Critical Steps to Secure Your Linux VPS

A Comprehensive Guide to Securing a Managed or Cloud Linux VPS.

inmotion hosting

Contents

Introduction

If you or your client had a catastrophic server failure, would the data be safe? Could you restore files in accordance with your **recovery time objective (RTO)** and other aspects of your **business continuity plan (BCP)**? What are the costs of all your clients' data if all that information was gone tomorrow? Your investment in building, promoting, and collecting valuable data for your business or your clients are likely extremely significant.

Protect your investments with advice and assistance from our in-house system administration experts in **Managed Hosting** who specialize in server configuration and optimization.

Securing your **Linux virtual private server (VPS)** takes specialized knowledge, technical savvy, and ***a lot of time***. Imagine cutting down multiple hours into a fraction per week to secure, update, and protect your data on a Linux VPS. Configuring the server to provide automated email reports for the server or website health, along with many other best practices covered here, will assist you in remaining proactive against threats from vulnerabilities presented by outdated, misconfigured, or initially insecure server functions and applications. Sure, getting this configured initially is challenging, but the reward is better peace of mind.

Here's who should be reading this eBook:

- Anyone **new to Linux** that wants to understand basic security measures.
- Shared Hosting users curious about the security advantages of VPS Hosting.
- Anyone with a website wanting to be proactive in protecting their intellectual property against theft.
- Linux VPS users wanting to understand the power of root access better.
- New Linux system administrators (sysadmins) who want to learn how to secure their own or their customers' data.

Welcome to **Critical Steps to Secure Your Linux VPS Server**. This guide introduces essential server hardening tasks recommended by our in-house technical experts for you to learn and implement. The information within this guide will give you insight into your Linux VPS security implementation and keep your (and your client's) data safe.

When it comes to security, there are no shortcuts.

Here's What You'll Learn

This guide aims to give you an easy-to-follow guide allowing you to implement better security on your webserver to protect your hosted data. This entry-level guide will introduce you to concepts and strategies for securing your web server and websites from intruders with topics ranging from strong passwords to port management.

You'll learn:

- **Essentials for securing your Linux VPS**
- **Importance of software updates and management**
- **Why passwords are great, but not the entire answer**
- **Server backup basics**
- **Steps to create a great base to build your security pathway**

A quick note before we begin. As you learn from the guide's steps for protecting your VPS, keep in mind that this knowledge applies to most managed Linux VPS servers. At times, we may cover info specific to the most popular operating systems (OSs), or distributions (distros), which we support - **Debian**, **Ubuntu Server**, and **CentOS**.

All command line interface (CLI) utilities listed within this guide should be executed by system administrators or power users with root permissions. Always create a full backup before making major changes, and when in doubt, test in a development environment such as a staging server or OS testing platforms such as **DistroTest.net**.

Important Links to Bookmark

- **VPS Product Guide**
- **Online Support Center**
- **SANS Security Awareness**

The Single Mistake Hindering Your Security

Everything you have built, stored, and launched on your server is at risk. Cybercriminals - black-hat hackers, social engineers, hacktivists, etc. - are always on the lookout for "soft" targets. Cybersecurity and IT specialists review the **National Vulnerabilities Database (NVD)**, **Common Vulnerabilities Exposures (CVE)**, and similar resources to learn about new bugs and mitigate them. However, malicious users do so to find vulnerabilities to exploit. With a mantra of no rules and total disregard for everyone's digital safety, criminals can steal your data without ever physically invading your home or person. This is frustrating, inconvenient, and fundamentally ground-breaking for all involved - the victim, developers for any software exploited, businesses you trusted to secure your data, and users.

At the climbing rate of cyber intrusions as of 2020, much of your data may have already been compromised regardless of how much you do to **secure your web activity**—months or perhaps even years of work. You don't want to be in a position to have to notify co-workers or clients that information was stolen because you failed to implement basic security measures.

> **The single mistake hindering security is people assuming cyber attacks will not happen to them.**

No one is ever truly 100% secure. With this guide's help, you can apply security measures at every network point to defend in depth hardening of your server and data.

> **Human error and social engineering are dynamic issues. The moving target of human error and the tactics of social engineering can be extremely clever. They can defeat even the latest security technologies and processes you have in place. Security goes beyond the hardware. Security is also human psychology.**

Note: Social engineering is the act of psychological and/or emotional manipulation of others into releasing confidential information to unauthorized personnel. Phishing, commonly combined with spoofed email, is the most common method for initiating social engineering attacks.

Linux Server and Security Environment

It all starts with the closed (proprietary) or free open source software (FOSS) on your Linux server. We prefer human-centered technology that is simple, maintained by technical experts passionate about it and its communities. The Linux kernel and the countless operating systems that run on it (over 300 listed at **wikipedia.org**) are FOSS created by communities of dedicated developers. They support the movement of software that's available to everyone regardless of financial status. Some of the most popular FOSS projects as of 2020 also include:

1. **WordPress** and **Drupal** content management systems (CMS)
2. **LibreOffice** office suite, a popular successor to OpenOffice
3. **Mozilla Thunderbird** desktop email client
4. Matomo **web analytics** application
5. **Firefox** internet browser

Open source code is more secure than its proprietary counterpart because it encourages others to find and contribute bug patches. The reason many big organizations create open source projects is due to a few key factors. Open source is free, diverse testing and outsourced community support.

OPEN SOURCE SOFTWARE
Supported by a community of accessible developers and users dedicated to improving the product with forums and Freenode internet relay chat (IRC) channels; many times, they are openly managed on project management systems, including Github, GitLab, and Launchpad.

PROPRIETARY SOFTWARE
When software is under a Proprietary license, source code is typically not available. This restricts the ability to audit the source code for security issues, or maintain it should the license holder(s) abandon it.

Like customer service, security is everyone's job. Everyone within communities and organizations should be trained to report suspicious online activity to website owners and management. Yet, despite companies' best efforts, so many of them often get hacked. A single device, process, software, or hardware can NOT fully protect your data. Better security requires a thorough defense-in-depth approach, starting with user security awareness training.

Security Basics: Software Updates, Server Backups, and Strong Passwords

Cyber intrusions have only risen as more organizations move data to cloud-based solutions. There are multiple factors that affect this:

- IT specialists, whose primary focus is on maintaining tech infrastructure, taking on cybersecurity duties that require more dedicated time and resources than allotted, such as incident response
- Undermanned, if present, cybersecurity staff
- Cybersecurity specialists undertrained and not supported with educational opportunities (e.g., refresher training time, industry, certifications, and degrees)
- Senior management not fully supporting and investing in security awareness training, diminishing possible improvements in taking cybersecurity more seriously
- Belief that responsibilities regarding security and backup related issues rest solely on a third party (e.g. web hosting company, security, and backup software vendor), an uninformed method of risk transfer and risk avoidance
- Belief that their data or company's data isn't valuable enough to be a valuable target

Phishing and credential theft have made up a greater percentage of malicious attacks over the last few years, according to the Verizon 2020 Data Breach Investigation Report (DBIR).

Cybersecurity and IT specialists must have support from senior management within an organization to make security a priority.

Below are some general guidelines to protect your organization's data against cyber attacks:

	Only grant root (sudo) permissions to those who need it when needed
	Remove unneeded user accounts promptly. Suspend users accounts during vacations to reduce account-based hacks
	Uninstall unused and unmaintained software to prevent cyber attacks resulting from older, well-known vulnerabilities
	Implement forced vacation policy to ease investigating insider attacks, espionage in employee's absence; also helps identify single points of failure
	Implement job rotation to mitigate single points of failure with vital tasks for when employees leave the company. Enforce separation of powers to ensure no single person has unlimited access without assistance and official documentation from another employee
	Close unneeded listening ports, including unencrypted POP3 (110) or IMAP (143) email protocols when applicable to reduce vulnerability to cyber attacks. • Use port scanners (e.g. Nmap) to see what info others can easily find • Use CLI tools such as lsof, ss, and netstat for more information
	Check server logs - cPanel access, error_log, Exim (email) - regularly for suspicious activity including IP address locations, brute-force login attempts, Business email compromise (BEC) / phishing / spam emails , etc.

Tech Tip: Be careful about when you reboot your server. It may clear important logs that could help you troubleshoot issues. Instead, try restarting specific services first.

Software Management

Software Installation

It's important to ensure any software you wish to install, and it's developers, have clear legitimacy before adding what could, in the worst case scenario be little more than **spyware** sending data from your systems elsewhere without your knowledge. There are many ways to verify a downloadable application is valid and benign:

1. What's the reputation of the developers and/or company maintaining it? Do they have a history of falling victim to cyber attacks or selling user information? How active are they on social media? Do they support a political stance that you don't? Do you feel like you can trust them?
2. Check with social media, forums websites, and IT professionals about prior experience and reviews with the software.
3. Is the software available on a reputable software downloading site like **SourceForge.net**? Are there a lot of views? Any complaints of malware?
4. When was the latest software version released? Is there a changelog or other way to see how often the application is updated?
5. Test the application download link on **VirusTotal.com**.
6. Do they have **checksums available** for you to verify upon download?

Introduction to Software Updates

Updating is an essential part of any software - web apps, OS, IT hardware, etc. From the firmware to specific drivers - anything you have installed likely needs to be updated at some point, even tech that doesn't receive updates. Server and software updates are a necessary evil in the business of today's digital world. Almost all industries across the globe rely on some sort of software:

- Email
- Databases
- Online portals
- And solutions that integrate these related protocols into a web application, **project management (PM)** and **customer relationship management (CRM)** solutions, and more

Whether software is open-source or proprietary doesn't matter. Software needs to be updated to mitigate found vulnerabilities. And you should aim only to use software that's actively maintained. If not, check whether something else you're already using can take over that function to mitigate new vulnerabilities. In many cases, you will. For example, you could configure automated Linux server backups with **checksum validation** using a cron job and the tar command.

Information technology has vulnerabilities that can potentially exploit or extract unauthorized information at all layers:

- Hardware firmware and BIOS (e.g. Intel processors had **Meltdown/Spectre** in 2018)
- OS kernels (e.g., **Thunder Spy** Thunderbolt vulnerability discovered in 2020)
- Operating system (OS) or distribution (distro) pre-installed software
- Applications (including the **cPanel** software itself)
- Actual user via social engineering, user error, etc.

Many maintainers of popular software are proactive with handling zero-day security issues. However, some end users see patches - security, performance, and just in general - as inconveniences. Some even ignore significant upgrades like new OS versions. This is common with **e-commerce** companies worried about updates disrupting customer user experience (UX) and sales.

This dangerous view towards updates leads to outdated software vulnerable to known exploits.

InMotion Hosting has custom internal scripts to assist customers with common tasks within cPanel managed VPSs (e.g., fix permissions, install optimized NGINX).

Backup Solutions for Disaster Recovery

Before you start major software updates, you need to make sure that you have an up-to-date full backup in case anything goes wrong during the process. Furthermore, you should've verified that backups aren't corrupt and extract data correctly without issues. Otherwise, you risk having to use digital forensics tools (or services) to recover lost data or start over.

> **Before you update any server, apply the 3/2/1 rule to prevent a data loss disaster. After all, backups and software updates go hand in hand.**
>
> **The 3/2/1 backup rule -**
>
> **(3) Three copies of data stored on...**
> **(2) Two different types of media (e.g., remote server and local external drive) with**
> **(1) One complete server backup stored off-site in a remote location (especially important in the case of natural disasters such as flooding)**
>
> **AUTOMATE AND VERIFY YOUR BACKUP PROCESS**
>
> **What is your website and data worth to you? Chances are, it's priceless. Verify all your backups and make sure they are in a secure area.**

Most updates are bug fixes for discovered vulnerabilities, possibly from the **National Vulnerability Database (NVD)**, **Common Vulnerabilities and Exposures (CVE)**, or other repositories which focus on specific software (e.g., **WPvulnDB.com** for WordPress core, plugins, and themes).

Backups are a vital part of any **disaster recovery (DR)** plan. Imagine a scenario where your VPS is compromised past the point where it can be cleaned manually or with services like **Sucuri** and **SiteLock** within a reasonable amount of time. A recent backup allows you to simply wipe your system(s) and restore from a last known good restoration point to recover quickly.

Always report cyber intrusions to your web hosting companies for further assistance. Even if they're unable to assist you in-depth, it'll help them investigate the infection's severity and spread.

Backups

File backups are copies of your data, usually to one or more compressed tar.gz or zip files. Backups allow admins at each level to restore specific or full data as needed. It's best to have weekly and monthly backups to ensure you can restore recent data if a cyber intrusion is found later. There are multiple data backup types:

Website backups, if using a CMS like WordPress or Drupal, may be handled with a third party plugin or module. We recommend **Total UpKeep** for WordPress and **Backup and Migrate Module** for Drupal. PrestaShop, **Opencart**, **Grav**, and some other CMSs have pre-installed features to export data. Linux VPSs include **tar**, **zip**, and **cron** CLI programs for manual backups as well.

Database backups - MySQL/MariaDB, PostgreSQL, **MongoDB**, etc. - can generally be created in the same multiple ways:

1. The website / CMS using it via native features or additional plugins
2. Respective CLI commands
3. Database management graphical user interface (GUI) software, for example:
    e. MySQL - **phpMyAdmin** server software or **MySQL Workbench** desktop software
    f. PostgreSQL - using **phpPgAdmin** server software or **pgAdmin** desktop software

Self-hosted analytics software, including **Matomo Analytics**, often use databases to store information.

Softaculous Instant Installer, available for purchase with our managed VPS and Dedicated server hosting, deserves a quick mention for two reasons:

1. Softaculous creates and manages websites and applications installed on cPanel servers
2. Some users may consider Softaculous **backups** more user-friendly than cPanel backups

cPanel has many ways to backup data depending on your level of access.

- cPanel users can use the **Backup** and **Backup Wizard** features to manually create and restore the account or partial data (files or databases)
- System administrators with Web Host Manager (WHM) access can **schedule automated cPanel backups** and full server backups to a specified backups folder or remote servers using FTP, Amazon S3, Google Drive, and more
- InMotion customers can purchase our Backup Manager for **cPanel** and **WHM**, which allows users to automate backups and restore specific files easily

Full server backups include all files on the server. Server backups can be achieved with pre-installed command line tools like **rsync**, tar, and zip. You can create scheduled tasks with these tools using **cron jobs** or try a CLI application such as **Rclone** or **restic**.

Differential backups include all changed files since the last full backup. For example, let's say you create a full backup on Sunday night and differential backups all other nights. If you need to restore data on Friday afternoon, you'd only need to restore your last full backup and Thursday's differential backup. The disadvantage is that restoration time increases as the differential backup overwrites original files from the previous full backup.

Incremental backups include all changed files since the last backup - full or incremental. Imagine the example from earlier, but instead of differential backups, you create incremental backups all other nights. If you need to restore data on Friday afternoon, you'd need to restore the full backup and the four incremental backups from Monday to Thursday. This can take longer than a full backup and latest differential backup, assuming all backups work.

Snapshots

Snapshots are different from the backup types described above in one significant way. Instead of a copied archive of all data, a snapshot is a single image file of your entire machine. This is different from a full server backup, a compressed archive file you can open to extract specific files. Snapshots can be quickly restored after a major configuration test or malware infection.

There are some key considerations for using snapshots:

1. You can't restore single files from a snapshot - only the entire snapshot
2. Because it's a single file, any corruption can affect multiple essential files, rendering the snapshot useless
3. In many cases, there's no way to test the snapshot before restoring it

Here's a recommended process for testing backup integrity:

1. Create the backup
2. Attempt to restore the backup on another machine or virtual machine in a testing environment to verify the backup works
3. Copy the backup file to other locations
4. Verify the backup files haven't changed while copied to other machines with **checksums** (e.g., SHA512 and RIPEMD)

If you use a third-party service for backup services, you should still maintain your backups and ensure you understand their terms and conditions.

Firewalls

A firewall is a network security component that controls incoming and outcoming network traffic. Firewalls are generally placed at one or more advantageous positions for maximum effect:

- Network firewalls are dedicated hardware such as the Cisco ASA 5506, available with our **Dedicated server hosting** or software on gateway machines such as routers and wireless access points (WAPs)
- Host-based firewalls are software installed on host machines (e.g., web servers and personal computers)
  - Linux **GUFW** and Firewall-config for **Firewalld**
  - **macOS Application Firewall**
  - BSD-based **pfSense**
  - **Windows Firewall**

For the focus of this eBook, we'll focus on host-based Linux server firewalls. Although we cover multiple firewall applications below, you only need a single firewall application to manage your VPS.

The **Iptables** program is pre-installed on Linux systems to manage the kernel-level packet filtering system netfilter. Because Iptables can be cumbersome to learn, we recommend installing one of the other firewall applications below to manage it. These firewall applications are easier to configure and allow you to maintain template configurations (e.g. one for production and application testing). Here are some popular Linux firewalls for cPanel/WHM or CLI:

- Uncomplicated Firewall (UFW)
- Advanced Policy Firewall (APF)
- ConfigServer Security & Firewall (CSF)
- Firewalld

Uncomplicated Firewall (UFW)

Uncomplicated Firewall (UFW) is preinstalled on many Linux OSs to manage the netfilter firewall instead of more difficult Iptables commands. It can be beneficial to understand basic UFW for that reason if, for any reason, you're "unallowed" to uninstall it. UFW is also commonly installed with Linux desktop distros where users can manage it with the **GUFW** GUI application.

Advanced Policy Firewall (APF)

APF is preinstalled on our **Managed VPS hosting** plans to enable you to **allow, block, and unblock IP addresses**. However, APF has a shortlist of CLI capabilities and WHM (**whitelist an IP address for SSH access**). For this reason, we often recommend server administrators serious about security uninstall it and instead use one of the other options below.

ConfigServer Security & Firewall (CSF)

Security & Firewall (CSF), developed by **ConfigServer**, isn't just a firewall but a suite of security tools available on over a dozen different OSs (including CentOS and Ubuntu) and virtualization platforms. Many users prefer CSF over others for a few reasons:

1. It's easy to use with straight-forward documentation online and within firewall files (mainly csf.conf)
2. Managed VPS administrators can take advantage of CSF's GUI plugins' capabilities for **cPanel**, **Webmin**, **Vesta Control**, etc.
3. Helpful server security features
    e. View open ports in real-time
    f. Check if your IP(s) are in real-time blackhole lists (RBLs)
    g. Temporary IP allow/block rules
    h. Use IPset to block multiple IPs at once
    i. And so much more

This long list of features and capabilities makes CSF a great cross-platform option you can learn and use on multiple server environments. For updates on new CSF features, follow the **ConfigServer blog RSS feed**.

Tech Tip: View a list of supported OSs on ConfigServer's website. Our Managed Hosting team recommends installing CSF to configure firewalls.

Firewalld

Firewalld has grown in popularity since its creation in 2011. The significant advantage with Firewalld is ruleset changes are updated without closing current sessions with the system. Linux desktop users can also manage Firewalld with the **Firewall-config GUI application**.

Hackers have a range of tools to test firewall misconfigurations and vulnerabilities including Nmap and Kali Linux. You can use them to harden your systems.

Keep in mind, there are several security options that we did not cover such as IP6Tables and NFTables.

SSH Key - The CLI Key to the Castle

As you may have heard, the command line is generally more powerful than the GUI. Sometimes, you'll need to leave the cPanel/WHM GUI to manage your VPS with Secure Shell (SSH).

Secure Shell (SSH) is a command line application for connecting to remote machines. It runs on port 22 by default. The terminal can be intimidating for new users but it's important to remember that it gives you access to a lot more capabilities than cPanel, WHM, and GUIs in general. Some common task examples that are generally faster in CLI for experienced users:

- Scheduling automated tasks (e.g. cron jobs)
- Chaining multiple commands together (similar to macros in office suite applications)
- In-depth details on changes in real time (e.g. server logs and resource management)
- Full control to customize changes throughout the Linux OS (including the kernel on dedicated servers)

What is a Secure Shell (SSH) key?

An SSH key is one of the most popular identities, access, and server authentication management applications used by businesses of all sizes. SSH keys are encrypted using a public key infrastructure (PKI) to grant access and granular control to various server privileges for the end-users. Two types of SSH keys can be created, password-based and numerical (key-based) based. Both types of SSH keys can work on your server. The beauty of SSH is you can control access to a group, a particular user, and even limit the number of login attempts.

Why use SSH?

SSH provides end-to-end encryption for communication with a server. It's more secure than file transfer protocol (**FTP/FTPS**) and easier to set up than SFTP. Even when you're unable to access a website in your web browser, SSH may be a valuable option for gaining access and resolving the issue(s).

How do I use SSH?

When setting up SSH access to a VPS, once you **create an SSH key** and **whitelist your IP address** to connect to your VPS, that key pair becomes a major component of your security. That file grants access to your data on that server. For that reason, you should use a **strong passphrase** (password) for multi-factor authentication:

1. Something you have (SSH file)
2. Something you know (SSH passphrase)
3. Somewhere you are (whitelisted IP address)

Password Authentication or SSH key only?

Completely **removing the password authentication option** is an advanced way to prevent brute-force password attacks on your system. Removing the option can supplement brute-force login protection with software like fail2ban (discussed later) by requiring the user to have a private key file to match a public key file already on the system.

Before you begin, please make sure to review these items carefully

	Use a strong passphrase for additional security in case the key files are hacked.
	Ensure key files aren't stored in shared folders for user accounts on your computer.
	Consider storing SSH keys in an encrypted virtual drive (e.g., **VeraCrypt**).
	Use a password manager (e.g., **Keepass**, **LastPass**, **Bitwarden**, **Dashlane**).
	**Check cPanel and other server logs** (e.g., cPanel access, error_log, email logs) regularly for suspicious activity - IP addresses from other regions, attempted usernames in brute-force attacks.

Perception and Knowledge of IT Threats: The Consumer's Point of View found that 71% of respondents rely on their memory to recall passwords. 61% of consumers reuse passwords on multiple websites.

	**Change the default SSH port** from 22 to a rarely used port and close 22 to mitigate SSH-based cyber attacks.
	To further restrict SSH access, set your SSH port to only allow connections from whitelisted IPs.
	Only open the necessary ports in your firewall.
	When possible, set open ports before you apply firewall rules. Otherwise, you may lock yourself out of your server and need to reset the server to regain access.
	Use banner grabbing tools like Nmap and the Wappalyzer browser extension to see what info is readily available on your website and server.

Top Tips to Set a Strong Password

If you're using a password manager, use it to create complex passwords with a specified length and special, numerical, upper-case, and lower-case characters.
Try muscle memory instead of remembering a long password. Place your hands on the keyboard and create typing movements that you can remember. For some, this is easier than remembering the password itself.
Combine phrases that may make sense to you but not others or an algorithm (e.g., 3@rThC(o)p80W3).
Just say no to the dictionary. No word combinations, abbreviations, or other sequences which are all letters. Remember to mix it up.
Pop culture should not live with your passwords. Avoid references to movies, themes, characters, and anything well known about you and your interests.
Avoid basic number replacements. Replacing the letter "E" with the number "3" is not a safe bet.
Create a sequence that can be impossible to guess to **mitigate rainbow password attacks**. For example, Rm/8R75'G*NX is a much better password than Impa$$able.
Never use the same password twice.

Passwords are not that secure.
According to a survey from PCMag,
35% of people never change their passwords.

Other Tools to Secure Your Linux VPS Hosting

By default, your Linux server is configured to have excellent protection right off the shelf. But, it never hurts to have more of a very good thing. Below are some other options to harden your server security.

Fail2Ban

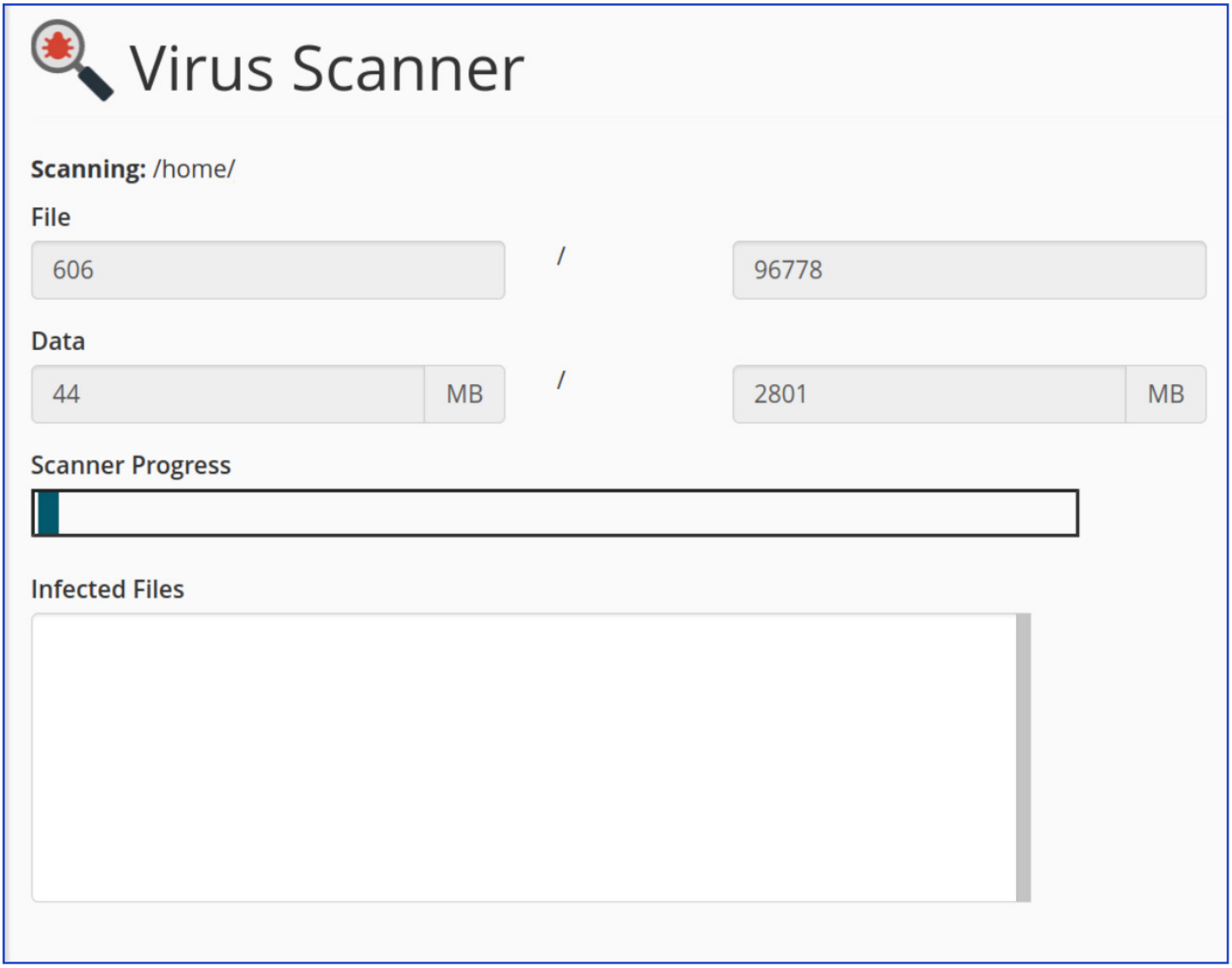
Fail2Ban is one of the most essential and popular brute force login prevention applications. It is available in repositories for many Linux OSs. It is a FOSS application that detects brute force attacks by scanning your server logs and banning **IP addresses** that demonstrate malicious behavior. That's why **we use it**.

Antivirus (AV) Scanners

It's important to have a server-level AV scanner that removes malicious files. We recommend using one or more of the following.

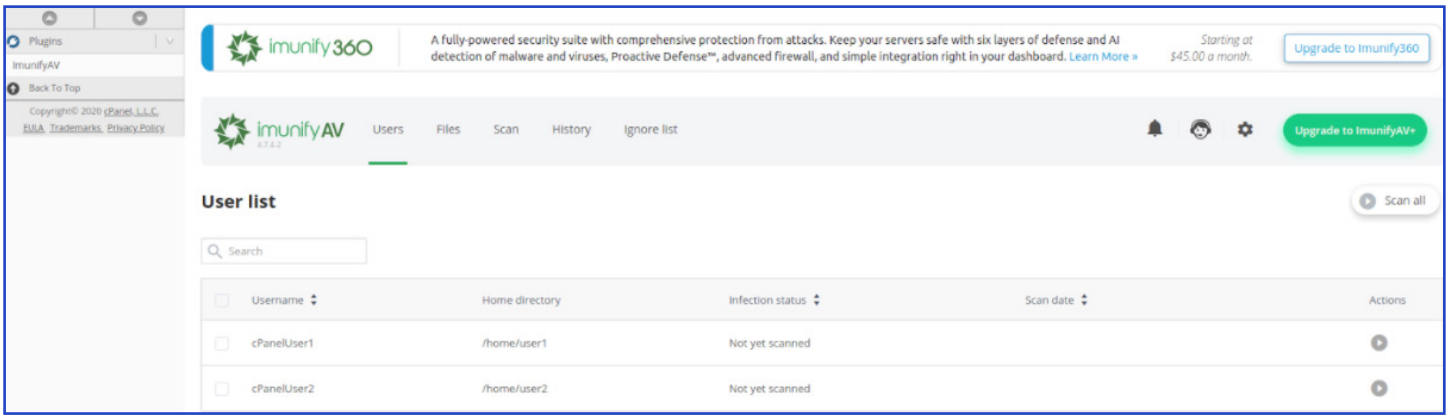
ClamAV

ClamAV allows users to scan their mail, home directory, full account, and even remote locations. The **ClamAV CLI application** includes more configuration options, while the **cPanel plugin** enables local scans. ClamAV can also integrate with many other web applications, including **Nextcloud** file hosting software and **Mattermost** online communication system, to prevent users from uploading infected files to your server.



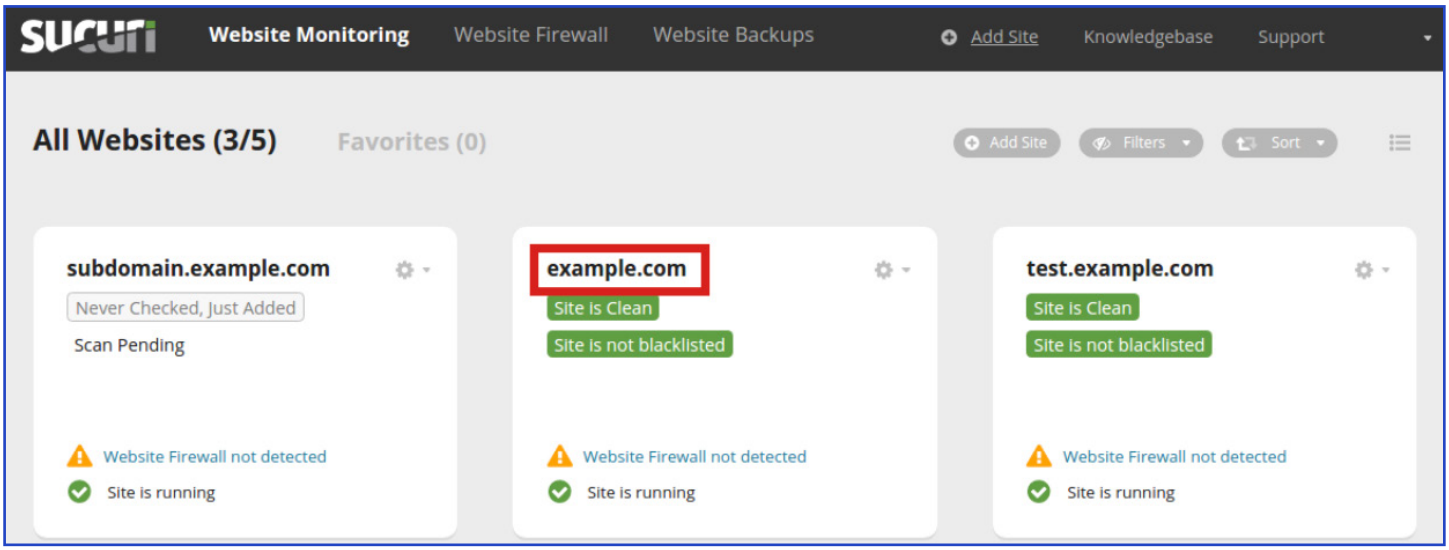
ImunifyAV FREE

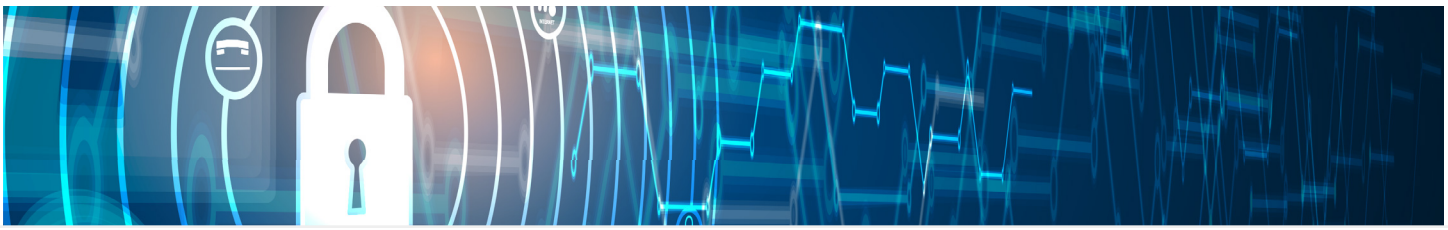
Compared to the ClamAV cPanel plugin, the **ImunifyAV** FREE **cPanel plugin** provides more features such as scheduled background scans and resource consumption options. ImunifyAV FREE includes a **CLI application** as well with additional options.



Sucuri Web Application Firewall (WAF)

Sucuri web application firewall (WAF), unlike the self-hosted software above, is an external web application placed between users and your VPS for server security via DNS. **Sucuri** is a security company we partner with to offer you the latest malware protection, recovery, and monitoring services.





PHP Versioning

PHP (PHP: Hypertext Preprocessor), the “P” in the LAMP stack, is used alongside HTML in web development with a lot of popular content management systems (CMSs) and software today (some of which we mentioned earlier):

WordPress	**Drupal**	**PrestaShop**
Nextcloud for collaboration	**phpBB** for forums	**Zenphoto** for photography
Kanboard kanban project management software	**Moodle** for learning management systems (LMSs)	**Joomla**

Because PHP is tightly integrated with server software and websites, it’s important to **use the latest version possible**. cPanel stops supporting outdated PHP versions shortly after the end of life (EOL).

cPanel users can change the PHP version for the entire account or websites individually with cPanel **MultiPHP Manager**.

WHM users with root access can do the same and change the default PHP version in WHM **MultiPHP Manager.**

Tech Tip: Follow the Official PHP Twitter for new versions updates!

The goal should be to only have the latest PHP version installed. Below are our recommendations for upgrading your server PHP version:

1. Install the latest PHP version in WHM EasyApache 4 (EA4).
2. Upgrade each website individually to the newest PHP version during downtime (use a maintenance mode function when possible) and troubleshoot any issues that arise.
3. Once all websites are upgraded to the latest PHP version possible, change the default PHP version in WHM MultiPHP Manager.
4. Remove the older PHP versions with EA4.

Tooltip: You can check your current PHP version in SSH with the “php --version” command.

Database Management

Databases can hold a lot of data and be resource-intensive. One of the most significant advantages of managed VPS hosting over shared hosting products is the additional server resources available for SQL tasks. Database tables are still data, so many best practices are similar to those for file management.

1. Upgrade MySQL/MariaDB, PostgreSQL, MongoDB, etc whenever updates are available.
2. Learn best practices for database security specific to your database software.
3. If you maintain more than one database application, but at some point remove all software that requires a database app, consider removing the database app until you integrate other software that depends on it.
4. Apply the least privileges to users and applications connected to databases.
5. Remove database users once no longer needed.
6. Audit data and server logs for suspicious activity and infections.
7. Monitor respective SQL ports for brute-force login attempts.
8. Create backups frequently.

Web Analytics

Web analytics applications are great for better understanding who or what is visiting your website, how, from where, when, and why. This information is helpful for multiple uses:

1. Learning what topics and SEO practices gain the most attention for your content.
2. A better understanding of user journeys for marketing and sales initiatives.
3. Tracking overall growth in web traffic to websites through time

Web analytics applications are great for better understanding who or what is visiting your website, how, from where, when, and why. This information is helpful for multiple uses:

1. Brute-force attempts on login URLs.
2. SQL injection, user enumeration, and other URL manipulation tactics using PHP.
3. Malicious black-hat SEO techniques that hurt your brand's SEO rankings.
4. Search engine results showing the most common ways visitors misspell your brand when looking for your website (e.g., cybersquatting and domain jacking).
5. Confirm "referer" HTTP header settings for URLs with sensitive info (e.g., forgot password link).

Here is a shortlist of popular analytics software that may apply best to your use case:

Google Analytics	Most popular choice, externally hosted with Google
Matomo	Most popular self-hosted option with plugins for more features
Webalizer	Included in cPanel
AWStats	Included in cPanel
Clicky	Easy externally hosted analytics software for beginners
GoAccess	CLI log parser software, great for cloud servers

What is an HTTP Security Header?

When your web browser requests a web page, you send HTTP header information, including your **user agent**. Likewise, the server responds with the page content and HTTP response headers that affect your user experience (UX) with the website. Here are some common HTTP headers:

- **HTTP version (e.g. 1.1 or 2)**
- Response codes including "301 Moved Permanently" (if the requests URL redirects elsewhere)
- OS and web server name (Apache, Nginx, etc.) and version
- Character set (e.g. UTF8)

HTTP headers also control how cookies are stored, displayed from within the website, browser feature settings, and more. You can learn more about which browsers support certain HTTP headers below with **CanIUse.com**.

Server Information

Showing your OS and server software version makes it easier for cyber attackers to find vulnerabilities to exploit on your server. To mitigate this, hide your **Nginx version** or **Apache version**, along with your OS, from HTTP Headers.

HTTP Security Headers

HSTS (HTTP Strict Transport Security)

HSTS protects website visitors from **session hijacking** (or cookie hijacking) and protocol downgrade attacks by forcing the browser only to request encrypted pages from your domain. HSTS is similar to a **301 redirect** from HTTP to HTTPS but at the browser level.

If you want to take it a step further, you can submit your domain to **HSTSpreload.org**. This eventually adds your website to web browsers' internal preload list, stating domains requests will only be in HTTPS.

HSTS header example with the max time to live (TTL) of the header (in seconds), including subdomains:

```
Strict-Transport-Security: max-age=10886400; includeSubDomains
```

Warning: Once enabled, HSTS prevents the user from bypassing an **invalid or self-signed certificate message** error. Your website will be inaccessible without a **valid SSL**.

You can configure HSTS with the **.htaccess file**, **Cloudflare**, and plugins for your website (e.g., **WordPress**, **Drupal**, and **Zenphoto**).

Content Security Policy (CSP)

CSP prevents Cross Site Scripting (XSS) and other code injection attacks by further defining what code in your website can display in a web browser. In a sense, a CSP header is a code firewall that whitelists every internal and external code type.

Tech Tip: All major browsers have some support for content security policy, including Google Chrome, Edge, Safari, iOS Safari, Android Browser, and Chrome for Android.

Example of Content Security Policy Header and how massive one can be:

```
default-src 'self' https://fonts.gstatic.com/; script-src 'self'
'unsafe-inline' https:; style-src 'self' 'unsafe-inline' https://
fonts.googleapis.com/css; img-src 'self' https://analytics.domain.
com/piwik.php https://i.creativecommons.org/ https://*.twitter.
com/; connect-src 'self'; font-src 'self' https://fonts.gstatic.com/;
report-uri 'self'; form-action 'self'; frame-ancestors 'self'; frame-
src 'self' https://www.youtube-nocookie.com/ https://www.youtube.com/
https://w.soundcloud.com/ https://*.twitter.com/ https://open.spotify.
com/; worker-src 'self'; manifest-src 'self'; base-uri 'self'; block-
all-mixed-content
```

Configure CSP with the .htaccess file and website plugins (e.g., **WordPress** and **Drupal**).

X-Frame-Options

X-Frame-Options prevent websites from being maliciously embedded in other websites with <frame>, <iframe>, <object>, or <embed> HTML tags for **clickjacking**. Remember iframes? Well, you may not, but the Internet does not forget.

Note: **Mozilla recommends** using the superseding Content Security Policy frame-ancestors attribute instead.

Example of X-Frame-Options:

```
X-Frame-Options: DENY
```

Configure X-Frame-Options in your .htaccess file or with plugins (e.g., **WordPress** and **Drupal**).

Feature-Policy

The Feature-Policy Header sets the allow or deny browser features that can be harmful to your website visitors. Feature-Policy mitigates attacks attempting to manipulate your visitor's browser to gathering information. For example, most websites don't need access to your camera, microphone, or geographic location. Does yours?

Example of Feature-Policy

```
Feature-Policy: autoplay 'none'; camera 'none'; geolocation 'none';
microphone 'none';
```

Configure Feature-Policy in your .htaccess file or with plugins (e.g., **Drupal** or **WordPress**).

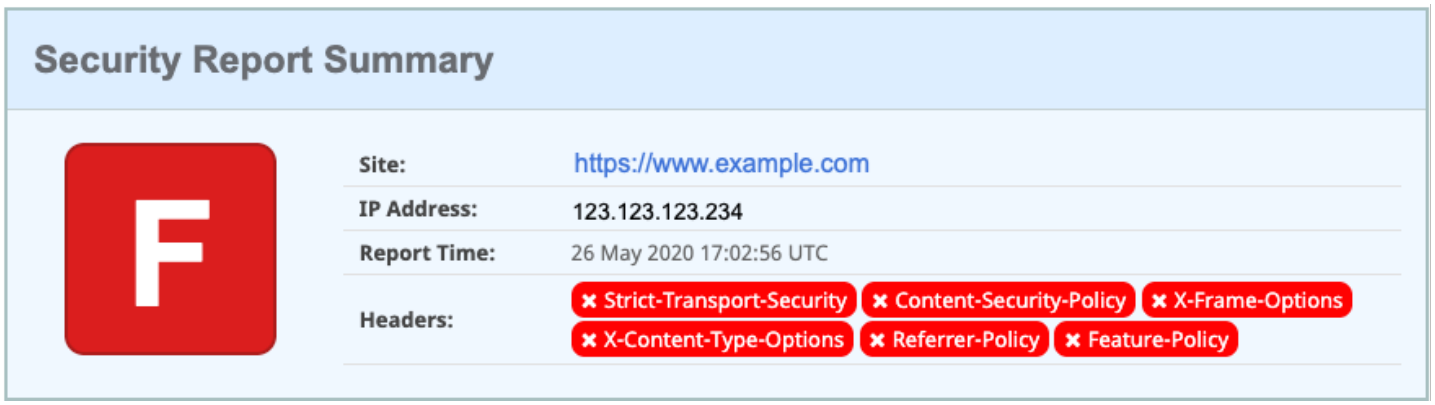
Check Your Website HTTP Security Headers

There are multiple ways to check a website's HTTP headers.

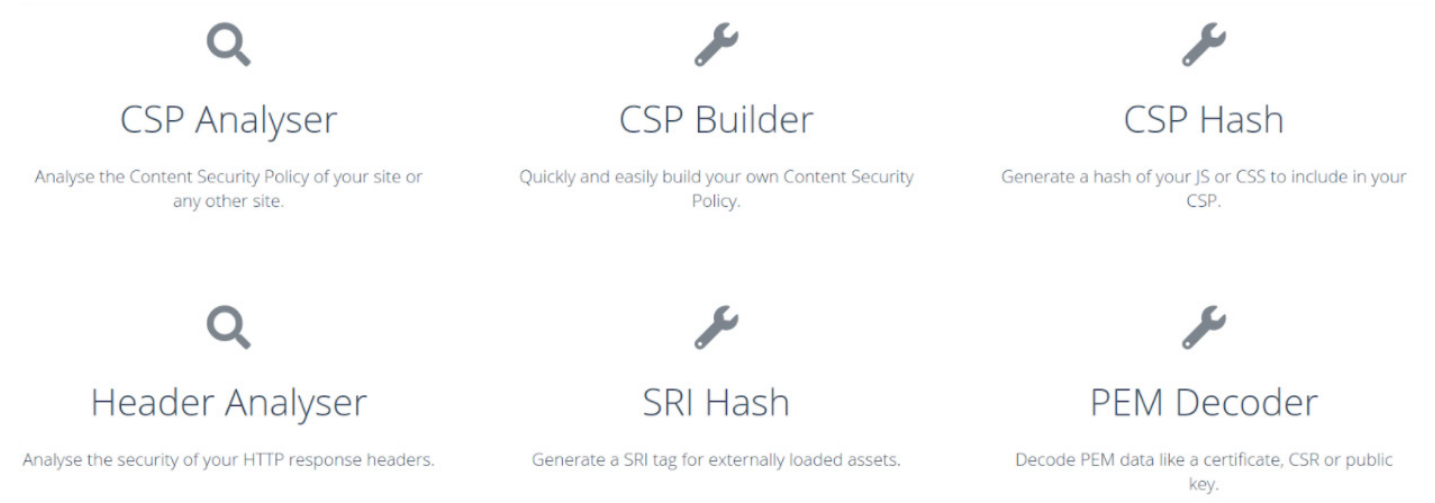
Online Tools

Visit **https://www.webconfs.com/http-header-check.php** and input your website address.

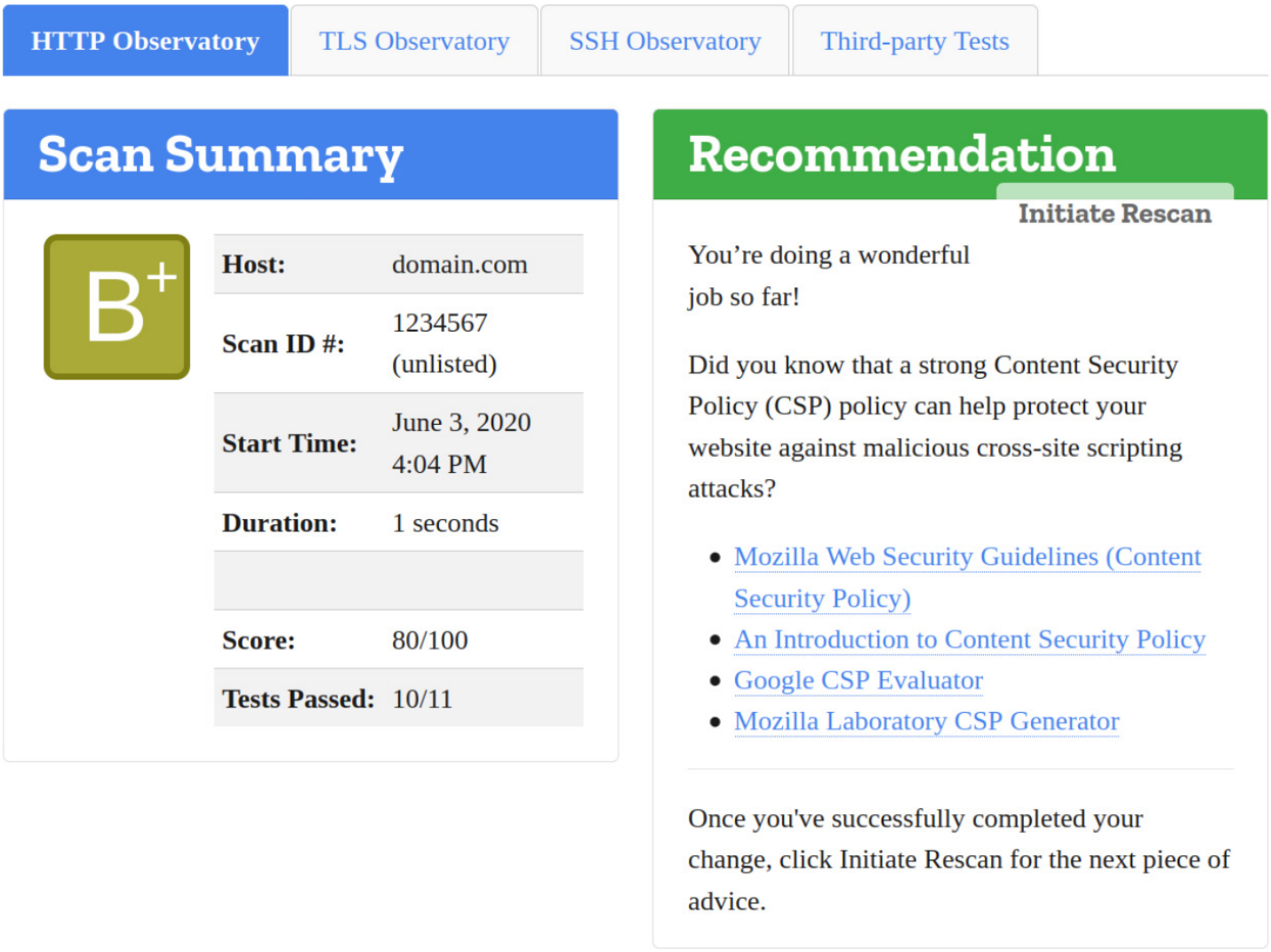
SecurityHeaders.com scans for HTTP security headers.



ReportURI.com provides tools to build a content-security-policy (CSP) header, generate **subresource integrity (SRI)** tags for externally loaded libraries, and more.



Mozilla Observatory scans HTTP headers, SSl/TLS server settings, SSH configuration, and more



Web Browser Extensions

Chrome DevTools

Access a set of authoring and debugging tools in your Google Chrome browser.

1. Open a Google Chrome browser. Input your website URL. Press Enter.
2. In the Chrome menu, select Tools > Web Developer > Network.
3. Click in the Network panel and press (PC) Ctrl + R or (Mac) Cmd + R.
4. You should see the Network pane is populated with the HTTP Header information.

Email Security

Lastly, we need to discuss email security, especially with reports of business email compromise (BEC) - email fraud aimed to hurt an organization in some way - on the rise. This is a more targeted type of phishing attack similar to spear-phishing and whaling. There are DNS records that help **mitigate email spoofing and incoming spam**, all easy to implement in cPanel but possible to add to any DNS configuration.

Domain Keys Identified Mail (DKIM) checks incoming email to verify it hasn't been modified since it was originated.

Sender Policy Framework (SPF) specifies what systems can send an email with your domain and how. Note that this only affects the email headers, not the "From" field.

On cPanel servers, DKIM and SPF can be enabled by default in WHM Tweak Settings.

Domain-based Message Authentication and Conformance (DMARC) allows email providers to check emails against SPF and DKIM rules to determine whether an email is legitimate and how to handle email deemed illegitimate. A strict DMARC record is often the solution for ***Mail Delivery Failed* bounceback messages for emails you never sent.**

Brand Indicators for Message Identification (BIMI) doesn't enhance security. But it does prove integrity by showing your organization logo alongside your email address within BIMI-supporting email providers.Domain Keys Identified Mail (DKIM) checks incoming email to verify it hasn't been modified since it was originated.

Spam Filters

Below are some options for filtering spam in cPanel. These are helpful because the DNS records covered above aren't full-proof. For example, spoofed emails from well-established domains such as Gmail and Yahoo can bypass strong DMARC and SPF records.

Spam Filters in cPanel, formerly known as SpamAssassin, filters incoming email for spam using a rating system and sends the suspicious email to spam or trash depending on your configuration.

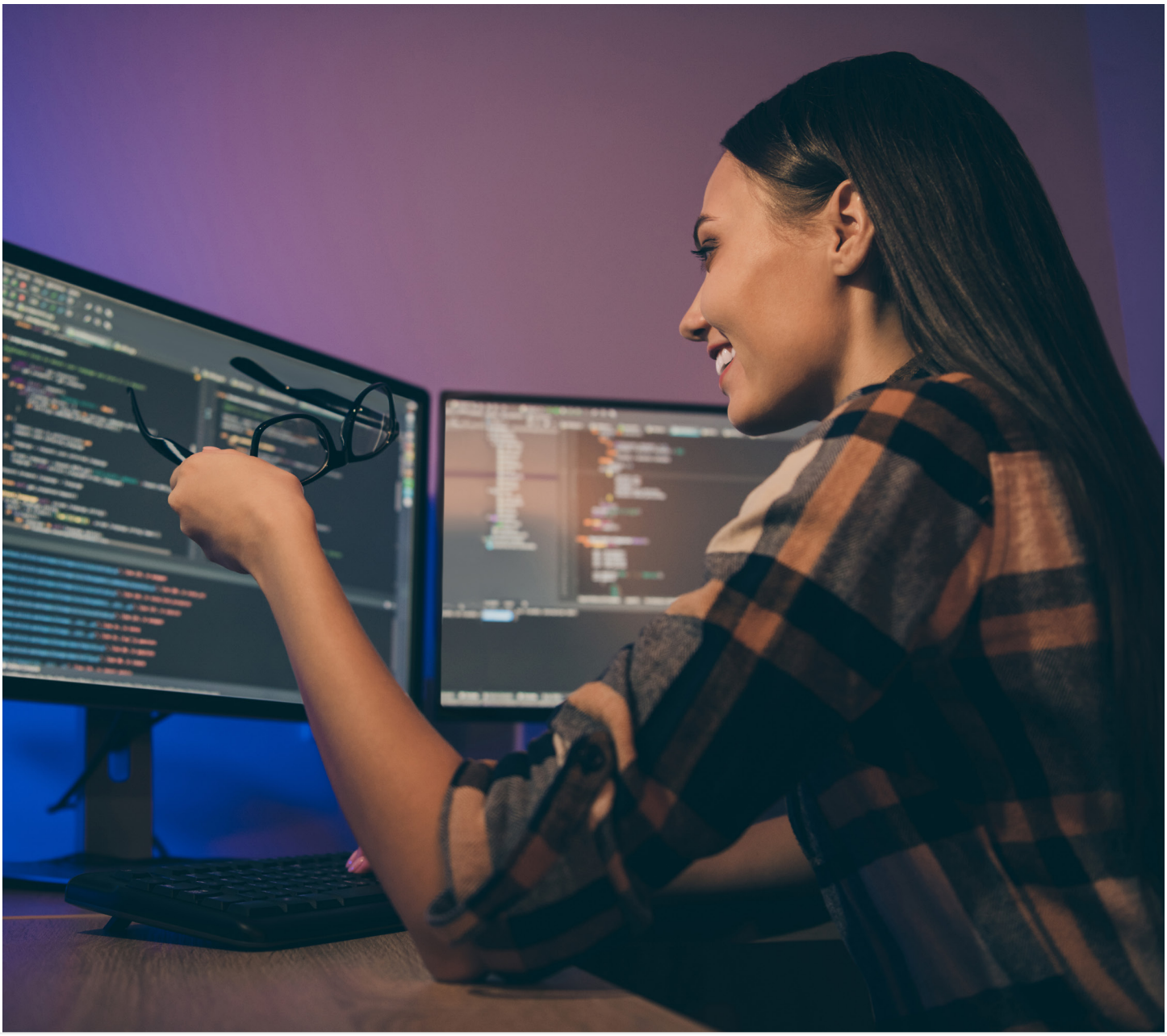
SpamExperts is a third party application InMotion cPanel hosting customers can use to block spam.

In 2020, WHM implemented two new **IP-based email filters**:

- Filter incoming emails by country origin
- Filter incoming emails by domain

Blackhole lists (RBLs) allow cPanel administrators to use third-party maintained lists to filter emails based on certain criteria including but not limited to:

- Newly registered domains (popular method for new phishing attacks)
- IPs with a **bad DNS reputation**
- IPs sending emails with faulty headers



Additional cPanel Security Functions

Below are some other security features to consider when looking into **ways to harden Managed VPS Hosting**.

- **DNS security extensions (DNSSEC)** verifies the DNS path of a requested domain to protect visitors from DNS poisoning attacks.
- **Security Advisor** can help you identify vulnerabilities within your cPanel server, such as cPanel account password strength.
- **cPHulk** protects cPanel users against brute-force login attacks.
- **ModSecurity** protects websites from attacks using common regular expression (regex) strings.

Additional Cloud Server Security Functions

Below are a few things to keep in mind when **hardening Cloud Server Hosting** without cPanel.

- Consider managing SSL certificates with automated **Certbot** software to ensure you always have valid SSLs.
- Use the **right server OS** for your needs.
- Research and follow hardening guides specific to your OS

Infosecurity Regulations

Below are some information security regulations you may need to know of, depending on your industry.

- Health Insurance Portability and Accountability Act (HIPAA) - requirements for managing personal health information (PHI) and personally identifiable information (PII).
- General Data Protection Regulation (GDPR) - requirements for handling information for the European Union (EU) and European Economic Area (EEA) residents.
- California Consumer Privacy Act of 2018 (CCPA) - requirements for handling information for residents in California, USA.
- Sarbanes-Oxley Act (SOX) - applicable to companies publicly traded in US markets, how to track, manage, and report financial data and safeguard data to ensure integrity.
- Payment Card Industry - Data Security Standard (PCI-DSS) Compliance governs how organizations must handle branded **credit cards** from the major **card schemes**. Learn more from our **Support Center**.

We, unfortunately, do not offer HIPAA compliant web hosting products at this time.

Additional Resources

• InMotion Hosting Support Center	• Web Host Manager(WHM) Edu Channel
• Ways to Harden Managed VPS Hosting	• InMotion Hosting YouTube Channel
• VPS Hosting Product Guide	• Customer Community Support Center
• Backup Manager cPanel Guide for VPS/Dedicated Servers	• Ways to Learn More About Cybersecurity
• cPanel Education Channel	• Free Cybersecurity Tools To Secure Your Server

Conclusion

We hope that this content has oriented you to better security and a deeper understanding of the Linux security environment of your VPS.

Why do we choose FOSS?

InMotion Hosting chose Linux servers because of the community's dedication to free open source software (FOSS). With great care and consideration from the open-source community, FOSS has evolved to become extremely reliable, community-driven with a developed sense of purpose to help businesses, entrepreneurs, and enterprises grow.

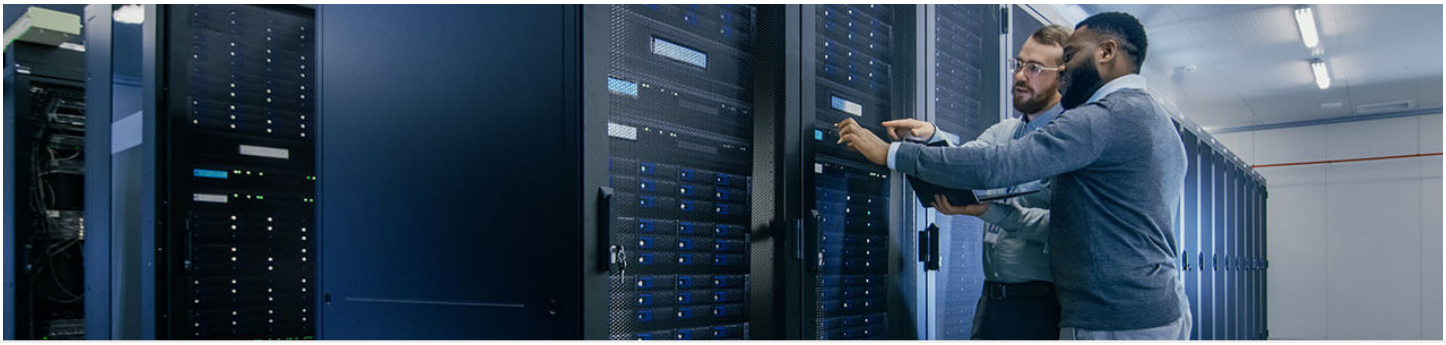
With millions of users, Linux has quickly become a mature open-source software with pull requests to harden projects, bug reports, and an entire community of developers and businesses continuously resolving issues.

The most important takeaways

Security is everyone's job. Everyone should report suspicious activity. From web designers, web developers, system administrators, web hosting providers, domain registrars, and the list goes on. No one is ever truly 100% secure, and hackers are always looking for a soft target

Apply security measures at every network point for defense in depth

No one device or software can truly protect you. Human error and social engineering can defeat anything if it is clever enough. Advanced persistent threats (APTs) use intel gathering and time to siphon data throughout a longer duration of time. Security is a moving target and cybersecurity professionals (and white-hat hackers) are always in a cat and mouse game with cybercriminals (black-hat hackers).



HTTP Security Headers

What is an HTTP Security Header?

When your web browser requests a web page, you send HTTP header information, including your **user agent**. Likewise, the server responds with the page content and HTTP response headers that affect your user experience (UX) with the website. Here are some common HTTP headers:

- **HTTP version (e.g. 1.1 or 2)**
- Response codes including “301 Moved Permanently” (if the requests URL redirects elsewhere)
- OS and web server name (Apache, Nginx, etc.) and version
- Character set (e.g. UTF8)

HTTP headers also control how cookies are stored, displayed from within the website, browser feature settings, and more. You can learn more about which browsers support certain HTTP headers below with **CanIUse.com**.

New security solutions are constantly met with new cyber attacks

Make sure it is in your weekly workflow, disaster recovery plans, and business continuity plans.

Never allow security to move in priority to a lower bracket; look to implement security early within the software development life cycle (SDLC), network building, and other solutions with your teams or clients.

Remember that security standards should be strict, but sensible enough that users don't feel justified working around them.

Create a strategic plan. Connect with your clients, teams, and others to make them aware that security plans are in place. Grow your security knowledge and impress your clients or team members with strategic plans in place in the event of an emergency.

Thank you, and let's get growing.

About InMotion Hosting

Join over 170,000+ customers supported by over 300+ team members. Get premium web hosting with 24/7/365 technical support, 99.99% uptime, and a risk-free money-back guarantee.

Get Onboard Quickly	**Launch Assist**	**Premium Managed VPS Hosting**
Your solutions are up and running in minutes.	Free **web migration** has never been easier or faster	**Fully Managed hosting** with complete management of your server.
Get Started	**Get Started**	**Get Started**

Cloud Server Hosting	**Always Safe & Secure**	**Managed Dedicated WordPress Hosting**
Hyperfast, ultra-reliable cloud server hosting.	Monitoring and defending your web hosting from online threats.	Exclusive Fully Managed WordPress-only servers for high-traffic websites.
View Plans	**View Plans**	**View Plans**

It's All About You and Your Business

InMotion Hosting provides a complete suite of digital tools and professional services for businesses, agencies, and professionals. Our intuitive and powerful online digital marketing product lines consist of domains, professional website hosting, drag, and drop website builders, eCommerce, search engine optimization tools, and professional design and online services that are supported by our award-winning, dedicated customer support team.

For more information on InMotion Hosting and a full suite of digital services, visit **https://www.inmotionhosting.com**.

@inmotionhosting

@inmotionhosting

@inmotionhosting

@inmotionhosting

@inmotionhosting

Glossary of Terms

Linux

Definition: Linux (or the Linux kernel) is an open-source software project that powers a diverse array of computing applications.

What is Linux?

Linux (or the Linux kernel) is an open-source software project that powers a wide variety of computing applications. Many of the world's most popular websites run on Linux-powered software. The Android phone operating system runs on a modified version of the Linux kernel.

Is Linux Free?

Yes, Linux is free, depending on what kind of application you're running and how you govern its usage. For example, operating systems that run on a "GNU/Linux" platform are free to download, modify, and use for personal applications. Red hat Enterprise Linux (RHEL), a notable exception, and some others may come with non-free licensing terms. Many Linux-based operating systems ship with proprietary (as in non-free) software components, which you can use without a monetary transaction but may inhibit other activities (such as selling that software in a package with other free software). Other distros such as Debian exclusively only preinstall FOSS, requiring administrators to add any other proprietary software desired.

Who Is Linus Torvalds?

Linus Torvalds began creating the Linux kernel in 1991 and, with the help of volunteers, created what we know as Linux today. He now works alongside others on continued development within **The Linux Foundation**.

Who is Richard Stallman?

Richard Stallman is a free software advocate that started the GNU Project and **Free Software Foundation (FSF)**. He's also the original writer of the GNU General Public License (GPL).

What Is The Linux Kernel?

A kernel is basically a set of instructions that speak directly to a computer processor. This software connects the system hardware to the operating system. Given these instructions, advanced software packages can function as needed.

Linux or GNU/Linux?

Terms surrounding the use of Linux vary slightly depending on who you're talking to or what kind of manual you're reading. When **learning how to use Linux**, it can be difficult to figure out what these various terms mean and how they're different. Often, you'll notice some users say "Linux" to refer to anything from open-source operating systems to their favorite set of software tools. Likewise, the "GNU/Linux" term might be applied to the same set of tools.

Don't let these different terms confuse you. "Linux" is often meant to refer to the Linux kernel itself regardless of what software is running on it. "GNU/Linux" often refers to the combination of the Linux kernel and various free software packages. Most often, "Linux" is used as a blanket term to cover the kernel, the software, and the philosophy.

What's the Difference Between Linux and UNIX?

UNIX was a popular operating system from the 1970s with many passionate users. Those most dedicated to enhancing UNIX noted that the proprietary system could be easily modified in accordance with its terms of service. The Linux kernel reproduced the best features of UNIX under a non-proprietary licensing structure. This meant the software could be modified or enhanced to suit different needs.

Is Linux Better Than Windows Server?

Linux and Windows servers can provide similar levels of service, but many users prefer to "live" in the Linux ecosystem for convenience purposes. The nature of free software means it can be easily ported to other systems. For example, a developer writing a program in one Linux-based operating system can easily "spin up" a different Linux environment to test his code there without going through a lot of extraneous setup. Also, Windows Server software is proprietary, so unless you pay upfront, you can't just jump in and start learning.

CentOS

Community Enterprise Operating System (CentOS) is one of the most popular open source community-supported computing platforms for Linux servers. This free Linux distribution provides functionality and compatibility with Red Hat Enterprise Linux (RHEL).

cPanel

What is cPanel?

Definition: cPanel, sometimes referred to as “Control Panel,” is an interface for customizing and making changes to your hosting account without the need to navigate the terminal. Some of the great features that cPanel includes are:

- **Email**: Within cPanel, you can create new email accounts, view/modify your existing accounts, modify your MX records, change email passwords, set up mailbox quotas, and much more.
- **Domains**: Under the domains section of cPanel, you can configure new domains to your account, set up parked domains (aliases), create subdomains, setup redirects, and much more.
- **File Management**: In the files section of cPanel, you can backup your cPanel account, access/modify files stored in your account, review your disk usage, and create/manage FTP accounts
- **Databases**: You can create new databases, set up remote access to MySQL/PostgreSQL, manage databases, and much more.

Why Do I Need cPanel?

cPanel takes laborious and difficult server tasks and places them in a user-friendly interface. For example, creating multiple subdomains involves editing your Apache configuration. Without cPanel, you would need to SSH into your server and edit configuration files manually (as the root user or a user with admin privileges). cPanel lets you complete this process with a few clicks.

Likewise, setting up and managing multiple email accounts on your server is a complicated and difficult task to do manually as you’d need to manage software for sending and receiving email (e.g., Sendmail and Exim). cPanel makes it easy to create new accounts or even migrate accounts over from a different host.

How do I find my cPanel?

It is easy for InMotion customers to **log into your cPanel account** through several gateways. You can log in via your Account Management Panel (AMP) for your hosting account. You can also use yourdomain.com/cpanel in most cases and use an assigned username and password of your choice.

Debian

Debian is a Linux distribution composed of free and open-source software, which gives you access to online repositories. These online repositories contain over 51,000 packages, including LibreOffice, Firefox web browser, VLC media player, and more. Debian is popular with those who prioritize security and exclusively using FOSS

Fedora

Fedora is a community-supported operating system (OS) for Linux, which provides an open source OS for your computer. Fedora comes preinstalled on a wide range of open source software and is designed to give you a complete set of tools to support business environments. Fedora is popular with developers who want the bleeding edge versions of software that will later be stabilized for use on CentOS and RHEL

Red Hat Enterprise Linux (RHEL)

Red Hat Enterprise Linux (RHEL) is an enterprise software strictly for servers. RHEL is a paid subscription with server versions for x86, x86-64, PowerPC, Itanium, and IBM System z. RHEL includes desktop versions for x86 and x86-64.

Ubuntu

Ubuntu is a free and open-source operating system (OS), which is based on the Debian GNU/Linux distribution. Ubuntu is one of the most popular operating systems for personal computers (PCs) due to its interface design, focus on ease of use, and proprietary software's ability to run on the platform. Ubuntu is also responsible for the user-friendly APT program for package management, which Debian later adapted to its OS.

Virtuozzo

Virtuozzo is designed to virtualize servers, centralize server management, and consolidate workloads by reducing the number of physical servers required. The software enables multiple Linux distributions to exist simultaneously on one server utilizing virtualization.

Web Host Manager (WHM)

Web Host Manager (WHM) is the software that provides administrative access to manage cPanel accounts. Typically, the software is utilized by agencies, resellers, and companies which specialize in providing digital services or manage multiple websites.

What Is An IP Address?

Definition: An IP address is a numeric identification of a piece of network hardware. This includes your computer, **small office / home office (SOHO) router**, and mobile devices. Your local IP address is generally only used and known within your local network. Find your broadcast IP address (used on the internet) with our **IP Address finder** tool. Your IP address can be used to identify your location within a large radius (state, region, or country).

How Do I Find My IP Address?

The easiest way to find your IP address is to do a Google or DuckDuckGo search for "IP." Google will be able to grab your IP address and display it as the top search result. Many websites and web applications (e.g., web analytics software) are able to display your IP address, but a search engine is probably going to be the easiest for daily use.

Remember, searching your IP address through a search engine is likely going to generate the IP address that your Internet Service Provider (ISP) has given you for the purposes of connecting to the web. This is different from the IP address of your website, email provider, and other applications you are engaging with on the web.

If you want to find the IP address for your website or other services, you can use the tools available from your hosting provider.

How Do I Get a Dedicated IP Address?

For your networking needs, it may become desirable to have a **dedicated IP address**. Maybe you want to further separate domains related to more taboo topics on your server. If you need a dedicated IP address for reaching the web, you can request it from your ISP. Be cautious that your extra services may affect your billing.

A dedicated IP address for a website will be requested similarly, except you will request it from your hosting provider and not your ISP.

How To Change An IP Address

Changing an IP address is a similar process in requesting a new one. In the case of your website, this can be a dangerous move if you have any resources that rely on the old IP address. If all of your applications use a domain name (which is common) instead of the IP address, you will be safe. It's always best to first check with your IT staff or developer before requesting a new IP address for your website.

inmotion hosting