BITNINJA
SECURITY

Prevent all types of cyberattacks and provide server-wide protection for your customers

Build a proactive security strategy to defend your servers from hacking attempts while making the internet a significantly safer place

BitNinja Whitepaper 2022

All online businesses need protection from threats

No online business is immune to cyberattacks. All are potential targets for hackers looking to steal data or cause disruption. Therefore, good cybersecurity is essential for any business, but for hosting providers, it’s crucial.

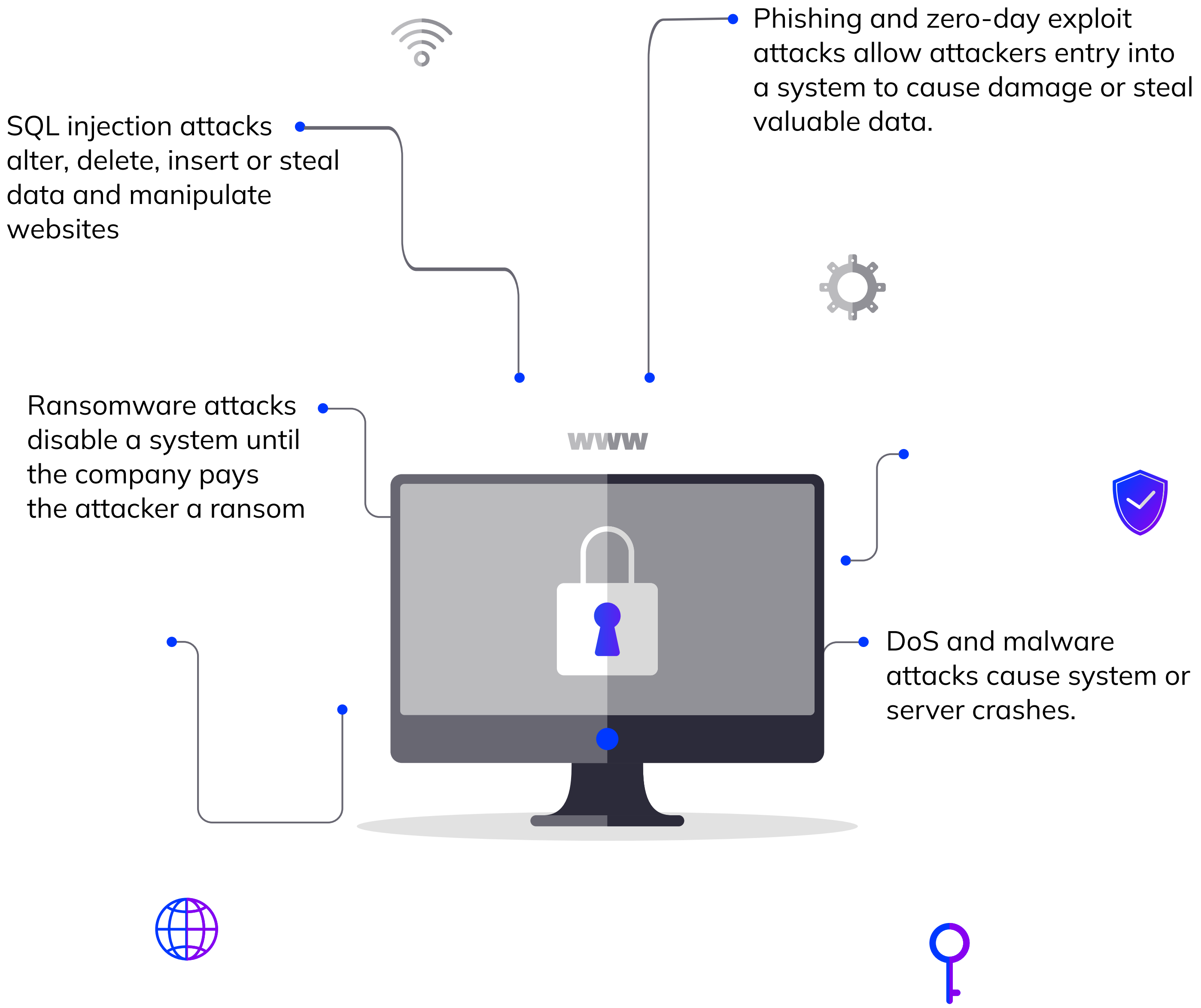
Cyberattacks come with many different motivations, but regardless of their reason, the result is always the same: a painful financial impact. Whether this occurs in the long or short term, it’s not just that they create monetary issues. They also cause reputational damage too.

On top of that, apart from data and money loss, you can face legal consequences because you are responsible for keeping this information and values safe. If you don’t do your best and leave your customers in trouble, you can be held legally accountable.

What can a cyberattack cause?

Successful cyberattacks can cause major damage to hosting providers and their customers equally. Theft or manipulation of data and downtime can result in significant losses, not only financially but also with lost customer confidence that may lead them away from your business completely!

EXAMPLES



SQL injection attacks alter, delete, insert or steal data and manipulate websites

Phishing and zero-day exploit attacks allow attackers entry into a system to cause damage or steal valuable data.

Ransomware attacks disable a system until the company pays the attacker a ransom

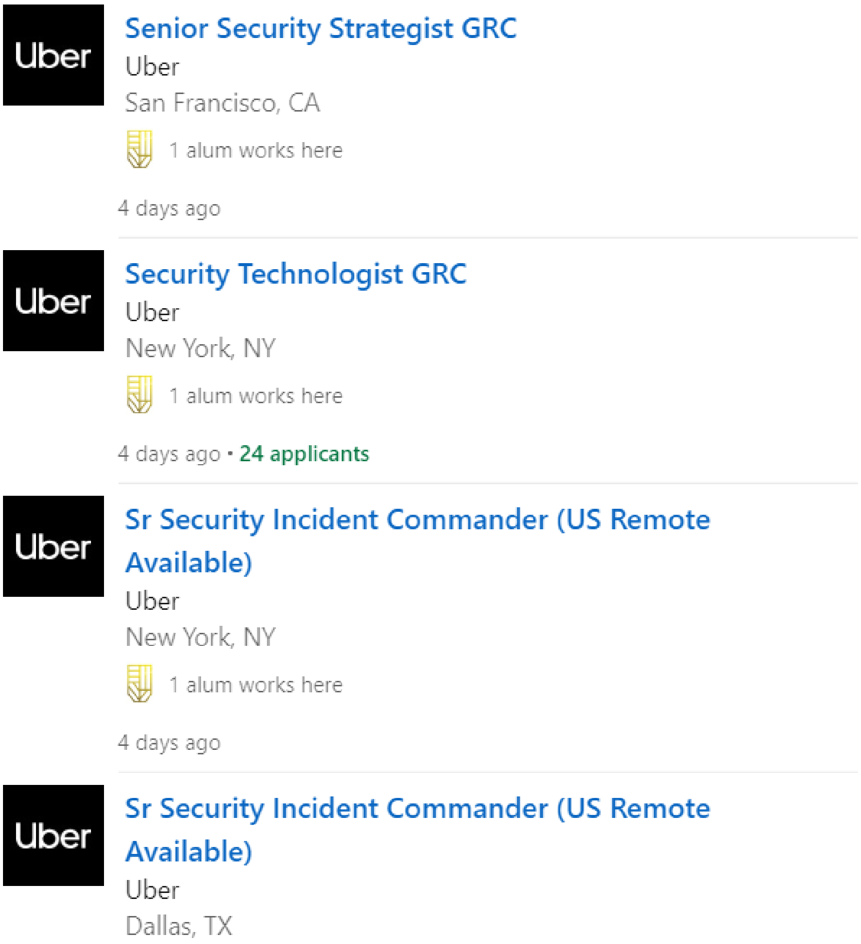
DoS and malware attacks cause system or server crashes.

A real-life example from 2022

An Uber EXT contractor had their account compromised by an attacker. The attacker likely purchased the contractor's Uber corporate password on the dark web after the contractor's personal device had been infected with malware, exposing their credentials.

Uber realized too late that they should have been proactive about their server security. The IT team was unaware of the malware lurking on their server until it caused financial and reputational damage.

Hiring cybersecurity experts was only logical after this point. However, it became clear just how much more harm could have been prevented if one small change had been implemented before disaster struck. This small change is implementing server security software.



Senior Security Strategist GRC
Uber
San Francisco, CA
1 alum works here
4 days ago

Security Technologist GRC
Uber
New York, NY
1 alum works here
4 days ago • 24 applicants

Sr Security Incident Commander (US Remote Available)
Uber
New York, NY
1 alum works here
4 days ago

Sr Security Incident Commander (US Remote Available)
Uber
Dallas, TX

What do your customers want?

> *“ With the rising number of online threats, fraudulent and abusive activities companies face on a daily basis, we as 1-grid must help our customers navigate these dangers and avoid costly business interruptions by providing comprehensive security protection at server level.”*
> ***- Nico Visser - DevOps Manager at 1-grid***

Customer Needs

UPTIME

LOW PAGE LOAD TIMES

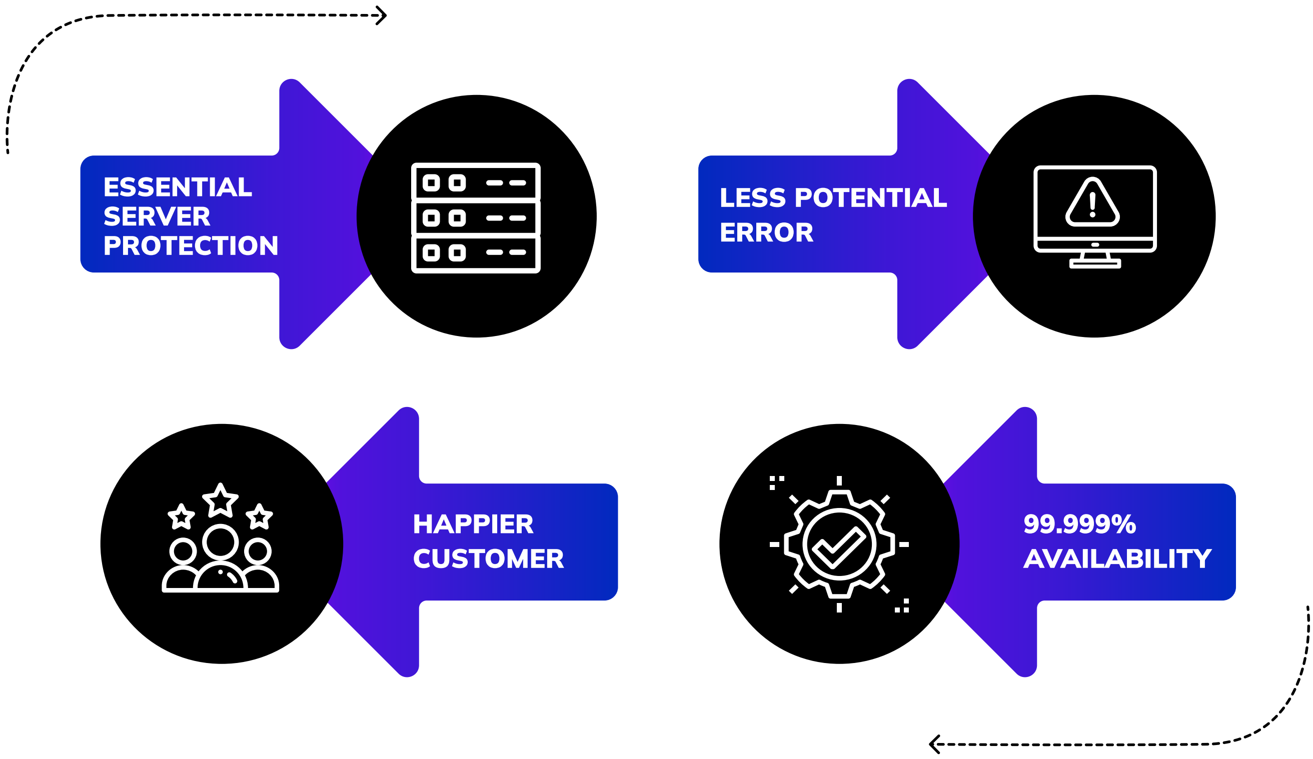
CONSISTENTLY RELIABLE SERVICES

If you don't protect your customers' servers from outside attacks, they'll be vulnerable. You have limited control over their actions and their security awareness. Therefore, it's crucial that there are no security holes for hackers in any of the following places: applications, databases, operating systems, or networks. As a hosting provider, you are responsible for ensuring that your client’s site is protected from all kinds of attacks and runs all the time without disruption.

For your customers, the only thing more frustrating than an unavailable website is one that’s constantly breaking. They’re looking for hosting providers who can offer them high availability, so they don’t have to worry about their site suddenly crashing and losing valuable data. As such, you should always strive for proactive strategies over reactive ones when it comes to selecting a cybersecurity strategy.

How can you provide safety for your customers?

Hosting providers can reduce cyberattacks with an effective server security system that uses the right technologies and practices. A reliable cybersecurity system detects and reports attacks and also prevents them too.



ESSENTIAL SERVER PROTECTION

LESS POTENTIAL ERROR

HAPPIER CUSTOMER

99.999% AVAILABILITY

SO WHAT DO YOU NEED

- A platform that **detects** threats
- A platform that **reports** these threats
- A platform that **cleans out** these threats
- A platform that **prevents** further attacks

It seems like a lot of tools to implement.

One of the most common mistakes companies make is to implement security tools when they discover a vulnerability and purchase a solution to address that problem—one tool for each attack angle.

Implementing a multilayered cybersecurity framework that provides server-wide protection against ever-growing attack vectors is a much better solution. There is no need for a bunch of tools and the extra effort to maintain them.

> *“It has everything that a web hosting company or sysadmin could dream of; a single interface that protects your servers from any kind of attack.”*
> ***- Rabi Hanna - CTO at Miss Group***

BitNinja provides a comprehensive security intelligence system for Linux servers that detects and cleans all types of threats and incidents and also prevents them and protects your servers and customers from continuously changing and renewable attacks.

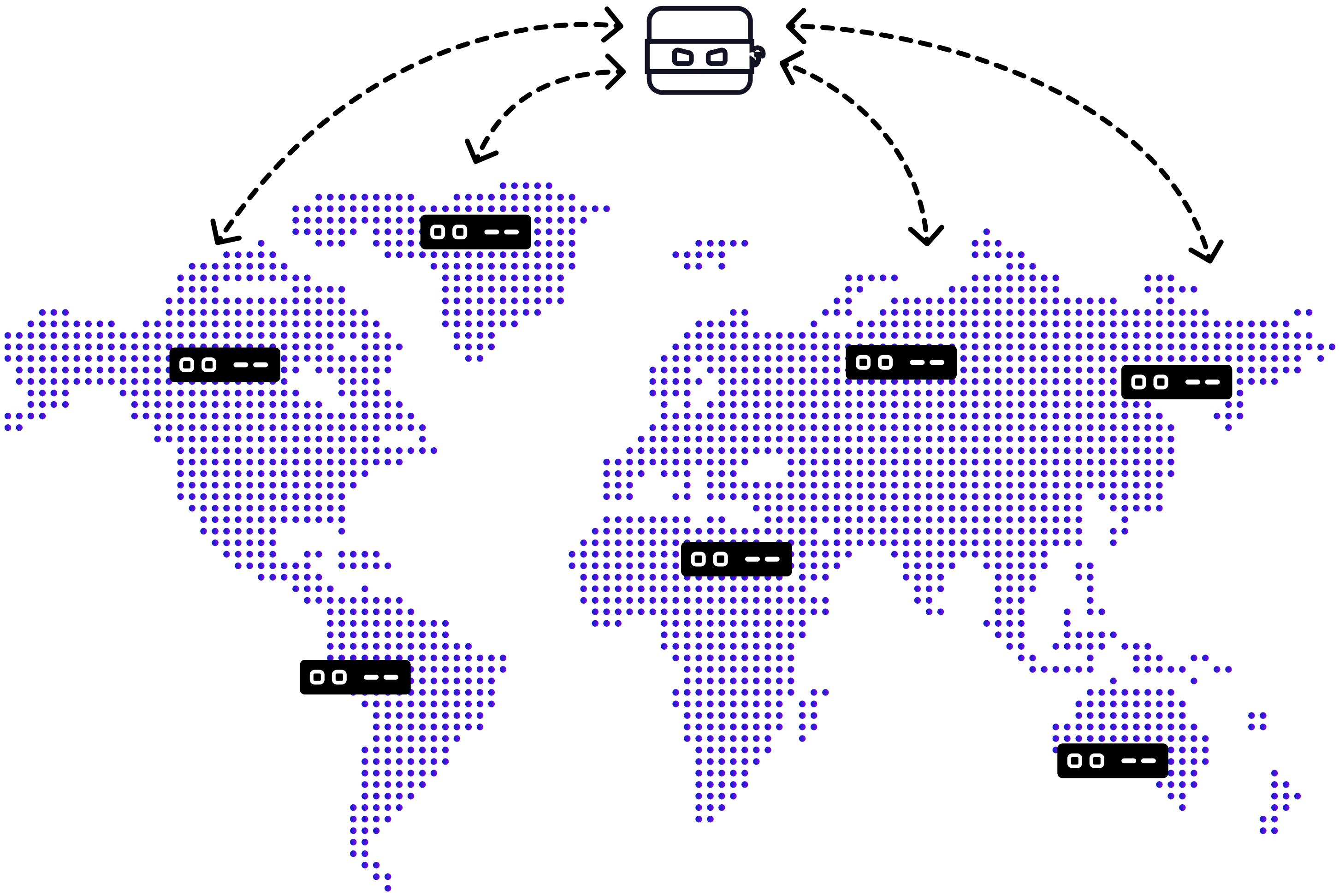
IT’S AN ALL-IN-ONE SAAS SOLUTION.

And even more...

This intelligent system does not just protect from malicious traffic and prevent further attacks; it gets stronger and smarter with every attack.

BitNinja wants to ***make the internet a safer place,***
and for that, the key is information!

Thanks to the crowd-sourced method we call the Defense Network, all the modules and all BitNinja-protected servers worldwide are effectively sharing attack information.



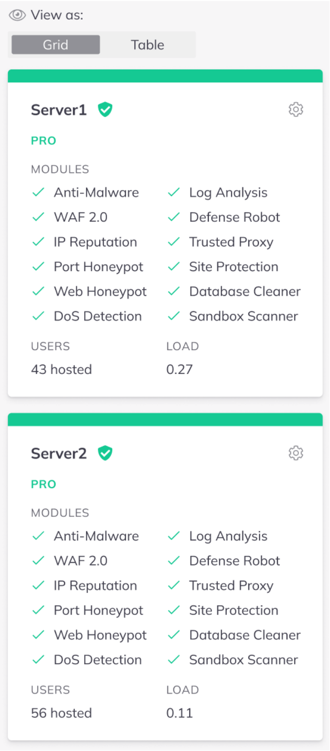
This power of our community results in
a **super safe and efficient shield** that protects the servers
from the latest vulnerabilities and zero-day attacks.

Saves time for you

> *“BitNinja has given our customers ease of mind knowing they are protected from reputational and business impacting online threats and has greatly reduced the time the internal team spent on cleaning infected websites.”*
> ***- Nico Visser - DevOps Manager at 1-grid***

How?

By providing an at-a-glance panel where you can check the most important, real-time information. You don’t have to waste time logging in and out of machines, all it takes is one login, and you can oversee your whole server infrastructure. If you want to specifically manage a smaller group of machines within the bigger one, you can manage servers individually or in server groups.



Server1 ✓
PRO

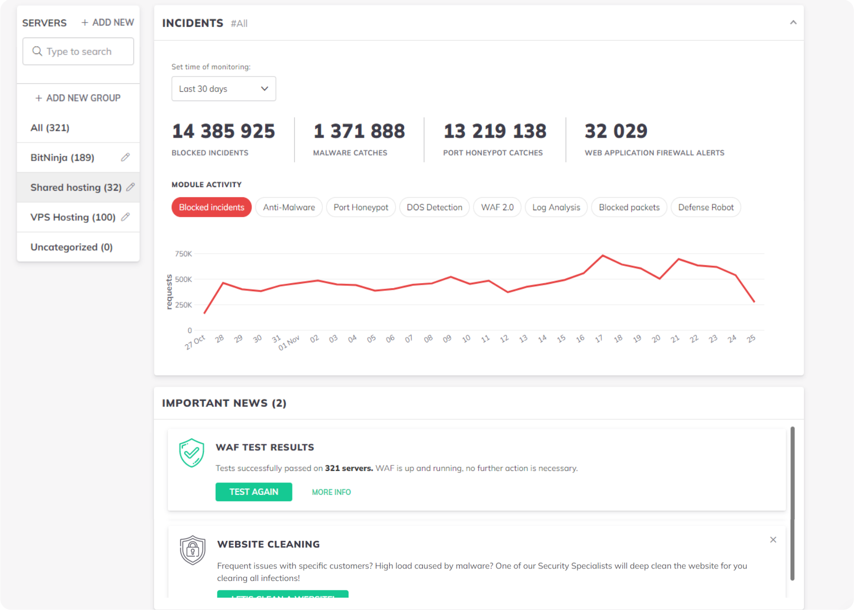
MODULES
- ✓ Anti-Malware
- ✓ WAF 2.0
- ✓ IP Reputation
- ✓ Port Honeypot
- ✓ Web Honeypot
- ✓ DoS Detection
- ✓ Log Analysis
- ✓ Defense Robot
- ✓ Trusted Proxy
- ✓ Site Protection
- ✓ Database Cleaner
- ✓ Sandbox Scanner

USERS	LOAD
43 hosted	0.27

Server2 ✓
PRO

MODULES
- ✓ Anti-Malware
- ✓ WAF 2.0
- ✓ IP Reputation
- ✓ Port Honeypot
- ✓ Web Honeypot
- ✓ DoS Detection
- ✓ Log Analysis
- ✓ Defense Robot
- ✓ Trusted Proxy
- ✓ Site Protection
- ✓ Database Cleaner
- ✓ Sandbox Scanner

USERS	LOAD
56 hosted	0.11



14 385 925	1 371 888	13 219 138	32 029
BLOCKED INCIDENTS	MALWARE CATCHES	PORT HONEYPOT CATCHES	WEB APPLICATION FIREWALL ALERTS

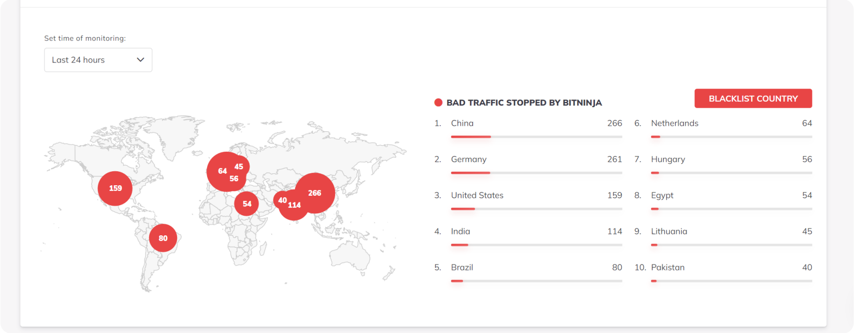
IMPORTANT NEWS (2)

WAF TEST RESULTS

Tests successfully passed on **321 servers.** WAF is up and running, no further action is necessary.

WEBSITE CLEANING

Frequent issues with specific customers? High load caused by malware? One of our Security Specialists will deep clean the website for you clearing all infections!



BAD TRAFFIC STOPPED BY BITNINJA

1.	China	266	6.	Netherlands	64
2.	Germany	261	7.	Hungary	56
3.	United States	159	8.	Egypt	54
4.	India	114	9.	Lithuania	45
5.	Brazil	80	10.	Pakistan	40

Reduces server load

> *“As a result, we have noticed a drastic decrease in hacked WordPress installations or server overloads due to minor DDoS attacks or brute force attempts. The drop was so dramatic that we decided to provide BitNinja for free to our web hosting customers.“*
> ***- Victor Jerlin - CTO, CISO, DPO - Internet Vikings***

BitNinja is lightweight, making it possible to run on even small VPSes, focusing on reducing load rather than increasing it.

Thanks to the **Defense Network**, we have the most extensive IP list. The IP-Reputation system blocks bot traffic automatically and significantly reduces server load.

We have already mentioned the first one, which is simple: By blocking more “bot” traffic.

That means we blocked 77 incidents every second (at the time of writing). These are just the numbers from our active protection.

TO PUT THINGS INTO PERSPECTIVE:

we have blocked **278,268** incidents in the last hour

or **6,256,539** in the last 24 hours.

In some cases, our users have experienced up to a 40% reduction in load when switching to BitNinja. Thanks to this pretty intensive number, they were able to add more users onto a machine than before, maximizing efficiency.

There are more reasons why we have achieved these results

Our “passive” protection via our blacklist also adds a large number to these. It’s safe to say that these numbers alone would be enough to drop your load, but we did not stop there.

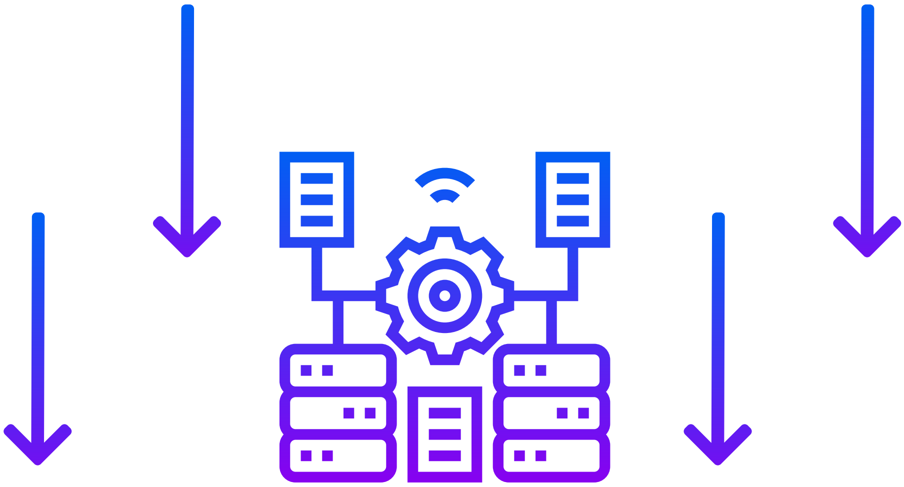
Another factor is the optimization under the hood. With each update, we are making our agent more and more efficient, despite adding new features along the way.

Furthermore, as we have already indicated above, our Defense Network contains intel of over 10 million IP addresses. That is a huge number. Therefore, to ensure effectiveness, we only fetch the full list on startup. After that, we keep it up to date by sending the latest changes.
Your servers are constantly getting updates on the newest bad actors, and your servers keep others updated too.

We call this "herd immunity"

Our agents share information between themselves, making them super efficient. This results in less worthless traffic and more quality customers. In this process, we also ensure the hosted domains get their ad revenue by cutting off the bots.

There is no more wasted CPU, memory, or network resources!



Provides you with the most effective malware protection

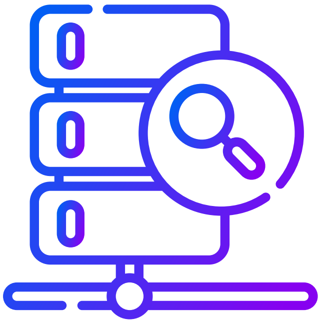
One way that cybercriminals can access a server is by using a backdoor. Typically, backdoors are installed as malware, and it's essential to block and remove the infected malware file as quickly as possible.

The BitNinja MalwareDetection module identifies and catches various malware and backdoors that are spying on you and your customers. Then the Defense Robot finds the backdoor and the attacking IP, blocks the attack, and prevents any further infections on the server. Our engine uses a hybrid approach. We use "simple" md5-based signatures, and we also use Structure Analysis, which generates a "skeleton" of the file's contents. Then, even if it is obfuscated with random strings, we are still able to match it to our signature generated by this method.

Furthermore, we are harnessing the power of machine learning in our Sandbox Scanner, which analyzes the behavior of the file, and if it is malicious, a signature gets generated from the contents. When we receive that signature, our automated system passes it through an automated system containing AI, several filters, and other "two-factor" authenticators. If any of them reports that it's a false positive, our Threat Management team checks them by hand.
Even though stating that BitNinja's malware scanner is the most effective in the market might sound overly self-confident, it is based on several tests and backed up with exact numbers.

The blazing-fast scanner first runs a quick scan of the customer's server. This scans for obvious signs of malware and takes significantly less time than a deep scan. After that, the scanner will automatically move on to the deep scan. If there is any malicious software, the scanner will quarantine the infected file(s) and notify the server's owner so that they can take appropriate action.

This two-phase approach ensures that the server is thoroughly scanned for malware without taking too much time.

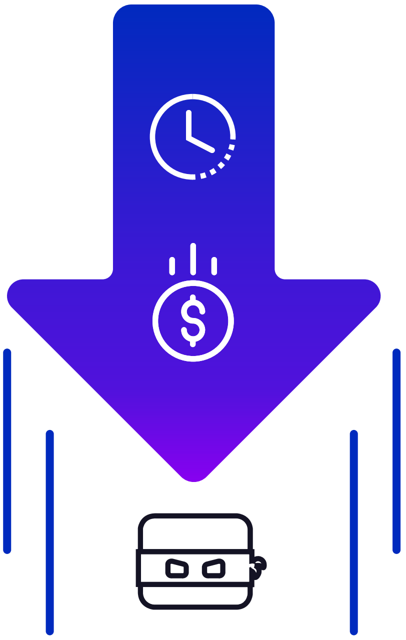


Good cybersecurity is already evolving on the pillars of proactive strategies and technologies that currently provide predictive and prescriptive insights to eliminate malicious attacks in real-time.

Conclusion

What does a hosting provider wants to achieve?

- Maintaining 99,999 % uptime by providing consistently reliable services
- Outstanding reputation thanks to a full-stack protection service
- The lowest possible page load times
- Happy customers and minimized churn rates
- Less cost hiring expensive security experts to scan and remove vulnerabilities in your network



Investing time and money in cybersecurity software can help you achieve all the above goals for less cost than hiring an expert team.

As a consequence, you retain a greater number of customers – which means more sustainable financial results for your hosting business. You need to start it at the server level with a proactive, all-in-one solution.

BitNinja can be your partner and guide in server security and beyond!

Why?

IT'S ESSENTIAL

You need to provide safety and the highest availability rate for your customers. You can reach that with a multi-layered, full-stack Linux server protection solution.

IT'S THE MOST EFFECTIVE

By detecting and cleaning the malware and database super-fast and preventing further attacks, you will have the most effective guardian. Thanks to our crowd-sourced solution, the Defense Network creates a strong protective shield that makes your server safer from every single attack.

IT'S ECONOMICAL

Our SaaS services were designed with hosting providers in mind. Therefore, providing highly competitive pricing for our partners and resellers, easy adoption, simple management, and limitless integration with popular tools and platforms are all parts of our service.

Moreover, you do not need to worry about implementing a new tool or removing other software already in use because BitNinja is control panel independent and supports all the most common systems.

IT'S ENJOYABLE

Thanks to its unified dashboard, you can see all data in one place and manage all your servers through one platform. Your customers will see a 100% protected server instead of error messages!

If you want to hear about it from other users, check our case studies and be inspired by them:

CASE STUDY

In case you prefer to see it for yourself, try it for free:

SIGN UP FOR FREE TRIAL

BITNINJA
SECURITY