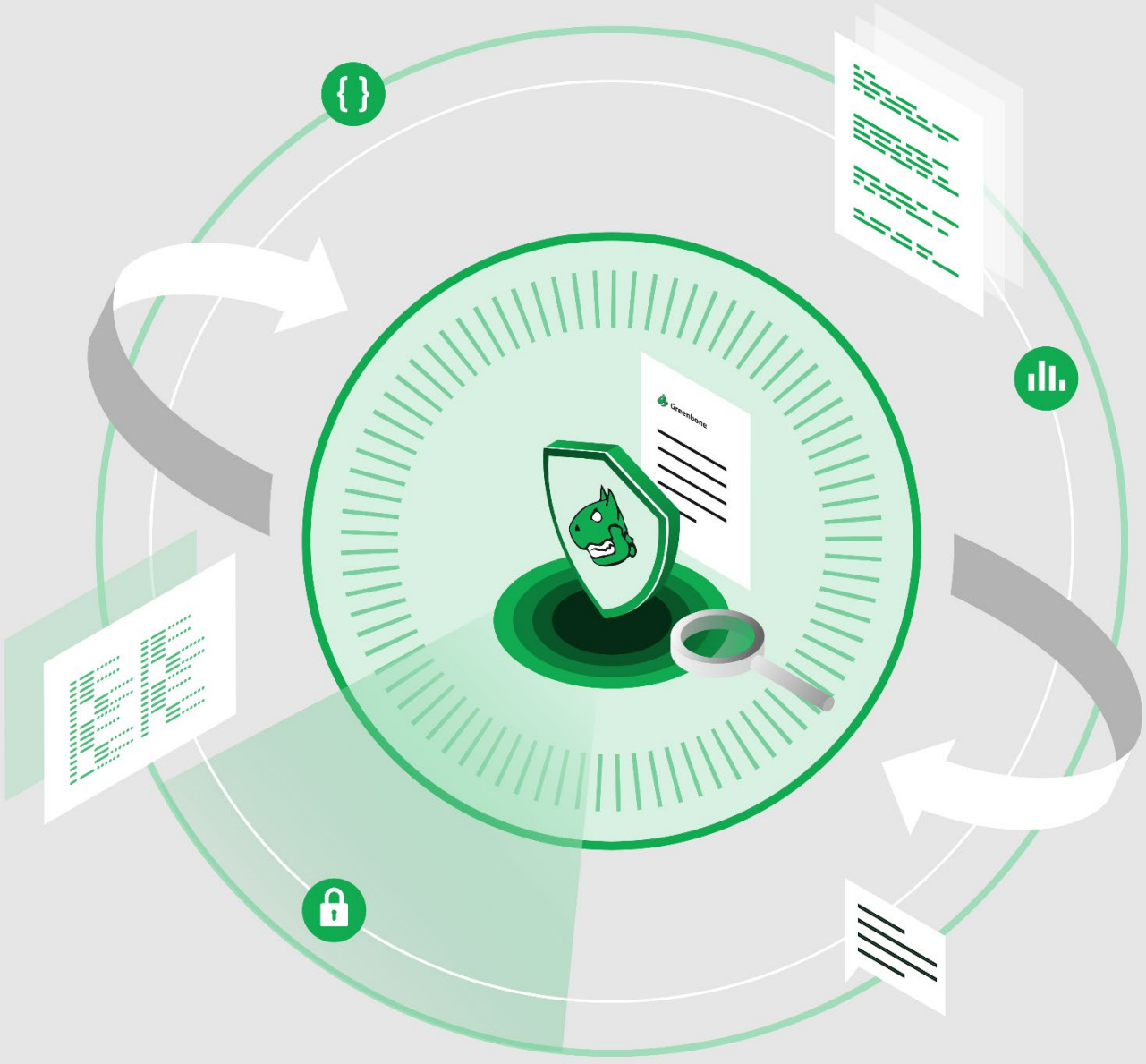
Greenbone

Our Solutions in Comparison

Greenbone Source Edition, Greenbone Enterprise Appliances and Greenbone Cloud Service



Date: 2022-05-05

Content

Open source IT security does not only deliver a high level of transparency of the solution itself. It is a contribution to the IT security community in general. We are related to this idea and committed to it. This whitepaper shall help our customers and users to understand the differences between the solutions.

1 Introduction

The **Greenbone Vulnerability Management** (GVM) is a framework originally built as a community project named “OpenVAS” and is primarily developed and forwarded by Greenbone Networks.

It consists of the **Greenbone Vulnerability Manager Daemon**, the **Greenbone Security Assistant** with the **Greenbone Security Assistant Daemon** and the executable scan application that runs vulnerability tests (VT) against targets.

The GVM framework is released under Open Source licenses as the **Greenbone Source Edition**. By using it, Linux distributions can create and provide GVM in the form of installation packages. In this way, private individuals can install and use GVM as well.

The Greenbone Security Assistant is the web interface that a user controls scans and accesses vulnerability information with. The communication occurs using the **Greenbone Management Protocol** (GMP) with which the user can also communicate directly by using different tools.

The **Greenbone Enterprise Appliances** are the commercial products and available as virtual or hardware appliances. They comprise the framework GVM as well as the **Greenbone Operating System** (GOS) which provides further functionalities.

The appliances receive the vulnerability tests for scanning from the **Greenbone Enterprise Feed**.

The **Greenbone Community Appliance** is a non-commercial virtual appliance and has a more limited feature set than the Greenbone Enterprise Appliance. It uses the less extensive **Greenbone Community Feed** instead of the Greenbone Enterprise Feed.

The **Greenbone Cloud Service** is a SaaS solution. Scan requests are forwarded via the cloud to the **Greenbone Scan Cluster**. From the Scan Cluster, scans are performed for external or internal targets. The GVM scanner is used for scanning and the vulnerability tests are also obtained from the Greenbone Enterprise Feed.

Neumarkt 12 • 49074 Osnabrück • Germany • www.greenbone.net/en/

2 Feed

The base of both feeds is identical. All content that is included in the Community Feed can also be found in the Enterprise Feed. However, the Enterprise Feed extends the Community Feed with some vulnerability tests and compliance policies.

Greenbone includes all self-developed Vulnerability Tests (VT) into its professional Greenbone Enterprise Feed, but not into the Community Feed.

Group	Greenbone Community Feed (Basic Coverage)	Greenbone Enterprise Feed (Extended Coverage)
VTs for Home Application Products (e.g., Ubuntu Linux, AVM Fritzbox, MS Office)	✓	✓
German “IT-Grundschutz”	✓	✓
VTs for Enterprise Products (e.g., MS Exchange, Palo Alto, Cisco, IoT/OT)	×	✓
Compliance Policies for CIS Benchmarks	×	✓
Additional Policies	×	✓
Access to Greenbone Enterprise Support	×	✓
Access to Professional Services	×	✓

3 Solution Delivery, Deployment and Support

The Greenbone Enterprise Appliances can usually be handled with much less effort in setup and operation compared to own Source Edition software installations for which the customer needs to take care of the underlying hardware, operating system, and database system.

Additionally, master-sensor deployments covering nation-wide enterprises with multiple locations or even a global network of branch offices are possible with very little effort using the professional solution.

The Greenbone Cloud Service is delivered as a cloud solution, which also means low setup effort. Gateway components enable scanning of internal IP addresses.

All elements of the Greenbone Enterprise Appliance and the Greenbone Cloud Service are covered by the Greenbone Enterprise Support.

The table below lists some more differentiating elements regarding solution delivery, deployment and support:

Criteria	Greenbone Source Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
Setup	Individual selection of operating system and hardware Built on own responsibility or installation of community packages	Turnkey solution Simple and uncomplicated setup within shortest time	Simple account registration, and configuration within shortest time
Feed Compatibility	Established on own responsibility	Assured with SLA	Assured with SLA
Performance	Optimized on own responsibility	Optimized for hardware	Variable according to requirements
Backup/ Recovery	Solved individually	Integrated	Integrated
Fixes/Improvements	Managed on own responsibility	Assured with SLA	Assured with SLA
Support	Via (external) community on voluntary basis	Assured with SLA	Assured with SLA
Software Updates	Manual source build updates and manual migration of data	Regularly and seamlessly	Continuously

4 Features

The GVM framework already provides a rich set of features around vulnerability scanning: scanning for plain software vulnerabilities, policy controls, checks for configuration controls and managing assets with additional information to prioritize identified vulnerabilities according to asset criticality.

Furthermore, the Greenbone Enterprise Appliances and the Greenbone Cloud Service provide a variety of functionalities tailored to the respective environment:

Criteria	Greenbone Source Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
Possibilities for Updates & Feed	Only Greenbone Community Feed	Daily automatic Possible via per appliance configurable sync ports, redundant proxy servers, USB or FTP Airgap, or master appliance	Daily automatic
System Update	Dependent on distribution or on own responsibility	Contains security updates Update from any version to latest release possible Grace periods for EoL and LTS Migration of data and configurations between appliances and versions	Automatic Continuous security and platform updates
Protocols	Configure and set up on own responsibility	NTP, GMP, OSP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS and more	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, LDAP, RADIUS and more
Integrations and Connectors	Not available	Different vendors like PaloAlto, Fortinet, Cisco FireSight, Nagios, Splunk, Verinice and more	RESTful API for all functionalities
Backup/ Recovery	Solved individually	Backup for user data, system data via LVM, transfer via SCP or USB	Automatic
Alerts/ Schedules	Configured on own responsibility via operating system	Via e-mail, HTTP, SMS, connector to a SIEM or ticket system and more Complete scheduling possible	Via e-mail, Slack or Microsoft Teams
Scan Architecture	Not available	Master/sensor, Airgap inside of high security zones	Cloud scanner, gateway components for internal scans