SECPOINT®

SecPoint® Penetrator™ Product Matrix

Penetrator: https://www.secpoint.com/penetrator.html
VIP Lounge Login at: https://vip.secpoint.com

SECPOINT® PENETRATOR-MATRIX

	S9 - SFF	S9 - 128	S9 - 256	S9 - 512	S9 - 2048	S9 - Virtual Appliance	S9 – Cloud
Architecture	64 Bit	64 Bit	64 Bit	64 Bit	64 Bit	64 Bit	-
Maximum Concurrent Scans	4-8 IPs	64-128 IPs	64-128 IPs	256-512 IPS	No software limit	1- 1024 + IPS	1- 1024 IPS
Maximum Cloud Users	Max 10 users	Max 100 users	Max 500 users	Max 1000 users	No software limit	No software limit	-
Maximum Ip Reporting in interface	500+ IP Reports	1000+ IP Reports	5000+ IP Reports	10,000+ IP Reports	No software limit	10,000+ IP Reports	No software limit
All Data stored locally	✓	✓	✓	✓	✓	✓	EU, US
WiFi Pen Testing WPA WPA2 WPS	✓	✓	✓	✓	✓	✓	-
Helpdesk Ticket System	✓	✓	✓	✓	✓	✓	✓
Customize Report Branding	✓	✓	✓	✓	✓	✓	-
Customize Interface Branding	✓	✓	✓	✓	✓	✓	-
Interfaces	4x RJ45	6x GE RJ45	6x GE RJ45	6x GE RJ45	6x GE RJ45	-	-
Local Storage	320 Gb	320 Gb	500 Gb	750 Gb	1 Tb	500 Gb	-
RAM / CPU	4 Gb / Quad	4 Gb / 13	8 Gb / 15	8 Gb / 17 Quad	8 Gb / 17 Quad	Min 2 Gb / 13 Recom. 8 Gb / 17	-
Power Supply	Single AC PS	Single PS	Single PS	Single PS	Single PS	-	-
Form Factor	Small Form Factor	Rack Mount 1RU	Rack Mount 1RU	Rack Mount 1RU	Rack Mount 1RU	-	-
Support & Firmware included	✓	✓	✓	✓	✓	✓	✓
Schedule Scans Support	✓	✓	✓	✓	✓	✓	✓
9 Scan profiles	✓	✓	✓	✓	✓	✓	✓
DoS – Aggressive Scan	✓	✓	✓	✓	✓	✓	✓
All data stored locally	✓	✓	✓	✓	✓	✓	✓
Distributed node scanning	✓	✓	✓	✓	✓	✓	✓
Multi user support	✓	✓	✓	✓	✓	✓	✓
Vulnerability scanning	✓	✓	✓	✓	✓	✓	✓
Full Linux no reboot required	✓	✓	✓	✓	✓	✓	✓

Copyright© 1999-2020 SecPoint® All rights reserved. SecPoint® Protector™ Penetrator™ Portable Penetrator™ Cloud Penetrator™ & certain other marks are registered trademarks of SecPoint®. & other SecPoint® names herein may also be registered &/or common law trademarks of SecPoint®. All other product or company names may be trademark of their respective owners. Performance & other metrics contained herein were attained in internal lab tests under ideal conditions & actual performance & other results may vary. Network variables different network environments & other conditions may affect performance results. Nothing herein represents any binding commitment by SecPoint®. Secpoint® disclaims all warranties wheatear express or implied except to the extent SecPoint® enters a binding written contract signed by SecPoint® Counsel with a purchaser that expressly warrants that the identified product will perform according to certain expressly identified performance metrics & in such event only the specific performance metrics expressly identified in such binding written contract shall be binding on SecPoint®. For clarity any such warranty will be limited to performance in the same ideal conditions as in SecPoint® internal lab tests. SecPoint® disclaims in full any covenants representations & guarantees pursuant hereto whether express or implied. SecPoint® reserves the right to change, modify, transfer, or otherwise revise this publication, without notice, & the most current version of the publication shall be applicable.

SecPoint® Penetrator™

Vulnerability Scanning Appliance

Windows Hyper-V™

ESXi

itsecurity

PROTECTSTAR AWARD 2012

CVE COMPATIBLE cve.mitre.org

HIPAA COMPLIANT

SECPOINT®
www.secpoint.com

- √ Full Privacy, Data Collection & Backdoor Free
- √ Advanced AI Machine Learning for Best Results
- √ 11 Scan Profiles, HIPAA,OWASP top 10, Prepare for PCI, Firewall Scan, SCADA and more
- √ Advanced Web Crawler - SQL Injection - XSS - SSL Vulnerabilities
- √ Bugtraq ID / Mitre CVE / Ubuntu USN / Microsoft / OSBDB
- √ Schedule scans daily,weekly,monthly
- √ Prevent Hackers To Access Your Server
- √ Vulnerability Scanning
- √ Vulnerability Assessment
- √ 60.000 + Vulnerabilities
- √ Launch Real Exploits and Denial of Service Attacks
- √ Distributed Scanning Capability
- √ Scan any OS or Network
- √ Reports Branding
- √ Detailed Remedies for Identified Vulnerabilities
- √ Secure Design All Data Stored on Unit
- √ Ticket System for easy Vulnerability Control

PREVENT HACKERS FROM ENTERING YOUR SERVERS AND NETWORK

Vulnerability Assessment is key to any security strategy

The latest automated hacking tools can inflict damage across a network and across the world in a matter of hours. Understanding the potential vulnerabilities within your system is vital to any security strategy.

Vulnerability Assessment
The Penetrator™ is a Vulnerability Assessment and penetration testing appliance for your network, which comes pre-loaded and ready-to-use out of the box. It is a powerful, easy to use and intelligent security assessment solution.

60.000 + Vulnerabilities
The Penetrator™ vulnerability database consists of more than 21 years of research. The database has a total of more than 60.000 unique remote vulnerabilities to test for. This database is updated multiple times daily.

Launch Real Exploits and Denial of Service Attacks
You can launch real exploits to verify that an identified vulnerability is exploitable. It is also possible to launch real Denial of Service attacks to test preproduction systems for stability.

Reports Branding
Branding and personalisation of reports and selling them as a service is permitted.

Unique Distributed Penetrator™ Capabilities
You can connect multiple Penetrators in a distributed network. This gives many unique advantages such as:
- Centralized reporting
- Centralized vulnerability assessment
- Centralized update point

Possibility to audit different locations from a master Penetrator located in another city.

Security Auditing of any Operating System or Network Device
The Penetrator ™ is designed to audit any operating system or network device. It is beneficial to audit any device in the network setup to find and rectify any identified vulnerabilities before an attacker can exploit the vulnerabilities.

Multi-User Support for Privacy
All Penetrators support multi-user login. This could be used to create different accounts with different targets to audit or resold as (SAAS) to your own customers.

SecPoint® Penetrator™

Vulnerability Scanning Appliance

Specifications	SecPoint® Penetrator™ S9 - 4-32 IPs	SecPoint® Penetrator™ S9 - 8-64 IPs	SecPoint® Penetrator™ S9 - 128-256 IPs	SecPoint® Penetrator™ S9 - 512-2048 IPs
Height	Small Form Factor (SFF)	1U Rackmount	1U Rackmount	1U Rackmount
Weight	SFF without packing: 2,5 Kilo SFFwith packing: 3,5 Kilo 1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo	1U without packing 6,5 Kilo 1U with packing 8,5 Kilo
Power Supply	60W power supply AC/DC 90-264V Full Range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range
Environment Temperatures	Operating : 0°C to 40°C Storage: -25°C to 75°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C
64 Bit Platform	√	√	√	√
SSD Harddrive Included	250 GB	250 GB	250 GB	250 GB
Network Ports	4x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit	6x 10/100/1000 Mbit
60.000 + Vulnerabilities	√	√	√	√
Launch Real Exploits & Denial of Service	√	√	√	√
Allowed to Change IP Addresses	√	√	√	√
Distributed Security Auditing	√	√	√	√
Automatic database and software updates	√	√	√	√

Features

Security Audit Features

- √ Vulnerability assessment
- √ 60.000 + vulnerabilities
- √ Unlimited auditing
- √ No software installation
- √ Advanced audit options
- √ Launch real exploits
- √ Security audit any OS
- √ Automatic web crawl script
- √ OS independent interface
- √ SANS top 20
- √ Malware Detection

Easy-to-understand Reporting

- √ XML PDF and HTML reports
- √ Reports branding allowed
- √ Option for syslog remote logging

Distribution Security Auditing

- √ Security audit remote locations from a centralized point
- √ Centralized reporting
- √ Centralized data storage
- √ Centralized control

Security Audit Configuration

- √ Virtual host auditing
- √ Audit specific ports
- √ Audit specific web directories
- √ Email notification when an audit is finished

Finds Cross Site Scripting, SQL Injection and Web Errors

- √ Automatic web crawling engine identifies known and unknown files on websites
- √ Finds Cross Site Scripting
- √ Finds SQL Injection
- √ Finds Web Errors
- √ Black Hat SEO Scanner
- √ Google Hack DB
- √ Advanced AI, Machine Learning

Multi User Support

- √ Supports multiple users to login at the same time
- √ Individual user accounts with different audit options and IP ranges
- √ Individual user security level
- √ Admin and regular users

Scheduled Auditing

- √ Automatic scheduled auditing
- √ Automatic alert about new identified security vulnerabilities
- √ Shows new vulnerabilities discovered and compares them with old records to show the progress in the security level

Scalable and Upgradeable

- √ All units can be upgraded for network growth via a software license
- √ Investment protection

Penetration Testing

- √ Launch real exploits for Windows, Unix, Routers, Firewalls and more
- √ Launch real denial of service attacks
- √ Launch distributed denial of service via distributed setup

Automatic Update

- √ Automatic daily database updates
- √ Automatic firmware updates with new features and functionality
- √ Centralized update point
- √ Automatic alerts when database is expired
- √ Option to upload updates manually via the interface

Support & Maintenance

- √ One year database subscription included
- √ Full support included in price
- √ Option for instant replacement hardware
- √ Web-based user interface (https)
- √ Quick setup wizard
- √ Configuration backup/restore
- √ Email alert and logging via syslog
- √ Build-in diagnostic function

Security Scanning of:

- √ Wordpress, Drupal, Magento, Shopify, Umraco, Joomla, Webshops

E-mail: info@secpoint.com

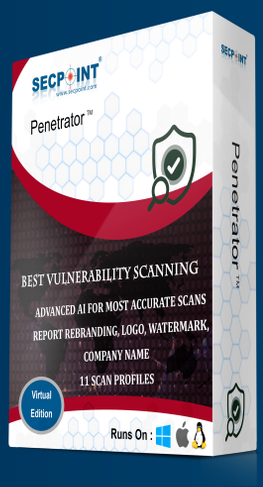
SECPOINT® www.secpoint.com

For more information on Penetrator, please visit
https://www.SecPoint.com/penetrator.html
https://support.SecPoint.com

VAR/VAD Contact

SecPoint® Penetrator™

- 64 Bit High Performance
- Scans Local & Public IPs
- Best Vulnerability & Assessment Scanning
- Easy Solutions to found vulnerabiliites
- Virtual VMware & Hyper-V Support



Windows Hyper-V™

ESXi

PROTECTSTAR AWARD 2012

CVE COMPATIBLE cve.mitre.org

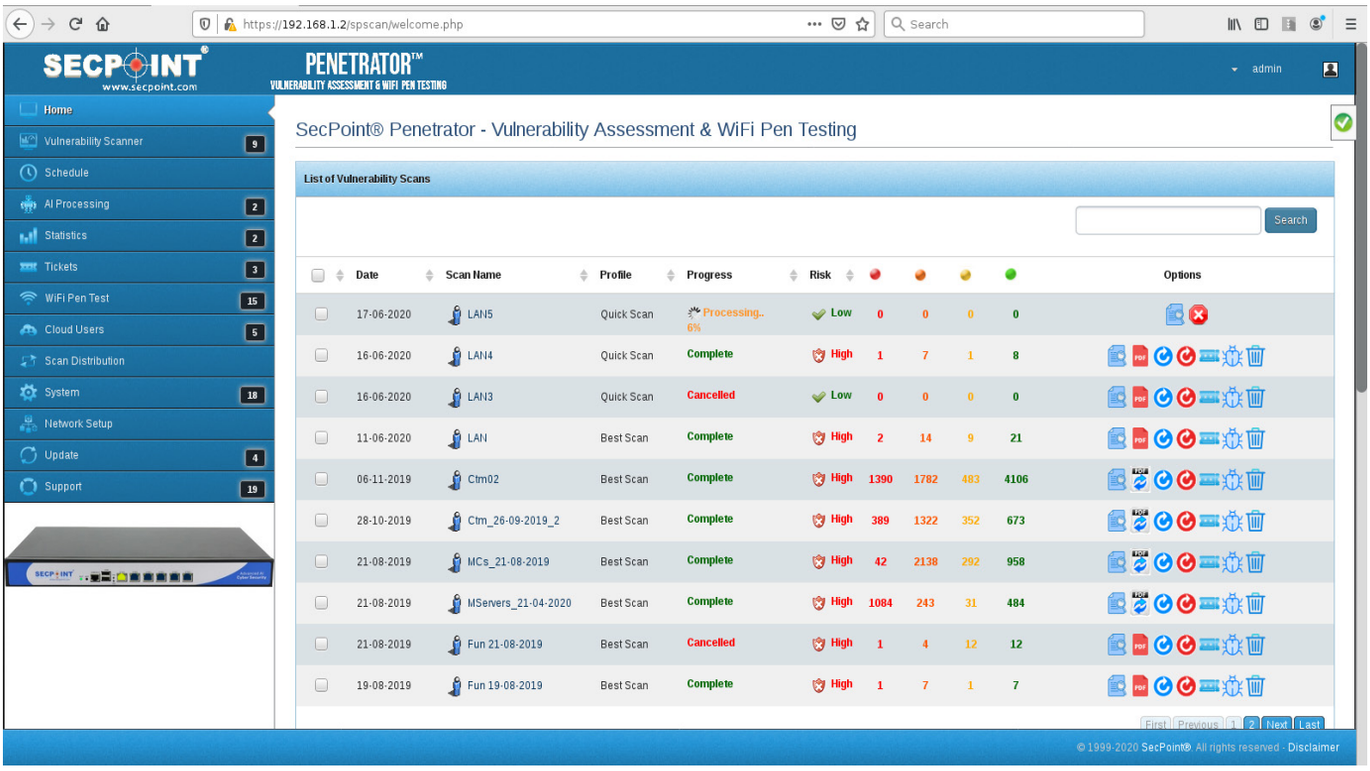
HIPAA COMPLIANT

vmware READY

Prevent Hackers from entering your server and network!
Vulnerability management is key to any security strategy

The latest automated hacking tools can inflict damage across a network and across the world in a matter of minutes. Understanding the potential vulnerabilities within your system is vital to any security strategy.

SECPOINT®
www.secpoint.com



Vulnerability management
is key to any security strategy

Vulnerability Management

ThePenetrator™isavulnerabilitymanagementandpenetrationtestingappliancefor yournetwork,which comes pre-loaded and ready to go.
It is a powerful and intelligent security assessment solution.

Comprehensive Vulnerability Scanning

Withitscomprehensivevulnerabilitydatabaseandtheapplicationofsophisticatedauditing techniques, the SecPoint ® Penetrator™ enables you to alwaysbeonestepaheadofeventhemostskilledandadvancedattackers.Ithasnolimitontheamountof auditingnorlimitonthenumberofIPaddressesandismostcertainlyoneofthestrongestandmostcompre-hensive vulnerability assessment solutions on the market.

Professional Skilled Support

Secondtononewiththefastestreplyandresponseratetosupportqueriesintheindustry.
The best 24 Hour skilled support team operation.
Fast remote login with problem solving via TeamViewer.
Follow Support Ticket Status via the Support Center.

SecPoint® Penetrator™

Penetration Testing Appliance

Easy-to-understand Reporting

Reportscanbecustomisedandareavailableas XML, PDF or HTML files.

System vulnerabilities are categorised as either high risk, medium risk or low risk, together with name and details of each vulnerability and its solution.. The report also gives a conclusion as to the overall security level of the audited system.

An executive summary is compiled specifically for management level review with both text and graphical details from the audit results.

Easy to install

The Penetrator is compatible with any operating system. It is easy to install, with minimal configuration. Installation wizards provide for fast setup.

Scalable and Upgradeable

The SecPoint® Penetrator™ is scalable for network growth and IP addresses.

Distributed Audit Capability

You can setup multiple SecPoint® Penetrator™ at different locations on the internal network and remotely via an encrypted secure connection connect them together. This allows distributed auditing, configuration and reporting from a centralized point.

Launch Real Exploits and Denial of Service Attacks

You can launch real exploits to verify that an identified vulnerability is exploitable. It is also possible to launch real Denial of Service attacks to test pre production systems for stability.

Features and Benefits

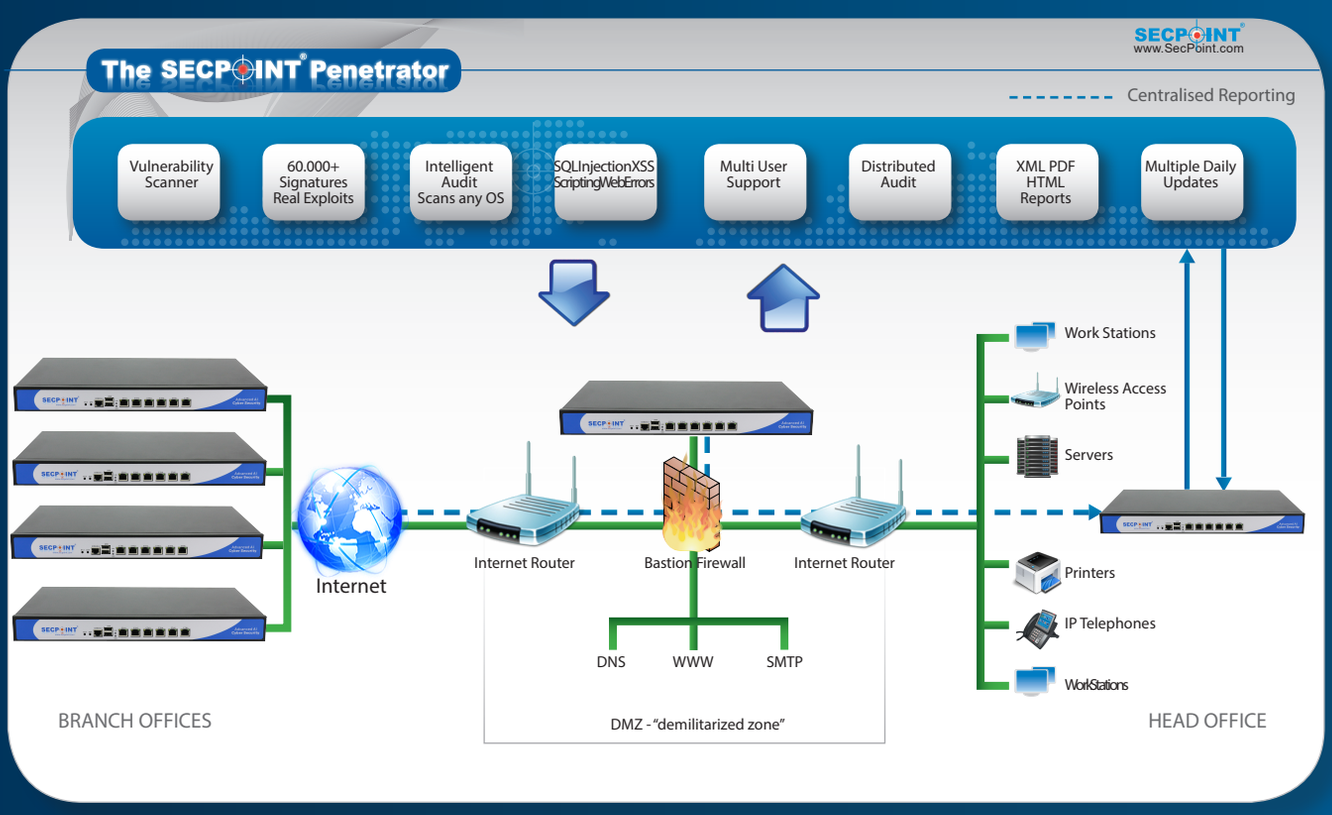
- No Data Collection, Backdoor Free
- 11 Scan Profiles, HIPAA, OWASP top 10, Prepare for PCI, Firewall Scan, SCADA and more
- Advanced Web Crawler - SQL Injection - XSS - SSL
- Bugtraq ID / Mitre CVE / Ubuntu USN / Microsoft / OSBDB
- Schedule scans daily, weekly, monthly
- Prevent Hackers To Access Your Server
- Vulnerability Scanning
- Vulnerability Assessment
- 60.000 + Vulnerabilities
- Launch Real Exploits
- Distributed Scanning Capability
- Report languages: English, Spanish, Danish, Italian, Korean, Dutch, Norwegian, Thai, Portuguese, Turkish & Croatian
- Scan any OS and Network devices
- Reports Branding
- Detailed Remedies for Identified Vulnerabilities
- Secure Design All Data Stored on Unit
- Ticket System for full Vulnerability Management
- Vulnerability Audit
- Launch DoS & DDoS attacks
- Advanced Audit Options
- Option for centralized update point
- Audits any OS
- Automatic Web Crawl Script Engine
- Stand-Alone SFF or 1U Appliance
- Multi User Support
- Launch Real Exploits
- Option for syslog remote logging
- OS Independent Interface
- Distributed Auditing
- XML, PDF and HTML Reports
- Finds SQL Injection

SecPoint® Penetrator™
Penetration Testing Appliance

SecPoint® Penetrator™ Models >>

	S9 - 4-32 IPs	S9 - 8-64 IPs	S9 - 128-256 IPs	S9-512-2048IPs
Height	1 U Rackmount Small Form Factor SFF	1U Rack mount	1U Rack mount	1U Rack mount
Power Supply	60W power supply AC/DC 90-264V Full Range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range	200W Power supply AC/ DC90-264 V Full range
Environment Temperatures	Operating : 0°C to 40°C Storage: -25°C to 75°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C	Operating : 0°C to 40°C Storage: -40°C to 85°C
Network10/100/1000 Mbpsh	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces
Automaticdatabase andsoftwareupdates	Yes	Yes	Yes	Yes

Are you ready for the next step?



E-mail: info@secpoint.com

SECPOINT®
www.secpoint.com

For more information on Penetrator, please visit
https://www.SecPoint.com/penetrator.html
https://support.SecPoint.com

VAR/VAD Contact