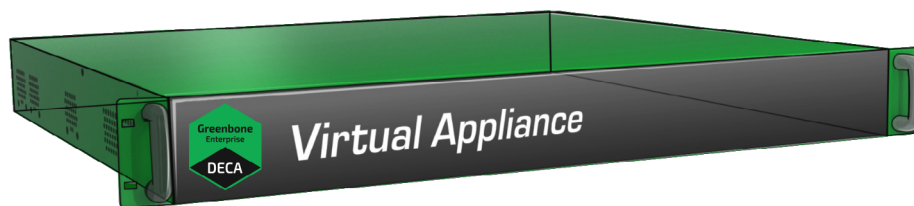# Greenbone Enterprise DECA

Data Sheet

The **Greenbone Enterprise Appliance** is a vulnerability management solution that integrates seamlessly and transparently into your security strategy, providing vulnerability assessment and threat management capabilities.

It also detects violations of corporate security policies and regulations. With a strong focus on third-party integration and open standards, the Greenbone Enterprise Appliance is a best-in-class security solution that enhances and complements your security posture. Furthermore, it enables automated vulnerability management.

The **Greenbone Enterprise DECA** controls sensors for up to 2 security zones and covers up to 300 IP addresses. The operational areas are mid-sized enterprise IT or larger branch offices.

Specifications

Hypervisor
The following hypervisors are supported:
- Microsoft Hyper-V
- VMware vSphere Hypervisor (ESXi)
- Huawei FusionCompute

System Requirements
- 64 bit Linux OS
- 4 vCPUs
- 8 GB RAM
- 220 GB HDD storage

Connectivity
- 4 virtual Ethernet ports

Benefits

- Turnkey solution: simple and uncomplicated setup within shortest time
- Powerful appliance operating system Greenbone OS with specially adapted, console-based administration
- Integrated Greenbone Enterprise Feed with more than 150,000 vulnerability tests with daily, automated updates
- Integrated backup, restore and GOS upgrade
- Integrated web interface for scan management
- No limitation on number of target IP addresses (effective number depends on scan pattern and scanned systems)
- Subscription includes the Greenbone Enterprise Support, the Greenbone Enterprise Feed and updates

Greenbone Enterprise DECA

Data Sheet

Scan Capacity
- Up to 300 IP addresses in 24 h
- Control of up to 2 sensors
- OpenVAS scanner for vulnerability tests and compliance audits
- CVE scanner for prognosis scans

Supported Standards
- Network integration: SSH, SMTP (e-mail), SNMP, SysLog, LDAP, RADIUS, NTP, DHCP, IPv4/IPv6
- Vulnerability classification: CVE and CPE
- Severity classification via CVSS
- Network scans: WMI, LDAP, RADIUS, HTTP, SMB, SSH, TCP, UDP, etc.
- Compliance policies: CIS Benchmarks, IT-Grundschutz, BSI TR-03116 etc.
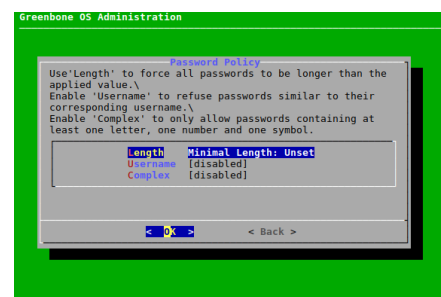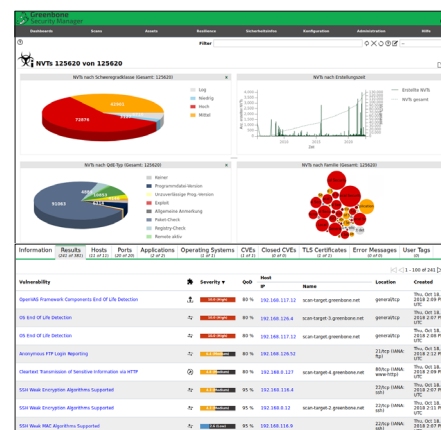
Graphical Web Interface
- Managing and starting scan tasks
- Report with filtering, sorting, notes, and risk scoring
- Automated scans through schedules
- Alerts, including on scan completion
- Multi-user support
- Clustering and distributed scanning via master-sensor mode
- Reports as PDF, HTML, text and XML
- Appliance performance overview

Integration/API
- Greenbone Management Protocol (GMP), encrypted
- All user actions of the web interface available via API
- Easy integration with other applications using the API
- Simple automation via command line tools (CLI)

Operating System Features
- Network integration and configuration
- Airgap function
- Backup, restore, upgrade