SecPoint® Penetrator™

- Scan Local & Public IPs
- Easy to Deploy Virtual Software
- Lethal Attack Blind SQLi & RCE
- SQL Injection, XSS and Reflected XSS
- Scans Websites, Webshops, Firewalls
- Dark Web Search - Find Data Leaks
- Whitelabeling
- Logo Branding, Watermark, Name
- 34 Vulnerability Scan Profiles
- CVSS v3 Support
- Powered by 146,000+ Vulnerability Signatures
- 1,400+ Web Shells Detection/ RCE
- WiFi Penetration Testing
- PDF, HTML, XML and XLS Reporting
- Advanced AI with High Accuracy
- IoT & SCADA Vulnerability Scanning
- Automatic Scheduled Scanning
- Managed Service Provider (MSP)
- Reporting in 28 Languages
- Authenticated Cisco, Linux and BSD Scanning

ESXi

Windows Hyper-V™

XPROXMOX

vmware READY

NCC-DK
DENMARK CYBERSECURITY COORDINATION CENTRE

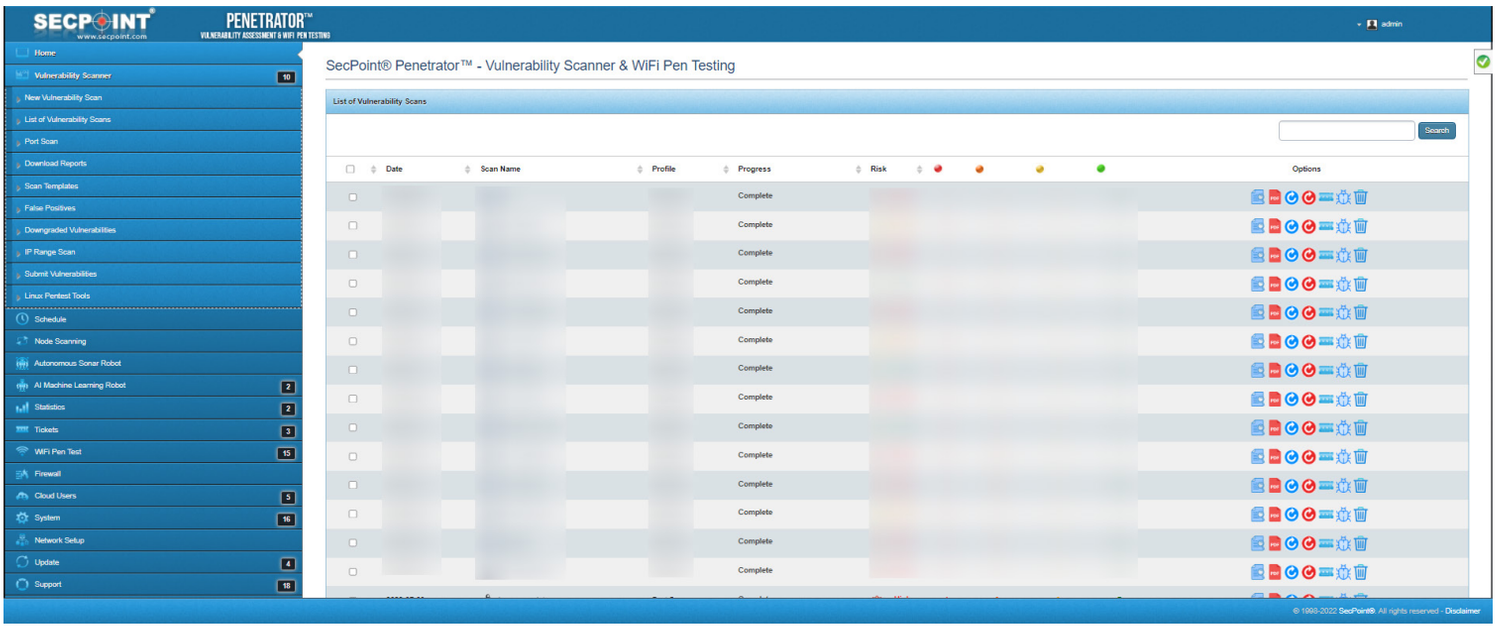
CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

CYBERSECURITY™ MADE IN EUROPE
European DIGITAL SME Alliance
Issued by the European DIGITAL SME Alliance

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.

SECPOINT®
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 34 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.

Expert Cybersecurity Support

Unparalleled in the industry, we pride ourselves on our swift reply and response times to support queries.
Our real human cybersecurity experts provide fast support, remote assistance when needed, and help customers understand scan results and remediation steps. No AI chatbots replace expert help.

Dark Web Search

Dark Web Search helps uncover leaked customer data, exposed credentials, and other sensitive information that may already be available outside the organization. This improves visibility and helps customers take action before leaked information is abused.

SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment

Professional Reporting

Reports are customizable and can be obtained in PDF, HTML, XML and XLS 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 multiple 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.

Transparent Data Privacy Menu

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
- 34 vulnerability scan profiles including OWASP, NIS2, DORA, CRA, CMMC & more
- Lethal Attack - Blind SQL Injection - RCE
- Dark Web Search 5.0
- 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
- Powered by 146,000+ vulnerability signatures
- Detection for 1,400 web shells
- WiFi Pen Testing - WEP WPA WPA2 & WPS
- SecPoint® RBL List protection
- Data leak detection capability
- Last 20 Scanned Locations World Map
- Assess for missing security headers
- Distributed Scanning Capability
- Supports 28 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
- Scan Target Geo Mapping
- Stand-Alone SFF or 1U Appliance
- Managed Service Provider (MSP)
- Multi User Support
- Vulnerabilities in SCADA & IoT
- OS Independent Interface
- Report Formats: PDF, HTML, XML & XLS
- 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 MFA Authentication
- Authenticated Scanning for Cisco & *Nix

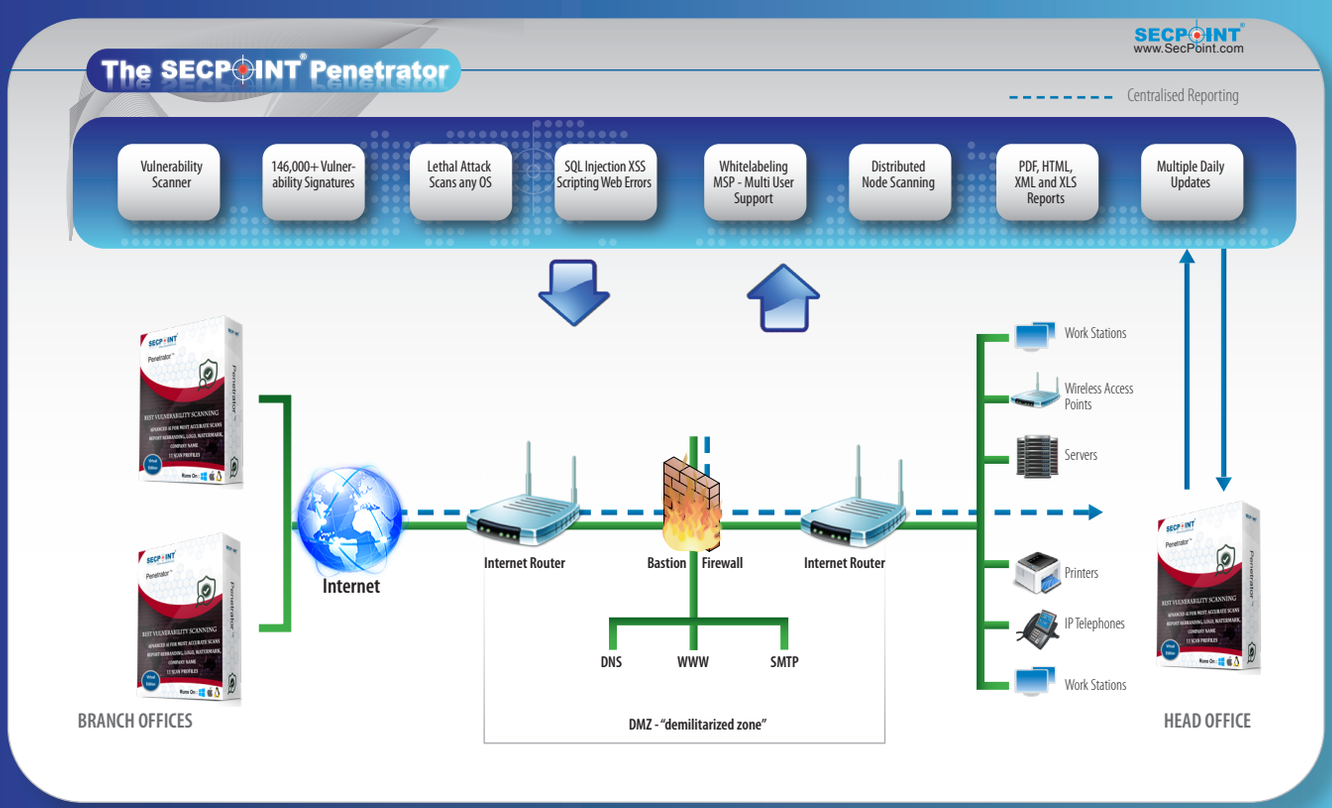
SecPoint® Penetrator™

Best Vulnerability Scanning & Assessment

SecPoint® Penetrator™ Models >>

	S9 - 4-32 IPs	S9 - 8-64 IPs	S9 - 128-256 IPs	S9 - 512-2048 IPs
Concurrent IP Address	Yes	Yes	Yes	Yes
Software Platform	VMware, Proxmox, Hyper-V, Azure & Linux G4L	VMware, Proxmox, Hyper-V, Azure & Linux G4L	VMware, Proxmox, Hyper-V, Azure & Linux G4L	VMware, Proxmox, Hyper-V, Azure & Linux G4L
34 Vulnerability Scanning Profiles	Yes	Yes	Yes	Yes
Add multiple Network Interfaces 10/100/1000	Max 6x	Max 6x	Max 6x	Max 6x
Automatic database and software updates	Yes	Yes	Yes	Yes

Are you ready for the next step?



SECPOINT®
www.secpoint.com

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

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

HAFS
Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision