Our Solutions in Comparison

Greenbone Source Edition, Greenbone Professional Edition and Greenbone Cloud Services

WhitePaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2020-10-29

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** (gvmd), the **Greenbone Security Assistant** (GSA) with the **Greenbone Security Assistant Daemon** (gsad) 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** (GSE). 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 GSA 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 Professional Edition** (GPE) is the commercial product line and available as a virtual or physical appliance. It is based on the **Greenbone Security Manager** (GSM) which comprises the framework GVM as well as the **Greenbone Operating System** (GOS) which provides further functionalities.

The GSM receives the vulnerability tests for scanning from the **Greenbone Security Feed** (GSF). The **Greenbone Security Manager TRIAL** (GSM TRIAL) is a virtual machine and serves as a free trial version of the GSM. By default, it uses the less extensive **Greenbone Community Feed** (GCF) instead of the GSF.

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

2 Feed

The Greenbone Security Feed (GSF) and the Greenbone Community Feed (GCF) differ in four main areas: content, quantity, quality and availability.

Features	GSF	GCF
Included VTs	All VTs	Only basic VTs
Quality Assurance (QA)	Consistent	Variable
Availability	Assured with SLA	No promise
Fixes/Improvements	Assured with SLA	No promise
Support	Assured with SLA	Via community on voluntary basis
Updates	Constantly/daily	Constantly/daily, but without enterprise features
Transfer	Encrypted	Unencrypted
VT Signatures	SLA for QA/fixes	Transfer integrity

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

These VTs can be grouped as shown in the following table:

Group	GSF	GCF
Hot VTs	Yes	Yes
VTs for Home Products	Yes	Yes
German “IT Grundschutz”	Yes	Yes
VTs for Enterprise Products	Yes	No
Compliance (e.g., PCI, ISO27001)	Yes	No
Operational Technology (ICS/SCADA)	Yes	No
Signed VTs	Yes	No

The following list shows some examples of products and applications for which no vulnerability tests are included in the Greenbone Community Feed:

- Generally, all enterprise-grade products and all operational technology (i.e., ICS/SCADA) products
- Microsoft Windows Server and Microsoft back office solutions (e.g., SharePoint, SQL Server)
- Products by Palo Alto Networks, Cisco, Juniper Networks and Fortinet
- Oracle Solaris IBM WebSphere products (e.g., IBM WebSphere Application Server)
- HCL Notes
- VMware paid products

All in all, the Community Feed encompasses about 30 % less VTs than the professional feed.

3 Solution Delivery, Deployment and Support

The Greenbone Professional Edition (GPE) can usually be handled with much less effort in setup and operation compared to own GSE software installations for which the customer needs to take care of the underlying hardware, operating system, and database system. That is why the GSM is always delivered as an appliance with all elements of the solution covered by the professional Greenbone Networks support.

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 Services (GCS) are delivered as a cloud solution, which also means low setup effort. Gateway components enable scanning of internal IP addresses.

All elements of the GPE and GCS are covered by the professional support of Greenbone Networks.

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

Criteria	Own GSE Installation	GPE	GCS
Setup	Individual selection of operating system and hardware Built on own responsibility or installation of community packages	Turn-key (approx. 10 min)	Turn-key (approx. 10 min)
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, GPE and GCS provide a variety of functionalities tailored to the respective environment:

Criteria	Own GSE Installation	GPE	GCS
Possibilities for Updates & Feed	Only Greenbone Community Feed	Daily automatic Possible via GSM configurable sync ports, redundant proxy servers, USB or FTP Airgap, or GSM master	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	RestFull 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, Splunk or Microsoft Teams
Scan Architecture	Not available	Master/sensor, Airgap inside of high security zones	Cloud scanner, gateway components for internal scans