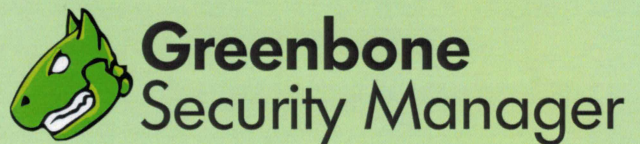


Turn-key Vulnerability Management



The solution for IT security in your organisation

Security holes:

How many? Where are they? How can I correct them?

Compliance:

Have they been met or not?

Overview:

What is the current state?

Is it getting better or worse ?

Risk escalation:

Who needs to be informed when and how?

Vulnerability Management

Vulnerability Management is an element of your IT compliance: within IT security, technical security must be ensured by an ongoing management process, the aim of which is to protect the system from dangers and threats, avoid damage and minimise risks.

Managing Directors and CIOs must ensure the complete protection of corporate data. In its simplest form, the continuing process consists of three steps:

Assessment -> Measures -> Control

The security measures taken must be adapted continuously to changing basic conditions. It is best to prepare the necessary regulation and control measures using an automated, integrated system..

Vulnerability Assessment

The Greenbone Security Manager (GSM) makes a major contribution to Vulnerability Assessment.

Our focus lies on preventive measures since, with regard to risks and costs, it is best to detect vulnerabilities before attackers manage to do so. The GSM is applied at the ideal point: security prevention. The GSM can be applied from different perspectives (combinations also possible):

Externally:

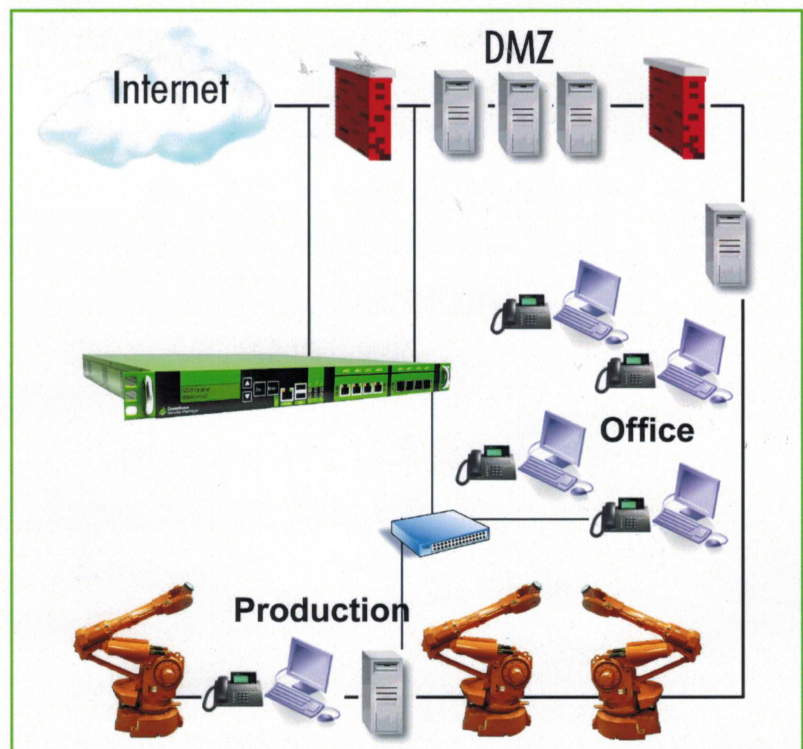
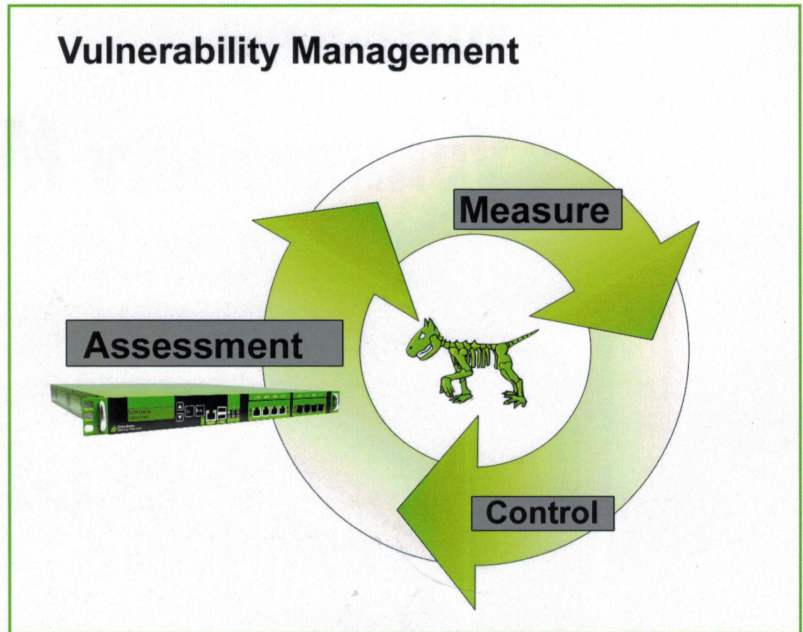
- Attacker's external perspective
- Identification of poorly configured firewalls
- Detection of highly security-relevant errors

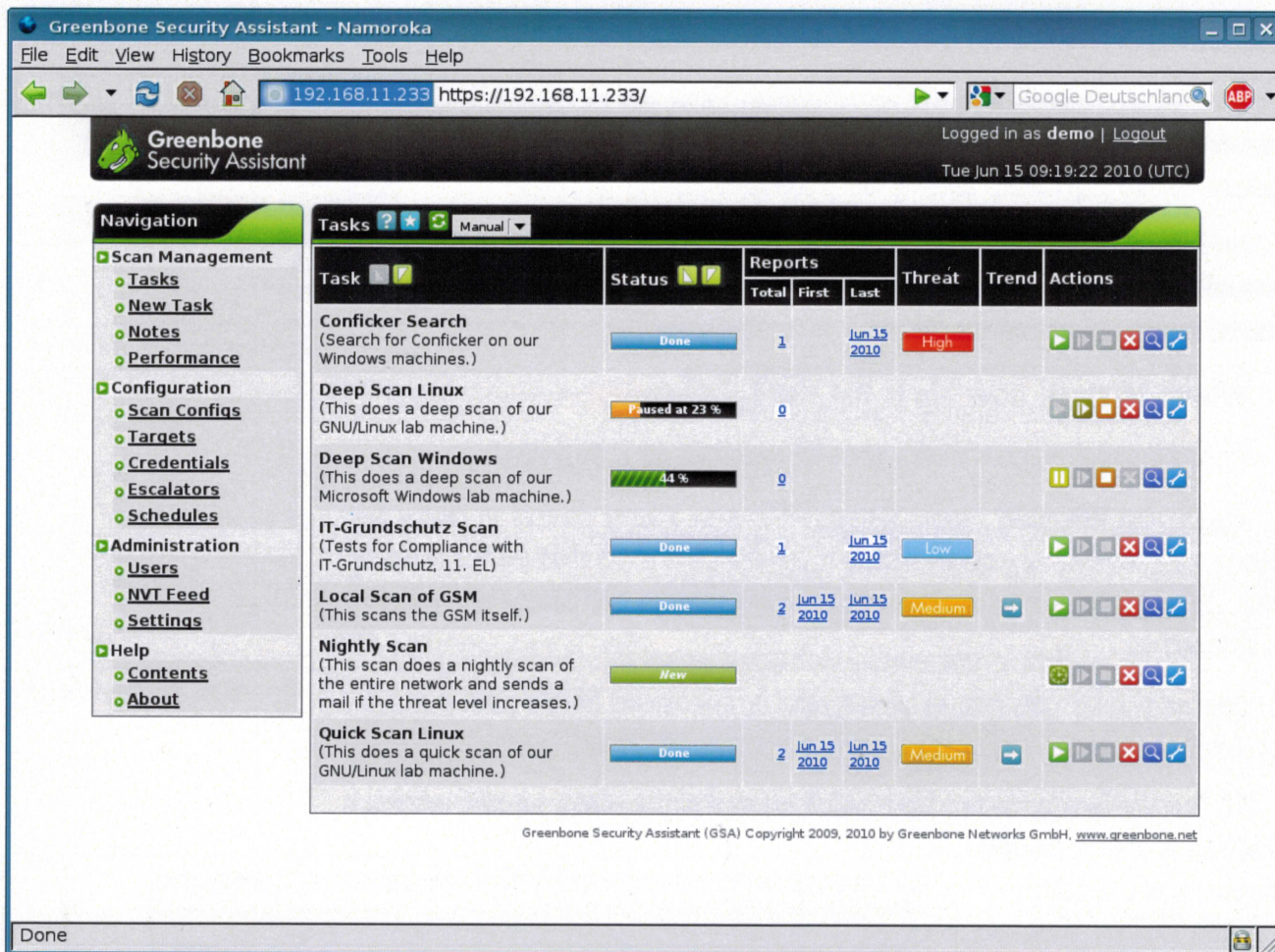
Within the DMZ:

- What if ... the firewall fails?
- Identification of vulnerabilities within the security zone

Within the network:

- Internal attacker's perspective or computer worm
- Detection of potential damage, classification according to risk
- Complete scope of detection can be used





Greenbone Security Assistant (GSA) Copyright 2009, 2010 by Greenbone Networks GmbH, www.greenbone.net

Clearly structured front-ends give you full visibility of vulnerabilities in your network. The scan also identifies breaches of your corporate security policies or statutory regulations.

The Greenbone Security Manager (GSM) is ideal for completing IT security with a permanent integration into the existing infrastructure. Auditors and solution providers who offer the solution to customers as a service, however, can also benefit from the GSM. The GSM offers maximum automation for the security process.



Greenbone Security Feed

Your threat scenario changes daily. To be able to react quickly to new vulnerabilities, Greenbone Security Feed ensures test routines are up-to-date: based on CVE reports and information provided by manufacturers, we create new certified tests every day. Over 21,000 test routines are currently active for heterogeneous IT networks (as of December 2010). The GSM automatically receives the Greenbone Security Feed via the encrypted daily update process

Common Vulnerabilities and Exposures (CVE) is the manufacturer-independent industry standard for the explicit identification and description of vulnerabilities.



Measures:

Vulnerabilities often emerge by pure misconfiguration. Classic examples are an administration password "12345678" or shared disks accidentally exposed to the internet. Vulnerability scans represent the first step towards detecting such problems.

The technical IT department must also have the means to close, or at least defuse, the detected vulnerabilities. Security guidelines to help prevent misconfiguration likewise need to be mapped through an organisational process.

Where to start; how big is the risk?

Practical experience suggests starting where the operational risk is the greatest.

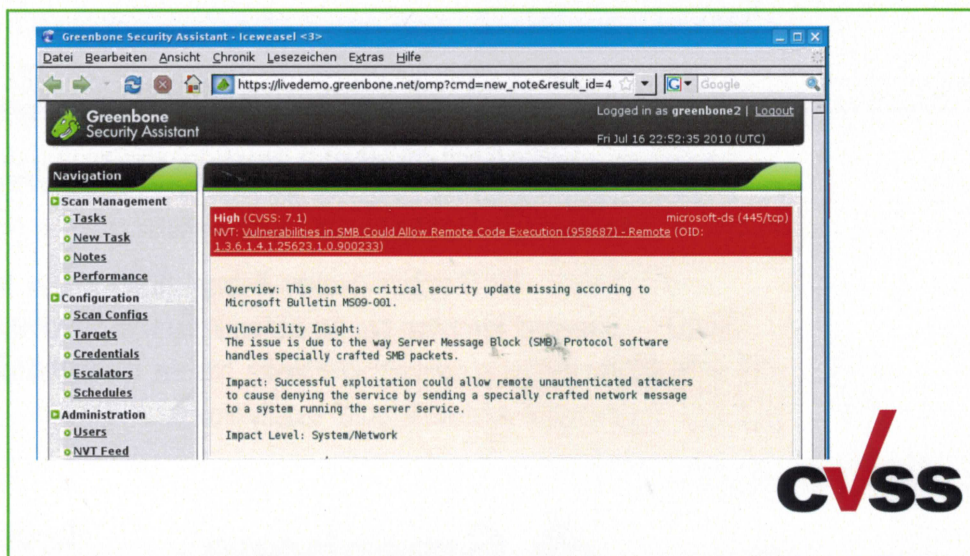
The Common Vulnerability Scoring System (CVSS) is an industry standard to classify the severity and vulnerability of computer systems to prioritise the time and effort required to defuse them. The assessment is based on criteria such as security relevance, total damage to be expected or dissemination.

Detection of vulnerability must be followed either by their removal (update, patch or reconfiguration) or by a reaction through other security mechanisms (IDS, firewall rules).

IDS (Intrusion Detection Systems) and firewalls are often a quick remedy regarding vulnerabilities if no updates are available to close the security holes.

But beware:

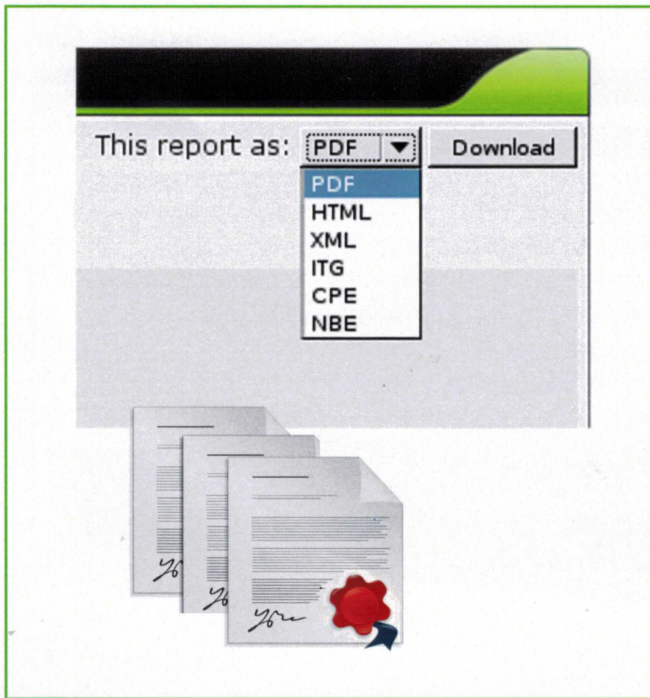
The more exception rules firewall and IDS collect against known problems without identifying and closing the actual security holes, the greater the risk of damage and the higher the failure and removal costs once damage occurs.



The screenshot shows the Greenbone Security Assistant web interface. The browser address bar displays https://livedemo.greenbone.net/omp?cmd=new_note&result_id=4. The page is titled "Greenbone Security Assistant" and shows the user is logged in as "greenbone2". The navigation menu on the left includes sections for Scan Management, Configuration, and Administration. The main content area displays a scan result for a "High (CVSS: 7.1)" vulnerability. The vulnerability details are as follows:

- Severity:** High (CVSS: 7.1)
- Product:** microsoft-ds (445/tcp)
- Vulnerability Name:** NVT: Vulnerabilities in SMB could Allow Remote Code Execution (958687) - Remote (OID: 1.2.6.1.4.1.25627.1.0.909233)
- Overview:** This host has critical security update missing according to Microsoft Bulletin MS09-001.
- Vulnerability Insight:** The issue is due to the way Server Message Block (SMB) Protocol software handles specially crafted SMB packets.
- Impact:** Successful exploitation could allow remote unauthenticated attackers to cause denying the service by sending a specially crafted network message to a system running the server service.
- Impact Level:** System/Network

In the bottom right corner of the screenshot, the CVSS logo is visible, consisting of the letters "CVSS" in a bold, black font with a red checkmark above the "V".



Controls:

The Greenbone Security Manager (GSM) enables the state of security; respective changes to it and security benchmarks to be documented.

By transferring scan results to the management process, simple figures or traffic lights can be used to show whether vulnerabilities exist, whether they have since been addressed by IT administration or whether new vulnerabilities have been discovered within the ongoing vulnerability assessment.

As part of the organisational process, it is possible to implement testing for compliance with security guidelines in Greenbone test routines. The resulting automation of compliance testing substantially improves ease of work.

These countermeasures must also be documented in this process to assess their technical effectiveness. This can be performed by a repeated vulnerability assessment scan or a detailed test with another software tool.

Audit support:

While in the past security audits could only be carried out sporadically, the GSM provides automatic reports updated daily or alarms.

An example: IT-Baseline Security (BSI IT-Grundschutz):

The Greenbone Security Manager can carry out automatic tests on the IT-Baseline Security catalogues of the German Federal Office for Information Security (BSI). The latest supplementary delivery is supported by over 100 measures. This is the maximum number of measures that can be supported by automatic tests. Some measures are quite comprehensive, meaning that far more than 100 individual tests are conducted per target system. The Greenbone Security Manager is then a rapid assistant when it comes to conducting IT-Grundschutz audits, enabling breaches to be tested automatically as a regular background process.



Product overview:

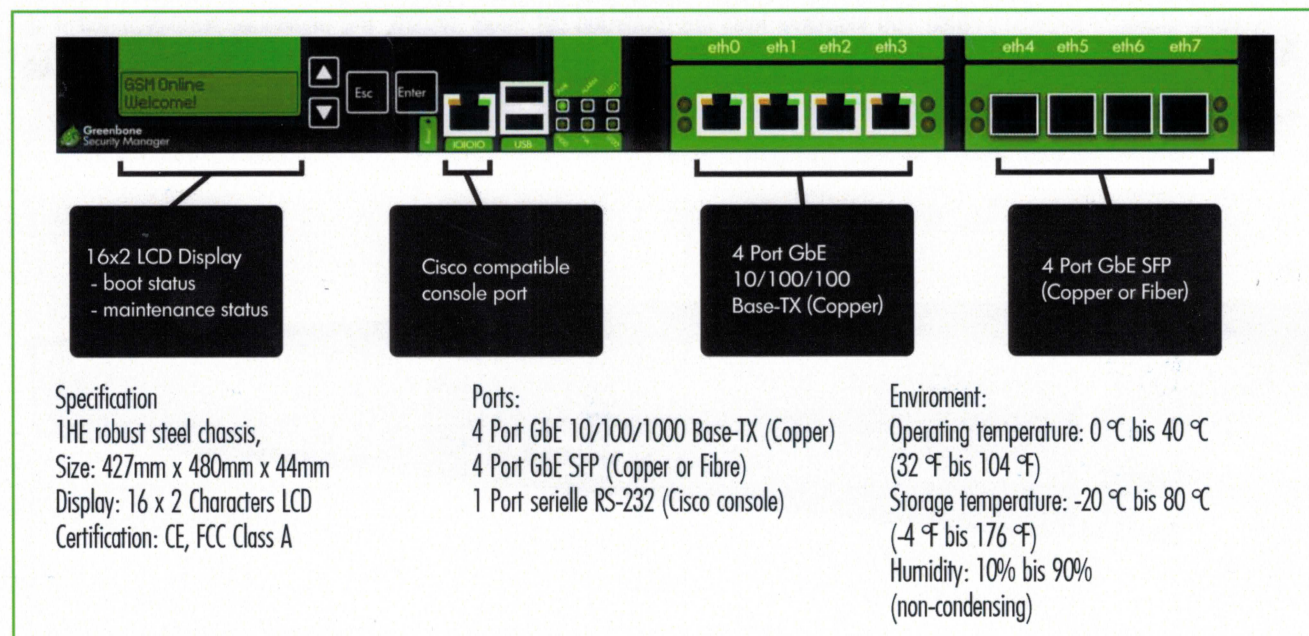
The Greenbone Security Manager (GSM) is a dedicated Vulnerability Management security appliance. It integrates transparently into your vulnerability and threat management systems.

With a choice of front-ends, security scans gives you full visibility of vulnerabilities in your network. The scan also identifies potential breaches of your corporate security policy and of statutory regulations.

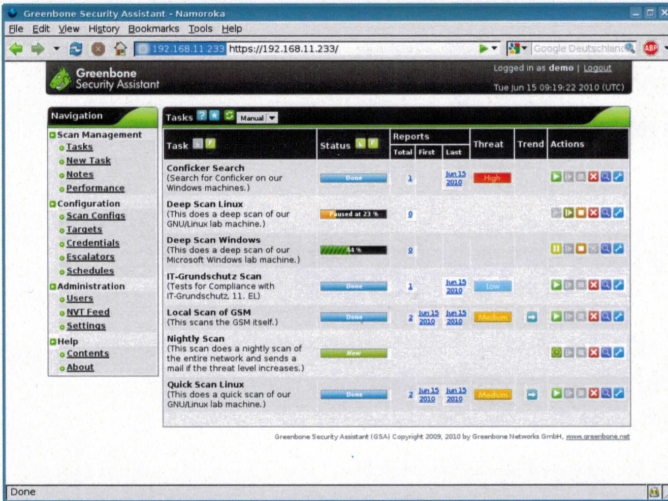


Benefits

- Turn-key solution: operational within 10 minutes
- Powerful appliance operating system with special command line administration based on a comprehensive security design
- Integrated Greenbone Security Feed with over 21,000 Network Vulnerability Tests, automatically updated daily
- Integrated Backup, Restore, Snapshot and Update
- Integrates Greenbone Security Assistant as central web interface
- No limitation on number of target systems or IPs
- GSM subscription is a flat rate, and includes exchange of defective hardware as well as access to the Greenbone Security Feed, feature updates and support



Web Interface



Features

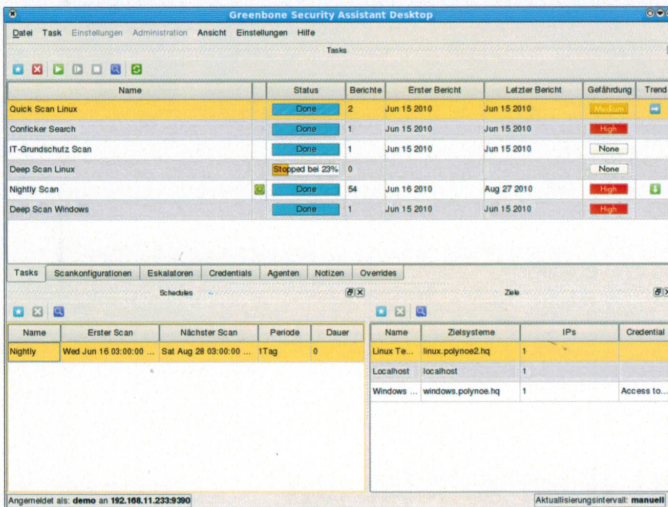
Supported standards

- Network integration: SMTP (e-mail), SysLog, NTP, DHCP, IPv4/IPv6
- Vulnerability detection: CVE, CPE, CVSS, OVAL
- Network scans: WMI, LDAP, HTTP, SMB, SSH, TCP, UDP, ...
- Policies: IT-Grundschatz, PCI-DSS, 27001, 27002

Application web-based interface (HTTPS)

- Scan tasks management with false-positive marking
- Multi-user support
- Report browsing aided by filtering, sorting and notes
- Report export as PDF or XML
- Appliance performance overview

Desktop Interface



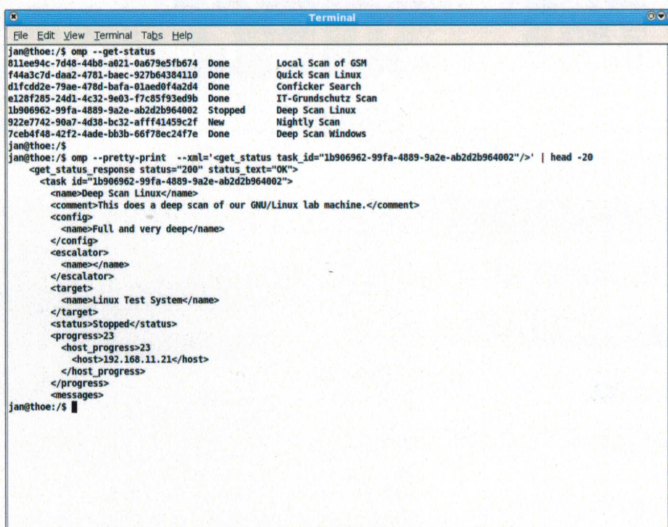
Application remote control

- OpenVAS Management Protocol (OMP, SSL-secured)
- All user actions of web-based interface available
- Supported by desktop applications
- Automated via scriptable command line tools

Administrative console interface (shell via SSHv2 / RS232)

- Network integration configuration
- Backup, Restore, Snapshot, Factory Reset, Update

Command Line Interface



Smartest solution for the market:

The Greenbone Security Manager's unique selling point is its independently verifiable security. Since the technical processes of the scan engine are available as open-source software, it can be audited by customers or state testing and certification bodies with regard to complete correctness and quality.

Investment and benefits

Our price is entirely independent of the number of scanned systems or the frequency or number of scans used. The daily update of test routines (Greenbone Security Feed) with the latest information about security holes is included in this flat-rate subscription. The basic investment includes the procurement of a GMS appliance, including Greenbone Security Manager, and a one-year subscription (GMS-SUB) with Greenbone Security Feed and support.

Via its value-added reseller, Greenbone also offers customisation to specific IT environments, the preparation of testing schemes according to individual specifications and close integration into existing management frameworks

Benefits of Greenbone Security Manager Subscription (GSM-SUB)

Subscription period for 1 year:

- Greenbone Security Feed (GSF): daily vulnerability tests
- E-mail and hotline support
- All feature updates free of charge
- Hardware guarantee
- RMA via Greenbone distributor

Greenbone technology partners



business partner



Version 02/11

Your Greenbone Security Solutions partner:



ComWorth Solutions Pte Ltd

Tel: +65 6748 2260

Fax: +65 6748 2267

Email: info@comworth.com.sg

URL: www.comworth.com.sg



Neuer Graben 17

49074 Osnabrück

Germany

Fon: +49 (0)541 33 50 84-0

Fax: +49 (0)541 33 50 84-99

E-Mail: info@greenbone.net

Internet: www.greenbone.net