

SERVOYANT® ACTIVE MONITORING

BUSINESS CONTINUITY BEGINS WITH EFFECTIVE NETWORK MONITORING

With so many companies relying on their information technology systems to conduct operations, network reliability has become a competitive advantage. Companies that would be negatively impacted by unplanned downtime rely on Servoyant® Active Monitoring.

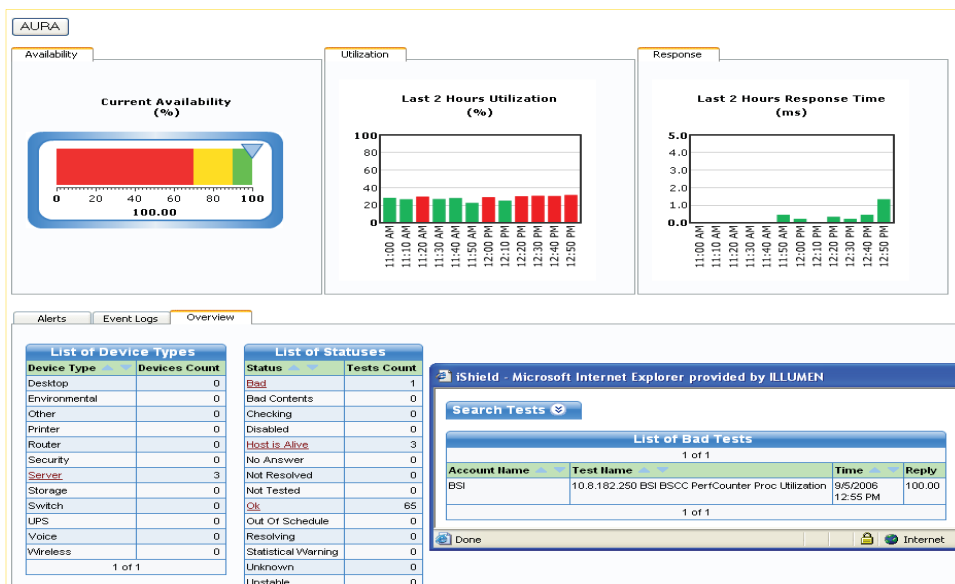
More Than a Monitoring Platform

If you are unaware of what is happening on your network, how do you effectively manage it? 24 hours a day, seven days a week, 365 days a year, Illumen monitors the availability, health, and performance of your most critical IT systems and keeps you informed.

With Servoyant® Active Monitoring, your critical network elements receive the constant attention of Illumen's highly skilled and experienced engineering staff.

Our certified network engineers triage all alerts to determine which are most critical, and notify your organization or resolve issues through pre-defined escalation procedures.

Stay informed of all network activity by accessing the Servoyant® Portal for real-time monitoring reports.



KEY BENEFITS

- Avoid business interruptions
- Address critical issues before they impact your business
- Maximize employee productivity
- Extend the life of network assets
- Access real-time monitoring reports through a web portal
- Management reports help you easily measure ROI
- Reduce administrative costs and network complexity
- Does not require purchase or maintenance of new hardware or software
- Can be setup in a single day

SERVOYANT® ACTIVE MONITORING

STANDARD AND CUSTOMIZEABLE TESTS GIVE YOU GREATER INSIGHT

Servoyant® Active Monitoring reports on custom applications and devices in addition to standard monitoring templates. Choose the elements to monitor based on critical network needs. The following are standard tests for many common network elements:

STANDARD MONITORING TESTS

Basic Server Health

Ping (Response Time and Packet Loss)
CPU Utilization
Memory Utilization
Disk Utilization
Network Interface Card (Errors and Discards)
Server Event Logs (System, Applications, and Security)
Critical Windows Services (Status and Response Time)
Critical TCP Ports (Status and Response Time)

Backups

Critical Backup Services (dependent upon product being used)
Backup Application Event Logs
Backup Application Status via SNMP (where possible)

Internet Information Server

WWW Services
TCP Port 80
IISAdmin Service
IIS Application Logs
URL Requests and Content Integrity

Anti-Virus

Critical AV Services (dependent upon product being used)
Application Event Logs
Application Status via SNMP (where possible)

Switch

Ping
Device health as applicable via SNMP, includes items such as:

- CPU Utilization
- Memory Utilization
- Power Supply
- Fan Status
- Chassis Temperature

Interface Bandwidth
Interface Errors

Router

Ping
Device health as applicable via SNMP, includes items such as:

- CPU Utilization
- Memory Utilization

Interface Bandwidth Utilization
Interface Errors
Buffer Statistics
Packet Loss

Microsoft Exchange

Critical Exchange Services, Including:

- Information Store Service
- Message Transfer Agent Service
- SMTP Service

Message Queues
Work Queues
Private and Public Information Store Size
Application Event Logs

Microsoft SQL

Microsoft SQL Service
SQL TCP Port 1433
SQL Application Error Logs
Synthetic Transaction Testing

Citrix

Citrix TCP Port
Citrix Browser Port
Citrix XML Port
IMA Service
Metaframe Event Logs

Terminal Server

Terminal Server TCP Port
Terminal Server Service
Application Event Logs

Firewall

Ping
Device health as applicable via SNMP, includes items such as:

- CPU Utilization
- Memory Utilization
- Power Supply
- Fan Status
- Chassis Temperature

Security Alerts for Numerous Attacks
Interface Bandwidth Utilization

UPS/Environment

Device health as applicable via SNMP, includes items such as:

- Battery Life
- Battery Power
- Input/Output Voltage
- Time Remaining Until Shutdown

Server Room Temperature
Humidity/Wetness Levels