whalebone

ŽELEZNIČNÁ SPOLOČNOSŤ SLOVENSKO

Railway Company Slovakia
Protecting employees all over the country and in the field

Whalebone Immunity Case study

> **Our regional service technicians are all over the country. When we see a spike in malicious traffic we alert them. They can see precisely which device is in danger and react immediately to stop the cause of the threat.**
>
> **Patrik Malý** | IT specialist, Railway Company Slovakia

Railway Company Slovakia is the **largest passenger transport railway operator in Slovakia**. The company is owned by the Slovak government, maintaining 1,500 train routes and 698 stations all over the country.

It provides a vital service to the country and its citizens and thus needs reliable and powerful protection for all of its employees.

The situation

How to secure employees all over the country?

Given that Railway Company Slovakia covers the whole country with hundreds railway nodes, it needs to constantly ensure the security of both the core team, technicians in the field, and office employees in the entire territory.

This situation required a security layer which operates on the network level covering all the devices without the need to constantly check and maintain any software. Also, it was vital to **protect technicians and other employees** who take care of the railways **in the field**.

The challenge

Implementing a security product to a large segmented network

> **Even though I was not used to working with Linux, I was able to deploy Whalebone Immunity in half a day thanks to comprehensive product documentation.**
>
> **Patrik Malý** | IT specialist, Railway Company Slovakia

The company director decided to start the proof of concept to try Whalebone Immunity out. The IT team found out that they are able to implement it to the current infrastructure based on the documentation provided by Whalebone, even without deep knowledge of Linux.

It has integrated with both their VPN and firewall systems. The responsible team has utilized automation tools which re-direct DNS traffics in devices all over the network. In parts of the network where this was not possible, the regional technicians made sure all of the DNS traffic was forwarded to Whalebone DNS Resolver.

In the very beginning, there were some small technical discrepancies on both sides, since the infrastructure of Railway Company Slovakia is specific and does not allow communication across the whole network, which poses a problem for many security vendors.

Nevertheless, thanks to cooperation of the local IT team and Whalebone's technicians, the initial hiccups were promptly worked out and the proof of **concept was successful for both sides.**

> **Whalebone Immunity smoothly integrates with all of our security measures, adding an important security layer to stop threats other solutions might miss.**
>
> **Patrik Malý** | IT specialist, Railway Company Slovakia

The solution

Protective DNS as a cornerstone of cybersecurity

The Railway Company has set-up security policies and alerts according to the best practices provided by Whalebone, and monitors leaks of sensitive information using the Identity Protection feature.

The core IT team receives regular reports and checks the DNS traffic in the UI. If they see any suspicious behavior, they provide access to the regional technicians who are able to immediately identify the vulnerability and which device and user was compromised. This allows them to deal with any potential threat before it can cause any damage to the network.

> **Our regional service technicians are all over the country. When we see a spike in malicious traffic we alert them. They can see precisely which device is in danger and react immediately to stop the cause of the threat.**
>
> **Patrik Malý** | IT specialist, Railway Company Slovakia

Solving problematic online behavior of employees

The Railway Company's IT team could see that there was an excessive amount of traffic in a remote location near the country's eastern border. The office was out of bounds for the monitoring tools due to technical difficulties, but after setting up Whalebone Immunity, it quickly became clear that the traffic is caused by **playing online games and mining cryptocurrencies. Whalebone Immunity was used to block both activities,** solving the problem immediately.

The result

Whalebone Immunity is now an **integral part** of Railway Company's security stack, running in the background to make sure no threats manage to penetrate the network's defenses. "Each vendor has a different approach to cybersecurity, different metrics and threat databases – it is important to **combine multiple products to ensure a high level of security** for the whole environment," says Railway Company's IT specialist Patrik Malý.

> **Whalebone Immunity runs smoothly, the UI is easy to use, and it integrates well even in our complex infrastructure. Overall, it is a great security product.**
>
> **Patrik Malý** | IT specialist, Railway Company Slovakia

Panasonic · A1 · Telefónica · TELE2 · BAUHAUS · Raiffeisen BANK · ALD Automotive · COLT CZGROUP

In just a few hours, you can set-up Whalebone DNS Resolver and try out Whalebone Immunity for 30 days for free.

Learn more about our product at whalebone.io/whalebone-immunity, ask for a demo call or contact us via e-mail:

immunity@whalebone.io

Secure your network's blind spots today:

www.whalebone.io

Follow us on LinkedIn for more information on DNS security.