CASE STUDY

# Security DNS Filtering in AERO Vodochody AEROSPACE

**Company AERO Vodochody AEROSPACE continuously seeks and deploys technologies that improve the security of internal information systems and data. In the autumn of 2017, AERO was approached with an offer to test a tool that is aimed at protecting against malware. The customer was particularly interested in a simple concept that allows you to protect a wide range of endpoint types without the need for a complex configuration.**

After consultation with AERO's IT partner SOLEDPRO the solution was evaluated as a suitable addition to the existing methods of enterprise network protection.

**„For the first time in my career, I have experienced a quick and seamless integration of security technology into the whole network."**

**Miloš Vodička, manager ICT**

## Test deployment

In the company they demanded a thorough technical verification of the technology offered to evaluate the compliance of all tracked attributes.

The obvious requirement was not to disrupt the functioning of existing IT infrastructure, especially **Active Directory**, which relies on DNS.

One of the deployment options was to use the Whalebone cloud DNS resolvers to enable testing without having to deploy server components into the internal environment.

However, AERO opted for the Whalebone DNS resolver on-premise when the primary resolvers are located on the corporate network. To ensure high availability of DNS traffic it was decided to operate three independent DNS resolvers.

The installation required customer cooperation in the form of installing three Linux servers. Resolver installation was performed using a script generated directly in the Whalebone web console.

The script provides all the necessary checks and installs the dependecies, and at the end the DNS resolver runs on the server. After the installation there is only one step left, to set up the forwarding to the Domain Controllers.

## Production deployment and protection

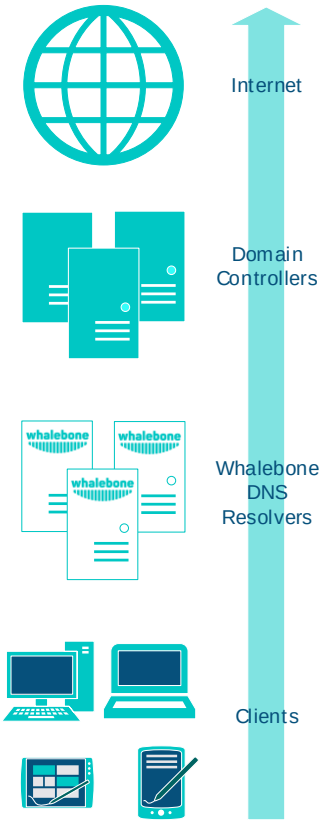
After testing the DNS resolution functionality, including the test of Active Directory, it was planned to redirect test clients to a new DNS resolver using DHCP. Configuration change has gone smoothly and infrastructure has started to use new resolvers. All without a single outage and without having to communicate changes made to the users.

The Whalebone DNS traffic protection policies were set according to the customer expectations - **block maximum threats**, but ensure the least amount of administrator interaction required. The policies have been set in a restrictive way, but avoiding the usual risks of false positives. Blocking began to work and several incidents were blocked during two weeks of testing without any false positives.

## Conclusion and operational experience

**Testing was considered successful** and the solution was approved from the technical point of view. The next step was to settle the business matters. The offer was prepared as a monthly subscription for hundreds of users. The price was reasonable for the customer and did not hinder the transition to full operation. Technically, this did not mean any change, because the test topology and installation fully complied with the requirements of the production environment.

**Aero Vodochody AEROSPACE is the world's largest manufacturer of training jet airplanes. In total, it produced 11 000 aircrafts with a total of 13 000 000 flight hours. Aero has developed and manufactured more than 6 700 jet airplanes, accounting for 70% of world production.**




A lower number of incidents blocked than usual in AERO Vodochody network implies a greater emphasis on company security. However, Whalebone still managed to detect and block suspicious software on machines fully managed by an external contractor. After communication with the contractor the machines were remedied. Other incidents in daily traffic concern the user's network in particular and are blocked without the need for administrator intervention.