Additional Security Software

- Overview
- APF Firewall
- Atomicorp
- BitNinja
- chkrootkit
- CloudLinux
- ConfigServer software
- CXS
- Imunify360
- KernelCare
- LMD
- Modify the Logwatch configuration file
- Patchman
- RootKit Hunter
- Additional documentation

Overview

This document lists third-party software and modifications that you can install to help secure your server.

Note:
Among the options that this document lists, cPanel Technical Support can **only** provide direct support for CloudLinux™ if you directly license it through cPanel, L.L.C. Otherwise, contact the appropriate software developer for assistance.

APF Firewall

APF Firewall offers an advanced firewall for Linux systems.

For more information about APF Firewall, visit the APF Firewall website at r-Fx Networks.

Atomicorp

Atomicop offers a hardened and secure shell for Linux servers.

For more information about Atomicorp, visit the Atomicorp website.

BitNinja

BitNinja offers a security suite that provides protection against multiple forms of attack.

For more information about BitNinja, visit the BitNinja website.

chkrootkit

The `chkrootkit` shell script examines your system's binaries for rootkit installations. Rootkits allow a malicious user to gain undetected administrative access to the server.

To install the `chkrootkit` script, perform the following steps:

1. Log in to your server as the `root` user via SSH.
2. Run the `cd /root` command to change to the `root` directory.
3. Run the following command to download `chkrootkit`:

```
wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz
```

4. Run the `tar -xvzf chkrootkit.tar.gz` command to decompress the downloaded file.
5. Run the `cd chkrootkit-0.50` command to change directories.
6. To begin the `chkrootkit` installation, run the `make sense` command.

The system will install the `chkrootkit` script on your server.

To run the `chkrootkit` script, run the following command:

```
/root/chkrootkit-0.50/chkrootkit
```

> **Note:**
> We **strongly** recommend that you run the `chkrootkit` script often and add a cron job that runs the above command.

For more information about the chkrootkit script, visit the chkrootkit website.

CloudLinux

CloudLinux offers a secure version of Linux that provides advanced functionality for shared hosting environments. CloudLinux integrates with cPanel & WHM, and it provides detailed resource management tools and other improvements to system management and stability.

You can purchase CloudLinux from the cPanel store. For more information about CloudLinux, visit the CloudLinux website.

ConfigServer software

Many of our Technical Support Analysts recommend that you use CSF (ConfigServer Firewall), a free product that ConfigServer provides. CSF contains a stateful packet inspection (SPI) firewall, a login and intrusion detection mechanism, and a general security application for Linux servers.

To install CSF, perform the following steps:

1. Log in to your server as the `root` user via SSH.
2. Run the `cd /root` command to change to the `root` directory.
3. Run the following command to download CSF:

   ```
   wget https://download.configserver.com/csf.tgz
   ```

4. Run the `tar -xzf csf.tgz` command to decompress the downloaded file.
5. Run the `cd csf` command to change directories.
6. To begin the CSF installation, run the `./install.cpanel.sh` command.

To configure CSF, use WHM's *ConfigServer Security & Firewall* interface (*WHM >> Home >> Plugins >> ConfigServer Security & Firewall*). The installation script should enable the correct ports in CSF, but we recommend that you confirm this on your server.

After you configure CSF, you **must** disable testing mode. To take CSF out of testing mode, perform the following steps:

1. Click *Firewall*.
2. Change the value of *Testing* from `1` to `0`.
3. Click *Change.*

For more information about how to use CSF, visit the CSF website.

> **Note:**
> ConfigServer also provides ConfigServer Mail Queues (CMQ), a free add-on product for cPanel & WHM. The product provides a full-featured interface to cPanel's Exim mail queues from within WHM. For more information about how to install and use CMQ, visit the CMQ website.

CXS

ConfigServer eXploit Scanner (CXS) scans all uploads to a server for malware, and it quarantines any suspicious files. It integrates with cPanel & WHM.

For more information about CXS, visit the CXS website at ConfigServer Services.

Imunify360

Imunify360 offers a security suite that protects servers against a wide range of attacks. It integrates with cPanel & WHM, and it provides reports to the system administrator on the server's status.

You can purchase Imunify360 from the cPanel store. For more information about Imunify360, visit the Imunify360 website.

KernelCare

KernelCare automatically updates your system's Linux kernel without the need for a reboot. It also provides patches that secure vulnerabilities, such as the symlink race condition.

You can purchase KernelCare from the cPanel store. For more information about KernelCare, visit the KernelCare website.

> **Important:**
> You can **only** install KernelCare on systems that run CentOS 6 and CentOS 7.

LMD

LMD offers a shareware malware protection scanner.

For more information about LMD, visit the LMD website at r-Fx Networks.

Modify the Logwatch configuration file

The Logwatch customizable log analysis system parses your system's log files for a given period of time. In addition, it creates a report that analyzes specified data.

If your server does not include Logwatch, run the `yum -y install logwatch` command to install it and any dependences that Logwatch requires.

The Logwatch configuration file exists in the `/usr/share/logwatch/default.conf/logwatch.conf` location.

We recommend that you use a text editor to change the following parameters:

Parameter	Description
`MailTo = user@example.com`	Change the `user@example.com` address to the email address that you wish to receive Logwatch notifications.
`Detail = 5` or `Detail = 10`	Change this parameter to set the detail in the log files. • `5` represents a **medium** level of detail. • `10` represents a **high** level of detail.

Patchman

Patchman detects vulnerabilities in software and sends notices to customers to teach them how to resolve the issue. If the customer does not resolve the vulnerability, Patchman can fix it automatically.

Patchman integrates with cPanel & WHM, and it provides reports to the system administrator on the server's status.

For more information about Patchman, visit the Patchman website.

RootKit Hunter

Important:

- cPanel, L.L.C does not provide RootKit Hunter (rkhunter).
- The Rootkit Hunter project team has not updated rkhunter in over one year.
- You may experience false positives if you use rkhunter. If you need assistance with rkhunter, contact your system administrator.

The `rkhunter` script scans for rootkits and other exploits.

To install the `rkhunter` script, perform the following steps:

Note:
In this section, `version` represents the Rootkit Hunter script's version. You can download the latest version from Rootkit Hunter project's website.

1. Log in to your server as the `root` user via SSH.
2. Run the `cd /root` command to change to the `root` directory.
3. Run the following command to download the `rkhunter` script:

```
wget https://sourceforge.net/projects/rkhunter/files/rkhunter/version/rkhunter-version.tar.gz.asc/download
```

4. Run the `tar -xvzf rkhunter-version.tar.gz` command to decompress the downloaded file.
5. Run the `cd rkhunter-1version` command to change directories.
6. To begin the `rkhunter` script installation, run the `./installer.sh --layout default --install` command.

The system will install the `rkhunter` script on your server.

To run the `rkhunter` script, run the following command:

```
/root/rkhunter-version/files/rkhunter -c
```

For information about how to configure the `rkhunter` script, read the rkhunter FAQ.

Note:
We **strongly** recommend that you run the `rkhunter` script often and add a cron job that runs the above command.

Additional documentation

Suggested documentationFor cPanel usersFor WHM usersFor developers

- Additional Security Software
- CVE-2015-0235 GHOST
- How to Set Up (PHP) Composer
- CVE-2016-3714 ImageMagick
- Third-Party Software End Of Life Policy

- Virus Scanner
- Security Policy
- SSL TLS

- ModSecurity
- Directory Privacy

- Additional Security Software
- CVE-2015-0235 GHOST
- How to Set Up (PHP) Composer
- CVE-2016-3714 ImageMagick
- Third-Party Software End Of Life Policy

- Guide to Third-Party AutoSSL Provider Modules
- WHM API 1 Functions - installed_versions
- WHM API 1 Functions - fetch_security_advice
- WHM API 1 Functions - get_autossl_log
- WHM API 1 Functions - get_autossl_providers