BITNINJA
SECURITY

imunify360

BITNINJA - IMUNIFY

MALWARE SCANNER COMPARISON

Malware poses a significant threat to anyone with an internet connection, particularly to hosting providers who are exposed to multiple IP addresses, hundreds of websites per server, and various fronts to defend against. With mixed results on both sides, providers often struggle to determine the most effective solution against cyber criminals.

One option for them is to seek out comparisons from reliable sources, but these can be hard to come by. Another option is to conduct internal testing, but this can be costly in terms of time and resources. It requires extensive testing and analysis to yield meaningful results.

To assist hosting providers in making an informed decision about server protection, BitNinja has conducted extensive testing to provide an objective and fact-based comparison of the leading malware scanner options available on the market.

THE TESTING METHOD:

During testing, all machines were run with the latest software versions. To ensure accuracy, the test was repeated three times. Three identical machines were used, each with the following specifications:

- 2 vCPUs (AMD Epyc-Rome)
- 4096 MB of RAM
- 100 GB NVMe storage
- CentOS Linux release 7.9.2009
- cPanel version 104.0.8 (Imunify requirement)

A total of 54792 benign files and 82846 malicious files were tested. The files were distributed as follows:

- JavaScript: 36612
- PHP: 17271
- TXT: 838
- Other: 28125

SCAN TIMES AND LOAD AVERAGES

Server performance is a vital concern for both providers and customers. Ensuring servers and websites run smoothly while maintaining security can be challenging, particularly with the abundance of misinformation. **The performance of the two solutions will be compared, with a focus on key metrics such as time and load averages.**

During testing, **137,680 files were analyzed**, both malicious and benign, and found that **BitNinja's "quick" scan took six minutes** to complete, while the **"deep" scan took 92 minutes**. In contrast, **Imunify required 182 minutes** for the same task.

Additionally, **Imunify's approach** of scanning files first and then cleaning them resulted in an additional three hours of processing time, making it **380% slower than BitNinja**.

Furthermore, load averages were also a significant factor in the comparison. **Imunify's performance** was hindered by its longer processing time and lack of optimization, resulting in **load averages peaking at 3.0**, which is considered high. In contrast, **BitNinja's loads were significantly lower**, exactly half of it, **even when cleaning was included in the process**.

These tests were conducted multiple times to validate the results, which consistently showed the superior performance of **BitNinja**. In fact, they have plans to further reduce the load on the system by **implementing a cloud scanner method in the first quarter of 2023.**

CLEANING AND QUARANTINING PERFORMANCE

It should be noted that while the test servers are in a controlled environment, the results may not entirely reflect real-world scenarios.
However, BitNinja maintains the validity of their testing method and results.
The dataset used in the testing contains a diverse range of malware "unknown" to the engines, and samples were collected from various sources, including the internet and internal test machines.

The main focus of the **test is on Javascript and PHP-based malicious files**, as they are the two primary players in this league.

With regard to **PHP-based malware, the results are relatively similar**. **BitNinja performed slightly better** with an overall 0.89% increase over Imunify. While this may seem small, it is important to note that even a slight increase could make a significant impact on customer satisfaction.
BitNinja's success rate was attributed to their PHP Behaviour Analyzer and Defense Robot, which generated more signatures.

When it comes to **Javascript-based malware, BitNinja caught an average of 25000, while Imunify caught 1960.**

To better reflect real-world results, the quarantining and cleaning results were combined. **Imunify prefers to clean all files**, including those that contain not only malware, and will **leave empty files behind** instead of quarantining them completely.
On the other hand, **BitNinja will quarantine purely malicious files** and **only clean injected malware** from benign files.
Neither approach is inherently better, they are simply different methods of dealing with malware.

When all file types were taken into account, **BitNinja outperformed Imunify, catching or cleaning an average of 69899 files**. Imunify's performance was weaker, catching an average of 34002 files. The significant differences in the results led BitNinja to question the validity of the results, but after multiple checks, the numbers remained consistent throughout the entire testing process.

FALSE POSITIVES

It is important to note that the occurrence of false positives is a concern for both providers and customers in the realm of server performance.
The possibility of a false positive causing a website to crash can cause great stress and frustration.
Fortunately, in the tests conducted, it was found that neither BitNinja nor Imunify360 generated any false positives. This is a positive outcome and provides assurance in the reliability and accuracy of both solutions.

SUMMARY

In conclusion, **both BitNinja and Imunify are effective solutions for server protection against malware**, but they offer different components and have different approaches to dealing with malware.

Based on the testing **BitNinja's solution was found to have superior performance** in terms of scan times, load averages, and cleaning and quarantining performance.

Imunify's approach of scanning files first and then cleaning them **resulted in longer processing time and higher load averages.**

However, it's important to note that **both solutions had no false positives**, and they are reliable and accurate.

Ultimately, the best solution for a hosting provider will depend on their specific needs and requirements.

MEASUREMENTS	BITNINJA	IMUNIFY
Detection Accuracy	82.68%	40.47%
False positives	0%	0%
Scan time*	6 min	182 min
Reaction time	1 sec	1 sec
Server load	0,55	3

*First phase scan time

In case the complete data set is needed, it can be provided upon request!