As a hosting provider, every day can seem like a gamble: over 450,000 new pieces of malware are detected every day in an incredible competition to make newer and more dangerous malware. Luckily, there is fierce competition on the prevention side, too, to build smarter, lighter and smoother security solutions. **We believe the secret to build the no.1 prevention tool is immensely useful for the industry, but let us show you where this race is headed to.**

WHICH OFFERS THE BEST SECURITY SOLUTION FOR YOUR LINUX SERVER

We breakdown the benefits and features to help you pick the security solution best suited to your needs.

To get to the big picture quickly, just head instantly to the **wrap up** section.

Both BitNinja and Imunify360 are well-known security suites for your Linux server. However, when you compare the two, which one offers the best overall security platform?

- At a Glance
- Dashboard and Management Features
- Malware Scanning Features
- Bot Blocking
- IP Management
- Web Application Firewalls (WAF)
- Customer Support

A QUICK BACKGROUND ON EACH SERVER SECURITY PLATFORM

ABOUT IMUNIFY360

- Imunify360 is a comprehensive security suite for Linux-based web servers. The company also offers other solutions, such as Imunify AV, which centers on the anti-virus component. Therefore, we will concentrate on Imunify360 in this comparison.
- Imunify360 provides antivirus, firewall, WAF, phishing notifications, and port scanning protection. It focuses on providing an automated process on a server-by-server basis as it relies heavily on control panels such as cPanel, Plesk, Direct Admin, or CyberPanel. This is where it shines the most. While it also has a standalone install method, it is much less optimized for this scenario.

ABOUT BITNINJA

- BitNinja is a fully featured, multi-layered Linux server protection platform. Much like Imunify, you get a WAF, IP reputation anti-malware, port scanning protection and phishing notification systems. However, the two solutions approach these in vastly different ways, which we will delve into later, among other differences such as additional features, like technical support and ease of use. BitNinja is also much less resource intensive, and we will explain the ins and outs later in this article.
- **BitNinja has a standalone management panel.** While it is fully compatible with control panels, it's also completely independent of them and works across all forms of servers, including shared hosting, managed service, VPS, and many more, no matter how big or small your cluster may be.

DASHBOARD AND MANAGEMENT FEATURES

Depending on your use case, this category can go either way. So, we will call this one a draw.

ABOUT IMUNIFY360

Imunify360 integrates with popular control panels. The integrated security dashboard is easy to use and easily accessible. Imunify360 works on a "server-by-server" basis. You can choose to link the servers together with a bit of work to add some additional functions like managing blacklist entries together. However, it still isn't a fully streamlined experience.

ABOUT BITNINJA

Alternatively, BitNinja has its unified dashboard, where you have the freedom of managing the black and white lists for server clusters or on a per server basis.
The BitNinja dashboard is completely independent of control panels. BitNinja's installation process uses a one-line installer, so you can implement it on multiple servers with minimal effort.

Starting with Imunify360, as previously mentioned, the system integrates with popular control panels. Users of these platforms will find the integrated security dashboard easy to use and easily accessible.

Imunify works on a "server-by-server" basis, meaning each server is individually managed, without a dashboard where you can oversee them all together. You can choose to link the servers together with a bit of work to add some additional functions like managing blacklist entries together. However, it still isn't a fully streamlined experience, and there is no way to connect them through some code installation. So, as an owner of multiple machines, you will run into extra work while installing, configuring, and managing your cluster, which could rob you of some precious time.

Alternatively, BitNinja has its **unified dashboard**, which is completely **independent of any control panels.** The black, white, and grey lists are **account-wise**, granting all of your servers herd immunity against any IP that has attacked one of your machines within seconds. You also have the freedom of managing the black and white lists on a per server basis, and the choice is yours.

BitNinja's installation process uses a one-line installer regardless of whether you use any control panels or not, so you can implement it on multiple servers with minimal effort.

BitNinja's dashboard is ideal for both large server clusters or just a single machine. For those who prefer a single server management panel, BitNinja can **reduce workload and blind spots**. It can also be beneficial for single server owners or managers of small groups of machines, as you are not "vendor-locking" yourself with any control panels but still keeping your machines fully secured.

MALWARE SCANNING FEATURES

Despite offering similar levels of protection, BitNinja provides a more flexible approach while imposing less load on your machine.

ABOUT IMUNIFY360

Imunify360's malware engine can chew up a considerable amount of resources when scanning. Imunify360 offers a database cleaner that is more mature when compared to BitNinja's beta database cleaner. You can not add any user-level signature.

ABOUT BITNINJA

BitNinja focuses on flexibility above all without being resource intensive. You can add unique, user-level signatures and can mitigate command and hard-to-deal-with risks with BitNinja's custom rules.
Recently added sandbox Sandbox Scanner and JS Sandbox Scanner perform behavioral analysis to ensure no malware is left undetected.
The newly added YARA engine catches all types of malware such as JS, XML - it caught 12 million infected files since implementation!

Both BitNinja and Imunify360 have a powerful system that regularly checks your server from multiple angles, looking for file system changes or malicious activity. However, comparing the two makes it clear that the implementation of Imunify360's malware engine leaves something to be desired, as it can chew up a considerable amount of **resources** when scanning.

Despite the heavy load, it's indisputable that it can achieve great results on infected shared hosting and accounts, cleaning a mess of the malware. On the downside, with Imunify360 you lack some **flexibility** because you cannot add any user-level signature once you've identified a common malware that was left untouched.

BitNinja focuses on flexibility above all **without being resource intensive.** It lets you add your **unique user signatures** if you identify something new. Where you are blindsighted by your systems, BitNinja's custom rules and signatures will mitigate these common yet hard-to-deal-with risks.

One great advantage of Imunify360 is that it has a **database cleaner** that is more mature when compared to BitNinja's beta database cleaner. This is an important feature you'll be using to clear your server's database of malicious entries.

Imunify360's malware detection module prefers **cleaning** over quarantine. Their engine will usually remove all contents of a file even if they were completely harmless. This can lead to some confusion, as the files stay in place but are left empty.

On the other hand, BitNinja will **only quarantine files containing malicious code** and clean files containing injected malicious code. As a result, BitNinja does not leave empty files behind. In addition, recently added modules called Sandbox Scanner and the more recent JS Sandbox Scanner perform **behavioral analysis** to ensure no malware is left undetected. They run the PHP and JavaScript files in safe environments and analyze their behavior to decide their intentions, and quarantine or clean them if necessary.

BitNinja's powerful malware scanning arsenal also includes the **Defense Robot Module.** We generate a malware signature when we find suspected files from malicious IP addresses. We thus **generate signatures that are unique** and powerful because sets of malware signatures. Consider it like your own personal assistant, who is also a secret agent, protecting you from the baddies!

Recently, BitNinja has implemented a new malware engine known as YARA, allowing the system to catch all **types of malware such as JS, XML, etc. The new system has caught over 12 million infected files since its implementation.**

BOT BLOCKING

The two tools apply similar strategies against bot attacks, both uses IP filtering on the first line of defense. Due to the massive difference in IP reputation size BitNinja undoubtedly achieves better results.

ABOUT IMUNIFY360

Imunify focuses on creating simplified reports so you can easily read the results of scans and attacks. However, these are at the expense of being slightly less detailed for the tech-savvy.
Imunify simply blocks attacked ports, which leaves them without intelligence gathered from these IPs.

ABOUT BITNINJA

BitNinja offers more detailed information regarding an attack, such as the request body itself.
The Recaptcha, captcha, an additional layer, can be set on any URL and will automatically challenge all requests.
BitNinja runs all attack data efficiently through a comprehensive defense system resulting in a false positive rate of about 0.0012% and an additional decrease in server load.

Both Imunify360 and BitNinja protect against bot attacks, although in slightly different ways.

The first stage of bot defense through both pieces of software involves **IP filtering**, which we will discuss later in this article. BitNinja has an additional layer, called **URL captcha**, that can be set on any URL and will automatically challenge all requests. **Normal** users are met with a Browser Integrity Check or "Silent CAPTCHA," which means real visitors will not have to fill out anything to pass, but suspicious ones will be stopped.

Imunify focuses on creating **simplified reports** so you can easily read the results of scans and attacks. However, these are at the expense of being slightly less detailed for the tech-savvy. On the other hand, Imunify **blocks these ports**, which leaves them without intelligence gathered from these IPs.

BitNinja takes attack data through a comprehensive defense system, resulting in a false positive rate of about 0.0012%. Using data from existing attacks BitNinja server owners to maintain high levels of security with limited server load.

IP MANAGEMENT

Even though Imunify is no slouch when blocking IPs, BitNinja leads the way by a significantly huge margin: due to its 65 times larger than IP database it has an objectively better automated blocking rate, resulting in less "noise" traffic.

ABOUT IMUNIFY360

Imunify360 reports an IP list the size of 15,000 entries. Imunify360 lets you white or black list IP addresses and countries on a sever basis.

ABOUT BITNINJA

On average, BitNinja's IP database is around 65 times larger than Imunify's. BitNinja's greylist contains one million entries on every machine.
This large number of IPs combined with BitNinja's lightweight footprint usually results in a reduced load of 20-25% compared to other security software.
With BitNinja it is effortless to block or allow IPs, countries, or even ASNs for entire clusters of machines.

While in most other categories, the two solutions are trading blows, in this one, **BitNinja smashes the competition by a huge margin. Its more than 65 IP database is around 65 times larger than Imunify's. To put it in numbers, Imunify reports a list size of 15,000, while on average, BitNinja's greylist contains one million entries on every machine.**

This large number of IPs combined with BitNinja's lightweight footprint usually results in a reduced load of 20-25% compared to other security software.

Both software solutions let you **white or black list** IP addresses and countries. However, using Imunify, it's a bit more complicated managing these for a group of servers due to the previously mentioned **server-by-server management** issue. On the other hand, it is effortless to block or allow IPs, countries, or even ASNs **for entire clusters of machines.**

This might mean your servers get fewer "not single moms in your area" emails, but I believe that's a worthy sacrifice!

WEB APPLICATION FIREWALLS (WAF)

The two solutions offer very similar features (ModSecurity rules, Zero-day patching, etc.) and performance. However, the customizability of BitNinja, means it comes out slightly ahead.

ABOUT IMUNIFY360

Imunify360 offers efficient WAF with crucial features like zero-day patching.

ABOUT BITNINJA

BitNinja uses a separate NGINX instance, utilized as a reverse proxy. As a result, BitNinja can fully control every aspect of the process.

Web Application Firewalls are an essential part of blocking malicious requests. Imunify360 and BitNinja work with ModSec and both offer similar performance levels. However, their implementation differs.

While both use **ModSecurity rules**, Imunify injects them into the web server itself. BitNinja uses a **separate NGINX instance**, utilized as a reverse proxy. This adds some complexity to the system. However, as a result, BitNinja can fully control every aspect of the process.

Imunify offers a solid level of protection with low configurability for those who aren't tech-inclined. However, as most servers have unique needs, BitNinja might be preferred due to its high levels of **configurability**. After all, most server managers like to control what's going on with their servers.

Unlike Imunify, BitNinja allows you to **granularly control** each domain's rules one by one if you decide to do so. This allows you the freedom to configure a domain to your liking or let BitNinja do it for you.

As far as additional features, like **Zero-day patching**, go, both solutions offer these.

CUSTOMER SUPPORT

Both BitNinja and Imunify have extensive documentation that is useful for more experienced customers. Customer expertise is clear with either provider, but BitNinja arguably offers a better user experience.

No one likes to contact support, particularly support teams that are slow to respond. Therefore, a fast reply is an essential item of urgency, as downtime can and will cost you money.

Imunify360 offers free **24/7 customer support**. However, based on customer feedback, it can sometimes take an extended period of time to hear from them.

By comparison, **BitNinja offers 24/7 chat that often gives response times of less than five minutes.** Time is of the essence, and in security, it's even more vital, as a few minutes can be the difference between a hacked server and a safe machine.

Both BitNinja and Imunify have extensive **documentation** that is useful for more experienced customers. Customer expertise is clear with either provider, but BitNinja arguably offers a better user experience.

WRAP UP

So, when comparing BitNinja and Imunify360, which offers the better experience? It's a hard call and will most likely come down to the extra benefits each offer.

In terms of security, both products offer similar levels out of the box, so we must look deeper to see their advantages and disadvantages respectively.

Imunify is great if you work with one server, use one of the control panels it supports, and you aren't using a smaller machine with limited resources such as a smaller VPS. Their large footprint could lead to some severe system slowdowns. However, their database cleaner is a great benefit that BitNinja currently works on in an early Beta stage. The Imunify360 UI is also specifically tailored to be more "human-readable," which can be an advantage or disadvantage depending on your preferences.

One of BitNinja's most significant advantages is its unified dashboard, which can house any number of servers and does not rely on any control panel. Therefore, you don't have a deeply integrated interface with the same control panels you may not use BitNinja's own. The customizability and reduced load are also a huge benefit, especially on crowded machines, because we all know that response times are king when it comes to user satisfaction. Customizability is also another huge factor for many. Unlike Imunify, BitNinja gives you the freedom to configure each and every module to your liking.

In terms of additional "features," BitNinja has a faster customer support team with much lower response times.