OPENVAS Basic

Vulnerability Management
for Small Companies

The “OPENVAS Basic” virtual appliance was developed to **protect small and medium-sized companies**. It is characterised by simple commissioning and operability and offers important **functions for the professional vulnerability management** of IT infrastructures.

Advantages

Scan capacity

- Coverage of up to 200 IP addresses within 24 hours*
- Execution of vulnerability tests and compliance audits
- CVE scanner for predictive vulnerability analysis

Supported standards

- Network integration: SSHv2, LDAP, RADIUS, NTP, IPv4/IPv6
- Vulnerability classification: CVE, CPE, CERT-Bund, WID-SEC, DFN-CERT

Features

- Intuitive web interface for managing and executing scan tasks
- Advanced reporting features with filtering, sorting, notes & risk assessments
- Automated scans based on customizable schedules
- Automatic notifications upon scan completion
- Reports available in PDF, HTML, text, or XML formats
- Appliance performance overview
- Integrated certificate management
- Backup functionality via VM snapshot
- No API support (GMP)
- No sensor integration**
- No support***

*Estimated value. The actual achievable number depends on the scan configuration, the scan targets, the network infrastructure, the utilisation of the system resources and the frequency of the scans.

***„OPENVAS Basic“ can neither control other appliances as sensors nor be controlled as a sensor by another appliance.

***Technical support can be purchased separately.

Specifications

Hypervisor

The following hypervisors are supported:

- Microsoft Hyper-V, version 5.0 or higher
- VMware vSphere Hypervisor (ESXi), version 6.0 or higher
- VMware Workstation Player, version 16.0 or higher
- VMware Workstation Pro, version 16.0 or higher
- Oracle VirtualBox, version 6.1 or higher

System requirements

- 64-bit Linux operating system
- 2 vCPUs
- 12 GB RAM
- 500 GB HDD

Connections

- 4 virtual ethernet ports