

Project – Endpoint Security Solutions

By Joshua Edwards

Situation – The antivirus solution in place at the organization is due to expire, therefore we need to research the current solution and the alternatives. The current solution has discontinued support for the Windows Server 2008 R2 version, therefore we are potentially looking for a solution which is compatible with the server versions in use at the site and which also provide endpoint protection at host level in addition to server level protection.

Task

The first step is to research potential antivirus solutions which can protect more than 120 devices including pcs and VM servers. Gather quotes from 3 providers which can provide the service. Select a solution based on cost, features, compatibility. Implement the solution to the devices on the network, create suitable antivirus, web and firewall policies to suit various groups within the organization. Test the solution on VM image. Deploy the system into production.

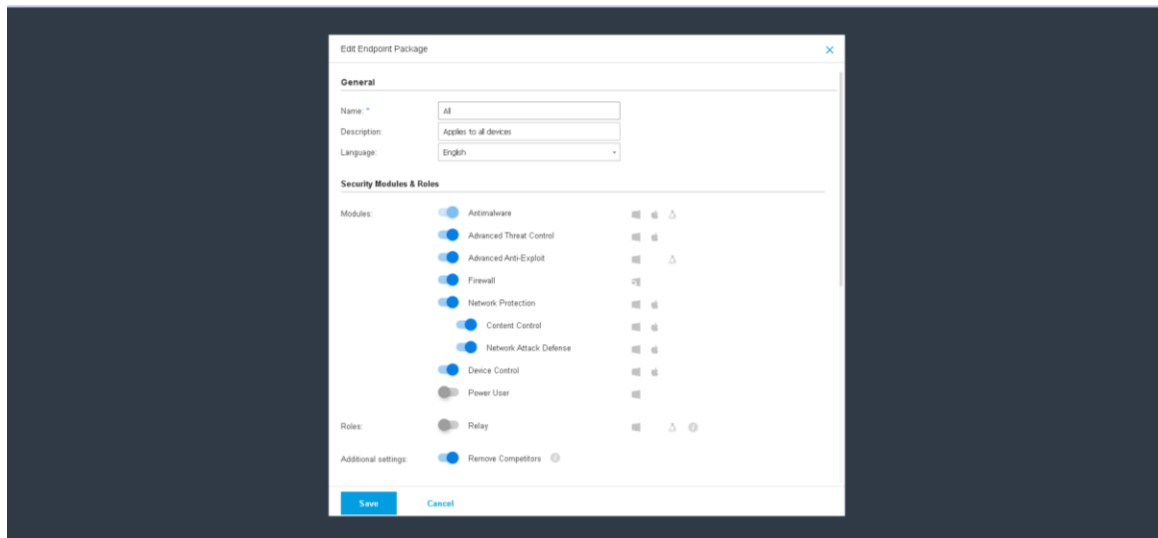
Action

I researched the available solutions

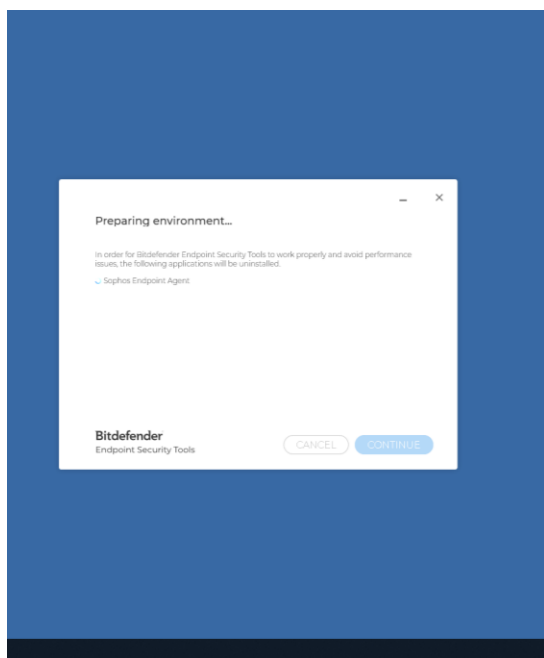


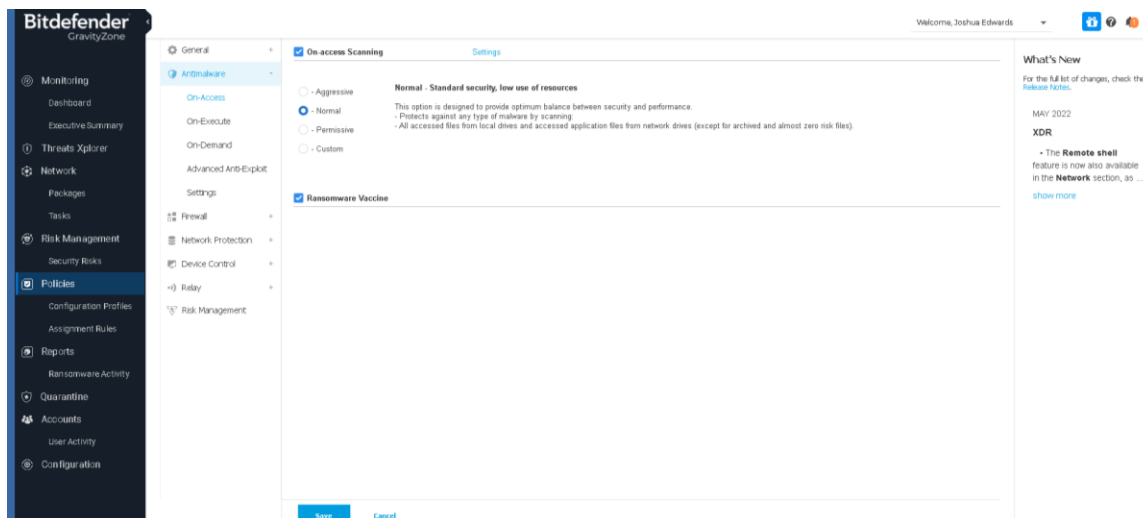
Contacted each of the providers for more information on their solution. I also gathered quotes, then arranged a demo for the most suitable product.

We decided to go with the Bitdefender Gravity Zone solution, it was cheaper than the others and also came bundled with the firewall included. Below, I configured the policies for the endpoints.

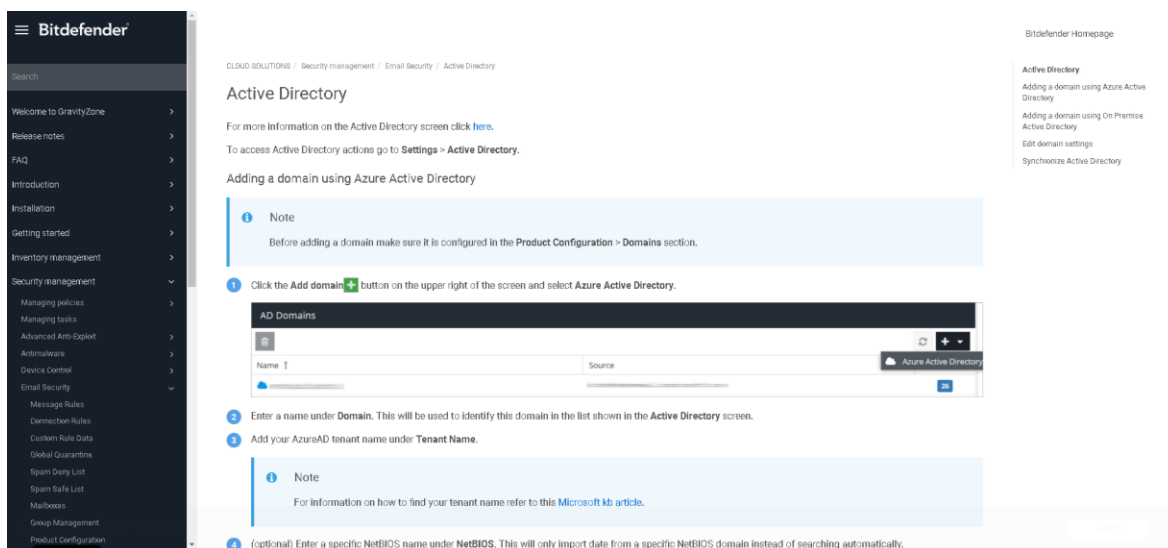


The system allows for a relay endpoint to be installed onto the domain controller, which is then used as a central installation point for the other devices on the network.





Connect all devices on the network via network discovery scan from the relay device.



I Tested installation in VM area

Result

The new security solution is in place and has been deployed to all workstations and servers and is working well. The feedback received from users has been positive, we are further reviewing policies for improvement.

