



iThemes Security

Description

ITHEMES SECURITY IS THE #1 WORDPRESS SECURITY PLUGIN

iThemes Security (formerly Better WP Security) gives you over 30+ ways to secure and protect your WordPress site. On average, 30,000 new websites are hacked each day. WordPress sites can be an easy target for attacks because of plugin vulnerabilities, weak passwords and obsolete software.

Most WordPress admins don't know they're vulnerable, but iThemes Security works to lock down WordPress, fix common holes, stop automated attacks and strengthen user credentials. With advanced features for experienced users, our WordPress security plugin can help harden WordPress.

MAINTAINED AND SUPPORTED BY ITHEMES

iThemes has been building and supporting WordPress tools since 2008 like BackupBuddy, our WordPress backup plugin. With our full range of WordPress plugins, themes and training, WordPress security is the next step in providing you with everything you need to build the WordPress web.

GET PLUGIN SUPPORT AND PRO FEATURES

Get added peace of mind with professional support from our expert team and pro features to take your site's security to the next level with iThemes Security Pro.

Pro Features:

- Two-Factor Authentication – Use a mobile app such as Google Authenticator or Authy to generate a code or have a generated code emailed to you.
- WordPress Salts & Security Keys – The iThemes Security plugin makes updating your WordPress keys and salts easy.
- Malware Scan Scheduling – Have your site scanned for malware automatically each day. If an issue is found, an email is sent with the details.

- Password Security – Generate strong passwords right from your profile screen.
- Password Expiration – Set a maximum password age and force users to choose a new password. You can also force all users to choose a new password immediately (if needed).
- Google reCAPTCHA – Protect your site against spammers.
- User Action Logging – Track when users edit content, login or logout.
- Import/Export Settings – Saves time setting up multiple WordPress sites.
- Dashboard Widget – Manage important tasks such as user banning and system scans right from the WordPress dashboard.
- Online File Comparison – When a file change is detected it will scan the origin of the files to determine if the change was malicious or not. Currently works only in WordPress core but plugins and themes are coming.
- Temporary Privilege Escalation – give a contractor or someone else temporary admin or editor access to your site that will automatically reset itself.
- wp-cli Integration – Manage your site's security from the command line.

ITHEMES SYNC PRO INTEGRATION

Manage more than one WordPress site? Manage Away Mode, release lockouts and keep your themes, plugins and WordPress core up to date from one dashboard with iThemes Sync Pro. Start your free trial of Themes Sync Pro.

ITHEMES BRUTE FORCE ATTACK PROTECTION NETWORK

iThemes Security takes brute force attack protection to the next level by banning users who have tried to break into other sites from breaking into yours. The iThemes Brute Force Attack Protection Network will automatically report IP addresses of failed login attempts and will block them for a length of time necessary to protect your site based on the number of sites that have seen a similar attack.

PROTECT

iThemes Security works to protect your site by blocking bad users and increasing the security of passwords and other vital information.

- Prevents brute force attacks by banning hosts and users with too many invalid login attempts
- Scans your site to instantly report where vulnerabilities exist and fixes them in seconds
- Bans troublesome user agents, bots and other hosts
- Strengthens server security
- Enforces strong passwords for all accounts of a configurable minimum role
- Forces SSL for admin pages (on supporting servers)
- Forces SSL for any page or post (on supporting servers)
- Turns off file editing from within WordPress admin area
- Detects and blocks numerous attacks to your filesystem and database

DETECT

iThemes Security monitors your site and reports changes to the filesystem and database that might indicate a compromise. iThemes Security also works to detect bots and other attempts to search vulnerabilities.

- Detects bots and other attempts to search for vulnerabilities.
- Monitors filesystem for unauthorized changes.
- Run a scan for malware and blacklists on the homepage of your site.
- Receive email notifications when someone gets locked out after too many failed login attempts or when a file on your site has been changed.

OBSCURE

iThemes Security hides common WordPress security vulnerabilities, preventing attackers from learning too much about your site and away from sensitive areas like your site's login, admin, etc.

- Changes the URLs for WordPress dashboard areas including login, admin and more
- Completely turns off the ability to login for a given time period (away mode)
- Removes theme, plugin, and core update notifications from users who do not have permission to update them
- Removes Windows Live Write header information
- Removes RSD header information
- Renames “admin” account
- Changes the ID on the user with ID 1
- Changes the WordPress database table prefix
- Changes wp-content path
- Removes login error messages

RECOVER

iThemes Security makes regular backups of your WordPress database, allowing you to get back online quickly in the event of an attack. Use iThemes Security to create and email database backups on a customizable schedule.

For complete site backups and the ability to restore or move WordPress to a new host or domain, check out BackupBuddy.

OTHER WORDPRESS SECURITY BENEFITS

- Makes it easier for users not accustomed to WordPress to remember login and admin URLs by customizing default admin URLs
- Detects hidden 404 errors on your site that can affect your SEO such as bad links and missing images

COMPATIBILITY

- Works on multi-site (network) and single site installations
- Works with Apache, LiteSpeed or NGINX (Note: NGINX will require you to manually edit your virtual host configuration)
- Features like database backups and file checks can be problematic on servers without a minimum of 64MB of RAM.

All testing servers allocate 128MB to WordPress and usually don't have any other plugins installed.

TRANSLATIONS

- Spanish by Andrew Kurtis

Please let us know if you would like to contribute a translation.

WARNING

Please read the installation instructions and FAQ before installing this WordPress security plugin. iThemes Security makes significant changes to your database and other site files which can be problematic, so a backup is strongly recommended before making any changes to your site with this plugin. While problems are rare, most support requests involve the failure to make a proper backup before installation.

LICENSE

Released under the terms of the GNU General Public License.

FAQ

Why does iThemes Security require the latest WordPress version? Can't I use a slightly older version?

One of the best security practices for a WordPress site owner is keeping software up to date. Because of this, we only test this plugin on the latest stable version of WordPress and will only guarantee it works in the latest version.

Will this plugin completely stop all attacks on my site?

No. iThemes Security is designed to help improve the security of your WordPress installation from many common attack methods, but it cannot prevent every possible attack. Nothing replaces diligence and good practice. This plugin makes it a little easier for you to apply both.

What changes does this plugin make that can break my site?

iThemes Security makes significant changes to your database and other site files which can be problematic for existing WordPress sites. Again, we strongly recommended making a complete backup of your site before using this plugin. While problems are rare, most support requests involve the failure to make a proper backup before installation. **DISCLAIMER:** Under no circumstances do we release this plugin with any warranty, implied or otherwise. We cannot be held responsible for any damage that might arise from the use of this plugin.

Note that renaming the wp-content directory will not update the path in existing content. Use this feature only on new sites or in a situation where you can easily update all existing links.