BitNinja
SERVER SECURITY

CASE STUDY

FastComet

https://www.fastcomet.com

The Company

FastComet is one the trendiest web hosting companies these days. They have more than 45,000 customers from 83 countries, over nine years of experience in system administration, and they've been providing public cloud hosting services since 2013. FastComet has a very high rating on HostAdvice, thanks to their high reliability, excellent 24/7 support, affordable pricing, easy usability, and fantastic features.

FastComet joined our Ninja Community in 2017 and we are delighted that since then they've become one of our biggest partners. Now, it's time to share the story about how BitNinja brought a new era to their business.

The marketing manager of FastComet, Elena Tileva, will tell you the kind of challenges they had before using BitNinja and how these things changed after protecting their servers with the Ninja Power.

BitNinja: Why did you start to use BitNinja?

„One of our biggest challenges as a hosting company is keeping our servers and customer sites secured. We take security very seriously, implementing active and passive measures to stop attacks and malicious intent in its tracks.

Like most solutions, starting to use BitNinja was a decision made out of necessity. With the increasing rate and intelligence of attacks, some of our customer's sites that ran on vulnerable code or out of date software were nonetheless being compromised. This was mostly due to the maturing sophistication of the attacks, making them increasingly difficult to detect. Not only that but by also with the rapid growth of our customer base we needed to scale not only in terms of hardware infrastructure but also enhance the tool systems and software we use. After an in-depth evaluation of the most common security and performance products issued we determined that the concept of protecting hosting nodes individually is a major bottleneck for the scaling process.

We needed a centralized system that can learn and record infrastructure-wide incidents in order to protect all servers proactively – a system that can prevent attacks before they would even reach our infrastructure instead of trying to mitigate them. We started looking for full spectrum solutions such that can put together several protection methods and consistently work through them to deliver a security protection at a level never seen before. During our research on the subject, we were pleasantly surprised to discover that not only others had already realized this idea into a strong security concept, but a few great teams have already developed sophisticated products in this niche. After extensive testing and evaluation, we came to the conclusion that the BitNinja product is very mature and provides all the tools we wanted to build our infrastructure."

BitNinja: What kind of attacks did you face before using our software?

„Compared to most of our competitors, our hosting is already much more secure. We have a heap of custom security systems under the hood to keep customers' websites safe. However, in spite of the robust security, with the increasing rate and intelligence of attacks, some of our customers' sites that ran on vulnerable code or out of date software, were nonetheless being compromised. Outdated WordPress installs and plugins. It is the plugins that cause the most grief, leading to malware and phishing files exposed to customer accounts. The reason for this is largely due to the growing sophistication of the attacks, making them increasingly difficult to detect."

BitNinja: What kind of solutions did you use before our product?

„Prior to starting using BitNinja, we have used various Open-Source and commercial scan services and application security extensions - ModSecurity, ClamAV, Patchman just to name a few.

It is a common truth that hosting providers suffer on a daily basis from the consequences of the many security vulnerabilities found in commonly used CMS's such as WordPress, Drupal, and Joomla. 90% of the customer websites we host are actually WordPress ones. Yeah, really. The most common cases we face are outdated WordPress scripts and plugins being exploited. Hackers would manage to upload phishing files to the account or they would SPAM and we'd get abuse emails sent to our datacenter. To fix this, we tried integrating Patchman on our servers.

Patchman detects these vulnerabilities and is able to safely patch them without assistance from your customer. While the software seemed to work well and had some great features - e.g. the ability to roll back patched files, see detailed stats on the number of WordPress installs is patched, files modified, so forth, we still had abuse emails come. It seems Patchman was not able to completely find old plugins and patch them, which was where most of the exploits were coming from. What is more, Patchman used to scan files only based on predefined definitions for malicious files and usually the problem used to be not among the uploaded malicious files, but with the infected files of the application itself.

Few of the drawbacks of using Patchman were:

- *It took literally 60 seconds to start scanning for vulnerabilities and malware.*
- *It scanned once per day.*
- *There was no real-time protection against vulnerabilities.*
- *It ate a lot of server resources*
- *High percent false-positive rating*

We gave up after a few months. Opposed to Patchman, BitNinja doesn't just virtual-patch known CMS vulnerabilities. BitNinja provides protection for the whole server on every protocol against a wide range of cyber attacks. It is literally a one-stop 360-degree security solution."

BitNinja: What results did you experience after installing BitNinja?

„So far we are seeing great net results in terms of malicious traffic prevention. With the help of the integrated set of modules system, we have prevented countless potential exploits, malicious objects, unwanted bots but what is even more important – we have managed to save an enormous amount of server resources that can now be used for a meaningful and legitimate activity by our customers. What we truly like about BitNinja compared to other server security solutions is that doesn't take up a lot of resources."

BitNinja: What do you think are the most positive and useful features?

„Last year, BitNinja decided to create an even more convenient way to validate browsers and valid traffic. They came up with the idea to build in Browser Integrity Check (BIC) instead of using the reCAPTCHA alone. It does some background checking of the browser and after that, it automatically delists the IP address. A neat resolution for the former CAPTCHA problems. This is a much more easy and convenient way to validate normal visitors and malicious attackers.

Adding our stable services and their Ninja security power, together we are able to defend hundreds of customers from the risks of cybercrime."

Still not convinced?

Try BitNinja for free. Register to our **7-day trial** and enjoy the protection immediately. In case of any question, please contact our team at ***info@bitninja.io***.
We are always happy to help.