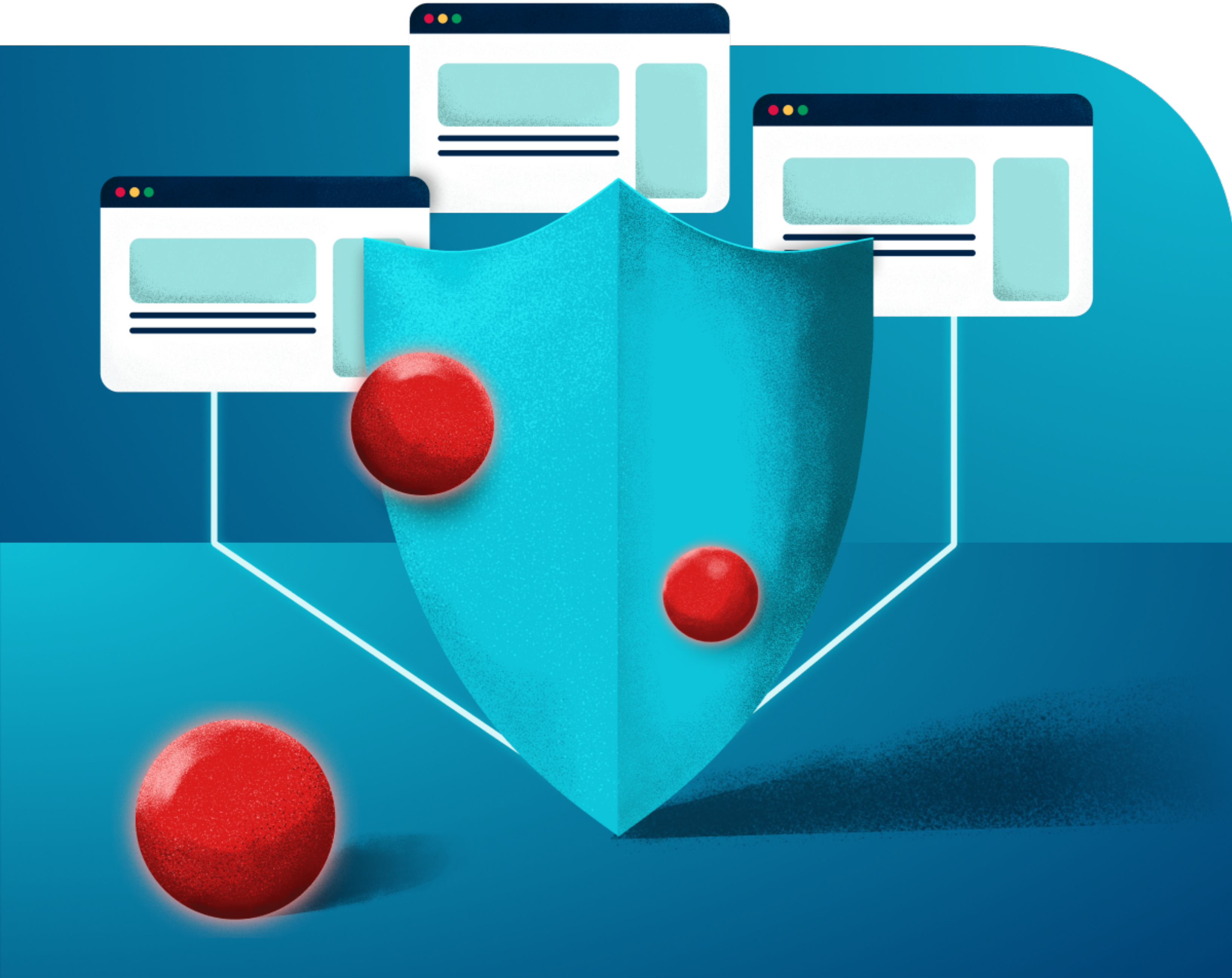
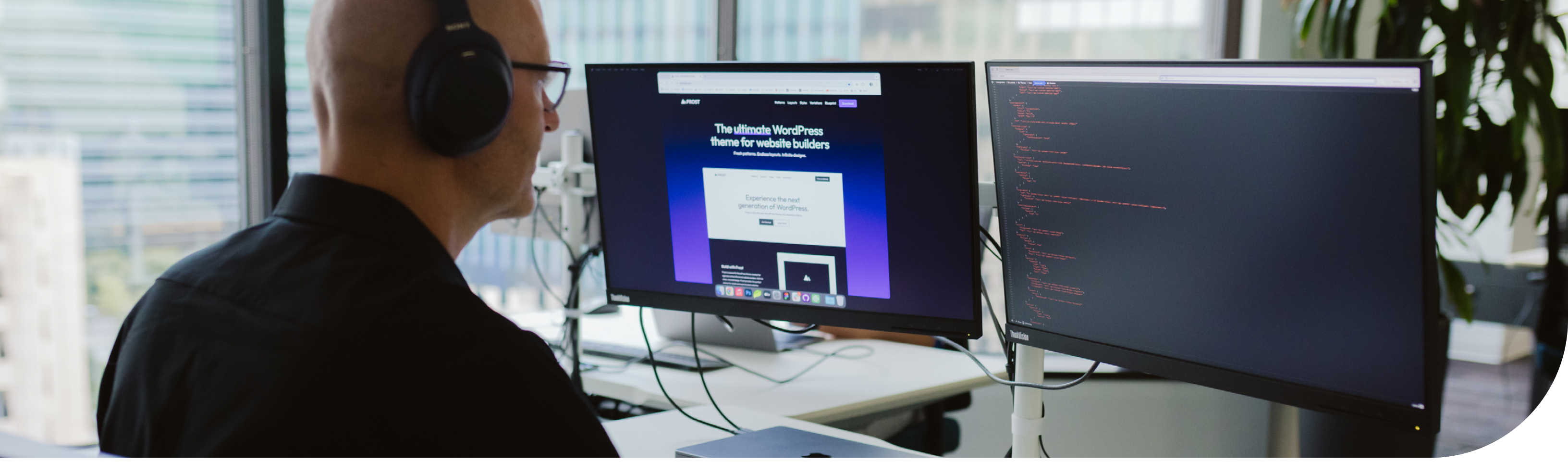
Securing Your Sites With WP Engine

Prevention is Better Than the Cure





Introduction

Taking steps to prevent cyber attacks remains the best course of action, particularly as the threat landscape shifts from simple automated scripts to enterprising adversaries using artificial intelligence.

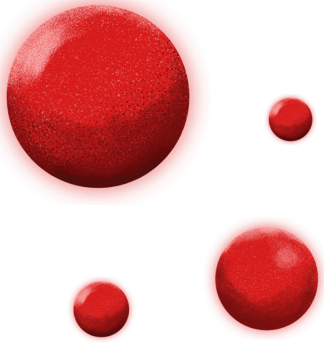
The security of your website is critical to your business, and in today's fast-paced digital world, failure to employ a robust security strategy (or choosing to neglect it for too long) will almost certainly result in some type of security incident.

While those incidents can range from the spread of malware to DDoS attacks to identity-based intrusions, 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, focusing on prevention is increasingly difficult in a world where adversaries use Generative AI to increase the speed and sophistication of their attacks.

In this ebook, we'll help you sort the noise with more detail on the specific types of attacks that websites 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.



Today’s cybersecurity landscape

The cybersecurity landscape of 2025 isn’t 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, high-stakes race.

This is due in part to the widespread availability of tools and technology used for cyber attacks today, 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 $4.4M**, according to a 2025 IBM report, meaning a company stands to lose that amount (or more) if its systems are compromised in an attack.

While proactive measures are 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.

Growing challenges require new solutions

According to the **CrowdStrike 2025 Global Threat Report**, today’s evolving slate of cyber threats includes a rogue’s gallery of new tactics.

The Race Against Time: Breakout Velocity

In previous years, defenders had hours or even days to detect an intruder before significant damage was done. That window has closed. CrowdStrike researchers found that the average "breakout time"—the time it takes for an adversary to move from their initial compromise to other systems on your network—has dropped to just 48 minutes. In the fastest cases, adversaries can break out in as little as 51 seconds. This "need for speed" means that automated defenses and managed platforms are no longer optional conveniences, they are necessities for survival.

The Rise of "Malware-Free" Attacks

Traditionally, security focused on stopping malicious software (malware) from being installed. However, modern adversaries have pivoted. CrowdStrike reports that in 2024, 79% of detections were "malware-free." Instead of "breaking in" using code exploits, attackers are "logging in" using valid credentials they have stolen. By mimicking legitimate users, these identity-based attacks are much harder to detect with legacy antivirus software alone.

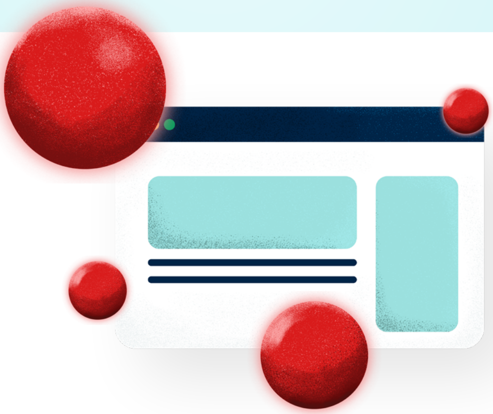
AI-Enhanced Social Engineering

The barrier to entry for cybercrime has lowered significantly due to Generative AI. Adversaries are now using Large Language Models (LLMs) to craft highly convincing phishing emails and even conduct "vishing" (voice phishing) attacks. In fact, CrowdStrike observed an explosive 442% growth in vishing attacks in the latter half of 2024. These AI-powered tools allow attackers to scale their operations, targeting employees and help desks with personalized narratives that are difficult to distinguish from reality.

Persistent Vulnerability Exploitation

While identity attacks are on the rise, software vulnerabilities remain a critical entry point. CrowdStrike data reveals that 52% of observed vulnerabilities in 2024 were related to initial access. Adversaries continue to scan for unpatched software at the network periphery, looking for any opening to establish a foothold.

> This reinforces the need for a rigorous update strategy for your core software, plugins, and themes.



A hurdle for digital transformation

While even the most robust security solutions face a myriad of challenges today, an ineffective security strategy stands little chance against the current landscape of persistent threats.

In addition to providing weak defenses against attacks themselves, an ineffective security strategy 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.

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**®[1] and 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.

[1] *WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademark is the intellectual property of the WordPress Foundation. Uses of the WordPress® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation.*

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 greatly matured 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 plugin and theme authors will also regularly update their software, and provide patches when a bug or security vulnerability has been discovered. This allows users to update their software and secure their sites before they are affected.

But updates are only effective if and when they're put to use, which is why a strategy for keeping things like WordPress core, plugins, and themes up to date is essential for overall WordPress security.

Even then, no business should have to defend its digital properties alone. Extensive website security should also 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

Causes, cures, and how to prevent

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.

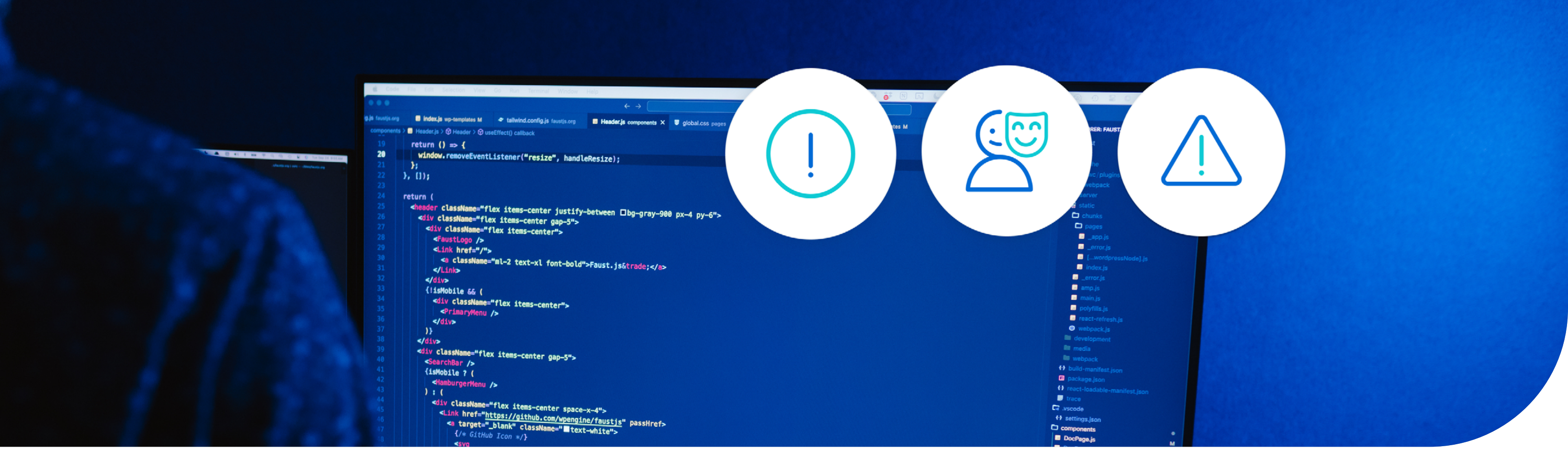
How to cure a DDoS attack

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 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

One of the best ways to 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.



```
      return () => {
        window.removeEventListener("resize", handleResize);
      };
    }, []);

    return (
      <header className="flex items-center justify-between □bg-gray-900 px-4 py-6">
        <div className="flex items-center gap-5">
          <div className="flex items-center">
            <FaustLogo />
            <Link href="/">
              <a className="ml-2 text-xl font-bold">Faust.js&trade;</a>
            </Link>
          </div>
          {!isMobile && (
            <div className="flex items-center">
              <PrimaryMenu />
            </div>
          )}
        </div>
        <div className="flex items-center gap-5">
          <SearchBar />
          {isMobile ? (
            <HamburgerMenu />
          ) : (
            <div className="flex items-center space-x-4">
              <Link href="https://github.com/wpengine/faustjs" passHref>
                <a target="_blank" className="■text-white">
                  {/* GitHub Icon */}
                  <svg
```

Identity-Based Attacks & Malware

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. Traditionally, malware was a primary tool for attackers. However, the landscape has shifted. According to the CrowdStrike 2025 Global Threat Report, 79% of detections in 2024 were "malware-free."

Instead of "breaking in" via software vulnerabilities, modern adversaries are "logging in" using compromised credentials. This is known as an Identity-Based Attack. Attackers use stolen usernames and passwords (valid account abuse) to enter a system legitimately and then move laterally to install malware or steal data. That said, classic malware is still used to exploit outdated software (e.g., WordPress, PHP, plugins, and themes) once access is gained.

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 an identity or malware attack

Recovering from an identity breach is complex. You must immediately revoke active sessions, reset all credentials, and audit your system for "backdoor" accounts created by the attacker. If malware was deployed, removing it yourself is difficult; malicious code is often well-disguised and spreads to other files. Because it is so difficult to successfully rid a site of malicious code or a persistent intruder, it is easier (and more cost effective) to invest in preventative measures.

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 identity and malware attacks

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.

Social engineering and 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. However, in 2025, this is often powered by social engineering.

CrowdStrike reports a 442% increase in "vishing" (voice phishing) in late 2024. In these attacks, criminals use AI-enhanced tactics to call IT help desks or employees, posing as legitimate staff. They persuade the victim to log in to a fake login page (the AiTM component) or download remote monitoring tools. The goal is to capture the user's session token or password in real-time, bypassing standard security filters.

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.

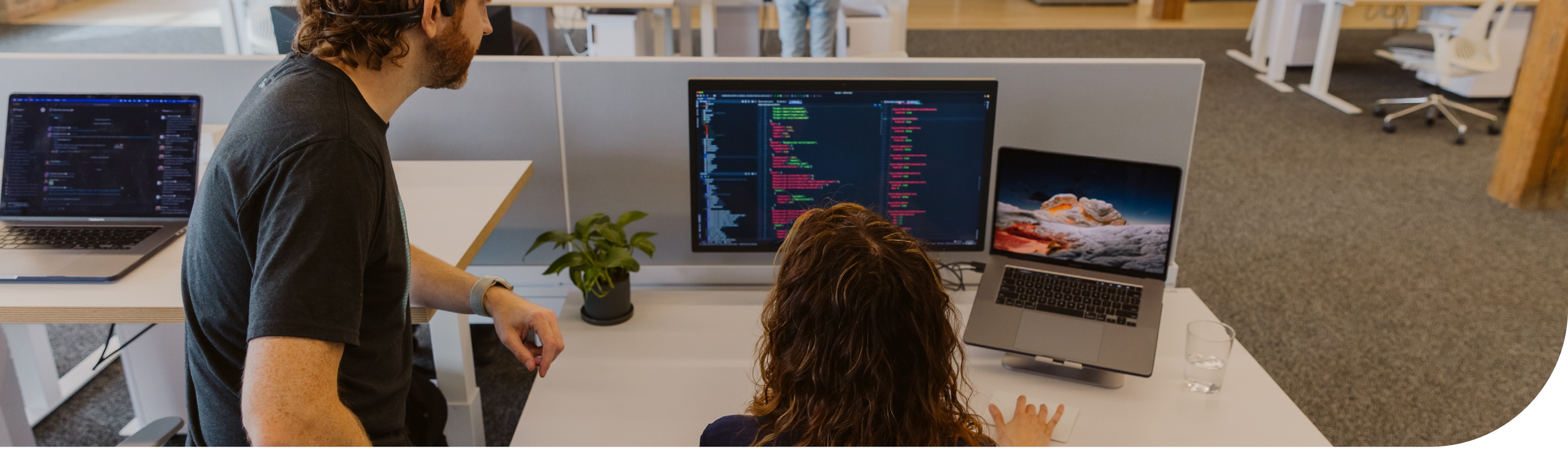
Recovering from an AiTM attack of course includes implementing measures to help prevent such an attack from happening again, however, the "cure" can be a labyrinth of operational, legal, and financial measures as you deal with the implications of whatever private information was compromised.

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 2025 IBM report, the **global average cost of a data breach is around $4.4M**.

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, it 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 time and engineering expenses

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).

> In 2024, 52% of observed vulnerabilities were related to initial access. This means that half the time, an unpatched plugin or theme is the open door an attacker walks through.

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.

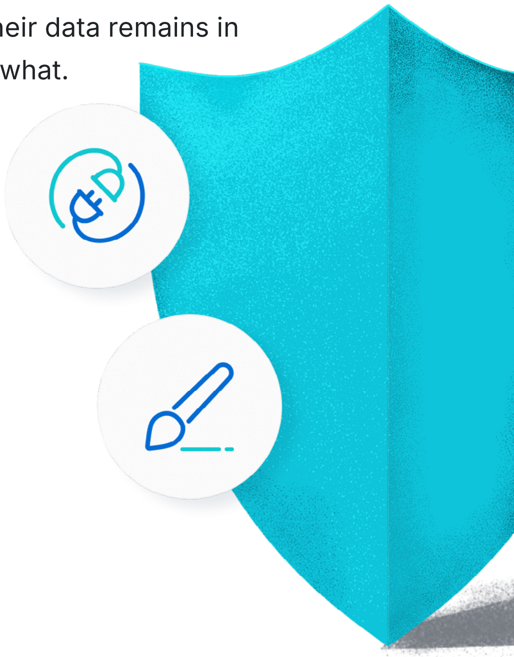
Nonetheless, regular website maintenance is time consuming, and updating software on your own can create other issues, including problems with compatibility. To ease this burden while keeping up with ongoing maintenance requirements, many businesses partner with a managed hosting provider, which provide 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.

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 hosting for WordPress** 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. add an entire security team to your organization, with the needed expertise to keep your WordPress sites 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 hosting for WordPress, 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.

WP engine™

WP Engine empowers companies and agencies of all sizes to *build, power, manage, and optimize* their WordPress websites and applications with confidence.

Serving 1.5 million customers across 150+ countries, the global technology company provides premium, enterprise-grade solutions, tools, and services, including specialized platforms for WordPress, industry-tailored eCommerce and agency solution suites, and developer-centric tools like Local, Advanced Custom Fields, and more. WP Engine's innovative technology and industry-leading expertise are why 8% of the web visits a WP Engine-powered site daily. Learn more at wpengine.com.

WP Engine is a proud member and supporter of the community of WordPress® users. The WordPress® trademarks are the intellectual property of the WordPress Foundation, and the Woo® and WooCommerce® trademarks are the intellectual property of WooCommerce, Inc. Uses of the WordPress®, Woo®, and WooCommerce® trademarks in this website are for identification purposes only and do not imply an endorsement by WordPress Foundation or WooCommerce, Inc. WP Engine is not endorsed or owned by, or affiliated with, the WordPress Foundation or WooCommerce, Inc.