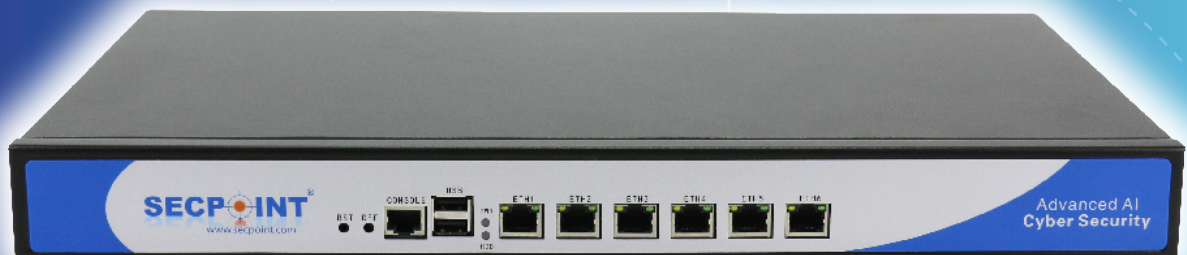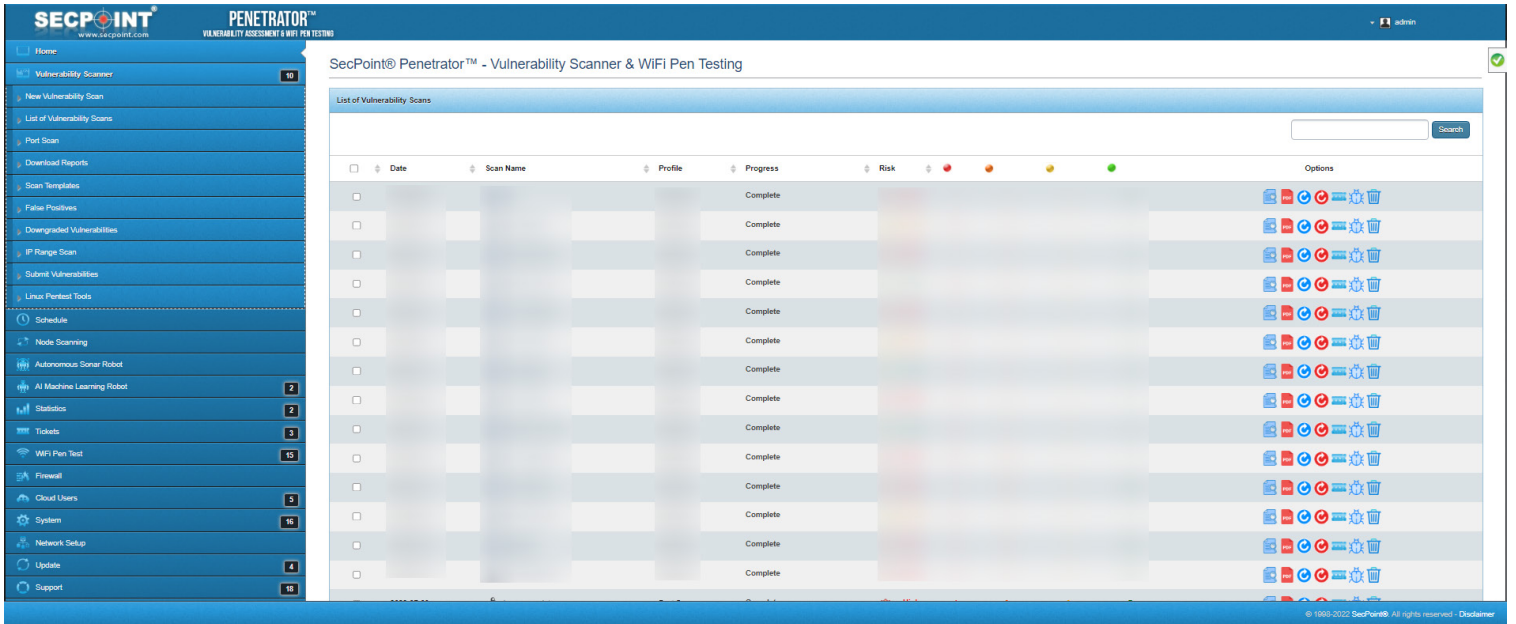# SecPoint® Penetrator™

- Scan Local & Public IPs
- Virtual Software & 1U/SFF Appliance
- Lethal Attack Blind SQLi & RCE
- SQL Injection, XSS & Reflected
- Scans Websites, Webshops, Firewalls
- Dark Web Search - Find Leaks
- Whitelabeling
- Logo Branding, Watermark, Name
- 30 Vulnerability Scan Profiles

- Over 133,000+ Vulnerability Checks
- 1,400+ Web Shells Detection/ RCE
- WiFi Penetration Testing
- Professional PDF & HTML Reporting
- Advanced AI with High Accuracy
- IoT & SCADA Vulnerability Scanning
- Automatic Scheduled Scanning
- Managed Service Provider (MSP)
- Reporting in 20 Languages

SECP⊙INT
www.secpoint.com
Penetrator™

BEST VULNERABILITY SCANNING
ADVANCED AI FOR MOST ACCURATE SCANS
REPORT REBRANDING, LOGO, WATERMARK,
COMPANY NAME
11 SCAN PROFILES

Virtual
Edition

Runs On :

Windows Hyper-V™

ESXi

Haking9
PRACTICAL PROTECTION
SECURING VOIP

CVE COMPATIBLE
cve.mitre.org

ProtectStar
AWARD
2012

NCC-DK
DENMARK CYBERSECURITY
COORDINATION CENTRE

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

CYBERSECURITY ™
MADE IN EUROPE

European DIGITAL SME Alliance

Issued by the
European DIGITAL SME Alliance

SECP⊙INT
www.secpoint.com

Advanced AI
Cyber Security

CONSOLE   ETH1 ETH2 ETH3 ETH4 ETH5 ETH6

HIPAA COMPLIANT

vmware READY

Protect Your Server and Network from Hackers!
Vulnerability Management is Essential for Security

With the advent of sophisticated automated hacking tools, threats can propagate across networks and globally in mere minutes. Recognizing and addressing potential vulnerabilities in your system is a cornerstone of a robust security strategy.

SECP⊙INT®
www.secpoint.com

Vulnerability management
is key to any security strategy

Vulnerability Management

The SecPoint® Penetrator™ stands as the pinnacle of vulnerability management and penetration testing platforms. Fully equipped and ready-to-use, this powerful security assessment solution is an essential asset for any network.

Comprehensive Vulnerability Scanning

Equipped with an expansive vulnerability database and advanced scanning techniques, the SecPoint® Penetrator™ ensures you always remain a step ahead of adept attackers. Users can select from 30 diverse vulnerability scanning profiles to best meet their needs.

Though the IP License restricts only concurrent scanning, it's easily upgradable, marking the Penetrator™ as one of the most thorough vulnerability assessment solutions available today.

Professional Skilled Support

Unparalleled in the industry, we pride ourselves on our swift reply and response times to support queries.
Our top-tier 24-hour support team is always at your service.
Track your inquiries and stay updated with our Support Center's ticket status feature.

Dark Web Search

The Dark Web Search feature helps uncover leaked sensitive customer data, allowing you to take proactive measures before it leads to security breaches.
This enhances your ability to protect customer privacy and maintain trust by identifying potential threats early.
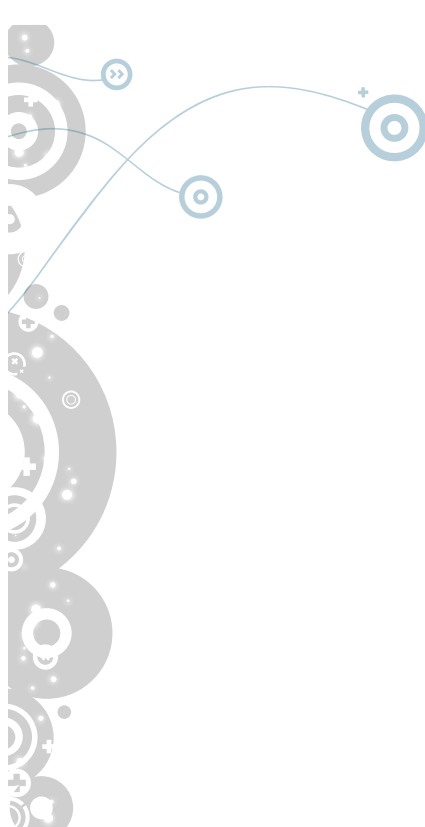
SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment

Professional Reporting

Reports are customizable and can be obtained in XML, PDF, or HTML formats.
System vulnerabilities are categorized into three levels:
High risk, Medium risk, Low risk
Each vulnerability is provided with its name, detailed description, and recommended solution. The report also concludes with an assessment of the overall security level of the scanned system.
An executive summary is crafted specifically for management-level review, presenting both textual and graphical information.

Blind SQL Injection & Web Shells Detection

Lethal Attack technology employs sophisticated methods such as blind SQL Injection, Remote Code Execution, upload vulnerability detection, data leak identification, and Web Shell Detection. These measures are designed to thwart even the most advanced cyber-attacks.

Scalable and Upgradeable

The SecPoint® Penetrator™ can scale with your network growth and accommodate an increasing number of IP addresses.

Distributed Scanning Capability

Set up multiple SecPoint® Penetrator™ units across various locations on your internal network. Connect them securely and remotely via encrypted connections. This enables distributed scanning, centralized configuration, and reporting from a single point.

Managed Service Provider (MSP) Functionality - Multi-User Support

Easily set up multiple users, each with distinct policies including expiration dates and scanning targets.

White-label Reporting & Interface

Reports can be customized with your name, logo, and watermark. Additionally, there's support for over 20 languages, allowing you to change the report's language as per your preference. Both the login logo and the top banner on the interface can also be personalized.

Enhanced Data Privacy

Gain access to our comprehensive Data Privacy Menu, ensuring you have complete control over data locations and permissions.

Features & Benefits

- No data collection guaranteed no backdoors
- 30 scanning profiles including Firewall, OWASP, and more.
- Lethal Attack - Blind SQL Injection - RCE
- Dark Web Search
- Advanced Web Crawler SQLi - XSS - TLS - SSL
- Mitre CVE / Ubuntu USN / Microsoft / OSBDB
- Schedule scans daily, weekly, or monthly
- Protect your server from hacker access
- Vulnerability Scanning & Assessment
- Over 133,000 known vulnerabilities
- Detection for 1,400 web shells
- WiFi Pen Testing - WEP WPA WPA2 & WPS
- SecPoint® RBL List protection
- Data leak detection capability

- Assess for missing security headers
- Distributed Scanning Capability
- Supports 20 Report Languages
- Compatible with Any OS
- Whitelabeling for Report Branding
- Detailed Remedies for Vulnerabilities
- Secure Design All Data Stored on Unit
- Ticket System for found Vulnerabilities
- Vulnerability Scanning & Assessment
- Launch DoS & DDoS attacks
- Advanced Scanning Options
- Centralized Update Point Option
- Scans All Operating Systems
- Automatic Web Crawl Script Engine

- Stand-Alone SFF or 1U Appliance
- Managed Service Provider (MSP)
- Multi User Support
- Vulnerabilities in SCADA & IoT
- OS Independent Interface
- Report Formats: XML, PDF, and HTML
- SQL Injection & Cross Site Scripting
- Comprehensive Data Privacy Options
- Error Detection for Websites
- Remote Code Execution(RCE)
- Automatic Network Discovery
- Blocks Millions of Toxic IPs
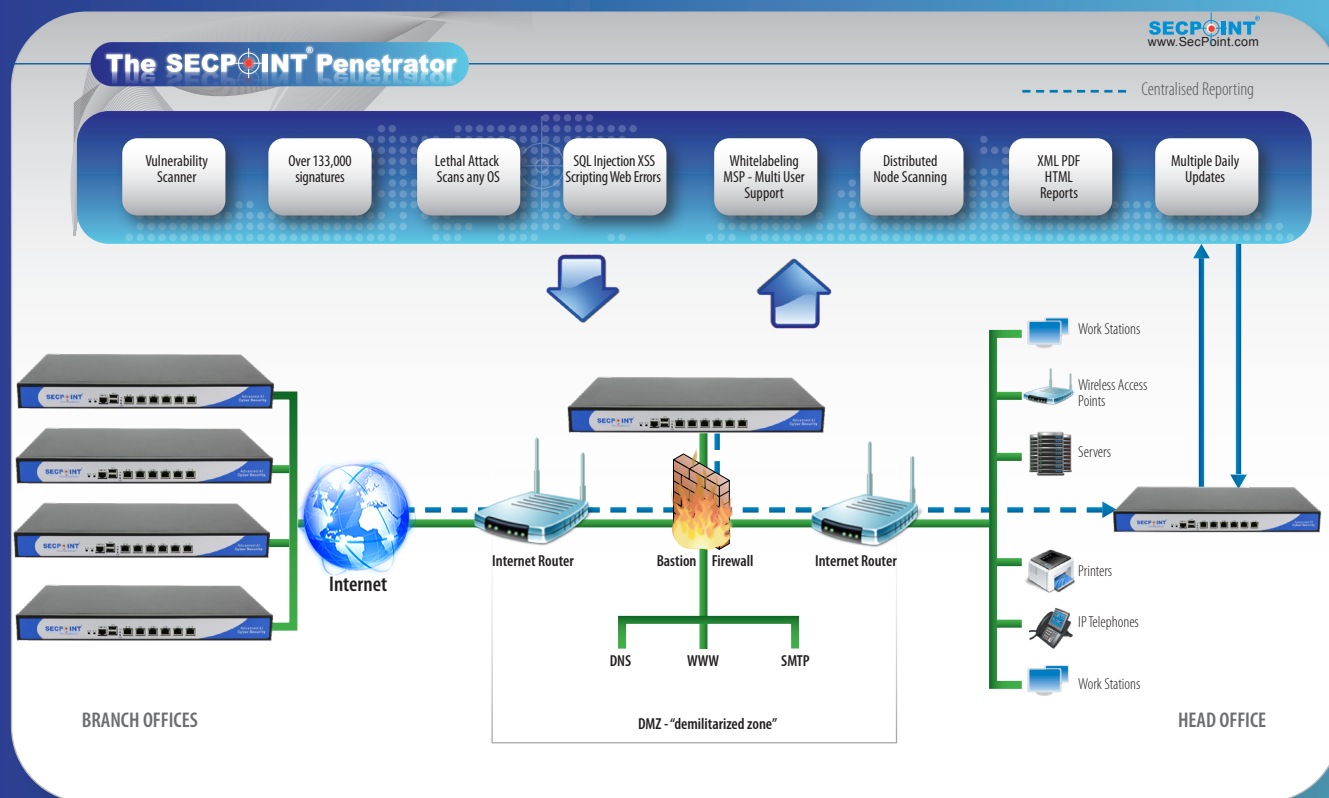- Support for 2FA Authentication

SecPoint® Penetrator™
Best Vulnerability Scanning & Assessment

SecPoint® Penetrator™ Models >>

Are you ready for the next step?

	S9 - 4-32 IPs	S9 - 8-64 IPs	S9 - 128-256 IPs	S9 - 512-2048 IPs
Height	1 U Rackmount Small Form Factor SFF	1U Rack mount	1U Rack mount	1U Rack mount
Power Supply	60w power supply AC/DC 100-240V Full Range	250w Power supply AC/ DC 100-240V Full range	250w Power supply AC/ DC 100-240V Full range	250w Power supply AC/ DC 100-240V Full range
Environment Temperatures	Operating: -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C	Operating: -20°C to 50°C Storage: -40°C to 70°C
Network 10/100/1000	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces	10/100/1000 Ethernet interfaces
Automatic database and software updates	Yes	Yes	Yes	Yes

The SECPOINT® Penetrator

www.SecPoint.com

Centralised Reporting

- Vulnerability Scanner
- Over 133,000 signatures
- Lethal Attack Scans any OS
- SQL Injection XSS Scripting Web Errors
- Whitelabeling MSP - Multi User Support
- Distributed Node Scanning
- XML PDF HTML Reports
- Multiple Daily Updates

Internet

Internet Router   Bastion Firewall   Internet Router

DNS   WWW   SMTP

BRANCH OFFICES

DMZ - "demilitarized zone"

Work Stations
Wireless Access Points
Servers
Printers
IP Telephones
Work Stations

HEAD OFFICE

Value Added Reseller(VAR) / Value Added Distributor(VAD)

SECPOINT®
www.secpoint.com

For detailed information on the SecPoint® Penetrator,
visit the official webpage at https://www.SecPoint.com/penetrator.html