PREVENTION IS BETTER THAN THE CURE

# Securing your sites with WP Engine

WP engine

## *Taking steps to prevent cyber attacks is the best course of action in today's growing landscape of evolving threats.*

The security of your website is critical to your business, and in today's fast-paced digital world, failure to employ a robust security strategy (or choosing to neglect it for too long) will almost certainly result in some type of security incident.

While those incidents can range from the spread of malware to DDoS attacks to the outright theft of customer data, each carries with it a massive setback to your business, and the sterling reputation you've worked so hard to create.

Remedying a security breach involves many factors, but in addition to fixing the immediate disruption to your digital channels, it will ultimately include repairing damage to your customer relationships, which in some cases can take years to fix, and in others, may be irreparable.

Putting the right measures in place to prevent security incidents is a far more favorable path than dealing with their aftermath, however, it can be difficult to focus on prevention in a world full of evolving cyber threats.

In this ebook, we'll help you sort the noise with more detail on the specific types of attacks that websites—including WordPress sites— face today, the measures required to recover from an attack, and the techniques you can use to prevent attacks from happening in the first place. Let's dig in.

# Table of contents

# Today’s cybersecurity landscape

Today’s cybersecurity landscape is not lacking in challenges. An increasing threat environment coupled with an expanding attack surface have made it harder than ever to stay ahead of what can feel like a never-ending game with critically high stakes.

This is due in part to the widespread availability of tools and technology used for cyber attacks, as well as the proliferation of remote work, unsecured networks, and sophisticated malware and phishing techniques that continue to evolve—and succeed.

While successful cyber attacks come in different shapes and sizes, the global average cost of a data breach is around $4.35M, according to a 2022 IBM report, meaning a company stands to lose that amount (or more) if its systems are compromised in an attack.

Even though proactive measures are clearly effective at preventing attacks from succeeding, security remains a moving target for many businesses, and requires exhaustive diligence and regular evaluation (i.e. time and resources) to maintain.

**$4.35M**

**IS THE GLOBAL AVERAGE COST OF A DATA BREACH**

# Growing challenges require new solutions

In addition to the Covid-19 pandemic and the changes and challenges ushered in by rapid digital acceleration, today's evolving slate of cyber attacks includes a rogue's gallery of threats both new and old:

## RANSOMWARE AND THE RISE OF "BIG GAME HUNTING"

While small-and-medium-sized businesses (and even individuals) remain in the crosshairs of cyber criminals, there has also been a documented increase in large businesses being targeted in ransomware attacks, specifically because they are viewed as more likely to pay a higher ransom to resolve the attack.

Leading security firm CrowdStrike observed an 82% increase in ransomware-related data leaks from 2020 to 2021, noting in its 2022 Global Threat Report, "the growth and impact of big game hunting in 2021 was a palpable force felt across all sectors and in nearly every region of the world."

## GEOPOLITICAL DISRUPTORS

In addition to more inventive and aspirational attacks, recent years have also seen an increase in nefarious cyber activity as a direct or indirect result of global instability.

The war between Russia and Ukraine, for example, has not only been tied to an increase in malicious cyber attacks from nation-state actors, individuals and non-state actors have also reportedly used the conflict as a distraction from their own online criminal activity.

At the same time, escalating tensions between China and Taiwan have led to growing concerns of a significant increase in cyber attacks, affecting everything from individual companies to the global supply chain.

## SEEMINGLY-ENDLESS EXPLOITS AND VULNERABILITIES

While keeping systems and software up to date is now a basic security requirement for even the smallest digital footprint, incessant, exploitable vulnerabilities continue to plague millions of websites every year.

**82% ⬆ IN RANSOMWARE-RELATED DATA LEAKS FROM 2020 TO 2021**

While vulnerabilities can be exploited across many types of software, sites built with WordPress are specifically bolstered by updates to its core software, as well as its individual plugins and themes. But other vulnerabilities extend beyond the codebase of a specific CMS, affecting web applications using many different systems and solutions.

The most high-profile vulnerability in 2021, for example, was Log4Shell, which exploited Apache's widely-used Log4j2 logging library. Log4Shell can be exploited by remote attackers to inject arbitrary Java code into affected services, which could result in unauthorized system access, the delivery of malware, or the acquisition of sensitive data.

The potential the AI ecosystem holds is massive, and marketers have much to gain here. Nonetheless, there is also a hurdle that threatens to block AI's advance—consumer fear, uncertainty, and doubt about the full ramifications of AI, and the potentially sinister machinations of such powerful technology in the wrong hands. Our study found that those concerns could slow the adoption rates outlined above, and significantly hinder the success of AI-based tools in consumer-facing initiatives, unless those concerns are tempered by human discernment, and specifically ethics and values to serve as a guardrail for this powerful technology.

## A hurdle for digital transformation

While even the most robust security solutions continue to face myriad challenges, an ineffective security strategy stands little chance in today's landscape of persistent threats.

In addition to providing weak defenses against attacks themselves, ineffective security strategies can drain budgets and digital projects with costly rabbit holes—including the management of individual security solutions as well as the need to integrate those solutions with existing systems.

Security can also derail larger plans for digital transformation. When faced with the continued use of out-of-date, legacy systems, many businesses choose to remain tied to ineffective digital solutions due to a belief that they are more secure than other, more agile choices.

**SECURITY**

**CAN DERAIL LARGER PLANS FOR DIGITAL TRANSFORMATION**

As an example, businesses in need of flexible solutions that will allow them to go to market faster may overlook viable options such as WordPress or other open source software due to outdated concerns regarding their inherent security.

That's unfortunate, as open source software and WordPress specifically have not only matured significantly in recent years, but also offer perfectly secure foundations on which some of the largest digital projects are being built.

With the right managed hosting partner, large-scale enterprises as well as small-and-medium-sized businesses (SMBs) are meeting their most rigorous security and compliance benchmarks while leveraging open source agility to build fast, modern digital experiences that reach audiences around the globe.

## Proactive prevention: The key to secure WordPress sites

While a proactive security posture will benefit any website regardless of its tech stack, keeping WordPress sites secure is closely intertwined with keeping them up-to-date.

WordPress core has matured greatly over its nearly two decades of existence, and in addition to WordPress' Bug Bounty Program,the global community of WordPress core contributors, as well as individual plugin and theme authors, all play an active role in flagging bugs and vulnerabilities as they're discovered, and working to patch them.

Professional-grade plugin and theme authors too will regularly update their software, and provide patches when a bug or security vulnerability has been discovered, allowing users to update their software and secure their sites before they are affected.

Even then, no business should have to defend its digital properties alone. Extensive website security should be available with any type of web hosting service, managed WordPress hosting included.

Failure to address security issues at the organizational level and with your hosting provider can be an unhealthy choice, leading to significant (site) health issues down the road.

# The most common types of attacks

While the types of threats facing any type of website continue to evolve, there are also many types of attacks that remain persistent, evolving in sophistication and creating headaches for businesses the world over.

## Distributed denial-of-service (DDoS) attack

### WHAT IS IT AND WHAT'S THE CAUSE?

A distributed denial-of-service (DDoS) attack is a harmful attempt to disrupt normal traffic of a network or server by overwhelming the infrastructure with a massive flood of traffic. It's designed to overwhelm the resources of a system so that it becomes unable to respond to legitimate server requests.

The desired outcome of a DDoS attack is to stop your business from running effectively, either disrupting or completely halting your website's ability to operate. As DDoS attacks become more advanced, more forceful, and more prevalent in today's digital world, DDoS mitigation has become a critical element of any security strategy.

### HOW TO CURE A DDOS ATTACK

If your site experiences a DDoS attack you may need to quickly employ defensive measures such as complicated DNS configurations or using a proxy network service such as Cloudflare to absorb and mitigate the attack. While proxy network strategies can be easy to implement, they are less so while a DDoS attack is occurring—especially if your email service is also unusable due to the ongoing attack on your domain.

### HOW TO PREVENT A DDOS ATTACK

The best way to ensure that you safeguard your site from DDoS attacks is to use a service like Cloudflare's Global Anycast network, which absorbs highly distributed attack traffic to keep you online. Origin infrastructure is protected by detecting and dropping attacks at the edge, and shared intelligence across 10 million websites helps block known bad signatures.

WP Engine's advanced network includes Cloudflare CDN and layer 3 & 4 DDoS protection for all customers, at no additional cost. Additionally, WP Engine offers Global Edge Security for advanced security solutions, including a managed Web Application Firewall (WAF) that blocks attacks at the edge, and DDoS protection at the network, transport, and application layers.

> ***WP Engine's advanced network includes Cloudflare CDN and layer 3 & 4 DDoS protection for all customer at no additional cost.***

## Malware and privilege escalation attacks

### WHAT ARE THEY AND WHAT CAUSES THEM?

Malware is malicious software that's installed on your website by an adversary who takes advantage of a vulnerability within your site, such as outdated software (e.g. WordPress, PHP, plugins, and themes) or when an admin user's credentials are compromised.

Malware and privilege escalation attacks can have a host of impacts on your site, from stolen user information, further distribution of malware, injecting hidden black-hat SEO links, or simply taking your site offline. In most cases, if your site has been compromised by malware or a privilege escalation attack, the adversary can pretty much do whatever they want with your website.

### HOW TO CURE A MALWARE ATTACK?

It's difficult to remove malware yourself once it has been inserted into your website. By the time you identify and remove the infected files, the malware may have already spread to other files on your site, making it difficult to track the full extent of the issue. Malicious code sequences may be so well-disguised that they will look like the normal code you would associate with your plugins or other files, but if it isn't removed entirely, you'll likely deal with reinfection later on. Even if you do remove all of the hostile code, your website may still break, because the original code was corrupted and had to be removed.

Because it's so difficult to successfully rid a site of malicious code, it's easier (and more cost effective) to invest in preventative measures rather than fight an attack after the fact.

## HOW TO PREVENT A MALWARE ATTACK?

Managed hosting providers like WP Engine can be a powerful part of your security toolkit, offering support through advanced threat detection and protection from malware and other viruses. This can help prevent some attacks before they even start, it can stop active attacks, or alert you to malware present on your site. Additionally, WP Engine helps prevent malware threats with Web Application Firewalls, forcing strong passwords, supporting enterprise-grade SSO, and forcing security updates to key software used on your website (WordPress, PHP, MySQL, etc.).

In addition to this, keeping WordPress plugins and themes updated should be a critical part of your malware prevention strategy. WP Engine's Smart Plugin Manager automates WordPress plugin updates so your environment stays safe and secure, giving you the time (and peace of mind) back in your day to focus on driving your business forward.

# Adversary-in-the-middle attacks

## WHAT ARE THEY AND WHAT CAUSES THEM?

Adversary in the middle (AiTM) attacks (often called man in the middle attacks) describe those in which the cyber criminal positions themselves between a user and an app. Their goal is either to eavesdrop in the hopes of attaining important information from the user or to impersonate one of the parties, making the exchange seem normal while they wait for the user or application to release confidential information.

The information the hacker wants to extract varies. Common information they may target includes login credentials, account details, proprietary company information, or credit card details from a site visitor. For these types of attacks, there is a chance the adversary is after information about your business, but it's much more likely that they are targeting your end users. eCommerce sites and SaaS sites are common targets for these types of attacks since users often need to share their private financial details.

The data mined from these attacks can then be used for a myriad of purposes, such as identity theft, money transfers, or corporate espionage. Attackers may even change passwords to further compromise websites or user accounts for their own gain.

## HOW TO CURE ADVERSARY-IN-THE-MIDDLE ATTACKS

Once an AiTM attack has taken place, it can be both difficult and expensive to recover. If the attacker has compromised credentials, you'll have to reset passwords and notify users including your customers who may have been affected. This may also require those users to reset their passwords on other platforms where they've used the same (compromised) username and password. In a worst case scenario, your customers may end up with multiple accounts compromised due to the attack and their own relaxed approach of using the same password on multiple systems.

Of course, there is also the potential of great financial damage due to proprietary or embarrassing information being intercepted and used by the attacker in a wide variety of ways. These damages could easily balloon into the millions of dollars and the "cure" could include anything from endless billable legal hours to drastic changes to your customers' business strategies due to proprietary information being leaked.

Recovering from an AiTM attack of course includes implementing measures to help prevent such an attack from happening again, however, the "cure" can be a labyrinth of operational, legal, and financial measures as you deal with the implications of whatever private information was compromised.

## HOW TO PREVENT ADVERSARY-IN-THE-MIDDLE ATTACKS

There are a wide variety of types of AiTM attacks that each require their own defensive measures. This could include tactics like monitoring for or defensively buying domains of misspellings of your domain to prevent attackers from siphoning information from visitors who typo your primary domain name. It could also include requiring team members to use a VPN when managing your website.

Similarly, most preventative measures are focused around making sure everything your site communicates is encrypted, ensuring that in the event of a successful AiTM attack, the adversary will not be able to read the information. Using strong SSL encryptions and a well-configured Web Application Firewall on your site are both recommended preventative measures for AiTM attacks.

WP Engine offers end-to-end encryption for every system on our platform as well as free and easy to configure SSL for your website which includes automatic redirects from http to https. Choosing a host that enforces strong end-to-end encryption can be a critical part of your larger security toolkit, and is a great preventative measure for mitigating AiTM attacks.

# The cost of security incidents

The true cost of a security incident includes many factors, and can change significantly based on the size of the business affected and the motivations of the attacker.

When it comes to the monetary cost of a security issue, that number has risen every year, with no sign of slowing down. According to a 2022 IBM report, the global average cost of a data breach is around $4.35M.

In addition to financial losses, cyber incidents often leave a major mark on a company's brand and reputation, and can manifest beyond the incident itself. Read on for more detail about the specific costs of a security incident.

## LOST TIME AND ENGINEERING EXPENSES

If your site has experienced a security incident, you will need to enact "remediation and recovery" measures, which essentially entails discovering how the attack took place, fixing the vulnerability that led to the attack, and recovering any lost data or systems from the attack (if possible).

This could require hiring expensive outside consultants or services to help with these measures or at very least, will take time from your own web development, executive, and operational teams in order to address. This not only presents an economic impact, but it also affects your team's larger roadmap as they focus on recovering from the security incident instead of optimizing your website to drive further company growth.

## LOST SALES DUE TO OUTAGES

During a security incident, you may find that your website experiences a high amount of downtime, especially as you work to remedy the issues at play. In the case of a DDoS attack, your site cannot handle the volume of requests and completely shuts down.

Either way, increased downtime almost always has a negative impact on a business' performance and overall bottom line—especially if your website is where your customers purchase your products and services. If your customers can't reach you, sales will take a hit, and the odds of losing customers to your competitors increases.

## Legislation and regulatory fines

In some countries and industries, security incidents can also come with heavy financial penalties. GDPR for example, which applies to anyone processing or collecting customer data for people and businesses residing in the EU and UK, includes severe fines and penalties for businesses that fail to properly secure their websites (and experience a security breach as a result).

In addition to remedying the issues affecting your business, a security breach that violates GDPR would also require you to focus on responding to government oversight, not to mention legal action from customers for liability of financial and personal damages due to the security incident in question.

### CUSTOMER TRUST AND LOYALTY

One of the biggest costs to a business after a security incident is the loss of trust and loyalty that comes from even the most supportive customers. Even if the incident didn't result in the disclosure or theft of any customer data, the optics of a security breach alone will cause customers to lose faith and trust in your business. From a customers' perspective, it's better to cut ties and find a more reputable solution than to wait and see, and potentially deal with the consequences of having their data stolen.

## Loss of information and data

Another loss that may not be considered first when thinking about the cost of a security incident is the loss of information and data that occurs when it's deleted or corrupted. This could set your business back years in terms of resources and time, only to get back to operating at the level you were before the security incident occurred. You may not have the information or data you once did and this could cause disparity between systems if the information is unrecoverable.

# Staying one step ahead: A preventative security checklist

Against today's wide backdrop of cyber threats and the significant costs associated with remedying a cyber incident, taking steps to secure your site and preventing attacks from succeeding is a strategic imperative for any business.

While every organization has unique considerations, the following checklist provides an overview of key areas you can focus on to mitigate the risk of cyber attacks and bolster the security of your websites.

## Updates

One of the best preventative defense measures you can put in place is simply keeping your software up to date. Regular updates can alleviate a wide array of security concerns including exploitable vulnerabilities, and updates help ensure would-be attackers aren't able to take advantage of "low hanging fruit" (i.e. out-of-date software that provides them with an easy entrance).

When it comes to WordPress sites specifically, ensuring you're using an up-to-date version of its core software will help keep your site as safe as possible. According to a study by web security firm Sucuri, 39% of the WordPress sites hacked in 2020 were using an out-of-date version of the software. Keeping WordPress updated is the best defense against hackers who use vulnerabilities in outdated software to gain unauthorized site access.

## Maintaining Key Software Components

The same is true for other components of your WordPress site, including PHP, plugins, and themes. By regularly running updates and making sure you're using up-to-date software, you can greatly diminish the security threats facing your WordPress sites.

Nonetheless, regular website maintenance is time consuming, and updating software on your own can create other issues, including problems with compatibility. To ease this burden while keeping up with ongoing maintenance requirements, many businesses partner with a managed hosting provider, which provide peace of mind that security and updates are being handled, without having to rely on internal teams (whose time is often better spent elsewhere).

WP Engine's customer sites, for example, are always running on up-to-date versions of WordPress, and are ready to benefit from WordPress' latest features. Our WordPress update program intelligently tests your site before and after updates are performed to ensure everything works seamlessly.

With WP Engine, you never run an unsupported version of WordPress, and you can rest easy knowing you're always using the right version of PHP. With advanced security solutions including Global Edge Security and Smart Plugin Manager, you gain additional protections that can harden the security of your sites, while allowing to you stay focused on your business.

## REGULAR BACKUPS

Regularly backing up your site creates a critical safety net in case of an attack. In the event that your site is compromised, having a recent backup is your only option for recovering important data that was overwritten or deleted.

Given the importance of regular backups—for security, compliance, and other disaster recovery assurances—WP Engine provides all customers with automatic, encrypted backups every day, ensuring their data remains in safe hands no matter what.

## STRENGTHENING INTERNAL SECURITY PROCESSES

Preventative security also means establishing strong internal practices within your organization. This can include requiring a VPN when connecting to company sites, or forced system updates on company devices.

It can also be as granular as improving password strength across your organization. Strong passwords can prevent brute force attacks and other data breaches. As a rule of thumb, passwords should be around 15-20 characters long, and should use a mix of characters, letters, and numbers while avoiding memorable keyboard paths.

The use of two-factor authentication, which requires a secondary assurance after a user has logged into a device or a website, is another preventative measure that can greatly bolster organization-wide security.

## THE MANAGED HOSTING DIFFERENCE

Partnering with a managed WordPress provider like WP Engine provides your sites, and your business, with a secure hosting environment you can rely on.

WP Engine blocks 26B attacks a year with proactive threat detection, and our security team scans the risk and compliance landscape to ensure our platform is never compromised.

WP Engine's platform also meets the SOC 2 standards for Security and Availability Trust Services Categories and it has received ISO/IEC 27001:2013 certification for the Information Security Management System (ISMS) supporting its hosting platform.

When you host your website with WP Engine, you'll also be able to take advantage of the following benefits:

- Let's Encrypt SSL certificates: Ensure that your data transfers are encrypted and secure with the one-click addition of a free SSL certificate.
- Managed WordPress core updates: You can avoid many vulnerabilities by never missing minor core updates, and receive update recommendations for major version releases.
- Threat detection and blocking: Our security team actively monitors our platform for malicious activity, and we block any traffic that looks suspicious.
- Malware scanning and cleaning: If your site gets hit with malware, our Support Team is on call to help you locate it, remove it, and report back to you on the results.
- Disaster recovery: If the worst happens, we offer expert-level recovery assistance to get you back online as quickly as possible.
- Daily encrypted backups: Backups are the ultimate insurance policy, and if you ever need to restore your WordPress site from a secure backup, WP Engine makes it easy.

**26 Billion**

**ATTACKS BLOCKED A YEAR WITH PROACTIVE THREAT DETECTION ON WP ENGINE**

## How does Global Edge Security improve the security of your sites?

- Shared intel across 8M websites to build resilience to new forms of attacks at the edge
- Built-in rulesets mitigate WordPress-specific vulnerabilities
- Auto-updated to protect against latest known nefarious attacks
- Network of 151 DCs, capacity 10x+ larger than the largest DDOS attack

While the above comes standard with every WP Engine plan, advanced solutions such as Global Edge Security offer business continuity, revenue protection, and app-level security at the network edge all while providing performance benefits.

This additional level of protection includes managed web application firewall (WAF), advanced DDoS mitigation, and SSL/TLS encryption built in partnership with Cloudflare.

WAF rule sets are tailored and managed to identify new attack patterns and create rules accordingly. Managed WAF also protects against both WordPress-specific threats and emerging vulnerabilities, mitigating threats at the edge and automatically updating to respond to newly-discovered threats.

With SSL/TLS management, web traffic passes through the global network to prevent unwanted breaches, and site encryption keeps your WordPress site safe from prying eyes.

And because plugin vulnerabilities often make up the lion's share of security risks to WordPress sites, WP Engine offers Smart Plugin Manager as a solution to time-consuming plugin management tasks. The best part? You can add Smart Plugin Manager to any WP Engine plan for $100 per year.

How does it work? Smart Plugin Manager automatically updates a site's plugins on a customizable scheduled interval. It also runs a Visual Regression Test (VRT) using machine learning to identify if updates passed or failed. Updates regarding your plugin and theme upgrades are sent to you daily so you always stay ahead of potential issues.

For site managers or internal web teams overseeing a single or multiple WordPress sites, Smart Plugin Manager offsets the need to oversee the management and updates of your plugins, while keeping your sites secure and empowering you to focus on tasks that drive your business forward.

## INCREASE YOUR WEBSITE SECURITY WITH WP ENGINE

When you choose managed WordPress hosting with WP Engine, you not only gain access to essential developer tools and resources, you gain access to our WordPress-optimized platform and the security practices we've set in place to keep it secure.

LEARN MORE

# Conclusion: Prevention is better than the cure

Unfortunately, the fast pace of today's digital world and the rapidly evolving nature of cyber threats leaves little room for ineffective or neglected security strategies.

Failure to employ preventative measures and protect your website from attacks will lead to unhealthy outcomes down the road, and as this ebook has detailed, taking those preventative steps now is a far more favorable course than pursuing a cure once the damage has been done.

While today's threat landscape will undoubtedly continue to grow and evolve, there are steps you can take to beef up internal security practices, in addition to the services and expertise of security experts.

When you partner with WP Engine, you gain the knowledge, experience, and expertise we've collected from more than a decade of hosting WordPress sites building our own proprietary WordPress technology. You also benefit from our strong partnerships with leading security companies like Cloudflare, which bring global security expertise to managed WordPress hosting, perfected.

From automatic plugin updates and SSL certificate implementation to consistent monitoring by a team of real-life experts, WP Engine provides everything you need to keep your sites secure.

Paired with the simplicity of our service and the scalability of our platform, WP Engine gives you peace of mind and the power to create with WordPress, securely.

Speak with us today to learn more about our industry-leading WordPress platform, our advanced WordPress security solutions, and the ways we help our customers win online every day.

LEARN MORE    CONTACT US

WP engine®

## About WP Engine.

WP Engine, the WordPress technology company, provides the most relied upon and trusted brands and developer-centric WordPress products for companies and agencies of all sizes, including managed WordPress hosting, enterprise WordPress, headless WordPress, Flywheel, Local, and Genesis. WP Engine's tech innovation and award-winning WordPress experts help to power more than 1.5 million sites across 150 countries.