



## About SensePost

SensePost is an independent and objective organisation specialising in information security consulting, training, security assessment services and IT Vulnerability Management.

SensePost is about security. Specifically - information security. Even more specifically - measuring information security.

We've made it our mission to develop a set of competencies and services that provide our customers with insight into the security posture of their information and information systems.

## Why SensePost

Over more than a decade in service to the biggest and best organisations in the world, SensePost has built a reputation based on trust. Trust our integrity and objectivity, and trust that we will provide the highest available level of technical expertise.

## Contact Us

**Web:** [www.sensepost.com](http://www.sensepost.com)

**Tel:** +27 12 460 0880

**Fax:** +27 12 460 0885

**Mail:** [info@sensepost.com](mailto:info@sensepost.com)

## Introduction



Systematic Vulnerability Management for security and compliance is a key discipline for any mature modern organisation. With SensePost Managed Vulnerability Scanning (MVS) it is possible to identify and respond to weaknesses in systems and networks before they are discovered by hackers or malicious insiders.

SensePost Managed Vulnerability Scanning is a fully Managed Vulnerability Scanning service supported by SensePost and designed for the enterprise. Requiring no client software and accessible from any location via a powerful and easy-to-use web interface, MVS deploys a collection of specialised scanners to discover and analyse vulnerabilities across all the different components of a network.

## Features and Benefits

- A fully managed service, requiring no installation, configuration, or maintenance. No in-house security skills or experience are required;
- Full business-hours support included, with additional support available on request;
- Provides a single complete and comprehensive view of the enterprise vulnerability posture from inside and outside, for both Vulnerability Management and Payment Card Industry (PCI) Compliance purposes;
- Personalised reports in the form of dashboards can be presented to specific groups and users according to their role in the Vulnerability Management process;
- A powerful drill-down feature allows for quick and easy access to very detailed security information or high-level management metrics;
- Besides standard Vulnerability Scanning of networks, hosts and devices, the service can detect security issues in Active Directory , DNS, databases, and Web Applications;
- Automatic tagging and inventory of hosts enables easy and automatic classification for searching and reporting into groups, according to function, location, sensitivity or other attributes; and
- Multiple report formats allow for easy integration and distribution of vulnerability and remediation information.

## Multiple Vulnerability Scanners

SensePost's Managed Vulnerability Scanning service is comprised of the following types of scanning services:

- Internet Perimeter Vulnerability Scanning;
- Internal Vulnerability Scanning;
- Web Application Vulnerability Scanning;



- PCI Approved Scanning Vendor (ASV) Vulnerability Scanning;
- Database Vulnerability Scanning; and
- Active Directory Vulnerability Scanning

All scanners are accessed, managed, and configured via a single, easy-to-use web interface. The required technology is available as Software as a Service (SaaS), a VMWare image or as a hybrid deployment.

## Powerful, Flexible Reports



Each user on the system has a unique dashboard customised for their role within the Vulnerability Management process. Dashboards can consist of any number of widgets, called 'Blizzards', which can easily be added or customised. Examples of standard Blizzards include:

- **Technical:**
  - Most critical hosts;
  - Most vulnerable systems; and
  - Newly discovered issues.
- **Management:**
  - General Trends;
  - Number of new issues; and
  - Number of existing issues not remediated.
- **PCI:**
  - Non-compliant hosts;
  - Specific issues causing non-compliance; and
  - PCI pass/fail status.
- **Web Application Vulnerabilities:**
  - Vulnerability Hot List;
  - Hosts with dangerous SQL injection (SQLi) Issues; and
  - Hosts with dangerous Cross Site Scripting (XSS) issues.
- **Secure Sockets Layer (SSL) Certification Management:**
  - Lists of expiring or expired SSL certificates;
  - Overview of Certificate Issuers; and



- Overview of Certificate Common Names.

Pre-configured templates allow for role-specific dashboards with the relevant widgets to be easily assigned to specific users.

## Differentiators

- A fully **Managed Service**. No installation, configuration or maintenance required;
- Each client is assigned a **Personal Support Engineer** who is an experienced security analyst and penetration tester;
- Provides a **comprehensive overview** of enterprise vulnerability posture with specific dashboards for specific users and groups;
- Over **50 specialised report widgets** are available to each user. New widgets, dashboards and tests can be seamlessly added;
- Highly **configurable and customisable** via your Personal Support Engineer to meet individual requirements; and
- Unlimited users. **Unlimited** scanning.



## About SensePost

SensePost is an independent and objective organisation specialising in information security consulting, training, security assessment services and IT Vulnerability Management.

SensePost is about security. Specifically - information security. Even more specifically - measuring information security.

We've made it our mission to develop a set of competencies and services that deliver our customers with insight into the security posture of their information and information systems.

## Why SensePost

Over more than a decade in service to the biggest and best organizations in the world, SensePost has built a reputation based on trust. Trust our integrity and objectivity, and Trust that we will provide the highest available level of technical expertise.

## Contact Us

**Web:** [www.sensepost.com](http://www.sensepost.com)  
**Tel:** +27 12 460 0880  
**Fax:** +27 12 460 0885  
**Mail:** [info@sensepost.com](mailto:info@sensepost.com)

## Services

SensePost offer the following types of Managed Vulnerability Scanning services:

### Internet Perimeter Vulnerability Scanning

Continuous or on-demand vulnerability scanning of Internet-facing devices and systems, e.g. web servers, mail servers, ftp servers, DNS servers, routers, firewalls, etc. Delivered via SensePost infrastructure in the "cloud".

### Internal Vulnerability Scanning

Continuous or on-demand vulnerability scanning of servers, workstations, network devices and peripherals such as printers and scanners connected to the internal LAN or WAN environment.

### Web Application Vulnerability Scanning

Continuous or on-demand scanning of Internet-facing Web Applications for application-level vulnerabilities like SQLi and XSS.



### PCI ASV Vulnerability Scanning

Continuous or on-demand scanning of Internet-facing servers, e.g. web servers, mail servers and DNS servers, and Web Applications, e.g. e-commerce applications for the purpose of PCI DSS compliance. SensePost is a PCI-ASV.



SensePost offers a comprehensive support service around the vulnerability scanner that ensures the customer fully understands the findings and associated implications within the context of the report. Thus, in addition to the automated scans that the customer may request at

any time, SensePost will manually oversee the execution of each mandatory quarterly scan and oversee the findings in the report to verify their accuracy and relevancy with regard to the DSS. Moreover, experienced SensePost analysts are available on a business-hours basis to field any queries and provide support around scanner output.

### Database Vulnerability Scanning

Continuous or on-demand scanning of databases like MS-SQL, Oracle and DB2 for vulnerabilities, security misconfigurations and policy compliance.

### Active Directory Vulnerability Scanning

Continuous or on-demand monitoring of the Microsoft Active Directory (AD) group membership and changes. Reports changes to important sensitive groups like 'Administrators', 'Finance' and 'HR' so that potential authorisation breaches can be detected.

# MANAGED VULNERABILITY SCANNING



<b>Specifications</b>		
<b>Underlying Technology:</b>		
Active scanning	✓	Targeting can be manual or obtained from device attributes which are continuously collected and grabbed from LDAP data such as from AD
Host-based scanning	✓	Local policy or compliance scanning
Internet-based scanning	✓	Available on the Internet as SaaS. Otherwise a dedicated . can be placed in a DMZ to scan from the "outside"
Distributed and optimised scanning	✓	Agents can be placed at remote sites to reduce bandwidth costs or at a central location to allow for faster scanning.
Multi-operating system support	✓	Any device communicating over TCP/IP can be scanned
Multi-database support	✓	Compliance scanning includes DB2, Oracle and MS SQL
Manual scanning mode	✓	Scans can be scheduled or manually launched as once-off scans
Scanning for non-standard ports	✓	Full scanning mode will scan for all 65k ports
Attribute collection	✓	Gathers default configuration data and other attributes of all devices scanned - including IP address, hostname, open ports, installed service packs, SMS agents, Bind version etc. Attribute collection is used to either identify new asset groups or to report on specific issues.
<b>Administration Features:</b>		
Excellent reporting capabilities	✓	Management and full technical reports available
Detection of missing patches	✓	There are very specific Microsoft checks. Most other devices are included as well
Performance management	✓	Network bandwidth is monitored and scans are automatically adjusted to minimize impact on network performance
Vulnerability ranking	✓	Default ratings are given – but can be moderated depending on mitigating controls in place
Scalability	✓	Extra IP addresses can be scanned as required.
Easy updating	✓	Software updates are pushed down to the servers automatically as they become available
Detection of most vulnerabilities	✓	28 000 checks give or take a hundred
Detection of applicable vulnerabilities	✓	Continuous or on-demand scanning of Internet-facing Web Applications for application-level vulnerabilities like SQLi and XSS
Frequent updating of attack signatures	✓	Can be daily, depending on how they are released or developed
Graphical or web interface	✓	Web interface.
Hardware required	✓	Minimum specs are provided – client can provide the hardware
Installation procedures	✗	As a managed service, all installation, configuration and maintenance performed by SensePost.
Training	✗	Very little training is required but short courses are available at any time at no additional cost.
<b>Reporting features:</b>		
Format	✓	PDF and CSV formatting possible. PDF reports are sorted according to either IP address or Vulnerability. A summary report can be downloaded only presenting the vulnerability

# MANAGED VULNERABILITY SCANNING



		header and the IP address
Configurability	✓	Any reasonable report changes can be requested from SensePost that at no additional cost
Customisation	✓	Reports can be customised to include branding, specific names, data classifications, responsible persons etc.
Flexibility	✓	New tests, new attributes, and new reporting blizzards can be added without cost. Additional scanning engines can be requested costs
Prioritised reporting	✓	BY default reports are sorted according to either the highest risk (weighted issues) or according to the IP address with the highest weighted number of risks. Where a specific need is identified this could be develop to suite the customer
Sorting of data	✓	The online reporting feature allows for sorting according to weighting, IP address, issues, hosts etc.
Exporting to other programs and formats	✓	PDF and CSV.. XML output can be provided through an API.
Different view	✓	Targets and vulnerabilities can be viewed through a Vulnerability, Attribute and Desktop Blizzard view.
Time-series reporting	✓	The blizzard desktop can be tasked to show vulnerabilities or numbers of hosts scanned over a period of time.
Dashboard reporting	✓	Users are able to easily create personalised desktop views according to their security role in within the organisation. Each desktop can be populated with any number of widgets called "Blizzards". Blizzards are SQL queries that are displayed in individual windows as charts or tables. These Blizzards can also be downloaded as CSV or PDF reports - apart from the additional reporting features. Blizzards can be specific to a single scan, across all scans, in a time-series, xy graphs, or across a certain asset group.
Issue reporting	✓	Issues are reported to include descriptions, impact, CVSS numbers, CVE numbers, recommendations and external links. Raw output of scan results can be enabled if so required
<b>Performance:</b>		
Use of multiple scanners on enterprise network	✓	Agents can be placed at remote sites to reduce bandwidth costs or at a central location to allow for faster scanning.
<b>Support</b>		
Local Support	⊙	Telephonic and email support is available worldwide. On-site visits are available at no additional cost in the United Kingdom and South Africa.