



NIGHTVISION VIRTUAL APPLIANCE

IN-HOUSE AI FOR PRIVATE MALWARE DETECTION

Avira's NightVision Virtual Appliance delivers powerful on-premises malware analysis, without the need to connect and upload files to a cloud security service.

The NightVision Virtual Appliance from Avira allows you to apply Avira's NightVision™ machine learning capabilities within your own network. Combined with the proprietary algorithms of Avira's Advanced Scan Engine, it delivers a probability estimate of artefacts being malware. Avira's NightVision Virtual Appliance embeds Avira Protection Cloud-like capabilities within a private network bringing state of the art malware detection and protection systems in-house, while protecting the privacy of your data.

The benefits of using the Avira NightVision Virtual Appliance within a private domain include:

- Data privacy: There is no uploading of any data to a third-party cloud services for analysis
- Availability: No reliance on a continuous, low latency connection to cloud-based security services
- Cost efficiency: High volumes of malware analysis can be accomplished in-house without using a third party provider
- Ease of integration: The provided virtual machine image is ready to use – simply “plug and play”

Avira's NightVision Virtual Appliance is the closest thing to having the Avira Protection Cloud in-house. Suspicious files are uploaded to the NightVision Virtual Appliance through a simple REST API.

The NightVision Virtual Appliance then undertakes analysis using:

- Avira's Advanced Scan Engine. This engine, otherwise unreleased to the public, uses proprietary definitions and heuristic algorithms as well as powerful content extraction

and deobfuscation techniques to identify malware. This powerful scan engine can analyse far more thoroughly than any endpoint scanning tool quickly reaching a conclusion whether code is part of a known malware family.

- NightVision™, Avira's advanced machine learning platform. The virtual appliance is regularly updated and applies a classifier model built from an ensemble of machine learning techniques to analyze files. With knowledge of 200 million malicious and clean samples and 9000+ attributes (features), NightVision™ delivers a highly robust and accurate probability score indicating whether the analyzed file is malicious or benign.

Key Features:

- Powerful malware detection for private networks
- Zero-day threat detection using state-of-the-art AI technology
- Simple to deploy: The NightVision Virtual Appliance is provided as a complete, pre-configured virtual machine image. Simply start on a hypervisor and it is ready to go
- Scales simply by adding more virtual appliances
- Accessible using a REST API or web interface
- Combines Avira's in-house Advanced Scan Engine which leverages powerful proprietary algorithms with NightVision™, Avira's advanced machine learning system
- Delivers a malware classification, and a probability score of between 0 and 100% revealing how malicious a sample is



INTEGRATION

Avira's virtual appliance is straightforward to download and run. It takes just a couple of minutes to set up, which mainly involves configuring the network interface.

The appliance runs in approximately 8 GB of memory.

Depending on the level of privacy required, the NightVision Virtual Appliance can connect to the Avira master license server, or to a private license server within the customer's own domain. Regular image downloads keep the detection and classification model up-to-date.

A REST API or web interface is available to access the NightVision Virtual Appliance directly. Performance scales with the number of virtual appliances applied to the task.

SPECIFICATIONS

System requirements:

8 GB RAM
4 CPU cores
20GB disk space

Application type:

.ova

Supported platforms:

VirtualBox
VMWare

Implementation:

Accessed through a REST API or web interface

Performance:

100ms to a target of 60 seconds dependent on threat type

System and model updates:

As agreed, but typically daily

File attributes:

>9000

OUR AWARDS



FIND OUT MORE

Website: oem.avira.com

Email: oem@avira.com

Blog: insights.oem.avira.com

LinkedIn: Avira

Europe Middle East, Africa

Avira
Kaplaneiweg 1
88069 Tettngang, Germany
Tel: +49 7542 5000

Americas

Avira, inc
c/o WeWork, 75 E Santa Clara Street
Suite 600, 6th floor San José
CA 95113 United States

Asia/Pacific and China

Avira Pte Ltd
50 Raffles Place
32-01 Singapore Land Tower
Singapore 048623

Japan

Avira GK
8F Shin-Kokusai Bldg
3-4-1, Marunouchi Chiyoda-ku
Tokyo 100-0005, Japan