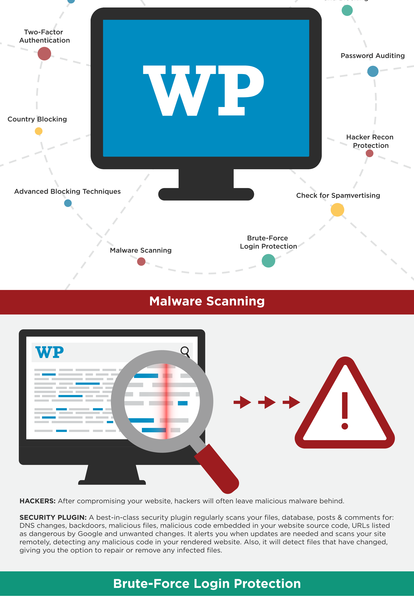
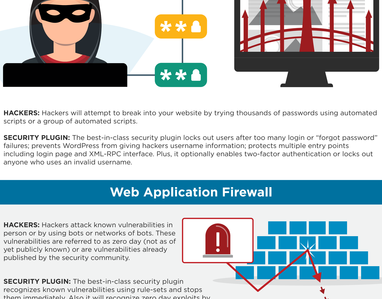
HOW BEST-IN-CLASS

WordPress Security Plugins

PROTECT YOUR WEBSITE



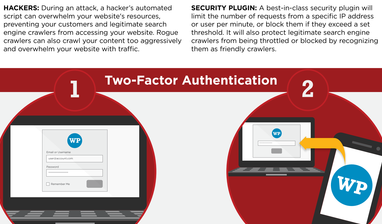
Malware Scanning



HACKERS: After compromising your website, hackers will often leave malicious malware behind.

SECURITY PLUGIN: A best-in-class security plugin regularly scans your files, database, posts & comments for: DNS changes, backdoors, malicious files, malicious code embedded in your website source code, URLs listed as dangerous by Google and unwanted changes. It alerts you when updates are needed and scans your site remotely, detecting any malicious code in your rendered website. Also, it will detect files that have changed, giving you the option to repair or remove any infected files.

Brute-Force Login Protection



HACKERS: Hackers will attempt to break into your website by trying thousands of passwords using automated scripts or a group of automated scripts.

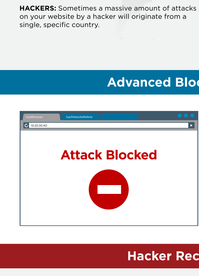
SECURITY PLUGIN: The best-in-class security plugin locks out users after too many login or "forgot password" failures; prevents WordPress from giving hackers username information; protects multiple entry points including login page and XML-RPC interface. Plus, it optionally enables two-factor authentication or locks out anyone who uses an invalid username.

Web Application Firewall

HACKERS: Hackers attack known vulnerabilities in person or by using bots or networks of bots. These vulnerabilities are referred to as zero day (not as of yet publicly known) or are vulnerabilities already published by the security community.

SECURITY PLUGIN: The best-in-class security plugin recognizes known vulnerabilities using rule-sets and stops them immediately. Also it will recognize zero day exploits by using generic pattern matching to stop attacks that are not yet publicly known.

Rate-Based Throttling and Blocking



HACKERS: During an attack, a hacker's automated script can overwhelm your website's resources, preventing your customers and legitimate search engine crawlers from accessing your website. Rogue crawlers can also crawl your content too aggressively and overwhelm your website with traffic.

SECURITY PLUGIN: A best-in-class security plugin will limit the number of requests from a specific IP address or user per minute, or block them if they exceed a set threshold. It will also protect legitimate search engine crawlers from being throttled or blocked by recognizing them as friendly crawlers.

Two-Factor Authentication

HACKERS: Strong passwords alone can't protect you if a hacker is able to attain your password using advanced techniques like spear phishing or social engineering.

SECURITY PLUGIN: Used by banks, government agencies and the military worldwide, two-factor authentication completely neutralizes password theft and guessing attacks and is a prominent feature of best-in-class security plugins.

Password Auditing

HACKERS: Hackers use advanced algorithms to determine which weak passwords to attempt during brute force attacks or password cracking attacks.

SECURITY PLUGIN: The best-in-class security plugins identify which of your administrators and users are using passwords that are easily crackable. It will give you the ability to easily change the password or request that the account owner change their password.

Country Blocking

HACKERS: Sometimes a massive amount of attacks on your website by a hacker will originate from a single, specific country.

SECURITY PLUGIN: When your website is attacked aggressively by a single country — regularly creating failed logins, a large number of page not found errors and is clearly engaging in malicious activity — a best-in-class security plugin will employ its country blocking feature.

Advanced Blocking Techniques

HACKERS: During an attack, you may notice that the attacker consistently originates from a range of IP addresses, uses the same referring website for each request or has a browser identification (user-agent) that is unique and stays the same.

SECURITY PLUGIN: A best-in-class security plugin will intelligently stop threats by blocking any combination of ranges of IP addresses, specific web browsers, web browser patterns or referring websites.

Hacker Recon Protection

HACKERS: Hackers start attacks by looking for information about your website and vulnerabilities on your website.

SECURITY PLUGIN: A best-in-class security plugin will prevent WordPress from giving hackers information about your website including software versions you are running, a list of software you are using and usernames that may exist on your system.

Check for Spamvertising

HACKERS: When hackers compromise your site they will often use your site for spamvertizing. This means they include a link to your site in a spam email campaign and your site then redirects visitors to a malicious website.

SECURITY PLUGIN: A best-in-class security plugin proactively checks to see if your site is spamvertised, sending spam or has been flagged as a spammer, allowing you to detect an infection and react quickly.