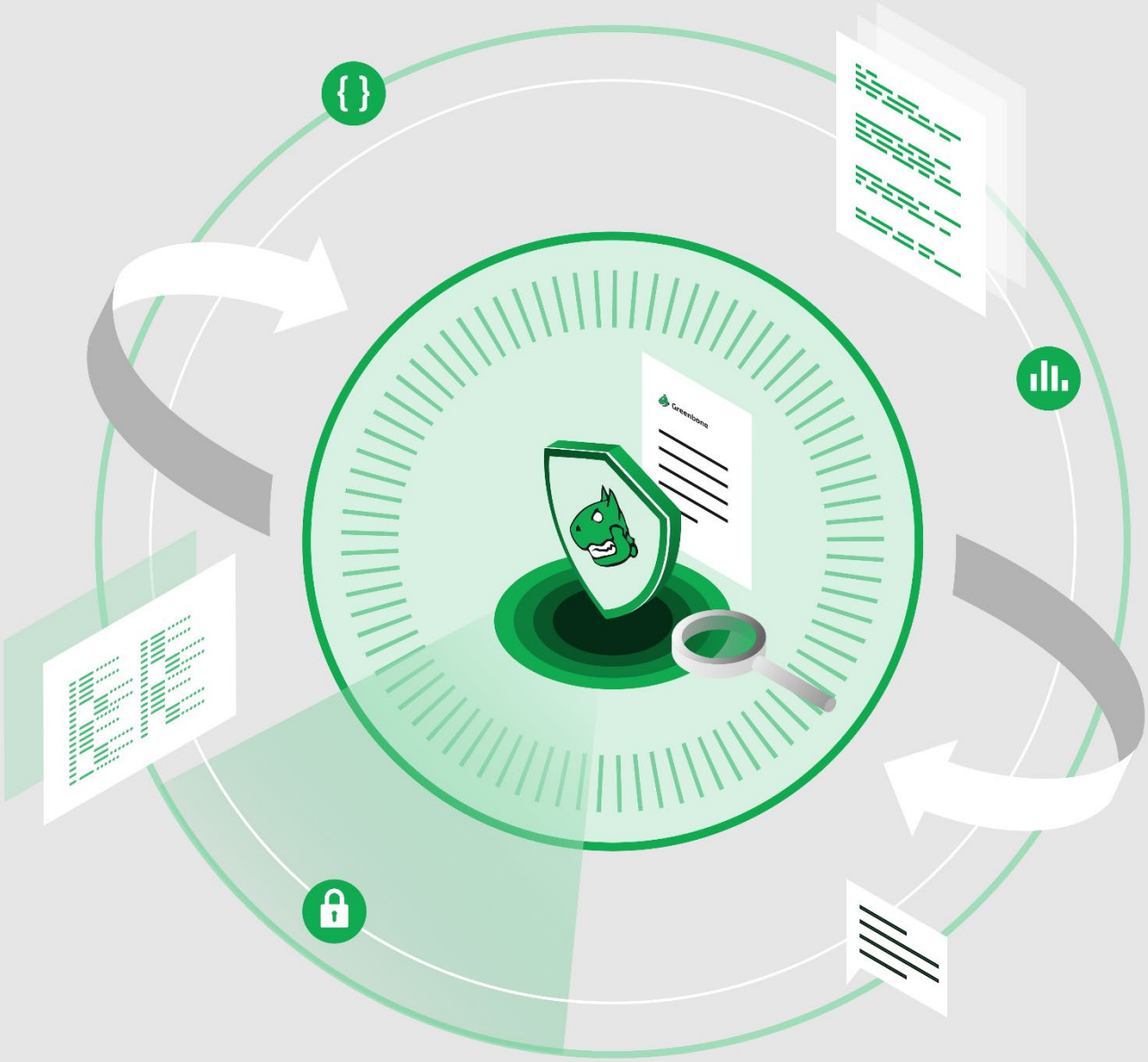
Greenbone

Unsere Lösungen im Vergleich

Greenbone Source Edition, Greenbone Enterprise Appliances und Greenbone Cloud Service



Datum: 05.05.2022

Inhalt

1 Einleitung 3
2 Feed 4
3 Lösungsbereitstellung, -einsatz und -support 5
4 Funktionen 6

Open-Source-IT-Sicherheit liefert nicht nur ein hohes Level an Transparenz der Lösung selbst, sondern ist auch ein Beitrag zur IT-Sicherheitsgemeinschaft im Allgemeinen. Wir sind mit dieser Idee verbunden und ihr verpflichtet. Dieses Whitepaper soll unseren Kunden und Nutzern dabei helfen, die Unterschiede zwischen den verschiedenen Lösungen zu verstehen.

1 Einleitung

Das **Greenbone Vulnerability Management** (GVM) ist ein Framework, welches ursprünglich als Community-Projekt unter dem Namen „OpenVAS“ entstanden ist und seit vielen Jahren maßgeblich von Greenbone Networks entwickelt und vorangetrieben wird.
Es besteht aus dem **Greenbone Vulnerability Manager Daemon**, dem **Greenbone Security Assistant** mit dem **Greenbone Security Assistant Daemon** und der ausführbaren Scanner-Anwendung, die Schwachstellentests (engl. Vulnerability Tests, VT) gegen Ziele durchführt.

Das GVM-Framework wird regelmäßig unter Open-Source-Lizenzen unter dem Namen **Greenbone Source Edition** veröffentlicht. Damit können Linux-Distributionen GVM in Form von Installationspaketen erstellen und bereitstellen. Auch Privatpersonen können GVM so installieren und nutzen.

Der Greenbone Security Assistant ist die Web-Oberfläche, über die Nutzende Scans steuern und Schwachstelleninformationen abrufen können. Die Kommunikation findet über das **Greenbone Management Protocol** (GMP) statt, mit welchem Nutzende mithilfe verschiedener Tools auch direkt kommunizieren können.

Die **Greenbone Enterprise Appliances** sind die kommerziellen Produkte und als virtuelle oder Hardware-Appliances verfügbar. Sie enthalten das Framework GVM sowie das **Greenbone Operating System** (GOS), das weitere Funktionalitäten bereitstellt.

Die Schwachstellentests zum Scannen erhalten die Appliances über den **Greenbone Enterprise Feed**.

Die **Greenbone Community Appliance** ist eine nicht-kommerzielle, virtuelle Appliance und hat einen begrenzteren Funktionsumfang als die Greenbone Enterprise Appliances. Sie nutzt den weniger umfangreichen **Greenbone Community Feed** anstelle des Greenbone Enterprise Feeds.

Der **Greenbone Cloud Service** ist eine SaaS-Lösung. Scananfragen werden über die Cloud an den **Greenbone Scan Cluster** weitergeleitet. Vom Scan Cluster aus werden Scans für externe oder interne Ziele ausgeführt. Zum Scannen werden der GVM-Scanner genutzt und die Schwachstellentests ebenfalls über den Greenbone Enterprise Feed bezogen.

Neumarkt 12 • 49074 Osnabrück • Deutschland • www.greenbone.net

2 Feed

Die Basis beider Feeds ist identisch. Alle Inhalte, die im Community Feed enthalten sind, finden sich auch im Enterprise Feed. Allerdings erweitert der Enterprise Feed den Community Feed um einige Schwachstellentests und Compliance-Richtlinien.

Greenbone bezieht alle selbstentwickelten Schwachstellentests (engl.: Vulnerability Tests, VT) in den professionellen Greenbone Enterprise Feed ein, allerdings nicht in den Greenbone Community Feed.

Gruppe	Greenbone Community Feed (Basisabdeckung)	Greenbone Enterprise Feed (erweiterte Abdeckung)
VTs für Heimanwendungsprodukte (z. B. Ubuntu Linux, AVM Fritzbox, MS Office)	✓	✓
“IT-Grundschutz”	✓	✓
VTs für Unternehmensprodukte (z. B. MS Exchange, Palo Alto, Cisco, IoT/OT)	×	✓
Compliance-Richtlinien für CIS Benchmarks	×	✓
Zusätzliche Richtlinien	×	✓
Zugriff auf Greenbone Enterprise Support	×	✓
Zugriff auf Professional Services	×	✓

3 Lösungsbereitstellung, -einsatz und -support

Die Greenbone Enterprise Appliances können im Vergleich zu einer eigenen Source-Edition-Softwareinstallation, bei der Nutzende sich um die zugrundeliegende Hardware, das Betriebssystem und das Datenbanksystem kümmern müssen, mit viel weniger Aufwand hinsichtlich Setup und Betrieb gehandhabt werden.

Außerdem sind Master-Sensor-Einsätze, um landesweite Unternehmen mit mehreren Standorten oder sogar globale Netzwerke von Zweigstellen abzudecken, mit der professionellen Lösung mit sehr geringem Aufwand möglich.

Der Greenbone Cloud Service wird als Cloud-Lösung geliefert, was ebenfalls einen geringen Aufwand bei der Einrichtung bedeutet. Gateway-Komponenten ermöglichen das Scannen interner IP-Adressen.

Alle Elemente der Greenbone Enterprise Appliances und des Greenbone Cloud Service werden vom Greenbone Enterprise Support abgedeckt.

Die Tabelle unten listet einige weitere unterschiedliche Elemente bezüglich Lösungsbereitstellung, -einsatz und -support auf:

Kriterien	Greebone Source Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
Einrichtung	Eigenverantwortliche Wahl des Betriebssystems und der Hardware Eigenverantwortlich zu bauen oder Community-Pakete installieren	Schlüsselfertige Lösung Einfache und unkomplizierte Inbetriebnahme innerhalb kürzester Zeit	Einfache Accountregistrierung und Konfiguration innerhalb kürzester Zeit
Feedkompatibilität	Eigenverantwortlich herzustellen	Zugesichert mit SLA	Zugesichert mit SLA
Leistung	Eigenverantwortlich zu optimieren	Für Hardware optimiert	Variabel je nach Anforderung
Backup/Wiederherstellung	Individuell gelöst	Integriert	Integriert
Fehlerbeseitigung/ Verbesserungen	Eigenverantwortlich zu verwalten	Zugesichert mit SLA	Zugesichert mit SLA
Support	Über (externe) Community auf freiwilliger Basis	Zugesichert mit SLA	Zugesichert mit SLA
Softwareupdates	Manuelle Updates des Source-Builds und manuelle Migration der Daten	Regelmäßig und nahtlos	Kontinuierlich

4 Funktionen

Das GVM-Framework stellt bereits ein umfangreiches Set an Funktionen rund um das Schwachstellenscannen bereit: Scannen nach einfachen Software-Schwachstellen, Richtlinienkontrollen, Prüfungen zur Konfigurationskontrolle und Verwalten von Assets mit zusätzlichen Informationen zum Priorisieren von identifizierten Schwachstellen gemäß Asset-Kritikalität.

Darüber hinaus bieten die Greenbone Enterprise Appliances und der Greenbone Cloud Service eine Vielzahl von Funktionen, die auf die jeweilige Umgebung zugeschnitten sind:

Kriterien	Greebone Source Edition	Greenbone Enterprise Appliances	Greenbone Cloud Service
Möglichkeiten für Updates & Feed	Nur Greenbone Community Feed	Täglich automatisch Möglich über pro Appliance konfigurierbare Synchronisationsports, redundante Proxy-Server, USB- oder FTP-Airgap oder Master-Appliance	Täglich automatisch Keine Compliance-Tests
Systemupdate	Abhängig von Distribution oder eigenverantwortlich	Enthält Sicherheitsupdates Update von jeder Version auf neuesten Release möglich Übergangszeitraum für EoL und LTS Migration von Daten und Konfigurationen zwischen Appliances und Versionen	Automatisch Kontinuierliche Sicherheits- und Plattformupdates
Protokolle	Eigenverantwortlich zu konfigurieren und einzurichten	NTP, GMP, OSP, HTTPS, SSH, SNMPv2, SNMP, Syslog, IPv6, LDAP, RADIUS und mehr	NTP, GMP, HTTPS, SSH, SNMPv2, SNMP, Syslog, LDAP, RADIUS und mehr
Integrationen und Konnektoren	Nicht verfügbar	Unterschiedliche Anbieter wie PaloAlto, Fortinet, Cisco FireSight, NAGIOS, Splunk, Verinice und mehr	RESTful API für alle Funktionalitäten
Backup/ Wiederher-stellung	Individuell gelöst	Backup für Benutzerdaten, Systemdaten über LVM, Transfer über SCP oder USB	Automatische(s) Backup/Wiederherstellung
Benachrichti-gungen/ Zeitpläne	Eigenverantwortlich über Betriebssystem zu konfigurieren	Über E-Mail, HTTP, SMS, Konnektor zu einem SIEM oder Ticketsystem und mehr Komplette Terminplanung möglich	Über E-Mail, Slack oder Microsoft Teams
Scanarchitektur	Nicht verfügbar	Master/Sensor, Airgap innerhalb von Hochsicherheitszonen	Cloud-Scanner, Gateway-Komponente für interne Scans