The Different Flavors of Greenbone's Technology

Greenbone Security Manager and Greenbone Community Edition

Whitepaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

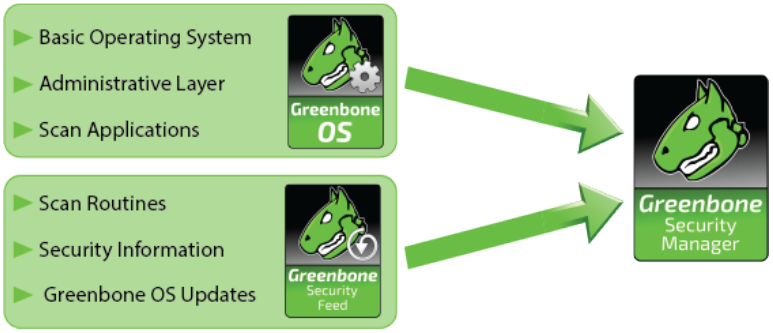
Greenbone
Sustainable Resilience

2018-02-05

Open, Transparent, Professional

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.

Introduction



Our Greenbone technology is architectured in two main components (Greenbone OS and Greenbone Feed) and it is available in two different versions.

The **Greenbone Security Manager (GSM)** is a feature-rich enterprise solution providing needed capabilities for its integration into an overall security architecture, even for high-security networks requiring an air-gap approach. It is built for the professional use in enterprises and administrations, delivered as a turn-key appliance. It delivers the full capabilities and features to our enterprise customers in a hassle-free way, where there is only one who is responsible for the functioning of your Vulnerability Management Solution – Greenbone Networks.

The **Greenbone Community Edition (GCE)** for the security-aware user in SOHO (Small Office Home Office) environments, delivered as a virtual machine or as source packages. Installation of hardware, operating system and additional components, even the compilation (in case of the source packages) is within the responsibility of the SOHO user. GCE is a light version of the commercial product for professional use, called the Greenbone Security Manager (GSM). The Community Edition is designed to operate stand-alone in small environments.

The project requirements make the difference. The following tables provide details about the difference between the two flavors of Greenbone's technology, summarized for the major aspects of the solution:

- Security Feed
- Solution Delivery, Deployment and Support
- Features

Security Feed

The Security Feed for both versions differs in four main areas: Content, quantity, quality and availability.

Features	Greenbone Security Feed	Greenbone Community Feed
NVTs included	Every NVT	Only basic NVTs
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
NVT Signatures	SLA for QA / Fixes	Transfer Integrity

Greenbone includes every self-developed Network Vulnerability Test (NVT) into its professional Greenbone Security Feed (GSF), but not into the Community Feed (GCF).

These NVTs can be grouped as:

Group	GSF	GCF
HOT NVTs	Y	Y
NVTs for Home Products	Y	Y
German "Grundschutz"	Y	Y
NVTs for Enterprise Products	Y	N
Compliance (i.e. PCI, ISO27001)	Y	N
Operational Technology (ICS / SCADA)	Y	N
Signed NVTs	Y	N

The following list gives some examples of those professional enterprise-grade products which are only part of the professional Greenbone Security Feed:

- Generally, all Enterprise-grade products and all OT (i.e. ICS/SCADA) products
- MS Windows Server and back office solutions (e.g. SharePoint, SQL Server, etc.)
- Products from Palo Alto Networks, Cisco, Juniper Networks and Fortinet
- Oracle Solaris IBM WebSphere products (i.e. IBM WebSphere Application Server)
- Lotus Notes or SAP products
- VMWare paid products

All in all, the Community Feed encompasses about 30% less NVTs than those included in our professional feed.

Solution Delivery, Deployment and Support

An appliance can usually be handled with less effort in setup and operation compared to software installations, where the customer needs to take care of the underlying hardware, Operating System, and database system. That's why the Greenbone Security Manager is always delivered as an appliance, where all elements of this solution are covered by the professional support of Greenbone Networks.

GSM Midrange Appliance (GSM 650A)

Master/Sensor deployments are possible with the professional solution, covering nation-wide enterprise with multiple locations or even a global network of branch offices.

The Greenbone Community Edition is used for trial/testing purposes and scales for small environments. The table below lists some more differentiating elements within solution delivery, deployment and support.

	Greenbone Security Manager	GCE or own installation
Setting-up	Turn-key (approx. 10 min)	Selection of operating system and hardware, then build on your own or install community packages; perhaps use the GCE.
Coverage	Concerted: All solution modules with several scan tools	Select and align on your own or take community defaults
Feed compatibility	Assured with SLA	Establish your own
Performance	Optimized for hardware	Optimize on your own
Backup/Recovery	Integrated	To be solved individually
Fixes	Assured with SLA	To be managed on your own, perhaps import Community-Fixes
Support	Assured with SLA	Via community on voluntary basis
Engine Updates	Regularly and seamless	Re-Install of a newer GCE or manual source build updates. Manual migration in both cases.

Features

The common technology used by the GSM and the GCE provides already a rich set of features around the vulnerability scanning capabilities, like scanning for plain software vulnerabilities, policy controls and checks for configuration controls as well as managing assets with additional information to prioritize identified vulnerabilities according to asset criticality.

GSM Enterprise Appliance (GSM 6400A)

There are features of GSM and GCE which are tailored to the environment:

	Greenbone Security Manager	GCE or own installation
Ways for Updates & Feed	Possible via GSM Sync Port, via Proxy S-Connect, via AirGap, via GSM Master	Only Community Feed
System Update	Contains Security Updates, can update from any version to latest release, Grace Periods for EoL and LTS, Migration of data and configurations between appliances and versions	Not available
Protocols	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS and more	HTTPS only for WebGUI; SSH, IPv6
Integrations and Connectors	Different vendors like PaloAlto, Fortinet, Cisco FireSight, NAGIOS, Splunk, Verinice and more	Not available
Backup/Recovery	Backup for User Data, System Data via LVM, Transfer via SCP or USB	Only via environment (HyperVisor)
Alarms, Schedules	Via Email, via HTTP, via SMS, via connector to a SIEM or Ticket system. Complete scheduling possible	Not available
Scan architecture	Master/Slave, AirGap inside of high-sec zones	Not available

About GCE, GVM, OpenVAS and GSM

Greenbone publishes the source codes for transparency and review. This includes the opportunity to build the applications from scratch for those who are experienced in compiling software solutions from source packages. The GCE is our solution in a readily available form for our community users. It is a virtual appliance for an easy evaluation of our technology and doing vulnerability scanning and Vulnerability Management for private and SOHO environments.

The Greenbone Vulnerability Management (GVM) is the latest evolution step of what has begun under the label of "OpenVAS". In the last decade, Greenbone turned the plain vulnerability scanner "OpenVAS" into a full-featured Vulnerability Management Solution. A currently ongoing transitional phase shifts the brand names to Greenbone for a clear statement that developed this leading Open Source Vulnerability Management System.