

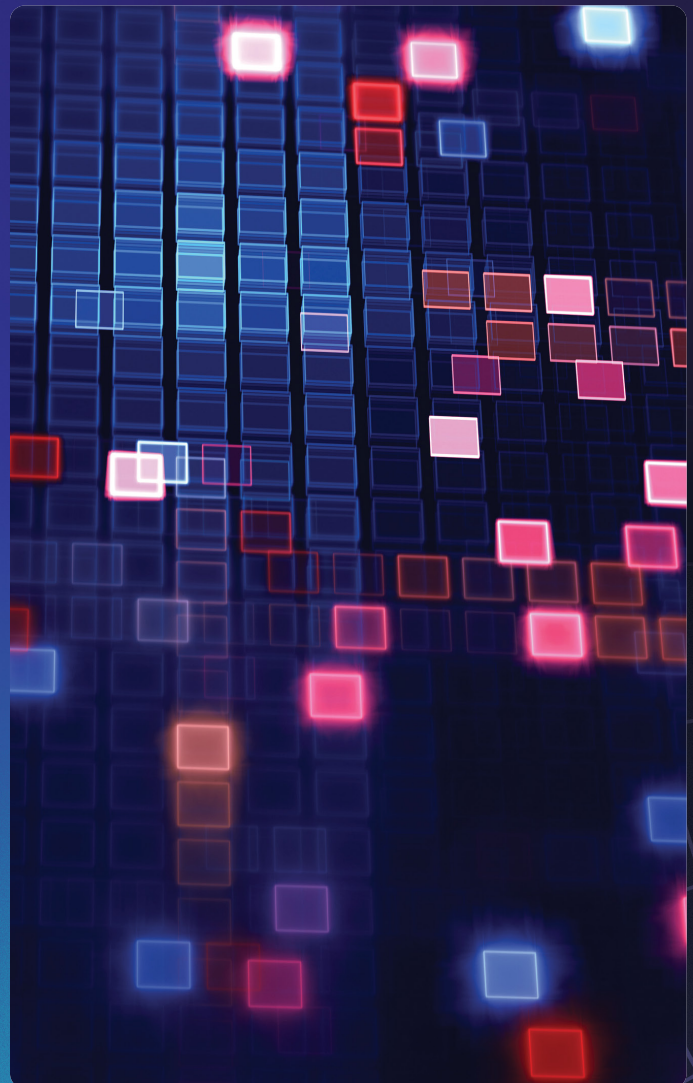
# Monetizing content filtering to increase profits

## bitCONNECT

“I was looking for a way to increase average revenue per customer and found Peacemaker to be an ideal product to upsell.”

---

LIONEL REDELINGHUYTS  
CEO AT BITCONNECT



## CHALLENGE

# How does the business work when everything is set up?

Lionel's decision was to give all of the customers the standard benefit of Peacemaker, so that all individuals and businesses are protected from malware, IoT attacks, phishing, and other cybernetic threats. This not only protects the customers, but keeps the network free of malicious traffic, minimizing the user-based security issues.

Lionel also describes the opportunity which arised thanks to Peacemaker's protection features: "One day a customer Whatsupped me and told me that their CEO received a phishing e-mail, and very nearly fell for it.

I told him that they are protected from the consequences, but it opened a dialogue and they subscribed for the content filtering as well. As Lionel says, this is the part of the process they are working on now – finding the best way to communicate the value in their materials and on BitConnect's website: "When we get to speak to the customer and explain what the product actually does, we usually get them to sign up for it."

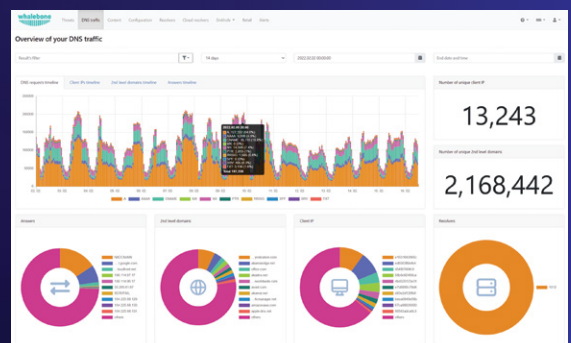
**What the ISPs appreciate about Peacemaker is the lack of maintenance and no demand for special hardware.**

After the setup, the only time when one needs to login into the portal is if there is a need to make a change to the policies or if a customer has an issue the ISP wants to look into.

**As Lionel describes: "It is set-up and forget type of thing; Peacemaker is really simple to run, the service is stable, I never have DNS resolution issues. It is scalable and flexible. Also, resource requirements to run Peacemaker are not high either, it does not cost me much to run the virtual machines where the software is located."**

"It took us two or three months to start making profit. Nowadays we make most money of the B2B segment – for example we have one business customer which has 8 offices, which brings three times more revenue than the whole price of our Peacemaker subscription."

**LIONEL REDELINGHUYS**  
CEO AT BITCONNECT



# Using Whalebone's capabilities, the filtering packages now have three main target groups, according to their needs:



## Protecting privacy and online identity

BitConnect's privacy protection hides IP of the user and filters out all of the requests by services such as Google Analytics or Facebook pixel, basically all of the standard tracking services.

**Higher tier of the package includes ad filtering as well.**



## Filtering of the adult content and unwanted usage

Ideal for the concerned parents, the family package filters out all of the adult content, abusive content, anything one would not want their child to come by on the internet.

**A stricter tier blocks torrenting and other unwanted usages as well, making it ideal for schools and public places.**



## Customizable packages for businesses

Businesses can opt for customizable package with their own rules and blocking pages. It allows them to find the exact mix of content and domain filtration to ensure that the work environment is effective and safe for all of the employees.

**The customers can just choose the package on BitConnect's website when they are signing up for their subscription.**

“It adds very little overhead to my network, and requires no interaction from the user. I just had to find a way of automating it as much as I can, so that we wouldn't have to manage individual IP addresses and so on. To my knowledge, there is no alternative, really, not that I'm aware of.”

**LIONEL REDELINGHUYS**  
CEO AT BITCONNECT

# How to start new revenue streams through DNS filtering?

- 1 Experience Whalebone – ask for an **individual demo** or a **14-day free trial**.  
**PRO TIP:** Contact your larger B2B customers individually with a special offer.
- 2 Create a virtual machine with minimal hardware—2 CPU cores, 4 GB RAM, 40 GB HDD—and run the Whalebone installation script. Forward DNS traffic to Whalebone resolvers. **The setup takes about an hour.**
- 3 Set up content filtering policies based on the needs of your individual, business, and institutional customers, as outlined in the product documentation.
- 4 Let new customers choose a package on your website and forward their traffic to the appropriate resolver. Reach out to existing customers for easy upsell opportunities.

“The implementation was easy. You obviously need to have some understanding of how to set-up the server and install some additional software on it, but there was not much to the process. Any questions I had were answered in the documentation. I did not log any tickets for the set-up process whatsoever.”

**LIONEL REDELINGHUYS**  
CEO AT BITCONNECT

## ADDITIONAL REFERENCES



Easily redirect part of your network traffic to Whalebone resolvers and try out our trial.

[peacemaker@whalebone.io](mailto:peacemaker@whalebone.io)  
We will be more than happy to answer any questions. Mutual satisfaction is our main goal and we will do our best to fulfill your requests.

[www.whalebone.io](http://www.whalebone.io)  
Learn more about our products at: [whalebone.io/peacemaker](http://whalebone.io/peacemaker)

 Follow us on LinkedIn for more information on DNS security.