scalar enterprises

My favourite plugins

Wordfence

WordPress statistics

- WordPress powers around 35% of the Internet in 2020
- Of all the CMS-built sites, about 60% of them are using WordPress
- Over 400 million people visit WordPress sites each month
- 661 new WordPress sites pop up daily
- WordPress.org offers over 50,000 plugins and over 3,500 GPL-licensed themes

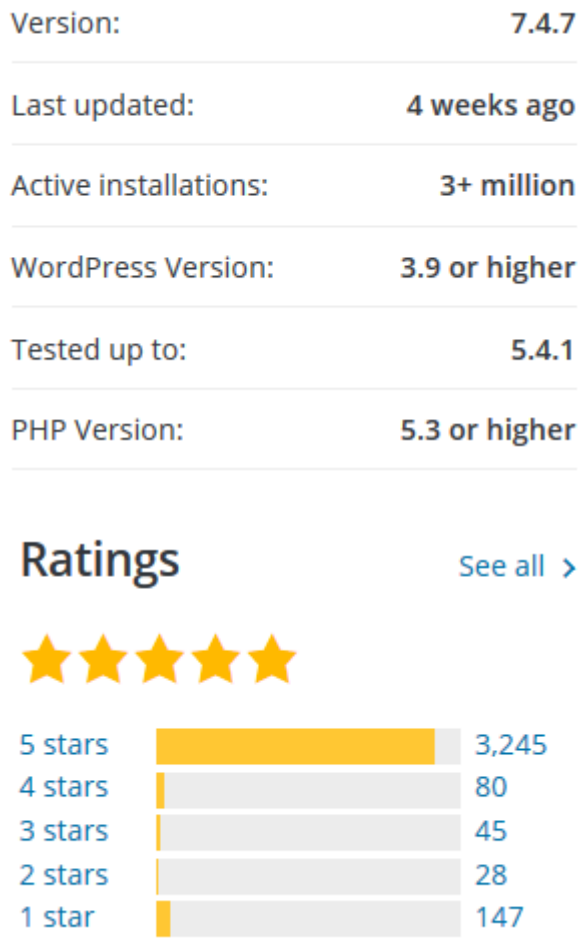
Details @ 20th May 2020

Software security

- Because of its popularity, WordPress is obviously a prime target for hackers.
- Even the most securely written code has potential flaws in it that can allow an attacker to gain unauthorised access to a site if they can find it.
- Vulnerabilities can exist in the core code of WordPress or in any of the many thousands of themes and plugins.
- Hackers set up “bots” that constantly trawl the Internet, looking for websites and then probing them to see what is installed and identifying any known vulnerabilities they can exploit.
- The original software developers are constantly updating their code to “patch” it to fix the problems and try to keep up with the hackers.
- Once a vulnerability is patched, the hackers start looking for new ones so it is a constant battle.
- One thing that the hackers rely on, in order to maximise the damage they can do, is that many website owners do not keep their software updated regularly so this can leave them wide open to attack.

Wordfence plugin

- Wordfence Security – Firewall & Malware Scan
  - The most popular WordPress firewall & security scanner
  - Over 150 Million Downloads
  - Free & Pro versions
- Statistics for last 30 days
  - Total Attacks Blocked: 5,350,193,633
  - Malicious IPs Blacklisted : 136,064
- https://wordpress.org/plugins/wordfence/

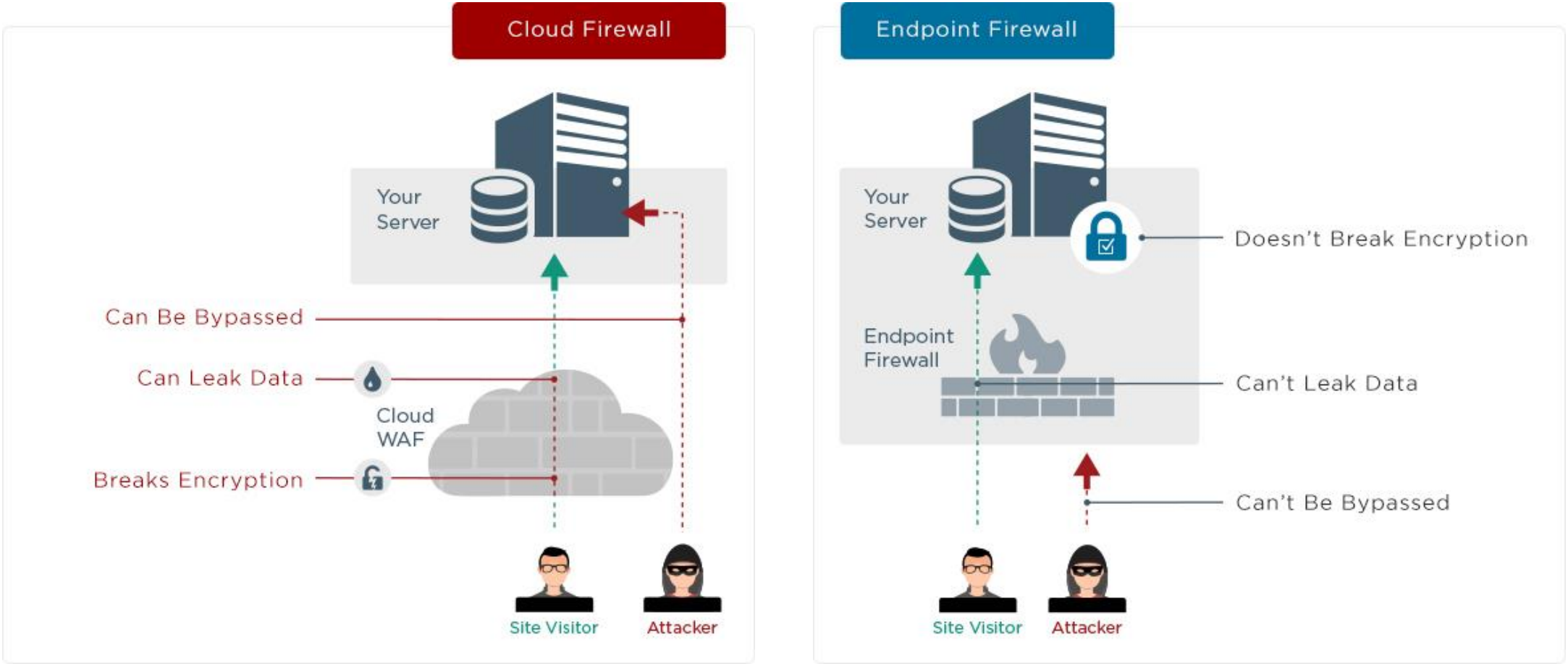


Details @ 20th May 2020

Web Application Firewall

- Wordfence includes a Web Application Firewall (WAF) that identifies and blocks malicious traffic.
- It runs at the endpoint, enabling deep integration with WordPress.
  - it does not break encryption
  - cannot be bypassed
  - cannot leak data
- The integrated malware scanner blocks requests that include malicious code or content.
  - defends against brute force attacks by limiting login attempts
  - enforces strong passwords
  - other login security measures

Firewall comparison

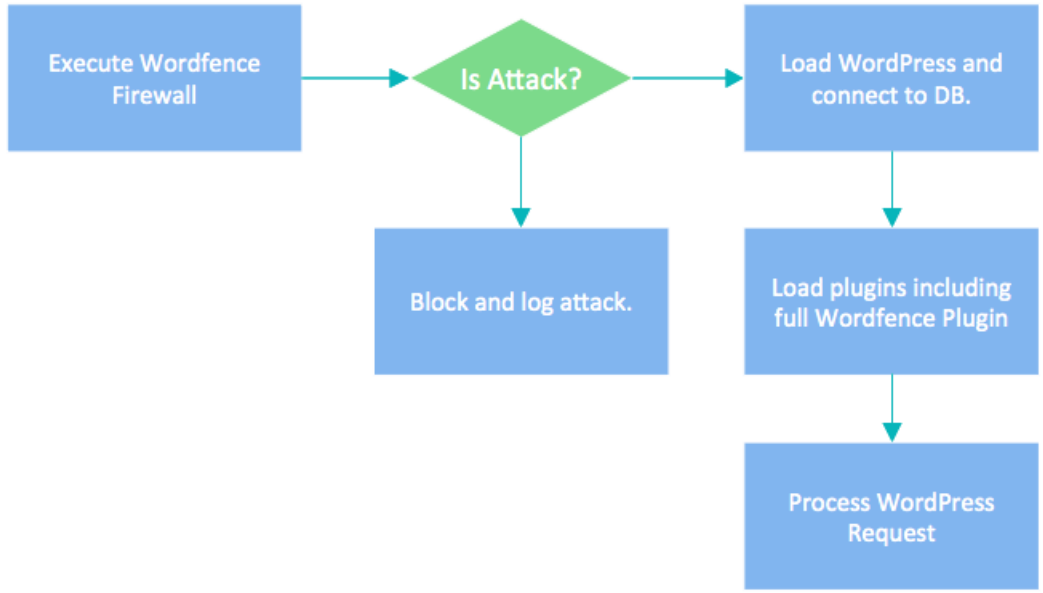


Threat Defence Feed

- The Threat Defence Feed arms the Wordfence plugin with the newest firewall rules, malware signatures, and malicious IP addresses it needs to keep your website safe.
- Wordfence protects several million WordPress websites, giving them unmatched access to information about how hackers compromise sites, where attacks originate from and the malicious code they leave behind.
- Wordfence's security analysts and developers are 100% focused on WordPress security, constantly adding updates as they discover new threats.
- Premium members receive the real-time version of the Threat Defence Feed. Free users receive the community version, which is delayed by 30 days.

How it works

- The Wordfence firewall code runs before any other PHP code on your website.
- Any request that arrives, no matter which PHP file it tries to access, will first be processed by Wordfence to check if it is safe or not and will make a decision to block the request or allow it.
- That means that the WordPress code has not loaded and the database is not yet connected. This makes the Wordfence firewall code ***incredibly fast***.
- It can block a malicious request before it even connects to your database and before the WordPress code and API environment is loaded up.



Security Scanner

- The Wordfence scanner checks core files, themes and plugins for:
  - malware
  - bad URLs
  - backdoors
  - SEO spam
  - malicious redirects
  - code injections
- It compares your site files with those in the WordPress.org repository, checking their integrity and reporting any changes to you.
- It allows you to repair files that have changed by overwriting them with a pristine, original version and easily delete any files that don't belong.
- It checks your site for known security vulnerabilities, abandoned and closed plugins.
- Content safety checks ensure that your files, posts and comments don't contain dangerous URLs or suspicious content.
- It also checks for weak passwords.

More powerful features

Leaked Password Protection

Protect your site against attacks that leverage password information stolen in data breaches. Block logins for administrators using known compromised passwords.

Live Traffic

Monitor visits and hack attempts not shown in other analytics packages in real time; including origin, their IP address and the time of day.

Advanced Manual Blocking

Quickly and efficiently block entire malicious networks and any human or robot activity that indicates suspicious intentions based on pattern matching and IP ranges.

Country Blocking

Blocking countries who are clearly engaging in malicious activity is an effective way to protect your site during an attack. Premium Feature.

Repair Files

Wordfence uses our source code verification feature to help you recover from a hack. It tells you what changed in core, theme and plugin files and helps repair them.

Two-Factor Authentication

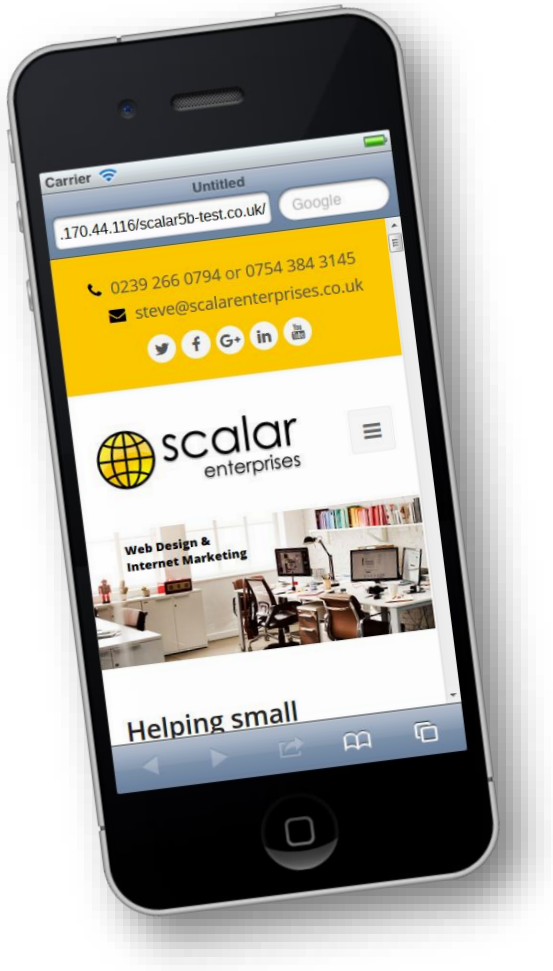
Stop brute force attacks permanently by using one of the most secure forms of remote system authentication available.

Wordfence plugin

Recommended as an essential plugin for all WordPress websites

https://wordpress.org/plugins/wordfence/

Always here to help …



Call Scalar Enterprises today to discuss how we can help you!

02392 660794

More details on our website

www.scalarenterprises.co.uk