIn data breach[13] was an example of this vulnerability being exploited. A second kind of vulnerability is applications permitting automated brute force attacks such as dictionary or credential stuffing attacks.

Users and identities are easier targets than application vulnerabilities

Tricking users into divulging credentials via social engineering or purchasing user credentials on a dark web marketplace requires less technical sophistication than exploiting an application vulnerability. Once acquired, credentials can be used for automated brute force attacks.

Two popular brute force methods of authentication attacks are credential stuffing and dictionary attacks. A dictionary attack tries hundreds or sometimes millions of likely credentials by using combinations of words such as those in a dictionary.

Credential stuffing takes advantage of user tendencies to reuse usernames and passwords across multiple websites. Once attackers get hold of compromised credentials for one site, they use automated injection to test the same credentials on other sites and gain access. For instance, the 2017 Zazzle data breach was carried out using brute force techniques to cycle through usernames and passwords that were stolen from a different unnamed site.[14]

In an effort to help users understand the dangers of credential reuse and track compromised accounts, researcher Troy Hunt has created 'HaveIbeenPwned.com'. By entering an email address users can check if their account that has been compromised in a data breach, and avoid using compromised credentials for additional accounts.[15] In the Sony and Yahoo data breaches, **Hunt found that 59% of all Sony users were using the exact same password on Yahoo, even a year after the Sony breach.[16]**

12 The OWASP top 10 is a list of the ten most critical vulnerabilities that are commonly found in web applications. It is maintained by the Open Web Application Security Project (OWASP).

13 More than 6 million LinkedIn passwords stolen
http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm

14 Zazzle resets "thousands" of accounts after hackers brute-force passwords
https://www.zdnet.com/article/zazzle-resets-password-after-brute-force-login-attacks/

15 https://haveibeenpwned.com/

16 What do Sony and Yahoo have in common? Passwords
https://www.troyhunt.com/what-do-sony-and-yahoo-have-in-common/

Network perimeters and VPN solutions do a poor job of preventing attacks

Traditionally, enterprises tried to address access control attacks with a 'network perimeter' model. This model relies on securing application access using Virtual Private Networks (VPN). But VPNs are not just hard to implement, but also compromise performance and security.

From an administrator standpoint, adding new users to a VPN can be tedious and involves configuring the cloud network, setting up the IPSec rules and firewall rules, and devoting time to testing these, increasing the chances of security misconfigurations.

For end users VPNs reduce application speed, causing them to potentially avoid VPNs and take their chances with unsecured networks, introducing a security hole.

Another major security flaw with VPNs is that any breach of the network perimeter results in a breach of ALL applications in that network, giving the attacker free reign for lateral attacks across the network. Additionally, the lack of application specific granularity increases the risk of potential exploits because of their one size fits all application policy.

For all of these reasons, **VPNs are unlikely to prevent sophisticated attacks carried out for data exfiltration.**

SECTION SUMMARY:

Broken authentication and access control are easy targets in the attack surface for attackers targeting users and identities rather than applications. Social engineering attacks in combination with brute force attacks such as credential stuffing are popular attack vectors used by criminals to take advantage of user tendencies to reuse passwords. ***Traditional network perimeter based access control models that use VPNs are no longer adequate to safeguard applications.***

Addressing the Increased Risks of Security Breaches

Three major holes in the attack surface that can increase enterprise risk to security breaches are:

- Web Application Vulnerabilities:
    - Attacks that exploit existing and zero day security vulnerabilities in popular platforms such as WordPress
    - Newer, more varied zero-day attacks exploiting the adoption of modern stacks that are less hardened and increase the attack surface
- SSL/TLS vulnerabilities:
    - Attacks exploiting vulnerabilities that target legacy version support in transport layer security (TLS)
- Identities and Access Control:
    - Attackers targeting authentication and access control by exploiting perimeter based access control models that rely on VPNs

Enterprises addressing these challenges need solutions that can detect and respond rapidly to attacks targeting new vulnerabilities as well as unpatched ones. Given the proliferation of web applications and codebases, one way a solution can detect and quickly mitigate zero day threats is

leveraging **scale** across thousands of web properties and translating learnings from one property into actionable security rules or policies for all of them.

The solution should ideally also address the vulnerabilities inherent in different versions of TLS including TLS 1.2 and facilitate end-to-end encryption. One way to address TLS 1.2 vulnerabilities is to leverage TLS 1.3 which has large scale improvements not just in security but also performance.

Broken authentication and access control are critical areas of the attack surface that organizations need to secure using newer and more pertinent authentication and access models. Both of these attack types can be prevented by measures such as multi-factor authentication, IP blacklisting, and monitoring and restricting the number of login attempts by rate limiting.

Fixing broken access control involves enterprises replacing the traditional 'castle-and-moat' model which was based around the concept of a network perimeter with a 'zero trust' model. The zero trust model discards the notion of perimeters and advocates that enterprises must verify anything and anyone trying to connect to its systems before granting access.

Ideally the solution should also fix broken authentication and access control by monitoring and restricting failed login attempts and using a VPN less approach and should offer granular **controls** for provisioning new users and policies without sacrificing usability and agility.

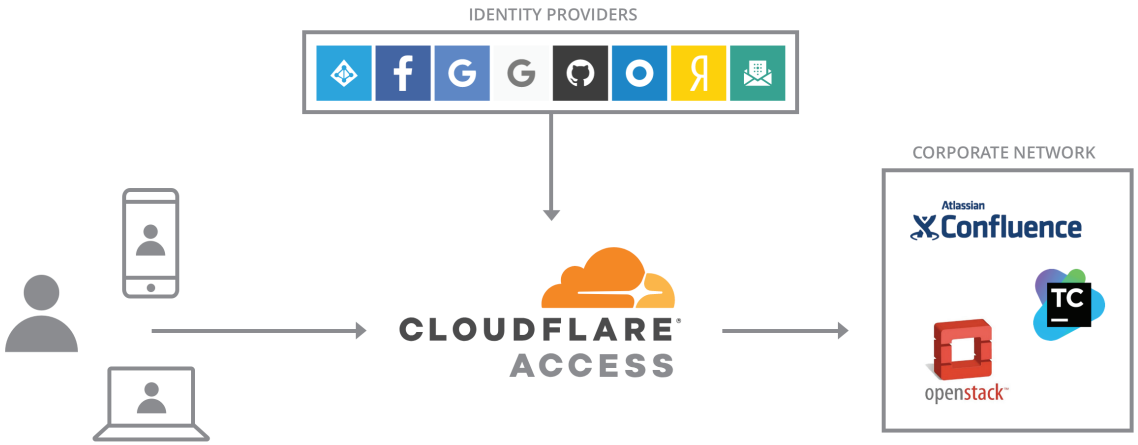
The Cloudflare Solution

Cloudflare's Performance and Security Services work in conjunction to reduce latency of web sites, mobile applications, and APIs end-to-end, while protecting against DDoS attacks, abusive bots, and security breaches involving data exfiltration.

Cloudflare's security services protect and secure critical components of the breach attack surface such as web applications and APIs, SSL/TLS, and authentication and access control systems. With its support for multi-cloud architectures, Cloudflare makes it easier for enterprises to maintain consistent postures.

Fixing Broken Authentication and Access Control

Zero trust access control without a VPN



Cloudflare Access is based on the "zero trust" model which requires verification from anyone and anything connecting to a corporate applications. It allows customers to secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare without the need for a VPN.

Customers can apply application-level and user-level access permissions using existing single sign-on providers such as Google and Okta.

Protecting WordPress Sites from Known and Zero Day Vulnerabilities

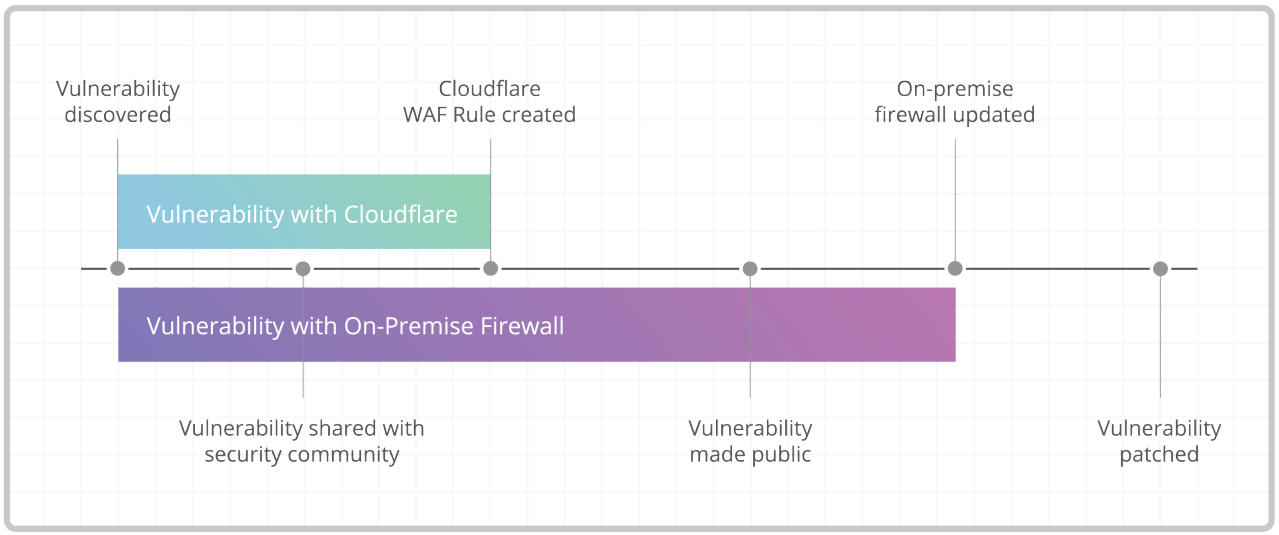
Cloudflare works with the WordPress security team to roll out protection in the form of security rulesets in the Cloudflare enterprise-grade cloud Web Application Firewall (WAF). For instance, in the content injection attacks that exploited a vulnerability in the WordPress REST API in 2017, Cloudflare protected its users by rolling out two rules WP0025A and WP0025B :

WP0025A	Prevent abuse against wp-json api Type A	Cloudflare WordPress	Block
WP0025B	Prevent abuse against wp-json api Type B	Cloudflare WordPress	Block

The WAF detects and blocks common application layer attacks including injection attacks, and cross-site scripting (XSS) with no changes to existing infrastructure. Cloudflare WAF not only supports the OWASP ModSecurity Core Rule Set by default but also includes application-specific rule sets and custom rule sets.

Cloudflare sees roughly **7.4 million http requests every second**, which the WAF leverages to better identify zero day attacks. When one customer requests a new custom WAF rule, Cloudflare analyzes whether it applies to all **8 million domains** on the network and automatically applies it to all WAF users on the network who have opted in for the Cloudflare custom rule set.

The WAF sits on the same Anycast network that powers Cloudflare's global CDN, HTTP/2, and web optimization features. WAF rule sets result in latency of less than 1 millisecond. **New rules propagate worldwide within 30 seconds.**

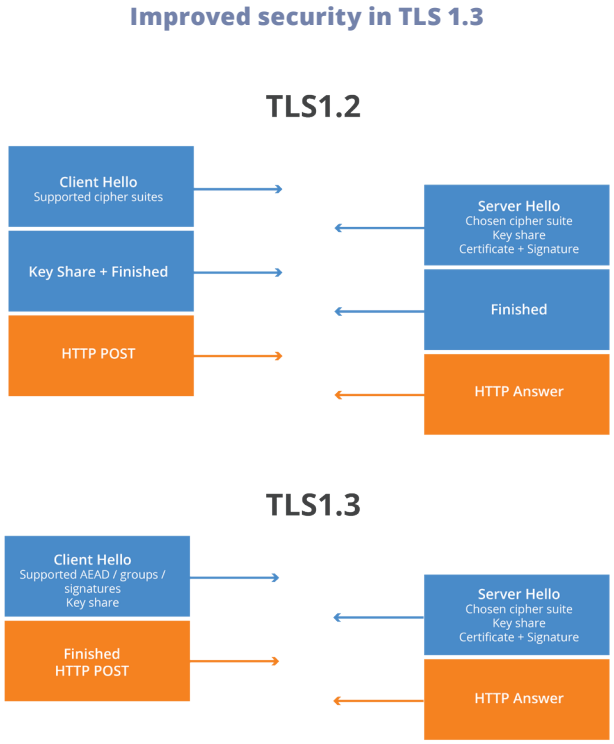


Preventing credential stuffing

Cloudflare's Rate Limiting protects against brute-force login attempts, and other types of abusive behavior targeting the application layer. Rate Limiting provides the ability to define thresholds by client (e.g. by IP) to specific endpoints that timeout for a certain duration. It also allows admins to specify mitigating actions based on custom response codes. This to prevent undesirable traffic from wasting bandwidth and gain valuable insights into specific URLs of websites, applications, or API endpoints.

TLS done right

Cloudflare is the first provider to offer TLS 1.3 support on a global scale which reduces latency, optimizes performance, and hardens the security of your encrypted connections.



TLS 1.3 plugs most of the security holes in TLS 1.2 by abandoning support for legacy key exchanges and cipher modes. A major countermeasure in TLS 1.3 for padding and timing oracles, is a ban on problematic ciphers such as CBC-mode ciphers, and insecure stream ciphers such as RC4. These have been replaced by a new construction called AEAD (authenticated encryption with additional data), which combines encryption and integrity into one seamless operation.

To offer better protection, version 1.3 has also done away with numerous obsolete features that have known vulnerabilities including RSA key exchange, 3DES, AES-CBC, MD5, RC4, SHA-1 and more.

Earlier versions of TLS, left the choice of the Diffie-Hellman parameters to the participants, resulting in several vulnerabilities because not all parameters were secure. In TLS 1.3, this choice was taken away and the parameters are restricted to those that are known to be secure.

Conclusion

Global costs and frequencies of data breaches are rising. Enterprises face heightened scrutiny and severe repercussions from even the smallest data compromise.

To manage the threats of an ever growing attack surface, newer zero days, increases authentication and access control exploits, vulnerabilities in TLS, and inconsistencies in multi-cloud security postures, web sites and applications require the resilience and intelligence of a scalable network that uses a single control plane for ease of use.

Cloudflare's 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 151 data centres and 15Tbps capacity, Cloudflare proactively safeguards enterprises by learning from attacks targeting 8,000,000+ domains on its network** and helps enterprises mitigate the risk of data breaches.

Quotes

"Data breaches are rampant and many people don't appreciate the scale or frequency with which they occur. 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 awardee 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 insurance providers it would be catastrophic for us to have any sort of data breach. When the stakes are this high having a security partner you trust as a first line of defense is crucial."

karma insurance.ca

"We wanted to bulletproof our site from sophisticated cyber security threats and data breaches. The value propositions of Cloudflare were outstanding. It offered competitive price bundled with everything we needed in one simple service (DNSSEC, SSL certificates, DDoS security, WAF, CDN), and quickly accommodated our customization requirements."

Montecito Bank & Trust

"The backbone of our partnership is the fact that like SiteGround, Cloudflare is a forward-thinking company that constantly improves its services and products, and uses these improvements to offer even more valuable opportunities to their partners."

SiteGround

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.

151 Data Centers
74 Countries
7.4MM HTTP Requests Per Second

(as of March 2018)

Forrester Wave for DDoS Mitigation Solutions Q4, 2017: Cloudflare is a LEADER

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

www.cloudflare.com/forrester-wave-ddos-mitigation-2017/

Gartner Magic Quadrant for Web Application Firewalls, 2017: Cloudflare is a CHALLENGER

Cloudflare was named a Challenger by Gartner for the second year, in the "Gartner Magic Quadrant for Web Application Firewalls, 2017".

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

https://www.cloudflare.com/

Cloudflare World Headquarters

San Francisco
101 Townsend St
San Francisco, CA 94107

+1 (888) 99 FLARE

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