Nexus Controls
a Baker Hughes business

Nexus OTArmor† Network Monitoring

What is Network Monitoring

Network monitoring provides some key information back to network administrators whose job is to determine, in real time, whether a network is running optimally. With the help of Network Monitoring Software tools, administrators can proactively identify and optimize deficiencies, optimize efficiency, and are able to visualize the network on its entirety.

Primary Benefits and Functionalities

- Using network monitoring, administrators can get a clear picture of all the connected devices in the network. See how data is moving among them, and quickly identify and correct issues that can undermine performance and lead to outages.
- Modern enterprises rely on a host of internet-dependent, business-critical services. This includes cloud service providers, ISPs, CDNs, as well as SaaS, UCaaS, VPNs and SECaaS providers. Each service operates over the internet, making them susceptible to performance fluctuations caused by internet outages or routing issues. Visibility into the network components beyond your control allows you to monitor issues that might impact employees or customers.
- Additional work for IT teams is reduced by the hardware and software tools available in network monitoring systems, allowing the specialist teams to allot more time to critical projects for the organization.
- Network monitoring systems can generate reports that show how network components behaved over time. Network administrators can predict when the organization may need to upgrade or adopt new IT infrastructure by examining these reports.
- Network monitoring aids enterprises in determining what constitutes "normal" network performance. When odd activity occurs, such as an inexplicable surge in network traffic, administrators may immediately identify the problem—and assess whether it poses a security risk.

Monitor Anything with an IP Address

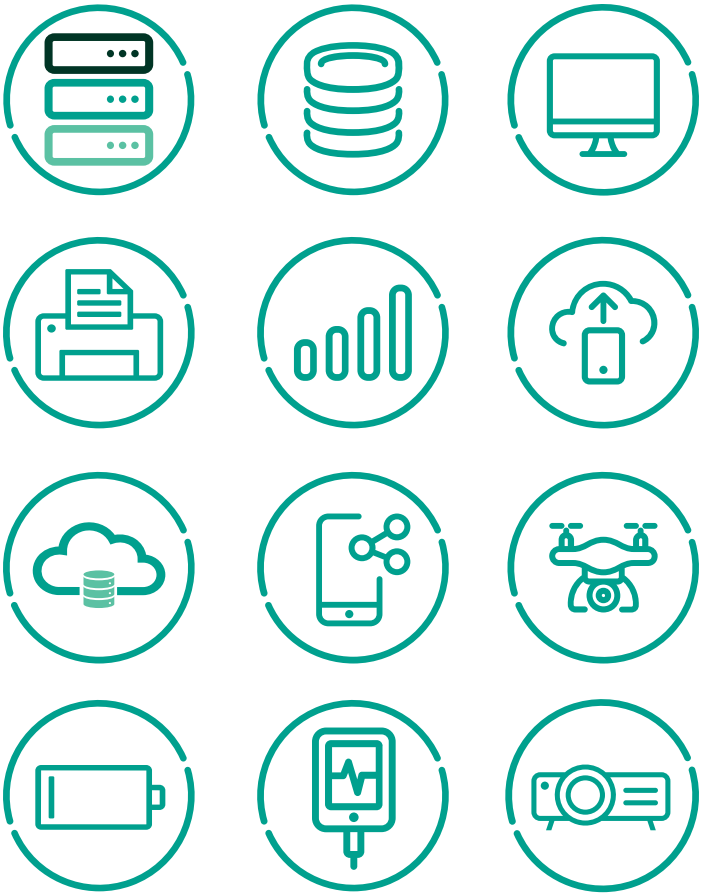
Withing the main functionalities of the tool that we are vetting, is the ability to monitor anything that can be accessed with standard monitoring protocols, including Ping, SNMP, WMI for Windows, and SSH for Unix and Linux. It should support scripting languages like VBscript and PowerShell. And finally, the capability to use SQL queries to create database monitors.

In general network monitoring tools should be able to provide the following functionalities:

- Active: Active monitors proactively poll to monitor device states. For example, Ping is an active monitor that is used to determine if a device is in the up or down state.
- Performance: Performance monitors capture actual performance metrics like CPU and memory utilization. For instance, the CPU utilization on a network device at a set range.
- Passive: Network devices and servers can be configured to send management information out on the network. Two common methods are SNMP traps and Windows events. As an example, a window server can be configured to send out an event every time someone logs into it. A dedicated network monitoring tool should be able to collect, alert and report on these events using passive monitors.

Additional Benefits of Network Monitoring Software

- Network Visibility & Analysis: Monitoring personnel receive up-to-date feedback on the devices connected, gain an understanding of how data is moved, and apply corrective actions that would otherwise result in performance issues and unwelcome outages. High bandwidth usage can also be detected using specific applications.
- Log management functionality allows for the retrieval of information related to Windows events and syslog; some applications include the ability to configure log searches and archive log to be used for regulatory compliance or diagnosis.
- All monitoring, discovery, mapping, alerting, and reporting capabilities are available for virtualized environments, regardless of size or application.
- The ability to monitor the performance of a specific application, allowing for the customization of application state definitions and assisting in SAL calculation. A Service Level Agreement (SLA) is a contract between a provider and a customer that specifies and commits to a certain level of service.
- Configuration management automates the configuration and change management of all network devices. Archies and network configuration audits, as well as alerts to changes in configuration.



† Registered trademark of Baker Hughes in one or more countries. Other names may be trademarks of the respective owners and are used herein for identification purposes only. Use of any names or marks owned by a third party does not imply endorsement by or a relationship with the third party.

Baker Hughes

Copyright 2022 Baker Hughes Company. All rights reserved.

BHCS39289 (07/2022)

nexuscontrols.com