WordKeeper

Security Features

General

- WordPress file probing and system file protections
- Server file probing and system file protections
- Automatic file name unsafe character removal
- Automatic protection from unauthorized changes to major core WordPress settings
- Automatic protection from unauthorized changes to WordPress user account data
- Protections from SQL injection, shell injection, PHP function injection, hex injection, forged/spammy referrers, forged IP headers, XSS, OS forgery, browser forgery, RFI, and LFI through a broad WAF configuration
- Configurable robots.txt control for known good crawler bots (search engines, SEO analysis tools) in WordPress sites
- Known “bad bot” blocking
- Direct bot POST login blocking
- Default access restrictions protecting core WordPress REST routes from public access
- Heavy restrictions on file permissions and account “firewalling” to prevent cross user access/ contamination
- Optional and configurable country-based restrictions for logins, password resets, account registrations, form submissions, and comment submissions in WordPress sites
- Optional blocking for comments, trackbacks, and pingbacks
- Optional removal of comment form URL fields
- Optional enforcement of PHP file editor restrictions
- Optional installation of WordPress Comment Blacklist
- Account access limited to SFTP, phpMyAdmin and SSH upon request. See SSH section for more detail
- Secure and restricted daily off-site/off-server backups
- Restrictions for supported applications (e.g. restricting duplicate WordPress installations)
- Prevention from server overcrowding to optimize user performance and experience. Much lower levels of competition for resources on shared servers
- Data centers are SOC 1 Type 2, SOC 2 Type 2, and PCI-DSS compliant. US data centers are also HIPAA compliant. Beyond those core compliances across our data centers, many data centers also include additional compliances/certifications such as: ISO 27001, ISO 9001, SOC 3, SSAE 16, and various other ISO and NIST compliances. Exact compliance lists vary per data center

MariaDB

- Careful segregation of MariaDB users (each site has its own user account and database)
- Unique passwords for system critical accounts (e.g. each server uses unique passwords and each MariaDB instance has its own separate unique root passwords)
- Publicly closed MariaDB port (local access only)
- Permissions and restrictions enforcement for MariaDB import functions
- Strict limits on site level MariaDB user permissions
- Optional support for Transparent Data Encryption (TDE) on private servers

Updates

- Routine security and server level updates and software patches, including kernel updates.
- Optional divestment of the tedious responsibility of updating WordPress core and plugins
- Automatic installation of selected high risk security patches for WordPress plugins and WordPress core (regardless of your optional update management selection)

Firewall

- A system level firewall that blocks both inbound and outbound port access – heavily restricted to allow only required/commonly used ports for basic website functionality
- Brute force login protections for WP
- Brute force login filtering for phpMyAdmin
- Strict limits on access to XML-RPC
- Public file access prevention for sensitive files like logs, config files, executable files, versioning repos, SQL files, temp files, and commonly named backup files
- Restricted approved referrers for WP comment submissions
- Brute force login amplification attack protections for XML-RPC
- Blocks for obvious spam or bot comment submissions
- Bot and user agent forgery detection
- Automatic bot blocking for WordPress logins and password resets
- Optional bot blocking for WordPress account registrations, comments, and form submissions
- Brute force login protections for SSH/SFTP (repeated failed logins result in progressive firewall level banning of abusive IPs)
- Automatic daily bans of known abusive IPs from multiple security data sources
- Progressive IP bans for abuse of WordPress login areas, WordPress comments, and xmlrpc.php
- Progressively longer IP bans for repeatedly banned IPs

Cron

- Cron execution time limits to prevent resource exhaustion
- Privilege escalation protection and jailed CLI crons
- No direct CLI cron access for end users, limiting system cron management to administrators

DoS Attacks

- Caching in Layer 7 (the WP level) to protect against Layer 7 DDoS attacks
- Extensive TCP related scalability enhancements to reduce the DoS attack surface
- Substantial optimizations to the server and services to maximize throughput, protecting against DoS attacks and improved handling of IP-based attacks
- Nginx to protect against Slow Loris attacks and further mitigate against other types of DoS or Apache-specific attacks

PHP

- Substantial restrictions in PHP file access locations, allowed functions, upload size limits, script timeout lengths, memory use, and so forth to ensure that the server performance while preventing the execution of many hacker tools. This includes disablement of harmful shell executions and other dangerous functions in PHP.
- Enforced PHP-FPM pool open_basedir restrictions/jail that prevent users from accessing/editing files that are not within their permissions group
- Enforced PHP-FPM dangerous PHP function restrictions/blocks
- Enforced PHP CLI mode open_basedir restrictions/jail that prevent users from accessing/editing files that are not within their permissions group
- Enforced PHP CLI mode dangerous PHP function restrictions/blocks

SSH/SFTP

- Disabled SSH access by default for non-admin users (enabled upon request only)
- SSH key-only access to admin user accounts
- No compiler access for non-admin SSH users
- Forced use of jailed SSH contexts for any non-admin users that have enabled SSH
- Whitelist of approved binaries accessible to non-admins using jailed SSH
- Jailed access to SFTP (prohibits systemwide file access)
- Non-standard SSH/SFTP port to dissuade basic attempts at brute force login
- Limits enforcing modern/strong encryption for all SSH connections

Web

- Strong SSL encryption (Qualys Grade A or better)
- Disabled support for conventional SSL encryption. TLS 1.2 and 1.3 encryption ONLY
- TLS 1.3 replay attack protections
- Modern/strong encryption enforcement for SSL connections
- Symlink attack protections
- CSP and security header defaults (e.g. XFrame-Options, Cross-Origin-Opener-Policy) to dissuade against browser layer attacks (e.g clickjacking)
- Rate limiting and excessive POST blocking (which throttles and/or prevents many types of hacker attack)
- Bogus/invalid request type blocking (e.g. image files can't receive a POST)
- Invalid/rare HTTP method blocking
- Blocks against PHP pathinfo exploitation (e.g. false URLs that try to trick PHP into running when it wouldn't otherwise by using specifically crafted URL formats will fail)
- HSTS support for SSL

Security Support

- 3rd party blacklist removal (e.g. if the site is blacklisted, even false positively)
- Malware removal assistance
- Site-specific security adjustment assistance
- PCI and security scan review/assistance
- Site security/integrity review (by request) if suspicious activity is seen
- Root cause analysis in the event of a site breach

Staff + Staff Access

- A shortlist of admins that have access to our servers
- A strict senior level requirement for all systems and support roles/staff (no junior staff)
- Privilege escalation protection in internal staff tools via enforcement of a "least privilege" approach to account operations
- Regular staff internal software updates (e.g. routine browser updates)
- Firewall use on all internal staff computers
- Ad blockers encouraged for all staff to prevent various types of browser attacks
- Routine internal security discussion, disclosure, or training
- Malicious and spam email filtering for internal staff
- Preference for Mac and Linux desktop (less prone to successful malware attacks when compared to alternatives)
- Security training and orientation amongst staff

Mail

- Outbound mail monitoring to catch and address excessive email script abuse by any tenant (which is often the sign of a hack)
- Outbound spam blocking (e.g drop emails with over 300 recipients, spoofed email addresses, etc)
- Publicly closed mail ports (e.g. SMTP, POP, IMAP). In other words, no open relay.
- SPF and DKIM support for improved deliverability

Logging

- Suspicious activity logging
- Server uptime/availability monitoring allows for prompt staff response in the event servers become unavailable
- HIDS for intrusion detection and automated response
- Logging of source IP and URL for requests that produce outbound mail
- High CPU use monitoring/auditing and response (prevents ongoing abuse of sites)
- High disk usage monitoring and response (prevents space-related crashes)
- High memory monitoring and automated management (prevents DoS through memory exhaustion and other problems)

Miscellaneous

- Ongoing research and development related to security to build new and better IDS type logging, incident response, attack prevention, and quick mitigation