

The Penetrator

Penetration Testing Appliance



**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

The Penetrator is a vulnerability management and penetration testing appliance for your network, which comes pre-loaded and ready to go.

It is a powerful and intelligent security assessment solution.

Comprehensive and Unlimited Vulnerability Scanning

With its comprehensive vulnerability database and the application of sophisticated auditing techniques, the Penetrator enables you to

always be one step ahead of even the most skilled and advanced attackers. It has no limit on the amount of auditing nor limit on the number of IP addresses and is most certainly one of the strongest and most comprehensive vulnerability assessment solutions on the market.

The Penetrator

Penetration Testing Appliance

Easy-to-understand Reporting

Reports can be customised and are available as 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 remediation.

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 set up.

Scalable and Upgradeable

The Penetrator is scalable for network growth and IP addresses.

Distributed Audit Capability

You can setup multiple 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 preproduction systems for stability.



Features and Benefits

- Vulnerability Audit
- 42.000+ Database Signatures
- Unlimited Auditing
- No Software Installation
- Advanced Audit Options
- Reports Branding
- Option for centralized update point
- Audits any OS
- Automatic Web Crawl Script Engine
- Stand-Along SFF or 1U Appliance
- Multi User Support
- Launch Real Exploits
- Option for syslog remote logging
- Launch DoS & DDoS attacks
- OS Independent Interface
- Distributed Auditing
- XML, PDF and HTML Reports
- Finds SQL Injection, Cross Site Scripting, and Web Errors

The Penetrator

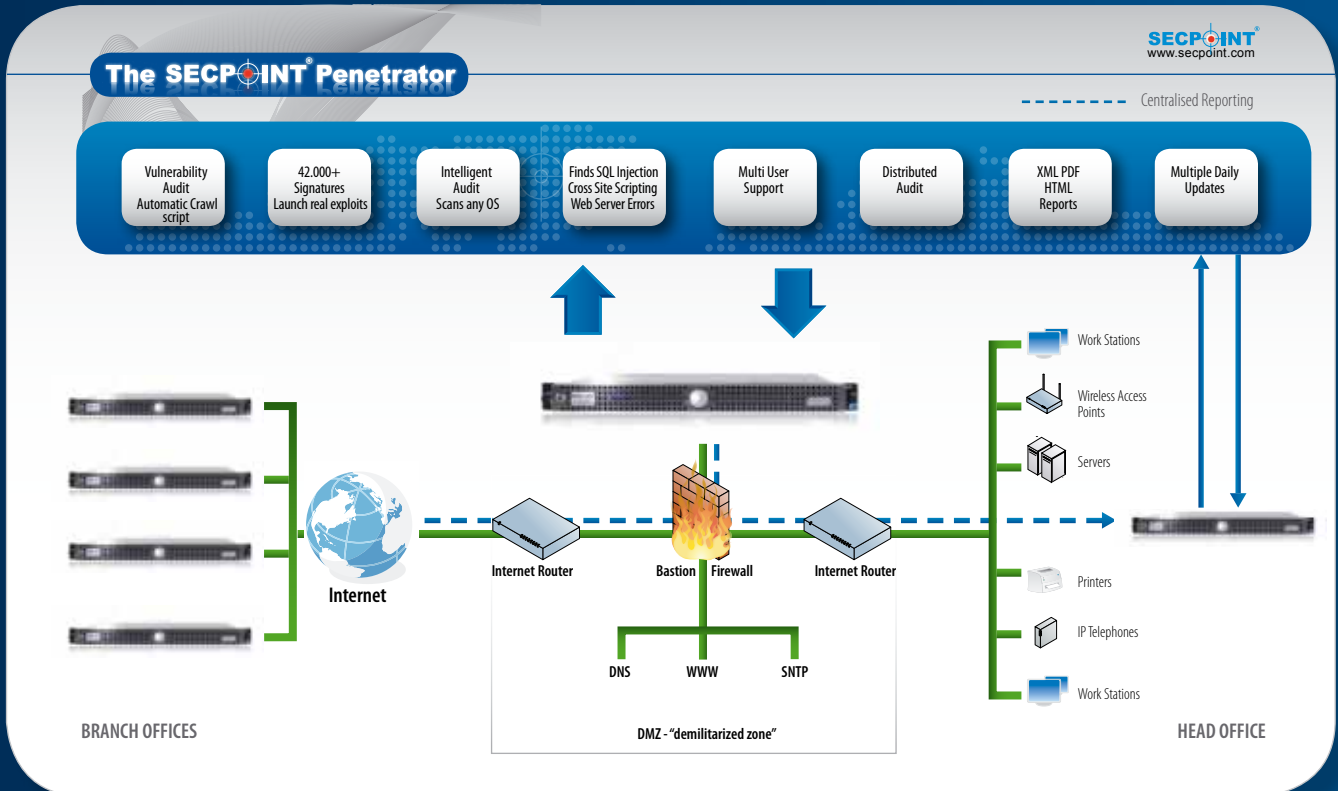
Penetration Testing Appliance

Penetrator Models >>



	S300/S700	S1100	S1600	S2100
Height	Small Form Factor	1U Rack mount Heavy-duty steel	1U Rack mount Heavy-duty steel	1U Rack mount Heavy-duty steel
Power Supply	180W ATX Power supply, AC / DC 90~264V full range	250W ATX Power supply, AC / DC 90~264V full range	460W Redundant Power supply, AC / DC 90~264VAC full range	460W 1+1 ATX Redundant Power supply
Environment Temperatures	Operating : 0°C to 40°C Storage: -20°C to 80°C	Operating : 0°C to 40°C Storage: -20°C to 80°C	Operating : 0°C to 40°C Storage: -20°C to 80°C	Operating : 0°C to 40°C Storage: -20°C to 80°C
Network 10/100/1000 Mbsh	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

Are you ready for the next step?



Internet: www.secpoint.com
E-mail: info@secpoint.com



For more information on SecPoint, please visit www.secpoint.com/penetrator.html

Partner Information