

## SNAPPiMON Datasheet

SNAPPiMON is part of IBM NOC-Inside services and is a scalable Enterprise IT Monitoring platform that provides **agentless** monitoring of networks, servers, databases, middleware and application. SNAPPiMON automatically detects IT availability and anomalies in IT performance and provides real time alerts via email or SMS, It provides multiple real time and historical analysis reports for enhanced capacity planning, root cause analysis, availability & performance management. SNAPPiMON correlates information across the IT infrastructure, prioritizes and identifies issues which impact business operations most and allows quick resolution of relevant IT problems.

### Features

- ✓ Network, Server, Application Monitoring
- ✓ Database & Middleware Monitoring
- ✓ Real time business, network & tree topology
- ✓ Multiple Historical Reports
- ✓ Agentless Monitoring
- ✓ Auto Discovery
- ✓ Analysis of IT Impact on Business
- ✓ Effective & Integrated correlation for efficient root cause analysis
- ✓ Generates Email & SMS notifications, escalations
- ✓ Includes out of the box reports, real time dashboards and analytics
- ✓ Provides role based access control for secure data access
- ✓ Automatic execution of actions on availability or performance breaches
- ✓ Integrates with external helpdesk applications
- ✓ Integrates with external EMS
- ✓ Supports LDAP and Microsoft ADS authentication
- ✓ Supports multiple tenancy support for Service Providers
- ✓ Highly scalable, distributed architecture with ability to support large number of elements

### Benefits

- ✓ Easy to use, does not require experts to operate, maintain and use
- ✓ Embeds Netsol's expertise in managing large & complex IT infrastructure
- ✓ Ensure enhanced IT support to business
- ✓ Eliminate negative impact of IT on business
- ✓ Proactive monitoring ensures increased business & end user satisfaction with IT
- ✓ Ensure resource capacity planning is based on historical trend data
- ✓ Eliminate IT Availability issues
- ✓ Ensure optimum IT Performance
- ✓ Agentless monitoring approach allows for non invasive monitoring with faster deployment & implementation
- ✓ SMS and email support ensures fast and reliable notifications during outages
- ✓ Integrated correlation across networks, servers, databases, middleware, application allows for faster & accurate Root Cause Analysis (RCA)
- ✓ Distributed collector architecture with data compression ensures minimal network overhead
- ✓ Secure, permission based access control ensures role based access to administrators
- ✓ Scalable architecture & design allows monitoring of thousands of network elements
- ✓ Open framework allows for easy and effective extensibility

### Network Monitoring

- ✓ Availability & Performance Monitoring
- ✓ Routers, Switches, Links, Devices, Printers
- ✓ Ability to upload custom MIBs at run time
- ✓ Scheduled Auto Discovery
- ✓ SNMP V1, V2, V3 support
- ✓ SNMP Trap processing
- ✓ Cisco IPSec/VPN and QoS
- ✓ Cisco IPSLA to monitor Jitter, Echo, Latency, etc
- ✓ Cisco Ping MIB to monitor latency **between** Cisco routers
- ✓ Cisco VOIP - Call Manager, Unity, Voice Gateway

## Server Monitoring

- ✓ IBM AIX 5.x and above
- ✓ Microsoft Windows - 98, NT 4.0, 2000 Server, XP, 2003 Server
- ✓ Sun Solaris 5.8 and above
- ✓ Linux – Red Hat and SUSE
- ✓ HP UX 11 and above
- ✓ IBM i Series (i5/OS & AS/400)
- ✓ Open VMS 7.x

## Application Monitoring

- ✓ Oracle 9i/10g/11g and above
- ✓ MS SQL 2000/2005
- ✓ IBM DB2 8/9 and above
- ✓ MySQL 4/5
- ✓ Sybase 11 and above
- ✓ Microsoft Exchange 5.5, 2000, 2003
- ✓ Lotus Domino 6.5 and above
- ✓ Apache Tomcat 5.x
- ✓ Microsoft IIS 5.x/6.x
- ✓ BEA WebLogic 8/9
- ✓ IBM WebSphere 6.x
- ✓ IBM MQ-Series 5.x
- ✓ Microsoft .NET applications
- ✓ Microsoft DHCP/DNS/Active Directory
- ✓ Application Availability of any port, process, service, daemon
- ✓ SQL Query response
- ✓ HTTP URL Response

## Extensibility & Integration

- ✓ Automated Action Engine allows for leveraging of existing script and programs for preventive, corrective and diagnostic actions
- ✓ Business Activity Monitoring allows for extensible polling using end user provided scripts, programs
- ✓ IT Service based monitoring allows for monitoring impact of IT Availability & Performance on business
- ✓ Efficient design allows deployment on cheaper and low end hardware
- ✓ Generates SNMP traps on availability & performance breaches
- ✓ Access control based on LDAP or Active Directory authentication

## Typical System Requirements

- ✓ Hardware sizing depends on the scope of monitoring. Listed below are typical requirements.
- ✓ Supported Operating Systems - Windows XP/2003 or Red Hat Linux 4 or Sun Solaris 10
- ✓ Supported Databases – IBM DB2 v9.5, Microsoft SQL 2005 SP2, Oracle 9i/10g/11g,
- ✓ Application Server – Single CPU, 2.4 Gz, 1 GB RAM free memory, 20 GB free hard disk space,
- ✓ Collector - Intel PIV 2.4 GHz CPU, 512 MB RAM,, 5 GB free hard disk space,
- ✓ Client Browser – Internet Explorer 6/7 or above
- ✓ Application Server, Collector(s), Database may reside on same or separate servers

---

For more information – visit us at [www.netsol.co.in](http://www.netsol.co.in) or call us at +91-80-25508365, +91-25535228 or send us an email at [contact@netsol.co.in](mailto:contact@netsol.co.in)