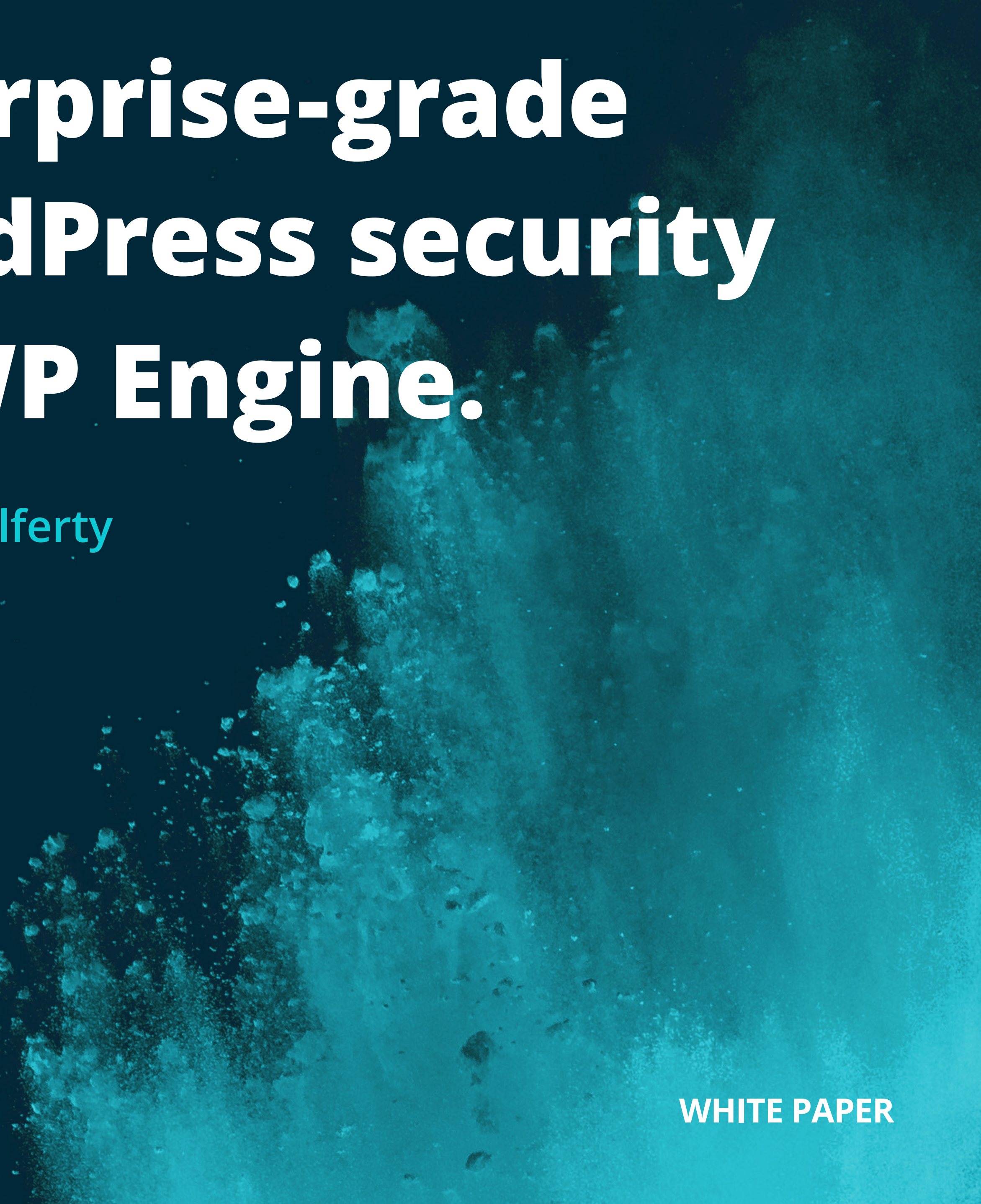
Enterprise-grade WordPress security on WP Engine.

By Janna Hilferty

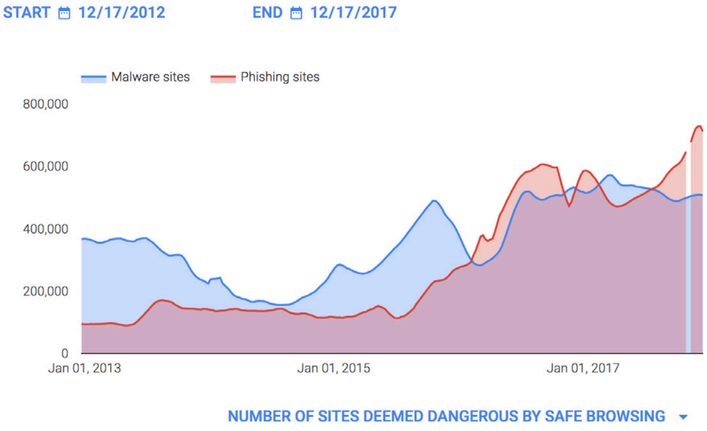


WHITE PAPER

Table of contents.

Introduction.

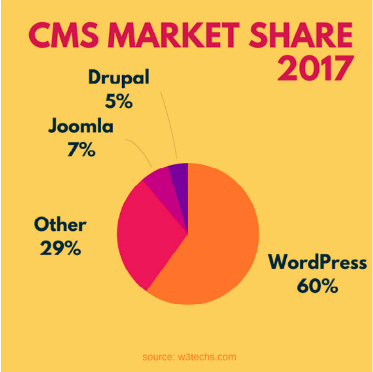
Security is paramount to the success of businesses of all sizes. With the number of hacked sites on the rise, the fear of potential downtime, income loss, or damage to your brand's reputation is not without merit. WP Engine supports businesses of all shapes and sizes in our secure server environment. We understand how important security is to the users and websites we support. With this in mind, WP Engine adheres to strong security guidelines and principles to protect your site from the most common attack vectors. In this document we will discuss the actions WP Engine and WordPress take to help protect your website, as well as best practices for security and hardening within your own team.



What WordPress does to secure your site.

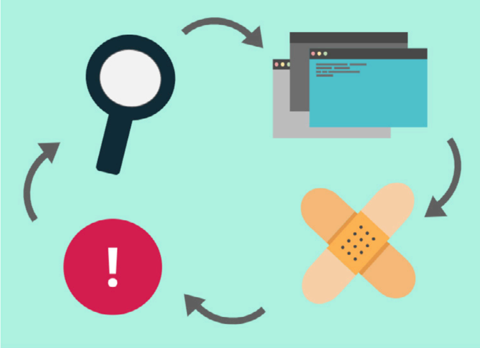
Security at the core of WordPress

WordPress is an open-source software with thousands of contributors worldwide. While many may think open-source equates to vulnerabilities, this really means they have thousands of eyes combing their code for errors and issues, and patching them with stealth and ease. WordPress powers 54 of the top 100 sites on Inc. 5000, and holds a 60% market share among Content Management Systems. Its community of matured developers translates to higher security, not less. WordPress also partners with HackerOne, a community of hackers dedicated to responsibly reporting vulnerabilities, to identify and resolve any potential security concerns. The core WordPress team has released a security whitepaper detailing their security procedures, practices, and what they do to prevent common security issues.



SECURITY RELEASES AND PATCHING

With a mature community of developers, the WordPress core team also maintains a mature release cycle, with planning, beta versions, release candidates, and backwards-compatible branches for security updates. In its review process for security vulnerabilities, reports are gathered and acknowledged via HackerOne. The WordPress Security Team reviews the report and verifies whether it exists, and how severe it is. The team then works to resolve the security vulnerability and if needed, releases a security patch to the WordPress community.



Plugin and theme review

WordPress.org hosts thousands of themes and plugins that extend capabilities and customize appearance. In order for a plugin or theme to be added to the repository, it must undergo manual review. The plugins and themes available on WordPress.org are not necessarily free of security risks, and this means it is best to be selective with the ones you choose. Be sure to select a theme and plugins that are regularly updated, widely used, and highly rated. You can also check the Support threads on WordPress.org to see if issues are commonly resolved. If a security threat is detected within a plugin or theme, the WordPress team reaches out to the developer to work together toward a fix. If the developer does not respond, the plugin or theme may be removed from the WordPress.org repository.

The WordPress team encourages developers of plugins to review and adhere to their security standards. And for theme developers, WordPress includes a guide to theme security which should be considered as well. A common theme among all the recommendations is that developers should use the pre-built WordPress APIs for fetching and validating data. This is because the APIs already securely handle sanitization and validation.

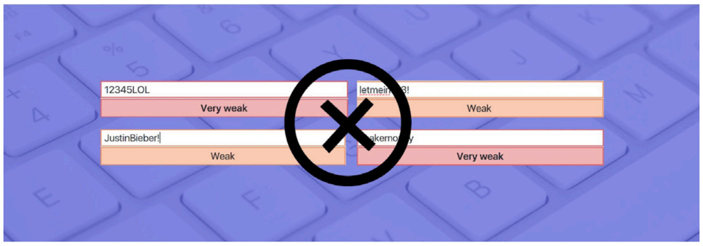
What WP Engine does to secure your site.

WP Engine has many features built in to our platform which benefit you and your site. In 2017, WP Engine blocked over 36 billion attacks. Read on to learn how the WP Engine platform takes care of everyday security concerns.

Updates and vulnerability scanning on WP Engine

AUTOMATIC WORDPRESS UPDATES COMBAT VULNERABLE SITE CODE

Outdated software is the leading cause of security breaches and hacking on websites. On our platform, we manage automatic WordPress updates. Security and maintenance updates are pushed out automatically and immediately to our platform. And for larger functional updates, these are tested for platform compatibility, then sites are automatically updated with 10 days notice. Functional updates are able to be deferred up to 60 days if needed. On top of this, WP Engine proactively performs regular vulnerability scanning and will notify site owners of any new vulnerabilities affecting them.



SECURE PASSWORDS REQUIRED FOR CONTENT CREATORS

Site owners are often given the impossible task of ensuring their users are using secure passwords. Since your login page is a gateway to authorized access to your site, it is extremely important that users with the ability to publish content maintain a strong password. WordPress itself helps by identifying when passwords are weak, medium, or strong. WP Engine takes it a step further by enforcing strong passwords for Administrator, Author, and Editor user roles.

Database containment and Filesystem security

LIMITED PRIVILEGES TO PREVENT UNAUTHORIZED DISK WRITES

If an insecure version of a plugin or theme is installed on your website, it is possible that code could trigger the site to write new files with more malicious code on your site. WP Engine helps limit damages by limiting disk write privileges, allowing only authorized users to write files on your server.

DATABASE CONTAINMENT PREVENTS SPREAD OF DAMAGES

Containment is a common security principle that states, should one entity become compromised, damages are limited by logically separating environments and users. WP Engine manages database containment by creating and managing separate database users for each of your WP Engine sites. This means if one of your sites contains vulnerable code, any resulting damages will not extend to your other sites.

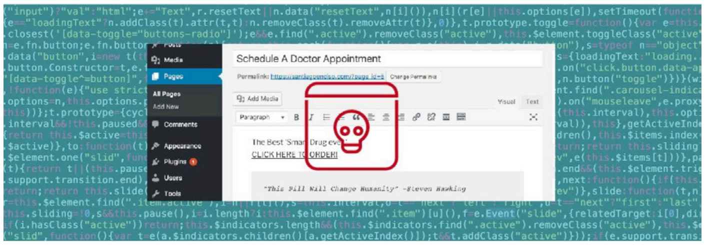
CONFIGURATION FILE PROTECTION AGAINST UNAUTHORIZED CHANGES

Some of the most important settings on your site are managed in a small handful of configuration files. WP Engine automatically protects these files so they cannot be accessed by the outside world. We also protect your site's uploads folder to ensure unauthorized file types are not recognized.

Behaviors WP Engine automatically blocks

INTELLIGENT BRUTE FORCE PREVENTION AND BLACKLISTING

Attackers often try to unintelligently "brute force" your login page by trying thousands of username and password combinations until they find the magic pair to login to your website. WP Engine detects when bots make fake requests for the login page and automatically returns an empty response.



AUTOMATIC BLOCKING OF SPAMBOTS AND BAD ACTORS

Bots are a common problem that often go unseen. A spambot often doesn't load your site's JavaScript files, meaning they aren't detected by Google Analytics, but they are present all the same. These bots can overwhelm your server's resources in a number of ways, or simply send spam emails, comments, and form entries. WP Engine automatically identifies and blocks bots with bad behavior to protect your site and server environment.

AUTOMATIC DETECTION AND BLOCKING OF COMMON ATTACKS

The XMLRPC.php file on your website exists to help apps and remote posting services create new posts. However, attackers often know of this file and send targeted attacks to it with fake requests. WP Engine blocks XMLRPC attacks by automatically detecting users trying to exploit this file.

Encryption on the WP Engine Platform

ENCRYPTION OF USER DATA

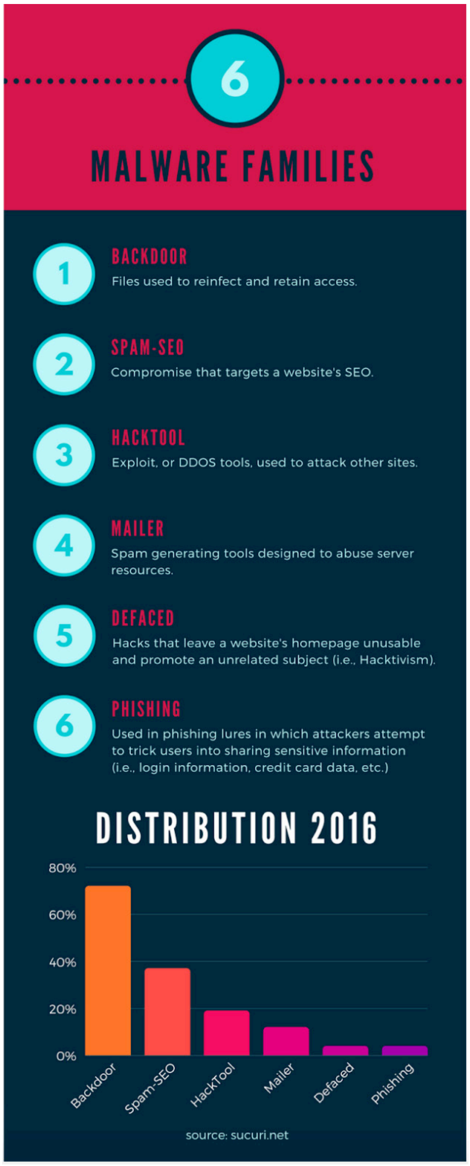
Another common area of concern is protecting the data users enter on your website. Interactive websites often feature contact forms, cart and checkout forms, or comment forms for posts. WP Engine offers free Let's Encrypt SSL Certificates. Protecting your site with an SSL certificate not only gives you a green lock in the URL bar, it also encrypts the data users input on your website.

FILE TRANSFER ENCRYPTION

Users may also be concerned about the security of their files when transferring them to and from their site. WP Engine enforces secured file transfers by requiring the use of SFTP. This means your files are safe and encrypted as they are transported, protecting them from any attackers who could be "listening" on the network.

SECURE, ENCRYPTED BACKUPS

If your site were ever to be hacked, defaced, or compromised due to a vulnerability, it's extremely important to have a backup from when your site was fine, and an easy way to get your site restored to normal. WP Engine automatically backs up your site every night. These backups are stored offsite and are encrypted at rest, meaning your data is secure. If you ever need it, these backups are easily restored to your site with the click of a button in the User Portal.



6 MALWARE FAMILIES

1 BACKDOOR
Files used to reinfect and retain access.

2 SPAM-SEO
Compromise that targets a website's SEO.

3 HACKTOOL
Exploit, or DDOS tools, used to attack other sites.

4 MAILER
Spam generating tools designed to abuse server resources.

5 DEFACED
Hacks that leave a website's homepage unusable and promote an unrelated subject (i.e., Hacktivism).

6 PHISHING
Used in phishing lures in which attackers attempt to trick users into sharing sensitive information (i.e., login information, credit card data, etc.)

DISTRIBUTION 2016

source: sucuri.net

Steps you can take to secure your Website.

The security practices of both WordPress and WP Engine help to protect your site from a wide vector of attacks. However, it's important to understand that there is not a "set it and forget it" type of solution for security. It is not a simple issue. With the freedom to use a wide variety of custom code in the form of themes and plugins, also comes a great responsibility. Security is a partnership WP Engine shares with our customers. With that in mind, there are a number of best practices we recommend for websites of all shapes and sizes.

Stay up to date

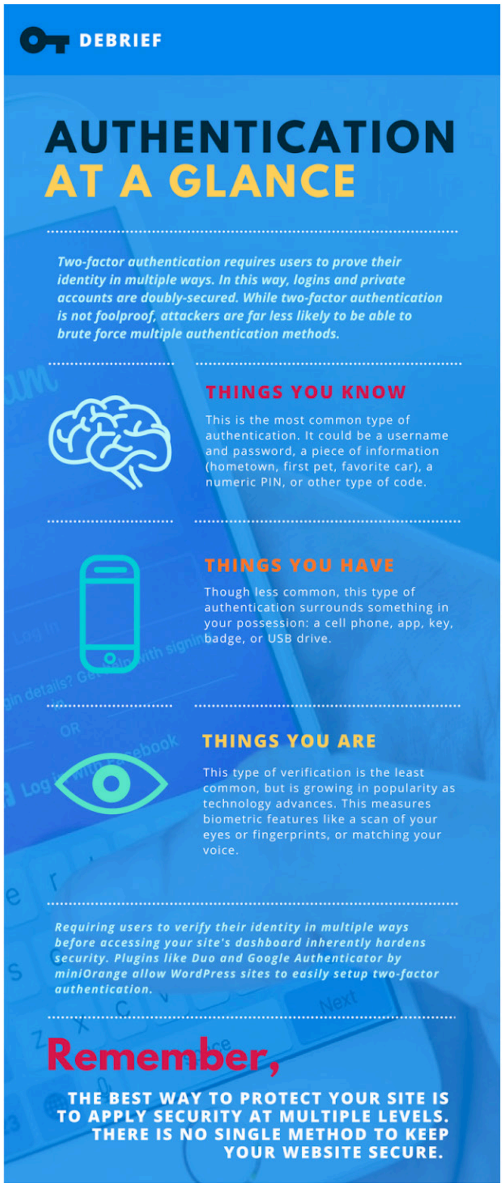
Outdated software is the leading cause of hacked websites and malware. As of Q3 2016, Sucuri reported 18% of all hacked WordPress sites were a result of three primary outdated plugins: Gravity Forms, TimThumb, and RevSlider. Each of these plugins has released secure versions at least a year ago which would have prevented infection. It is important to keep on top of all WordPress plugin and theme updates to ensure your site is secure.

Adhere to the Least Privilege Principle

The "Least Privilege" principle is the idea that users should only be given the access level they *need* to perform their *core role* and nothing more. If you are an Administrator on your WordPress site, the responsibility of determining the access level of other users falls to you. It is extremely important to ensure the other users on your site are only given the access level needed. Be extremely strict with users who publish content, and especially with other Administrators. Ask yourself: does this user truly need this level of access in order to perform their *core role*? If you are a developer on a website, your responsibility is to ensure your code is adhering to WordPress Coding Standards and using core WordPress APIs where possible.

Choose your code carefully

It is important to have a discerning eye when it comes to choosing the theme and plugins your site will use. Each addition also contributes more code to your site, which translates to more potential security flaws as well as additional pieces to maintain and update. For similar reasons, you should also be certain to fully delete any plugins or themes you are not actively using. A good first step is to ensure you download your plugins and themes through the WordPress.org repository, since these are subject to their stringent approval process. However, you should also be careful when picking from these plugins. Look for plugins and themes that are regularly and recently updated, have a wide and happy user base, and provide user help in the Support section. Not only are you more likely to have success with these plugins and themes overall, but these are also the most likely to respond quickly should a vulnerability be discovered.



DEBRIEF

AUTHENTICATION AT A GLANCE

Two-factor authentication requires users to prove their identity in multiple ways. In this way, logins and private accounts are doubly-secured. While two-factor authentication is not foolproof, attackers are far less likely to be able to brute force multiple authentication methods.

THINGS YOU KNOW

This is the most common type of authentication. It could be a username and password, a piece of information (hometown, first pet, favorite car), a numeric PIN, or other type of code.

THINGS YOU HAVE

Though less common, this type of authentication surrounds something in your possession: a cell phone, app, key, badge, or USB drive.

THINGS YOU ARE

This type of verification is the least common, but is growing in popularity as technology advances. This measures biometric features like a scan of your eyes or fingerprints, or matching your voice.

Requiring users to verify their identity in multiple ways before accessing your site's dashboard inherently hardens security. Plugins like Duo and Google Authenticator by miniOrange allow WordPress sites to easily setup two-factor authentication.

Remember,

THE BEST WAY TO PROTECT YOUR SITE IS TO APPLY SECURITY AT MULTIPLE LEVELS. THERE IS NO SINGLE METHOD TO KEEP YOUR WEBSITE SECURE.

Enforce Two-Factor Authentication

Your login page is the gateway to the administrative controls of your website. A simple way to double-down on security for your login page is to enforce two-factor authentication. This method requires users to verify their identity with a second method beyond a simple username and password. For example, two-factor authentication might require you to enter a code that rotates periodically on an app on your phone, in addition to your standard username and password combination. An attacker might be able to brute force your username and password, but they still would be unable to access your site's administration area if they didn't guess the right code at the exact right minute. WP Engine offers Two-Factor Authentication for the User Portal, and there are several plugins to help with this on your WordPress site as well.

Proactive security through monitoring

Both uptime monitoring and file integrity monitoring are proactive strategies to keep your site secure and available. File integrity monitoring keeps you aware of any file changes made to site code. Plugins like Sucuri Security and Stream can monitor file changes on your site. And uptime monitoring services like Pingdom and UptimeRobot will notify you if your your site is not behaving as expected. Increasing awareness allows your team to respond as quickly as possible if the unthinkable happens. And tools like Google Search Console help by monitoring your site's reputation and health, to notify you if your site ends up on any blacklists. Remember, WP Engine also backs up your site nightly and makes it easy to restore your site if you ever need to.

The Conclusion.

Defense in depth

As mentioned previously, there is no "set it and forget it" solution to website security. The concept of Defense in Depth states that, put simply, you should cover all your bases. Website security is never a one-size-fits-all kind of solution. It is extremely important to secure your site on multiple levels and vectors. The more secure vectors on your site, the tighter your overall website security will be. The idea behind this principle is that, should one security vector fail, the others can still provide the level of security needed. A multi-layered defense could look like: Securing your logins, staying on top of updates, coding according to best practices, using trusted plugins, and using monitoring, all in combination with WP Engine's enterprise-grade security practices.

About The author.

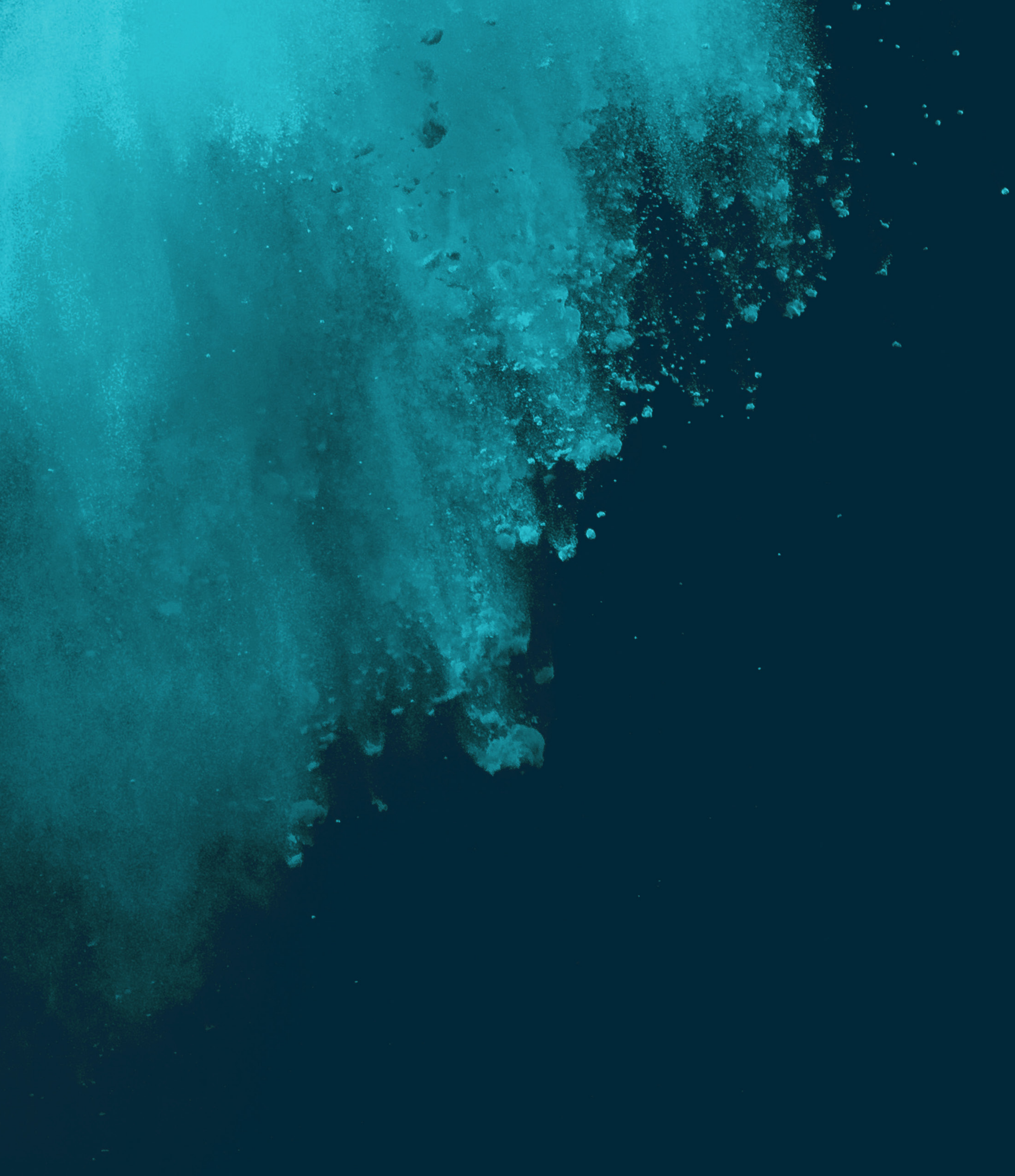
Janna Hilferty

Janna Hilferty is WP Engine's Site Performance Subject Matter Expert. She has lived in Austin since 2014 and enjoys hiking with her dog, painting, and both technical and free form writing.

About WP Engine.

WP Engine is the world's leading WordPress digital experience platform that gives companies of all sizes the agility, performance, intelligence, and integrations they need to drive their business forward faster. WP Engine's combination of tech innovation and an award-winning team of WordPress experts are trusted by over 70,000 companies across 130 countries to provide counsel and support, helping brands create world-class digital experiences. Founded in 2010, WP Engine is headquartered in Austin, Texas, and has offices in San Francisco, California; San Antonio, Texas; London, England; Limerick, Ireland, and Brisbane, Australia.

www.wpengine.com



WP Engine 504 Lavaca Street, Suite 1000, Austin, Texas info@wpengine.com wpengine.com