

FAQ

Content

- [1. Who are Greenbone?](#)
- [2. What is our approach?](#)
- [3. What are our products?](#)
- [4. How to buy our products?](#)
- [5. What are the differences between Greenbone Security Feed and OpenVAS NVT Feed?](#)
- [6. What are the differences between Greenbone Security Manager and a do-it-yourself OpenVAS installation?](#)
- [7. Are the Greenbone solutions in conflict with german law know as "Hacker-Paragraph" 202c StGB?](#)

Introduction

1. Who are Greenbone?

Greenbone Networks delivers a vulnerability management solution for enterprise IT which includes reporting and security change management.

The company was founded in 2008 by leading experts in the field of network security and Free Software with the goal to engineer products and concepts able to cope with the present and future challenges of next generation Open Source vulnerability assessment and management. We especially focus on a transparent white-box solution to provide a customer-provable level of security to operate in most critical fortune-500 environments as well providing a comprehensive cost-cautious turn-key solution for small and medium sized customers.

2. What is our approach?

At Greenbone we take a holistic approach to minimize and manage risks originating from system vulnerabilities.

Greenbone is the first in this market providing 100% Open Source solution. The full white-box approach enable our customers to eliminate the risk that a proprietary vulnerability assessment management solution draws into critical IT infrastructure.

Greenbone involves into the global multi-cultural security and Open Source communities in a cooperative manner. We do understand the concept of give and take as well as the joined development and community processes around Free Software.

3. What are our products?

The central product Greenbone Security Manager is a turnkey solution for network security scanning: It combines the Greenbone Security Feed, a Scan Engine and a web-based administration.

Our foundation product is the Greenbone Security Feed. It is a stream of little procedures to detect known and potential security vulnerabilities in all active elements of your IT infrastructure: desktop computers, servers, appliances and intelligent components like routers or VoIP devices. Other vendors can integrate the Greenbone Security Feed into their products with a OEM license.

4. How to buy our products?

You can read about how to order our products on the web page [How to Buy](#).

5. What are the differences between Greenbone Security Feed and OpenVAS NVT Feed?

Central differences between the subscription-based Greenbone Security Feed (executed with a GSM compatible scan engine) and the free-of-charge OpenVAS NVT Feed (combining this feed with the Greenbone Security Manager is not supported) are (as of March 2010):

	Greenbone Security Feed	OpenVAS NVT Feed
Quality Assurance (QA)	Consistent	Variable
Availability	Assured with SLA	No promise
Fixes/Improvements	Assured with SLA	No promise
Support	Assured with SLA	From community on volunteer basis
Compatibility	OpenVAS 3.0, 3.1 and 4	OpenVAS 2.0, 3.0, 3.1 and 4
Updating	Constantly	Irregular
Transfer	Encrypted	Unencrypted
NVT Signatures	SLA for QA/Fixes	Transfer integrity

Size/Coverage: Greenbone and its partners contribute their developments as Free Software into the OpenVAS community. Delay could occur e.g. due to conflicts in versions or interfaces. NVTs that do occur in the OpenVAS NVT Feed, but don't occur in the Greenbone Security Feed, have not passed our strict quality assurance measures.

6. What are the differences between Greenbone Security Manager and a do-it-yourself OpenVAS installation?

Central differences between the appliance Greenbone Security Manager (only available in combination with the Greenbone Security Feed) and the do-it-yourself OpenVAS installation (either combined with Greenbone Security Feed or with OpenVAS NVT Feed, as of May 2010):

	Greenbone Security Manager	Do-it-yourself OpenVAS installation
Setting-up	Turn-key (ca. 10 minutes)	

Coverage	Concerted: All OpenVAS modules with several scan tools	Selection of operating system and hardware, then build on your own or install readily available community packages; perhaps use a community VM
Feed compatibility	Assured with SLA	Select and align on your own or take community defaults
Performance	Optimized for hardware	Establish on your own, in case GSF is used Greenbone support is available
Backup/Recovery	Integrated	Optimize on your own
Fixes	Assured with SLA	To be solved individually
Support	Assured with SLA	To be managed on your own, perhaps import Community-Fixes
Updating	Regularly and seamless	From community on volunteer basis
		On your own pace and method

7. Are the Greenbone solutions in conflict with german law known as "Hacker-Paragraph" 202c StGB?

The short answer is: No.

For a detailed answer referencing german law, please see the [german version of this FAQ entry](#).