Pagely Security

Introduction

Pagely is a premier Managed WordPress Hosting service, powered by Amazon Web Services. We're experts in delivering secure, high-performance hosting solutions, tailored to meet the needs of agencies and businesses of all sizes. Learn more about our team of dedicated experts at https://pagely.com/about-us/

Our industry leading security suite, PressArmor, has been custom engineered to protect some of the busiest websites on the internet. Pagely's dedicated Security Team continuously improves and maintains our platform's security tooling, and all Pagely Teams are trained on security best practices. Our approach is to stay ahead of the ever-evolving security threat landscape. In this document we will highlight aspects of our service with a focus on security, including the important processes we follow.

Limitations

Every effort has been made to ensure the best possible security for our customers, providing a solid foundation to compliment their own security measures for whole-of-system security. Pagely identifies, investigates, remediates, and reports to you on issues relating to security, malware, software vulnerabilities, and dependency updates. Security is a shared responsibility, and our systems, defenses, and counter-measures in conjunction with your own measures and best practices ensure software development and everyday use of the service remains secure.

In certain instances where a breach is extensive or unusually sophisticated, the best course of action may sometimes be a restoration from backup followed by immediate corrective measures to avoid a repeat incident. Our toolset allows us to perform a comprehensive assessment of a given situation to help inform the decision of repair vs restore.

Learn more about our shared security model at https://pagely.com/solutions/secure-wordpress-hosting/

Security Measures Deployed at Pagely

Our platform employs a comprehensive set of proactive and reactive measures at each level of the technology stack to ensure maximum security of your data and applications. Enterprise WordPress security is a fundamental need for our customers, which is why we strive to offer the most robust, secure, and scalable solution available.

WordPress Security Features in Place

Below is a list of highlighted features we deploy by default across all of our hosting plan offerings. Our network and platform utilize Amazon Web Services exclusively, affording us the benefits of passing along AWS Shield Standard to your web presence.

Detection and Notification

- 24/7 Monitoring and Alert Response
- WordPress Core Security Patch Monitoring
- Plugin and Theme Security Patch Monitoring
- Automated Malware Scanning with human touch cleanup
- Site Security analysis and recommendations

Prevention and Remediation

- Automated Reboot-less Kernel Security Updates
- Automated WordPress updates
- Automated plugin updates
- Hardened customer environment, with write, read and execution protection
- Banned plugin list
- Daily Backups to Amazon S3, EBS volume snapshots performed multiple times per day, Point-in-time Database Restore
- Encryption at rest at all data layers (EBS, S3, Database) with hardware-backed key management (AWS KMS)
- Web Application Firewall with WordPress specific ruleset
- WordPress Bruteforce Login Protection
- Protection from basic Denial of Service attacks
- Hacked Site Cleanup and Cause Analysis
- SSL Certificate

Continuous Security Patching

Our platform continuously monitors our servers, ensuring compliance with security-related patches for the operating system and installed packages, including the Linux Kernel, PHP, WordPress Core, WordPress plugins, and WordPress themes. Resources that cannot be automatically patched are surfaced to our InfoSec team for manual remediation. Our custom integrations and workflows allow us to push updates out expediently in the event of a critical vulnerability disclosure. Standard update cadence is within 72 hours, often quicker, depending on the individual component.

KernelCare Live Kernel Patching

Pagely deploys KernelCareTM Live Kernel Patching functionality for all customer EC2 resources. The provider of KernelCare, CloudLinux, Inc., manages the creation and distribution of live patches to the Linux Kernel.

These updates are applied continuously as they are made available by CloudLinux, from an agent running on each server. Best of all, KernelCare patches do not require a server reboot!

PHP Security Patches

Pagely manages the PHP version for your WordPress applications. Each installation of WordPress is deployed with its own Docker container residing on the EC2 resources we provide for you. The containers run with images that Pagely builds periodically, as point releases and security patches are released. We publish these images into an internal ECR repository, and your application will fetch the new container image when the application is reloaded. Image updates are published within 24-72 hours. App Reloads are triggered automatically when making certain changes to your site or can be configured to occur automatically at a specific cadence.

Additionally, through our partnership with Zend, we offer PHP Long Term Support (LTS) for customers running older PHP versions. This ensures your site remains secure with necessary patches and bug fixes to the PHP runtime while you prepare to upgrade to currently supported versions of PHP. This extended support provides peace of mind and flexibility during your transition to newer PHP versions without compromising security or performance.

WordPress Core Updates

Pagely manages updates to WordPress Core. Whether it is a new release of WP, a maintenance release, or a security release, the management of WordPress Core is solely controlled by Pagely. Our typical cadence for applying security releases for WordPress Core is 24-48 hours.

WordPress Plugin Updates

Pagely's systems conduct a WordPress Plugin Update operation on a daily cadence. All plugins installed on an app, with the exception of WooCommerce, are updated on a daily basis by our automated systems, provided that the plugin is one published on wordpress.org or, in the case of a paid plugin, the vendor has configured the appropriate metadata to be able to fetch that update using the standard WP plugin update mechanisms.

Exceptions

Certain exceptions apply to our continuous security patching. These typically relate to problems occurring upstream that may prevent an update from being applied, or weekend availability. In all cases, any high severity security vulnerability disclosure will trigger immediate response from our InfoSec team.

Access Level Isolation

Different levels of user access are made available by our Atomic Control Panel in the form of "collaborators". These roles range from full access to instead only a specific website or even only billing concerns.

Our customers can benefit by permitting granular access to third parties relative to their access requirements.

Resource Isolation

We take advantage of Amazon EC2 instances which provide isolated, virtual environments for all VPS and Enterprise services. All memory, CPU, and other server resources are dedicated to each client. This means all of your hosting infrastructure at Pagely, including EC2 instances, EBS volumes, and networking are backed by resources dedicated solely to you. For database solutions, you can choose between our standard shared RDS database option or opt for a private RDS instance where all your applications' databases are hosted with dedicated resources as well. With a private RDS instance, we can also optionally enable external access using HAPROXY endpoints and IP-based access controls.

Preventative Care

The very best scenario is one where a security incident never occurs. We approach security with prevention as the primary goal. Our InfoSec team is actively monitoring, auditing and developing technology to ensure the greatest level of protection across all risks.

We are uniquely positioned in the market to be constantly developing best-in-class software tools which are specifically suited to the needs of our customers. Pagely ensures the security of its network, facilities, and access controls, with regular effectiveness assessments. Customers are responsible for configuring their services correctly, using provided security controls, and protecting their data through encryption, access management, and backups.

Incident Response

In the event of an incident, our customers can be assured of a prompt incident response program. This follows our thorough identification process, remediation and ongoing monitoring with a complete follow up report with the customer. In the event of an emergency, we will simply do the right thing for the customer.

These detailed reports include:

- Detected indicators of compromise.
- Attack vector details, including any most likely cause (should the vector not be positively identified). Steps taken to clean up the site.
- Our expert recommendations towards remediation to prevent further compromise. New files are scanned daily on all customer sites to search for known signs of malware.

It is not uncommon that our Incident Response program will detect an unreleased or 0-day exploit being used in the wild. If possible, for these matters we perform a patch for the exploit to remediate the immediate risk, then follow our Vulnerability Disclosure process with the author of the vulnerable code.

Additional Links

- How Does Pagely Handle WordPress Core & Plugin Updates?: https://support.pagely.com/hc/en-us/articles/200237360-How-Does-Pagely- Handle-WordPress-Core-Plugin-Updates-
- Pagely Security Blog: https://pagely.com/blog/category/security/
- Pagely Malwatch: A malware scanning system created at Pagely: https://pagely.com/blog/malwatch-malware-scanning-system/

Thank you.

Email us: sales@pagely.com

Pagely | pagely.com