

WP engine

10 BEST PRACTICES FOR A SECURE AND SUCCESSFUL ENTERPRISE WORDPRESS DEPLOYMENT

WHITE PAPER

Andrei Matei, Solutions Engineer
January 2015



Secure, Successful WordPress

WordPress is secure, but as with any technology that's experienced such rapid growth, following a series of best practices can help keep it that way. In this white paper, we'll dig into 10 best practices for keeping your WordPress deployment secure. Whether you're using WordPress to power your blog or your Enterprise website, following these best practices will help you protect your site from possible attacks and vulnerabilities, and ensure that your WordPress deployment is secure and successful.

WordPress as an Enterprise Platform

From single developers to Fortune 100 companies, the number of organizations turning to WordPress is skyrocketing. To date, there are more than 68 million active WordPress sites serving a whopping 3.5 billion pages each month. More than half of the top 100 blogs on the Internet now run WordPress, and not just for their blogging needs; many organizations leverage WordPress for their entire web presence. All told, nearly a quarter of all sites on the web are WordPress sites. Check out some of the more notable sites running on WordPress: <http://wordpress.org/showcase>.

WordPress Security Misconceptions

It's no question that WordPress security is mission critical. And when kept up-to-date, WordPress is extremely secure. The WordPress open source project has a large, talented, and dedicated set of contributors who manage regular releases, patches, and security fix schedules to complement carefully vetted feature introductions. The sheer number of eyes and hands across the world working in common cadence on the WordPress project is a key enabler of WordPress' success and growth as a web platform.

However, security goes beyond the WordPress core code base. Security management responsibilities still ultimately fall on internal IT departments, primary users, and external platform providers. It's imperative that all parties understand potential risks, and how to mitigate them.

Securing Content Systems

In most organizations, security is the responsibility of IT managers and their departments. For these technical leaders, security is a challenging topic to address in any environment; especially one with complex components, and the involvement of multiple departments such as Marketing. WordPress deployments are a key example of this. Whether securing critical core business data systems or reviewing the risks posed by a WordPress site, IT managers know that they need to have proficiency in the tools used in EVERY part of their enterprise.

With each part of an IT infrastructure having its own security best practices to follow, patching regimes to adhere to, and security assurances to validate, building in-house expertise may not be feasible or cost-effective. Even when such experience is present, a single security officer or small team usually cannot match the breadth and depth of a service provider that specializes in running a platform securely at scale. Thus, seeking an experienced partner to help with WordPress-specific security needs will reduce risk. Providers like WP Engine allow organizations to focus on other IT initiatives and take the heavy-lifting and worry away from the IT team.

Now, let's discuss some provider-agnostic WordPress security best practices, the specific benefits of Managed WordPress platforms (like WP Engine), and ways to ensure WordPress security for successful deployments within an Enterprise.

WordPress Security Best Practices

Whether the choice is made to leverage a partner to assist with WordPress deployments, or an organization wishes to attempt to configure things itself, here are common ways to proactively think about WordPress security and stay ahead of any possible issues.

Generally, WordPress security problems arise from three primary culprits:

- Out-of-date WordPress installations and weak password policies
- Inadequately developed or tested plugins and themes
- A default server environment and LAMP stack, poorly tuned for WordPress

The following 10 best practices can mitigate these issues and ensure a more secure and successful WordPress deployment, regardless of provider or method of hosting:

1. Make WordPress core code updates quickly.

Keeping “core” up-to-date is incredibly important for security. Un-patched core installations are often a primary attack vector since many of the WordPress updates and patches are designed to improve security. Using a tool like WP Updates Notifier can help organizations stay on top of important updates to the WordPress core. It’s important to always watch for updates and to make them as soon as possible.

2. Proactively upgrade plugins and themes as new versions become available.

Along with outdated core WordPress components (as listed above), out-of-date plugins and themes are among the most easily compromised components of a WordPress installation, particularly due to a lack of current patching. The plugin dashboard provides notifications as updates become available. Additionally, auditing currently installed plugins is easy with the “Plugins Last Updated” plugin or the “No Longer in Directory” plugin. “Plugins Last Updated” shows when an installed plugin last received an update, as long as it’s listed in the WordPress.org plugin repository. Complementarily, “No Longer in Directory” scans plugins to check for ones that have been removed from the WordPress.org repository.

If the plugin has been removed, there is usually a good reason why, whether it is a security issue, poor performance, or other such culprits.

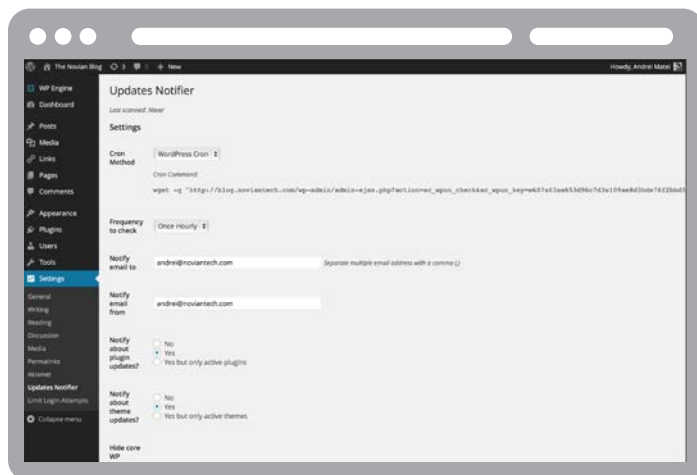


Figure 1: It is important to be notified of updates to plugins and themes frequently.

It’s often advisable to NOT use a plugin that has gone longer than a year without an update (*Figure 1*).

3. Prevent sniffed login attempts.

Securing the wp-login.php and wp-admin areas of a WordPress installation with an SSL certificate and/or VPN solution can greatly reduce sniffed login attempts. Additionally, utilizing a login solution based on directory services such as Google Apps Authentication, LDAP, or SAML is an important step in adding security to the login process. A great plugin for Google Apps Authentication is: Google Apps Login.

Furthermore, some organizations go as far as eliminating local WordPress login support altogether. Additional security is achieved by ONLY allowing logins from a particular set of users from a particular domain with one of the authentication mechanisms above. Overall, this not only reduces the chance of compromised WordPress accounts, but allows for hassle-free account creation and management as well.

4. Enforce strong passwords.

Weak passwords are one of the easiest ways to fall victim to brute force or “dictionary” attacks. It is imperative to ensure all users use strong passwords. An easy way to achieve this is by enforcing use of the “Force Strong Passwords” plugin.

In addition to a strong password creation policy, IT managers should regularly change administrator account passwords as well. The “Expired Password” plugin is an easy way to manage this for all users. Lastly, remembering complex passwords that change often can be difficult. Suggest using something like 1Password or LastPass to users helps to manage these passwords securely and easily.

5. Remove the “admin” account.

The “admin” account is a default account on every WordPress installation. If the “admin” account is kept active and not disabled or removed, half of the puzzle is already solved for an attacker. The

attacker no longer would need to guess a username AND a password to compromise a blog or website; a password is all that is needed. Removing the “admin” account or changing the username prevents a WordPress site from being open to automated attacks. Doing this is as easy as logging into your WordPress account, going to the “users” section, and deleting or renaming the “admin” account/username.

6. Actively block and log incoming security attacks.

It is vital to actively block security attacks, which are often run on a large set of web properties to test for “easy ins.”

An organization does not need to have specific enemies to fall victim to a security attack.

Using a security plugin like Securi enables organizations to take charge of their WordPress security. Securi’s Audit Log capability is a great example of a utility that helps people understand what is going on inside their WordPress installation from a historical perspective.

Other excellent tools and services to consider are ThreeWP’s Activity Monitor, The Auditor, and CloudFlare. Activity Monitor and The Auditor give insight into what is happening in your WP installation for tighter security and easier diagnosis of issues. Additionally, CloudFlare offers a unique “before-the-server” DDoS mitigation and security solution that is an easy way to add an additional layer of security to non-managed WordPress environments (Figure 2).

7. Ensure proper file permissions, isolate sites, and decouple databases.

When running multiple WordPress installations for different stakeholders in an environment, remember these sites should be isolated from each other. Should one customer’s file system become compromised, there shouldn’t be easy access to another customer’s data. Keeping careful tabs on proper file permissions is critical in achieving this, and configuring appropriate virtualization across the different environments is key for isolation.

Finally, one of the most important parts of a WordPress installation, the database, should be carefully isolated from other applications. This reduces the likelihood of malicious code jumping into a WordPress data base and wreaking havoc. Sharing a WordPress database with other applications, and adding other non-WordPress tables for auxiliary functionality, are key things to avoid. Keeping the WordPress database as isolated and restricted as possible is a best practice.

8. Conduct frequent, proactive vulnerability scanning.

Vulnerability scans, often referred to as “penetration testing,” are imperative for organizations of all sizes in order to discover hidden and hard-to-track-down security issues. It is recommended to run



Figure 2: A solution like CloudFlare can add an extra layer of security in non-managed WordPress environments.

quarterly scans on all critical infrastructure, from a systems and OS perspective, as well as an application (WordPress) perspective. To receive the most unbiased results, these scans should be run by an experienced third-party scanning partner. Prior to engaging with a scanning partner, it’s a good idea to use a WordPress-focused scanner such as WP Scan to shore up immediate issues.

9. Employ a robust backup strategy and disaster mitigation plan.

The worst can happen to even the most seasoned IT teams in the most robust data centers.

Ensure WordPress installations are backed up off-site, on schedule, and optionally, in an encrypted fashion.

Going a step further and having a secondary and tertiary backup site gives extra reassurance that all data will be stored safely and retrieval will be possible when needed. For user-friendly, off-site backups, VaultPress is a great tool.

10. Enforce a strong “Dev/Staging to Production” process.

The importance of a regimented process for moving development work from testing/staging to production can’t be highlighted enough. Pushing untested changes directly to production can have disastrous results. Encourage teams to test and test often in staging and they should be able to do so painlessly with tools built for them.

WP Engine's Enterprise-Grade Security

With the numerous general best practices outlined above, why should an organization look to a Managed WordPress platform like WP Engine to run their web presence securely? Here's why:

- The above suggestions are a bare minimum and may not be enough
- Implementing effective security is far harder to execute than to simply read and understand
- Providers like WP Engine are OBSESSIVE about great security and maintaining high security standards

WP Engine understands that setting up and successfully managing a properly secured WordPress environment can be daunting, especially if you or your team aren't seasoned security and WordPress specialists.

We have built our product offering from the ground up to allow organizations to focus on their core-competencies and leave the difficult WordPress configuration and infrastructure management to us.

WP Engine is committed to providing the most flexible, yet highly secure WordPress experience available today. Presently, we keep more than 20,000 customers, with over 200,000 WordPress deployments, secure and online through our comprehensive and proactive security solutions. In addition to managing and assisting customers with all of the security best practices listed in the "top 10" on the previous pages, here is a brief overview of some of the things that WP Engine manages for all of its customers.

Proactive patching and updates.

WP Engine proactively upgrades customer installs with minor "patch" releases (for example 3.5.1 -> 3.5.2) where no site functionality or plugin incompatibility issues can arise. For major releases (such as 3.5 -> 3.6), WP Engine thoroughly tests each release before recommending the upgrade to customers and also works with customers to help them through the process to make it as seamless as possible. Customers have the opportunity to test the functionality of new versions via one click in their staging environments, and can work with Support to be added to temporary "exclusion lists" if extra time is needed to perform modifications in preparation for a new version of WordPress.

Additionally, WP Engine is on Automattic's special preview list, thus updates and patches are received by the WP Engine engineering teams ahead of the general community release. A dedicated team at WP Engine focuses on security patches of the WordPress core and any specific issues found in common plugins and themes. More information on WP Engine security patching can be found here: <http://support.wpengine.com/how-and-when-do-we-perform-automatic-wordpress-core-upgrades/>.

Real-time mitigation of security threats.

WP Engine blocks tens of thousands of attacks each and every day for its customers. With advanced security pattern recognition and attack mitigation at the entry points of WP Engine's environment, WP Engine is able to:

- Block URLs that look like malicious JavaScript/SQL-injection attacks, incorrectly formed requests, and attempts to access restricted paths
- Immediately 404 common and missing file paths
- Block IP addresses dynamically determined to be spammers or hackers
- Mitigate and eliminate brute force / DDoS attempts
- Prevent well-known spam and automated hack attempts

Additionally, WP Engine realizes that customers may not always understand the differences between a safe plugin and a potentially harmful one. That's why the WP Engine technical sales team often coaches customers on safe vs. harmful plugins during the pre-sales process. We maintain an active list of disallowed plugins that can be found here: <http://support.wpengine.com/disallowed-plugins/>. These are plugins that have security-issues, negative performance implications, and are generally suboptimal for ALL WordPress installations, not just those in the WP Engine ecosystem.

Solid password enforcement and security due diligence.

As a basic step, WP Engine does not allow the use of the standard "admin" username in any regard. Furthermore, customers are required to employ strong passwords with the non-removable "Force Strong Passwords" plugin. This, along with our required "Limit Login Attempts" plugin, helps prevent brute force attacks. More specifically, the Limited Login Attempts plugin prevents attackers from performing a brute force attack by blocking an offending IP for a pre-defined period of time after a set number of failed attempts.

WP Engine also conducts periodic code reviews and security audits of all internal environments and processes. WP Engine partners with third-party security firms such as Sucuri and Kaspersky to ensure strong security measures are always in place. Finally, WP Engine offers a "read-only mode" that allows a site to be updated while locking down its code and can be used in combination with our git-push solution to eliminate a large portion of security entry points.

Enterprise-grade infrastructure for every customer.

From physical security in the datacenter, including biometric fingerprint/hand/retina scanners, to DDoS mitigation and customer separation at the file-system level, WP Engine looks at security through the enterprise lens. WP Engine takes the following steps to improve security:

- Running a combination of robust hardware and software firewalls
- Segmenting customers from one another at the kernel and filesystem level
- Utilizing advanced DDoS mitigation, IDS-IPS functionality, and network analysis monitoring tools
- Creating nightly, optionally encrypted, off-site backups for all customers

5. A finely tuned server and software stack.

When default server software environments are not properly configured, security and performance problems can arise. WP Engine's software stack includes special provisions to ensure WordPress runs optimally, including:

- A policy to only write to disk with authenticated system users
- PHP-tuning that disallows dangerous commands such as `exec()`, `system()`, and `passthru()`
- Disabling `include()` from URL strings to close a common attack vector
- Advanced performance and caching through EverCache technology

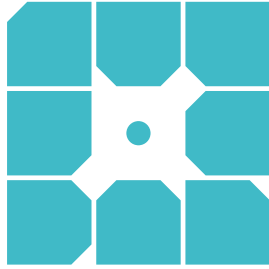
The tuning and security measures put in place by WP Engine are regularly audited internally, as well as through trusted third-party security firms to ensure comprehensive protection for customers.

Review and Conclusion

Developing a robust security strategy for WordPress implementations can be a daunting task whether tackling it alone or with a trusted partner. Just as with any CMS, WordPress requires active security management, which can be enhanced by following the above 10 best practices. A Managed WordPress platform like WP Engine comprehensively ensures the security of your WordPress environments, and can be critical for site security and success.

WP Engine prides itself on ensuring businesses stay online and operate securely. Enterprise-grade features deployable with one click are a primary reason to look towards a Managed WordPress provider like WP Engine. Additionally, a highly trained, expert staff of seasoned WordPress veterans is another key differentiator over traditional web hosts. Overall, WP Engine has become a trusted leader in the WordPress platform space due to a strong track record of security and a robust “no corners cut” approach to securing its customers.

If you'd like to learn more about what WP Engine does in detail to keep its customers safe, and how we can be an extension of your IT team, please contact us at info@wengine.com.



About WP Engine

WP Engine is a leading SaaS content management platform for websites and applications built on WordPress. The company powers thousands of websites and apps built on the WordPress platform delivering a fast, reliable and secure web experience. All levels of users including bloggers, marketers, SMBs and large corporations rely on WP Engine's platform to keep their websites up and running. The company's exceptional customer service team specializes in quickly solving technical problems, and creating a world-class customer experience ensuring that each user's WordPress site continues to perform at its full potential. Founded in 2010, WP Engine is headquartered in Austin, Texas and has offices in San Francisco, California, San Antonio, Texas and London, England.

