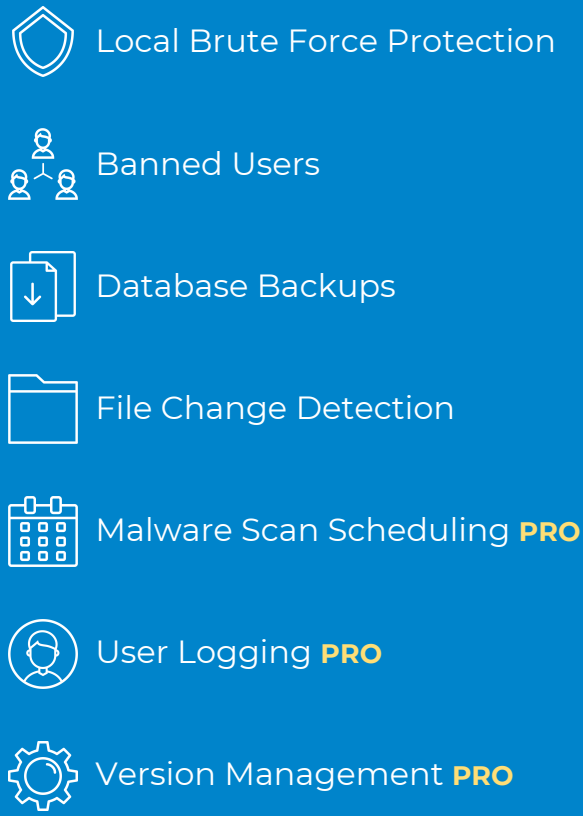
Using WordPress Security Logs to **Secure Your Site**

Adding WP Security Logs

You can use some of the developer functions and filters that WordPress provides to create a logging system, but the easiest way to start a security log is to install a WordPress security plugin like iThemes Security that will automatically keep track of site and user activity.

Once you've installed and activated the iThemes Security plugin, **enable the following features** in iThemes Security to get the most out of your security logs:



4 Important Events to Monitor in WordPress Security Logs

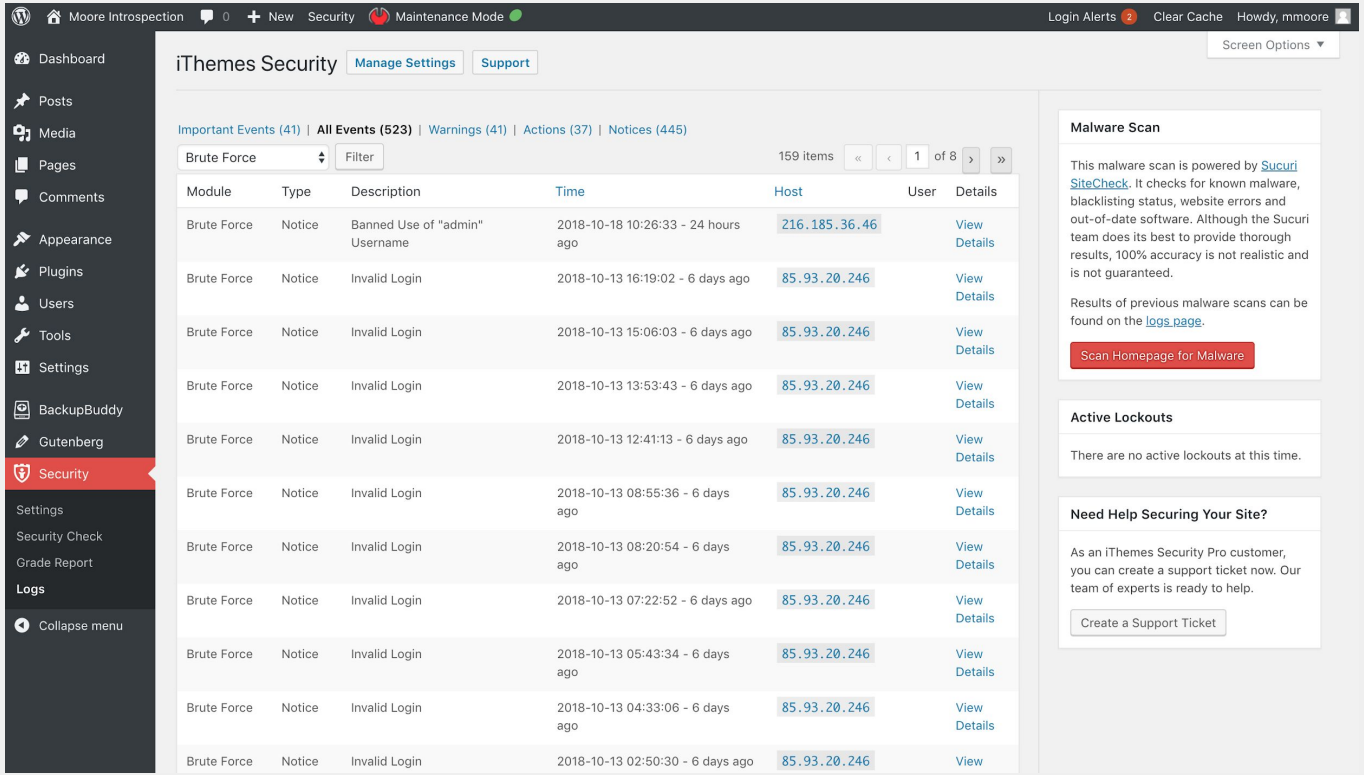
WordPress Brute Force Attacks

File Changes

Malware Scans

User Activity

1. WordPress Brute Force Attacks



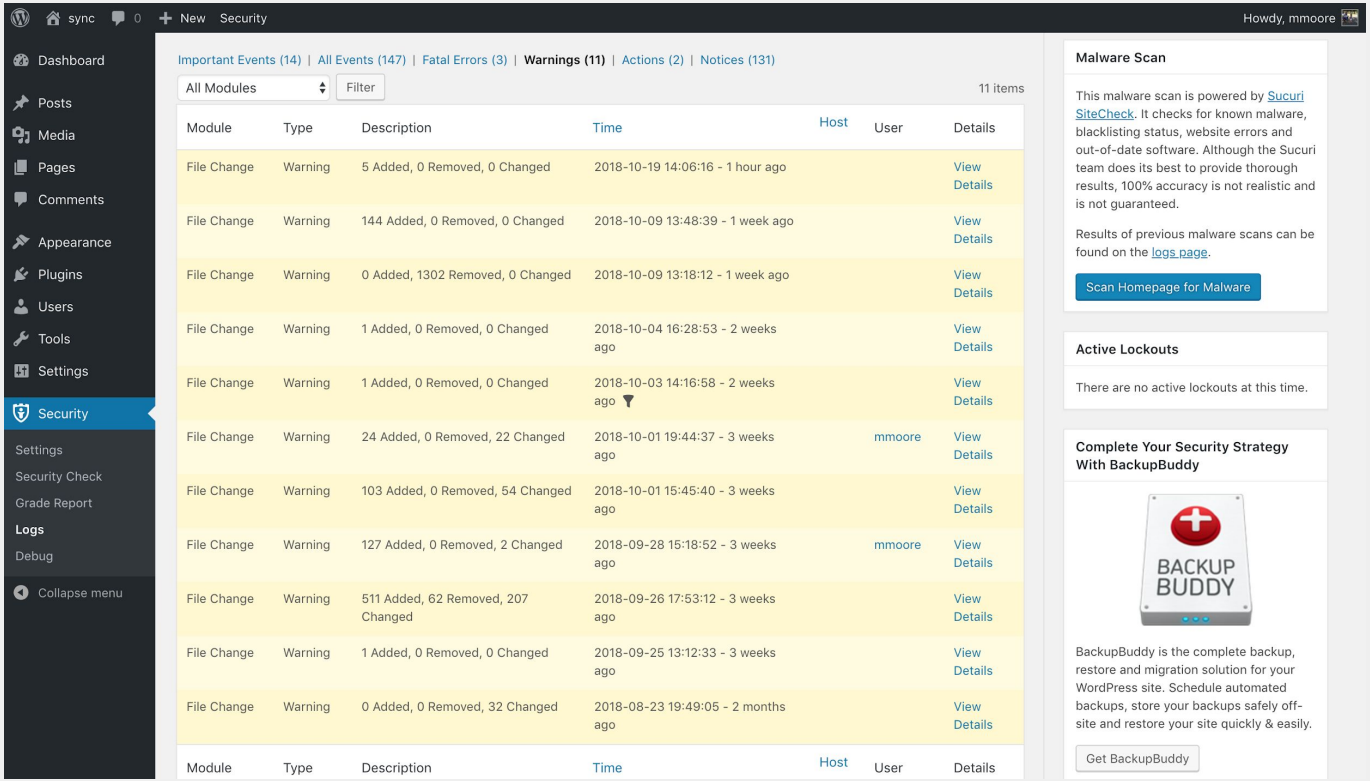
1. WordPress Brute Force Attacks

Brute force attacks refer to the trial and error method used to discover usernames and passwords in order to hack into a website. WordPress doesn't track any user login activity, so there isn't anything built into WordPress to protect you from a brute force attack. It is up to you to monitor your login security to protect your WordPress site.

If you see that a single username or IP has consecutive multiple failed login attempts, the chances are you are under a brute force attacks.

Identifying when you are under a brute force attack is a great start, but there is still more work to be done. You can increase the WordPress login security by limiting the number of failed login attempts a single user or IP is allowed to have before they are blocked from making any more attempts.

2. File Changes



2. File Changes

There are several legitimate reasons you would see new file change activity in your logs, but if the changes made were unexpected, you should take the time to assure the changes were not malicious.

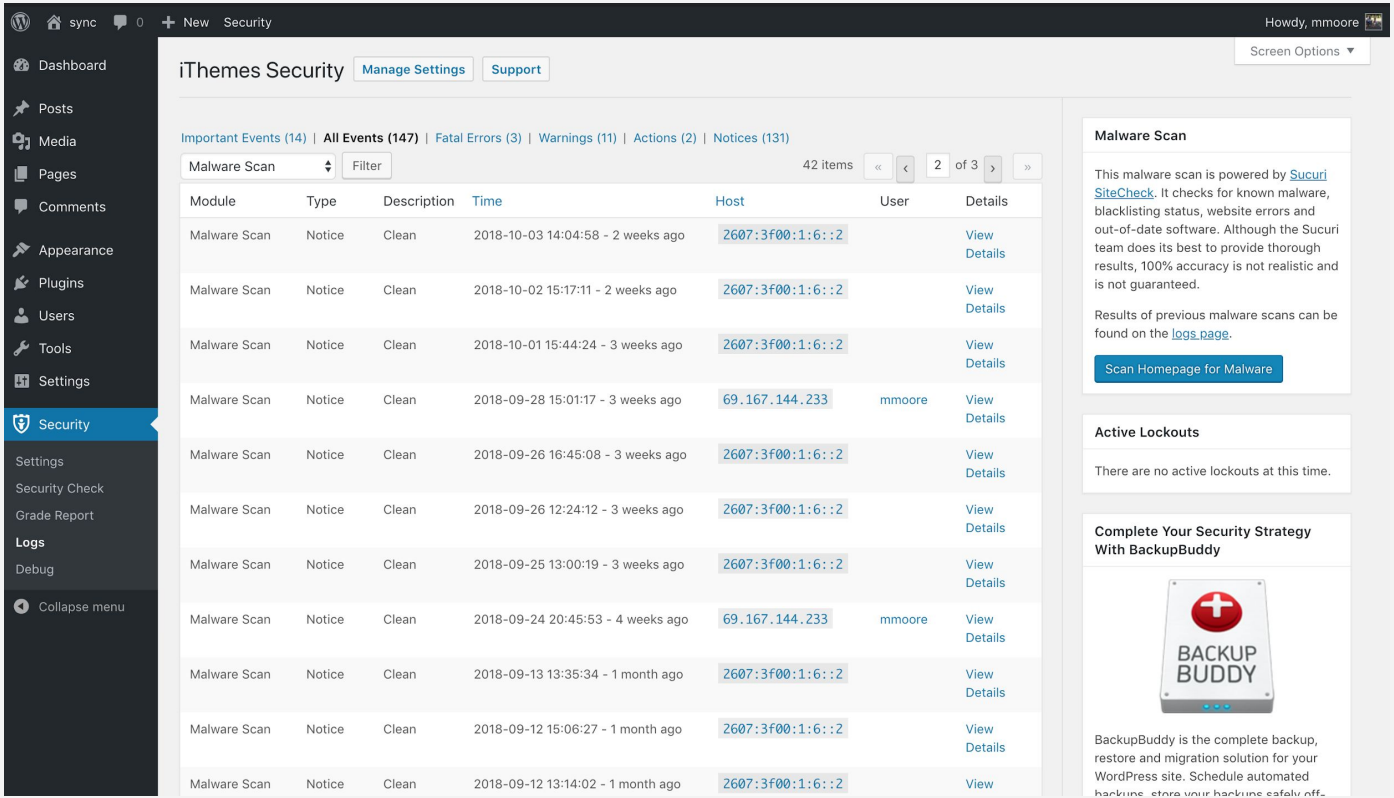
Comparing File Changes

WordPress provides WP-CLI commands to compare the file hashes of core and plugin files easily. For comparing WordPress core files use the wp core verify-checksums command, and for plugins, you can use the wp plugin verify-checksums command. There currently isn't a WP-CLI command to compare theme file hashes, but it is on the roadmap.

Enable the Compare Files Online option in the iThemes Security Pro File Change settings to automatically compare .org and iThemes file hashes.

Compare file changes by comparing differences in a Text Editor.

3. Malware Scans



3. Malware Scans

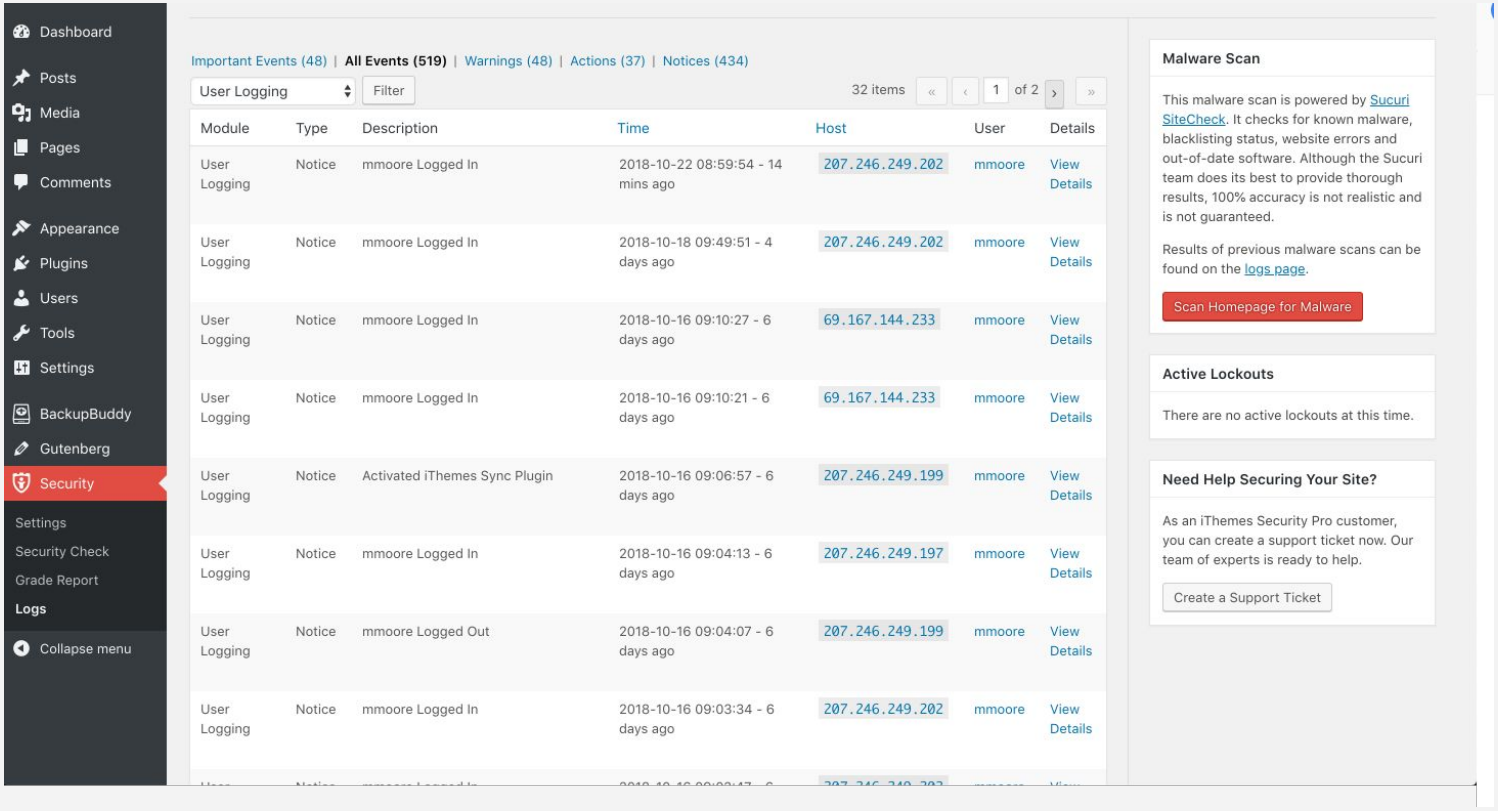
Make sure you have enabled Malware Scan Scheduling in your iThemes Security Pro settings.

It is crucial to be alerted as quickly as possible of a breach to your site. The longer it takes for you to know about a hack the more damage it will do.

Not only should you run malware scans, you should also be recording the results of every malware scan in your WordPress security logs.

Not knowing the scans are failing could result in your site not being regularly scanned for malware.

4. User Activity



4. Type of User Activity to Record

1. Log In / Log Out

3. Adding & Removing Plugins

2. User Creation

4. Changes to Posts & Pages

As we can see, having the right information can help stop an attack, alert you of a breach, pinpoint the time of the breach, access the damage, and help you with cleanup. Use the checklist below to aid you in monitoring your WordPress security logs:

1. Brute Force Activity

2. File Changes

3. Malware Scans

4. User Logging

Download Events to Monitor Infographic.

https://ithemes.com/wp-content/uploads/2018/10/WordPress-Security-Logs.png

Check out WP Security Logs blog post.

https://ithemes.com/2018/10/25/how-to-wordpress-security-logs/

We have a YouTube channel!

http://ithemes.com/youtube