Solutions Review

2020 NETWORK MONITORING BUYER'S GUIDE

MARKET OVERVIEW

The network is perhaps the most essential technology of the modern business. For just about every company, networks are the core technology that allows it to operate efficiently, promote collaboration amongst its staff, and communicate with clients. As such, companies need to ensure that their network is running smoothly at all times.

That's why continuously observing your network for performance problems is a critical aspect of maintaining a business network. Businesses rely on their network to perform at certain levels to satisfy the demands of executives and clients. Unfortunately, network performance issues are all too common, and they can put a strain on your company. Your company needs to be prepared to deal with an unexpected performance problem and fix it before it causes too much stress.

Performance issues and network outages are not just infuriating to deal with; they can also be incredibly costly to your company. NetRounds' September 2019 report *The Hidden Cost of Network Brownouts* revealed that companies lose $600,000 a year on average due to network performance problems. The survey also showed that network brownouts (or sudden drops in quality) are causing damage to 83% of large companies, with many employees citing frustration with the dips in network performance.

How can a business deal with network performance problems, though? Enterprise networks are constantly growing in complexity, adding new devices and new kinds of hardware as Internet of Things (IoT) deployments become more popular. It's also difficult to predict what performance issues are likely to happen (and where they're coming from) until it's too late. In 2020, businesses cannot subside on a reactive approach to problem solving if they expect to maintain solid network performance. Your users will most likely discover a major network performance issue on its own eventually, but it could take a long time to fix the issue after it's discovered. Instead, a company must enable a proactive defense infrastructure that actively searches for problems and alerts administrators to a potential performance-alerting issue before it even occurs.

To ease the burden on network administrators and engineers, companies need to consider deploying a network performance monitoring solution. For companies of all sizes, a network monitoring solution allows you to proactively deal with performance problems and gain valuable insights into how your network is functioning. However, as monitoring solutions become more integrated, adding services beyond network monitoring, it can be challenging to know which tool is right for your company.

That's where this Buyer's Guide comes in. We've detailed the top network performance monitoring vendors with individual profiles, key features, and capability references. The editors at Solutions Review cut through the rhetoric to provide an unbiased rundown of these unique vendors. Additionally, we provide the Bottom Line: our take on what makes the featured vendors unique, distinctive, or exceptional. This guide serves as a solid resource to have on hand while your enterprise is evaluating monitoring solutions for your business network.

Daniel Hein, Editor

5 Questions You Should Ask When Evaluating A Network Monitoring Solution

Does my business have a network performance goal?

Successful network performance isn't a "one size fits all" deal; every business will have different goals regarding network performance. Defining a network performance goal allows your company to know how they should approach performance monitoring, which will help your business evaluate potential solutions. This goal should not be set in stone forever; it should change periodically to reflect new performance trends or address common problems.

Are you using too many monitoring tools already?

One of the major issues with using many different monitoring tools is that it's often very difficult to keep them in sync. Multiple monitoring tools also means that you must install, configure and support every tool individually. By employing so many tools, your network teams are spending more time troubleshooting and less time working on other more pressing issues. Many companies are releasing unified monitoring tools that combine different solutions, helping to mitigate this issue.

Is it difficult to collaborate between IT teams and other departments?

When network performance drops, IT teams tend to claim innocence by sticking to their respective departments and tossing blame to others. With full network visibility gained from a network monitoring solution that delivers intelligent insights into the root causes of problems, IT teams are given a more defined focus to work with. This allows them to promote a more collaborative environment, letting both the IT team and other departments work in harmony.

Is your organization having problems troubleshooting network issues?

It's easy enough to realize that something's wrong with your network. However, it can be a struggle to discover what the problem actually is. Network monitoring solutions simplify the detection and remediation of network issues by offering visual displays of devices, flows, and packets. Most solutions also give users the ability to click on a particular device and see critical performance data, like availability, packet loss, response time, error rates, and more.

Is your organization concerned about network security?

A network monitoring solution provides the invaluable benefit of added network security. If a network monitoring solution reports a sudden increase in CPU usage or if network traffic metrics take a significant deviation from the norm, this information could quickly alert IT staff of a possible malware or phishing attack. Network monitoring software can easily be situated next to any of an organization's existing security solutions to provide a holistic view of network security.

5 Questions You Should Ask Your Potential Network Monitoring Solution Provider

How easy is it to deploy your network monitoring solution?

A quality network monitoring tool won't require that users go through an arduous process to get the tool up and running. If the product you're considering requires numerous tutorials or additional servers to be purchased, or if the features you need seem missing or non-essential, you may want to keep looking. Also, if it looks like purchasing a monitoring tool will drain too many vital resources from your organization, you should probably consider another solution.

Does your network monitoring solution deliver intelligent alerts?

One of the most critical (and sometimes underappreciated) features of network monitoring solutions is alerting your company to a performance issue. At the basic level, a monitoring tool needs to deliver insights about a problem — what it is, where it's located, when it started, etc. Other capabilities to consider include tiered alerts that sort issues by how critical they are, and timed alerts to only allow alerts to come through during the hours when someone can respond to them.

How does pricing work for your network monitoring solution?

An obvious one, but also something that plenty of organizations overlook; a network monitoring solution's total cost is a major factor in selecting a solution. Many network monitoring vendors offer pricing tiers that allow for a certain number of monitored devices. You should, however, make sure that cost isn't the only consideration; while a solution's price may give you a good idea of how effective it is, it's not always a perfect indicator.

Does your network monitoring solution offer remote access?

This is a feature that should come included on all modern network monitoring solutions. If your office isn't centralized in one location, a web-based network performance monitoring and management solution is absolutely essential. When your network administrators and engineers can access their network monitoring tool remotely, they'll be able to discover, address, and potentially solve performance problems regardless of whether or not they're in the office.

How flexible and scalable is your network monitoring solution?

Networks are not a static infrastructure; they're rapidly changing as new devices connect to the network and businesses extend their reach. If your organization is expanding its network, a flexible and scalable network monitoring tool is essential. A scalable solution will allow your network monitoring tool to grow as your business does. With a flexible network monitoring tool, you can disable device monitoring on the network you don't need to look at.

Solution Provider Profiles

Solution Provider Profiles

ACCEDIAN

Accedian Skylight PVX (formerly Performance Vision) is a unified enterprise network and application performance management solution. The product combines network flow monitoring, real-time application transaction decoding, and end-user experience tracking to generate performance data. With Skylight PVX, users can monitor traffic from both physical or virtual environments (including the cloud) and analyze OSI Layer 2 through Layer 7 network traffic in real-time. Skylight PVX can be deployed in either a virtual or hardware-based appliance.

Accedian
2351 Blvd Alfred-Nobel
Montreal, Quebec
Canada
+1 (514) 331-6181
www.accedian.com

Key Features

Passive Traffic Capture Appliances

Skylight uses both physical and virtual traffic capture appliances to collect network flows and application transactions; all capture appliances are linked to a central datastore. Accedian also offers a packet broker that remotely captures network data and delivers it to the datastore for analysis.

Application Performance Metrics

For every application running over an enterprise network, Skylight will track transactions and calculate performance metrics. Skylight displays performance data for every application flow and allows users to refine their searches using multiple filters.

Skylight as a Service

Accedian offers its network monitoring capabilities as a SaaS deployment named Skylight as a Service. This subscription-based model bundles Skylight's wire data solution with a Skylight-certified partner's professional services to provide users with tools and troubleshooting expertise.

Bottom Line

Following its acquisition of Performance Vision in 2018, Accedian integrated end-user digital experience monitoring capabilities into Skylight. While the vendor provides network monitoring capabilities, Accedian focuses on providing a comprehensive solution to suit all business cases — which may not be desirable to those solely looking for insights on network performance. Some in-market buyers have also noted that Skylight is more expensive than other comparable products.

AppNeta Performance Manager is a network monitoring tool that allows IT teams to monitor end-user experience across their cloud, network, and applications. It operates on a four-dimensional approach to monitoring, with capabilities that work together to analyze usage and performance across networks and applications. AppNeta offers a wide range of graphics and reporting to deliver greater analytical capabilities as well. The vendor also provides monitoring solutions for VoIP, UCaaS, and DNS systems, as well as monitoring for cloud deployments.

AppNeta
285 Summer St
Boston, MA
United States
+1 (800) 508-5233
www.appneta.com

Key Features

TruPath Technology

The core of AppNeta's technology is TruPath, which provides real-time diagnostics and reports on details and performance issues. TruPath periodically sends data packets to monitor every path from one end of a network to the other.

Deep Packet Inspection

AppNeta uses deep packet inspection to go beyond NetFlow and discover insights on 100% of a company's network traffic. Their deep packet inspection engine recognizes over 2,000 applications and sends the analysis to AppNeta's cloud platform.

End-User Focus

AppNeta's tools are designed to measure performance from the perspective of the end-user. IT teams can monitor the end-user experience and determine the location of performance issues, allowing administrators to proactively deal with them.

Bottom Line

AppNeta's network monitoring module constantly checks for latency, data loss, and other characteristics across networks, hosted services, and web applications. Additional features, such as virtual network interfaces and automated discovery and diagnosis, may be of interest to prospective buyers. AppNeta places focus on end-user satisfaction, though analyst house Gartner, Inc. notes that end-user experience monitoring only extends to voice/video tests and synthetic transactions.

DX NetOps by CA Technologies, a Broadcom-owned company, is a network monitoring and analytics software that unifies traditional network and systems monitoring with full-stack analysis. The solution gathers intelligence on inventory, topology, device metrics, faults, flow, and packet analysis for traditional, software-defined, and cloud-based network architectures. DX NetOps is also augmented by Broadcom's AIOps platform, bringing NetOps and AIOps together to proactively solve network problems through automated remediation capabilities.

Broadcom
1320 Ridder Park Dr
San Jose, California
United States
+1 (408) 433-8000
www.broadcom.com

Key Features

Single-Pane Network Monitoring

DX NetOps can discover multiple types of networks, including SDx networks, LAN, WAN, data centers, cloud architectures, and service provider networks — and displays them in a single-pane dashboard that allows users to create contextual monitoring workflows.

Artificial Intelligence and Machine Learning

With AIOps integration, DX NetOps features numerous AI and ML capabilities, including automated anomaly detection, algorithmic noise reduction, and root cause analysis. The solution can also match key IT assets with associated services to create more intelligent correlation.

Application Experience

Broadcom focuses less on traditional network performance metrics and more on application experience, ensuring that a network can run complex business applications at any time. To this end, DX NetOps provides application-centric root cause topologies.

Bottom Line

In November 2018, Broadcom completed its acquisition of CA Technologies, bringing CA's portfolio (including its Network Operations Analytics platform) into the fold. CA has a long track record of success in the network monitoring marketplace even before the Broadcom deal. While DX NetOps can integrate with other Broadcom and CA solutions, Broadcom's offerings are still sold separately, making them less than ideal for those seeking unified monitoring.

Catchpoint Network Insights is monitoring suite that provides network engineers and operations teams with full visibility into the OSI stack from Layer 3 to Layer 7. Network Insights consists of four primary capabilities: DNS monitoring, traceroute monitoring, BGP monitoring, and endpoint monitoring. Each of these capabilities provides visibility into different components of the delivery chain, which enables proactive detection and triage of problems that arise within network layers — endpoint, enterprise LAN/WAN, DNS, CDN, ISP, and cloud.

Catchpoint
150 W 30th St
New York, NY
United States
+1 (514) 331-6181
www.catchpoint.com

Key Features

DNS Monitoring

Catchpoint offers two DNS monitors: DNS Direct tests, which query the name servers to provide availability data, and DNS Experience tests, which run recursive queries to measure latency, performance, and availability of the various DNS servers in the pathway.

Traceroute Monitoring

Synthetic monitoring visualizations help ensure network reliability by showing the network path, mesh, and cloud/multi-cloud/hybrid cloud data. By collecting data from every hop, network ops teams can detect issues and pinpoint the root cause.

Endpoint Monitoring

Catchpoint enterprise monitoring nodes can be placed within the firewall to detect network performance or reachability problems. Combined with a browser plug-in for end-user device telemetry, this provides end-to-end visibility of the app delivery chain.

Bottom Line

Catchpoint provides synthetic monitoring for networks and applications on a global scale. With a global network of testing locations, users can combine multiple levels of network telemetry with application performance data, RUM data, and last mile data to get a complete view in a single platform. While Catchpoint may not be the best choice for those looking strictly for a network monitoring solution, the vendor's monitoring suite provide comprehensive IT monitoring for unified operations.

Cisco Prime Performance Manager, a subset of Cisco Prime, is a network monitoring application that pulls actionable information from the entire network, including core, aggregation, and access networks. This product features a web-based interface, providing access to performance reports featuring flexible options and detail searching. Cisco Prime allows network administrators to keep track of all devices on the network as well. Prime sends alerts if the network is being bogged down and collects data on devices and connectivity on a user-defined schedule.

Cisco
170 West Tasman Dr
San Jose, CA
United States
+1 (800) 553-6387
www.cisco.com

Key Features

Scalability

Cisco Prime can detect any device on your network and dynamically adjust its reporting system to match your network's scale. Cisco provides scalability options to support businesses and infrastructures of any size.

Data Collection and Processing

Networks are constantly analyzed by Cisco Prime, allowing a steady production of performance data. The product can also gather data on any SNMP-enabled device using a standards-based data collection method, then generate reports on a user-determined schedule.

User-Defined Views

Cisco Prime Performance Manager provides users with the resources to customize views of their network. Users can switch between Cisco's default views and their own configured views to provide a better scope of the network.

Bottom Line

Cisco does not put a large emphasis on network monitoring over its other branches — Gartner notes that many users are unaware of their network performance monitoring services. However, because of its scalability, Cisco Prime Performance Manager can be used by organizations of any size. Performance Manager can integrate alongside other Cisco Prime offerings, so companies that use other Cisco Prime products already should take note.

dynatrace

Dynatrace is a monitoring solution provider that offers network monitoring, application performance management, and digital experience monitoring capabilities. Its network tools can be correlated with application performance metrics to deliver insights on how network performance is affecting end-user experience. Dynatrace offers visibility that allows IT teams to quickly identify the services and processes experiencing network connectivity issues. In addition to identifying bottlenecks, Dynatrace analytics can help businesses plan for network and server resources.

Dynatrace
1601 Trapelo Rd
Waltham, MA
United States
+1 (781) 530-1000
www.dynatrace.com

Key Features

Process-to-Process Network Communication Monitoring

Dynatrace monitors network communication on a process-to-process basis, rather than monitoring them at the host level. Its platform reveals the quality and performance of all network connections between processes, even across virtualized cloud and datacenters.

Application Analytics

Dynatrace analytics allows users to analyze the content of critical processes across application hosts so that any performance bottlenecks can be identified. The product also accounts for blind spots in your network to provide a clear user experience.

Integrated Health Monitoring

Digital performance monitoring keeps track of all application tiers, including server hosts and network health. The tool collates network performance metrics with server resource metrics to provide an integrated view of network and server health.

Bottom Line

Dynatrace provides end-user focused network monitoring, giving organizations the ability to easily detect problems before they spread. Its network monitoring capabilities are augmented by APM features, which provide code-level visibility and root cause insights. While some users have reported limited UI options and lackluster flexibility, the use of drill down options like PurePath allows network teams to quickly identify and provide initial problem analysis.

exoprise

Exoprise is a leading provider of SaaS and cloud monitoring with unmatched support for Office 365, Azure, Salesforce and more. Exoprise CloudReady is the platform for total digital experience management, providing users with end-to-end network and application visibility via real user monitoring or synthetic transaction monitoring. With Exoprise CloudReady, cloud and network administrators can find and fix problems fast, manage changes, observe trends, and improve performance and operations for the entire business.

Exoprise Systems Inc.
260 Bear Hill Rd
Waltham MA
United States
+1 (781) 209-5653
www.exoprise.com

Key Features

Every App, Every Protocol

CloudReady proactively monitors the health and performance of Office 365, including SharePoint Online, Exchange Online, Microsoft Teams, and Azure AD. The solution can be deployed instantly from any branch office or network location and monitor all cloud service applications.

Digital Experience Monitoring for SaaS

Monitor any SaaS application from the end-user's perspective via browser add-ons configured for the apps and domains the business relies on. Track network path performance, pinpoint gateway or proxy performance bottlenecks and detect ISP or cloud service outages.

Flexible Deployment Options

CloudReady features one-click deployment to AWS, Azure or GCP Points of Presence (POPs) or internally behind any MPLS, SD-WAN, or cloud-based proxy environment for telemetry and end-user experience collection. It also provides real-time alerting for Splunk, Service Now, Microsoft OMS and SCOM.

Bottom Line

Exoprise CloudReady provides visibility and deep insight into the digital experiences across SaaS services, network transformations and cloud/app migrations. The vendor has a focus on digital experience monitoring to help users deal with the effects of cloud and network transformations. CloudReady helps administrators ensure optimal end-user experiences across applications, networks and services, especially for applications that have shifted to the cloud.

ExtraHop Reveal(x) is a cloud-based network detection and response platform that gives organizations real-time visibility into their network from the inside out. With ExtraHop network monitoring tools, IT teams can maintain a comprehensive view of the entire ecosystem with auto-discovery and auto-classification. ExtraHop gives users the ability to mitigate performance issues immediately with continuous and real-time end-user monitoring. Empirical metrics across defendant systems can be employed to accelerate troubleshooting as well.

ExtraHop
520 Pike St
Seattle, WA
United States
+1 (877) 333-9872
www.extrahop.com

Key Features

Real-Time Analytics

ExtraHop Reveal(x) performs real-time analysis of your network, automatically discovering and classifying key events. Users can see every action that occurs on the network as they happen to rectify any issues or mistakes.

Network Visibility

ExtraHop is always searching for devices and traffic flow to create an automated inventory of your system. This means that users will be able to understand the full scope of their network all the time and determine problem areas as they arise.

Automated Investigation

When ExtraHop Reveal(x) detects a problem or a suspicious event, it automatically investigates further using threat intelligence and responds according to its findings. The results of the tool's analysis are delivered to users through the dashboard.

Bottom Line

ExtraHop Reveal(x) provides network-derived business intelligence data, giving IT operations users the ability to get closer to the lines of business with greatly improved application visibility. Customers have noted that Reveal(x) is more difficult to navigate than other comparable products. However, because ExtraHop relies extensively on machine learning to provide analytics and reporting, it is a flexible tool that can cover a wide variety of network performance issues.

Flowmon

Flowmon is a network visibility vendor that offers a flow-based network monitoring product. Its solutions provide IT teams with an array of tools for network visibility and control, as well as cloud operations, security operations, and DDoS protection. Flowmon probes and collectors help organizations gather, analyze, and store critical network information as well. The solution features a number of modules that can extend and streamline the functionality of the Connector and Probes to allow for more advanced analysis of flow statistics.

Flowmon
Sochorova 3232/34
616 00 Brno
Czech Republic, Europe
+420 530 510 600
www.flowmon.com/en

Key Features

Network Behavior Analysis

Flowmon's network performance monitoring solution gives IT teams full visibility into network and application behavior. With behavior analytics, Flowmon helps to eliminate suspicious activities, attacks, and advanced threats.

Probes and Collectors

Flowmon Probes provide network traffic monitoring and analysis to determine any issues in network communication. Flowmon Collectors receive traffic data and provide constant visibility into every corner of the network.

Netflow Connector

The Flowmon network connector provides administrators and security engineers with a full understanding of everything happening on the network. The connector gives users control over bandwidth utilization, network optimization and performance.

Bottom Line

Flowmon is a highly scalable network monitoring solution with competitive pricing. The product is noted for its ease of deployment, giving network managers and administrators the ability to set up the solution quickly and with no extra skills. While some users reported confusion with the tool's UI and search functionality, Flowmon offers monitoring and visibility solutions for an array of personas and levels of business.

Hewlett Packard
Enterprise

Hewlett Packard Enterprise's network monitoring suite is comprised of Aruba AirWave and HPE Intelligent Management Center. AirWave provides granular visibility for wired and wireless networks and is designed to detect mobile devices and applications in addition to traditional sensors. Intelligent Management Center manages data centers and core networks while providing clearly defined network data for IT teams. IMC features a modular platform with tools that cover traffic analysis, remote network management, and intelligent reporting.

Hewlett Packard
3000 Hanover St
Palo Alto, CA
United States
+1 (800) 607-3567
www.hpe.com

Key Features

Network Traffic Analyzer

Network Traffic Analyzer is an optional module for Intelligent Management Center that integrates Layer 4 through Layer 7 monitoring, using the instrumentation in network devices (like routers and switches) to provide reporting on network application usage.

Virtual Application Networking

When combined with the HPE FlexFabric 5940 or 5950 Switch, Virtual application Networking delivers real-time visibility on microburst network congestion, informing IT leaders of network performance issues that last for less than a second.

Branch Intelligent Management System

HPE's Branch Intelligent Management System remotely manages enterprise network infrastructure using the TR-069 protocol, managing a number of branch networking equipment through devices that are remotely deployed, configured, and serviced.

Bottom Line

Hewlett Packard Enterprise boasts a portfolio of complementary monitoring products featuring integration with other HPE tools. While HPE is popular with large organizations, it's still struggling to catch on with smaller companies; the vendor offers a "Basic" offering for networks with 50 devices or less, but it has fewer features. Aruba AirWave has been praised by customers that commonly utilize Wi-Fi networks as being a good fit for operations on that scale.

infovista

Infovista VistaInsight is a network monitoring and service assurance solution that gives users full visibility over their network activity. The product supports digital transformation initiatives by simplifying hybrid NFV network operations and monitoring SD-WAN edge performance. Infovista diagnoses network and service performance and delivers insights to administrators through a scalable, open, cloud-ready platform. InfoVista's tools (including VistaInsight) support cloud and SSL-based applications, VXLAN, and several other features.

Infovista
20405 Exchange St
Ashburn, VA
United States
+1 (855) 323-5757
www.infovista.com

Key Features

On-Demand Enterprise SLA Management

VistaInsight helps customers ensure that their service level agreements (SLAs) are being met through automated customer SLA reporting, proactive service management, and service performance visibility in both ethernet and SD-WAN networks.

Accelerated Hybrid NFV Deployment

Through VistaInsight, users can reduce the time of NFV onboarding, design, testing, and operations by managing multi-vendor VNF performance, VNF capacity optimization, and service modeling through a single service assurance solution.

Multi-Vendor SD-WAN Performance Monitoring

VistaInsight allows users to correlate SD-WAN overlay performance with the performance of the underlaying infrastructure by monitoring at each site and assuring that your end-to-end SD-WAN network and services will honor enterprise SLAs.

Bottom Line

InfoVista's network monitoring solutions are highly scalable and provide visibility and performance analytics quickly. A subset of users reports a longer-than-normal implementation process and recommend that the product be integrated as part of an ecosystem of other tools. However, VistaInsight is a powerful product and looks to be a good fit for organizations that are looking to enhance their network monitoring infrastructure.

kentik

Kentik is a network monitoring and AIOps solution that provides full network visibility. The solution combines a NetFlow network monitoring with tools for ingesting data like VPC Flow Logs, business context, and application context. Kentik's machine-learning driven solution advises on network and security performance, troubleshooting, planning, and cost management as well. On one screen, Kentik provides visibility and insights wherever your traffic flows, from your network to applications, to the internet, to the cloud in real-time.

Kentik
625 Second St
San Francisco, CA
United States
+1 (844) 356-3278
www.kentik.com

Key Features

Full Multi-Network Visibility

Kentik provides insights about your traffic as it flows through the network, internet, hybrid/multi-cloud, and edge. You can recognize issues and their impact on performance and customer experience in customizable dashboards.

Leverage Network Data with Business Data

Kentik captures a view of your network traffic data and enriches it with critical business data, allowing every network event or analysis to be tied to business information — revenue and costs, customer and user experience, performance and risk.

Open APIs

With Kentik, enterprises can facilitate SaaS delivery with open APIs. No additional hardware, development, or maintenance is required, and the product can integrate with your management stack. If preferred, on-prem solutions are also available.

Bottom Line

Kentik unifies network operations, performance, security, and business intelligence. It digests traffic flow wherever it travels, enriches it with business data and provides insights via dashboards. Its AIOps capabilities ensures that all insights are intelligent and actionable. Some users have noted that implementation and fine tuning of the solution is difficult, but Kentik has also been described as one of the better cloud-based NetFlow analysis tools right now.

LiveAction LiveNX is a network performance and analytics platform that eases network monitoring and configuration. The LiveNX interface allows for thorough insight into a network's topology with in-depth views of devices, interfaces, and network flows. Apart from visualization, LiveNX gives IT teams the ability to access performance metrics and take the appropriate action to address issues. LiveNX comes with User Experience, Insight, and Endpoint Agent, features that enable users to analyze connectivity, detect network patterns, and monitor endpoints.

LiveAction
3500 West Bayshore Rd
Palo Alto, CA
United States
+1 (888) 881-1116
www.liveaction.com

Key Features

Network Capacity Planning and Baselining

LiveAction LiveNX utilizes NetFlow, QoS, and IP service level agreements to help with capacity planning and performance baselining. Users can also generate synthetic network traffic with LiveNX to perform pre-deployment assessments.

LiveNX Insight

LiveNX Insight is a machine learning-based module for LiveNX that continuously identifies patterns and insight from customer metadata, providing users with "human-in-the-loop" interaction and enabling users to train the system on important performance knowledge.

Bandwidth Management

LiveNX enables multi-site organizations to measure current bandwidth usage, reduce bandwidth costs, and proactively predict capacity needs. Enterprise network administrators are able to effectively manage bandwidth usage and plan for growth as well.

Bottom Line

LiveAction LiveNX features unique SD-WAN traffic steering capabilities paired with overlay views of control plane and network flow data. The tool offers impressive visualization of network topologies, helping with troubleshooting and problem diagnosis and allowing users to easily interpret network issues. Because LiveAction's resources are heavily focused on North America, businesses in other regions should check to ensure they'll be supported.

LogicMonitor is an agentless SaaS-based network monitoring solution that gives organizations the ability to discover all network devices and interfaces. Through alerts and interface metrics, users are given greater visibility into error rates, network usage, and throughput. With support for a variety of different technologies, IT teams can collect and analyze network performance data from all of their networking gear. In addition to switches, routers, and firewalls, LogicMonitor can also cover cloud and hybrid IT environments.

LogicMonitor
820 State St
Santa Barbara
United States
+1 (805) 617-3884
www.logicmonitor.com

Key Features

Full Data Center Visibility

LogicMonitor has a library of over 1000 pre-built monitoring templates that provide automated discover, monitoring, and alerting for several apps and deployments, include AIX, VMware, and Tomcat.

Website Performance

LogicMonitor automatically conducts availability tests for websites on a worldwide basis, analyzing performance from multiple locations around the globe. The solution lets you know if any areas of the world are having trouble connecting to your site.

Flexible Alerting

The LogicMonitor platform features alerts that are preconfigured with thresholds set using best practices to get monitoring up and running quickly; thresholds can be easily tuned on a global, group, or object level.

Bottom Line

LogicMonitor is an enterprise-grade network monitoring solution with a flexible web portal. The product includes custom dashboards, configurable alerts, and customizable network reports. Due to the extensive customization options, this solution provides complex network monitoring services to its customers. Users report being impressed with LogicMonitor's visibility capabilities and scale, though some have also reported slow feature updates and challenges in adopting the service.

LogRhythm NetworkXDR is a network security solution that detects network-borne threats in real-time and features SOAR capabilities. It offers ease of use without requiring sophisticated network forensics expertise. Using purposed, versatile sensors that generate advanced network details, LogRhythm NetworkXDR incorporates multiple machine analytics approaches to expose evolving threats more effectively. The result is full coverage against threats, both known and unknown, without requiring heavy tuning or lengthy supervised machine learning training periods.

LogRhythm
4780 Pearl East Circle
Boulder, CO
United States
+1 (866) 384-0713
www.logrhythm.com/ndr

Key Features

Threat Detection

LogRhythm NetworkXDR recognizes thousands of applications at Layer 7 with advanced analytics and customizable dashboards for threat hunting, corroborating high-risk network activities at the network and application level to minimize false positives.

Network Forensics

To gain insight into your network, LogRhythm NetworkXDR searches rich Layer 2 through Layer 7 network traffic metadata with full, selective intelligent packet capture for the times when you need complete detail.

SOAR Capabilities

LogRhythm NDR provides guided, customizable playbooks for tracking, documenting, and enforcing defined workflows, alongside case management for end-to-end collaboration and management of alerts, evidence, and escalations.

Bottom Line

LogRhythm's network detection and response (NDR) solution goes beyond the limits of network traffic analysis. Combined with LogRhythm NetMon, your enterprise can detect, analyze, and respond to threats with advanced security analytics, centralized search and visualizations, and security orchestration, automation, and response (SOAR) technology. While LogRhythm offers a separate network monitoring product, its main focus is on network security tools like NDR.

ManageEngine OpManager Plus is an integrated monitoring tool that allows for full visibility into networks, applications, and infrastructure. OpManager is written in Java and uses a local installation of Tomcat for its interface. A local database stores collected information and provides a communication path between the OpManager and plug-ins. The OpManager Applications Manager plug-in brings in supported commercial applications including databases from IBM, Microsoft, and Oracle, as well as other open-source products.

ManageEngine
4141 Hacienda Dr
Pleasanton, CA
United States
+1 (925) 924-9500
www.manageengine.com

Key Features

Network Monitoring

OpManager Plus monitors the health of all a user's network devices in real-time through various protocols. The solution monitors critical network metrics (including packet loss, errors, and discards) and the health of device hardware as well.

Server Monitoring

ManageEngine allows users to monitor the status, availability, health, and performance of physical and virtual servers. This enables you to examine CPU, memory, and disk utilization. The product can also observe exchange servers, application servers, and Active Directory.

Network Configuration Management

With automated device backup changes and detailed information on all network configurations, OpManager Plus provides network configuration management capabilities with support for multiple hardware vendors and real-time configuration change tracking.

Bottom Line

ManageEngine's OpManager provides an impressive selection of network monitoring tools for IT generalists and specialists alike, including application performance management, network monitoring, and infrastructure management. Users report simple integration and configuration as well. However, there are several missing features which are present in similar solutions, most notably for clipped management.

NETSCOUT™

NETSCOUT nGeniusONE is a network monitoring and service assurance platform that offers full visibility into infrastructure, interdependencies, and applications. The tool utilizes adaptive service intelligence technology to allow for continuous monitoring and analysis of network traffic data. NETSCOUT combines network and application performance management to provide macro-level insights into performance, allowing for the identification of capacities and network shortfalls. NETSCOUT's customers are largely enterprise organizations.

NETSCOUT
310 Littleton Rd
Westford, MA
United States
+1 (888) 357-7667
www.netscout.com

Key Features

Continual Performance Monitoring

With its topology and health diagnostics features, NETSCOUT nGeniusONE continuously baselines current traffic patterns and application response times to ensure the user's network performance is maintained throughout digital transformation projects.

Testing and Analytics

nGeniusONE users can test wired and wireless network performance to stay ahead of performance problems pre-and-post-deployment. NETSCOUT can analyze wire-traffic, NetFlow and MIB2 data in the same solution.

Packet Analysis

NETSCOUT presents packet-level analysis to users and administrators based on workflow context. nGeniusONE also provides a collection of forensic evidence relevant to the findings it gives you.

Bottom Line

nGeniusONE provides (and is especially suited for) packet-level analysis and generating network monitoring reports. The product also includes a universal monitor that features clear insight into your network's performance. Some buyers have expressed concern with the cost of this product, and ease of use is not a strength of the offering. However, NETSCOUT remains an interesting option for organizations that don't require real-time network performance evaluation.

Monitis is a web-based network monitoring tool that allows businesses to take control of their IT system no matter their location. With this monitoring solution, all server, sites, networks, and applications can be accessed through one simple dashboard interface. Monitis provides users with alerts and reports 24/7 through emails, SMS, calls, and mobile applications, even when the network is down. Customers don't need to download or install any software as the entire platform can be run through the Monitis portal via supported web browsers.

Monitis
5741 Rio Vista Dr
Largo, FL
United States
+1 (800) 920-4963
www.monitis.com

Key Features

Network Monitoring

Monitis' web-based network monitoring solution provides users with agent-based and agentless monitoring for network devices. It also features network bandwidth monitoring, SNMP devices, TCP protocols, and WAN link capabilities.

Website Monitoring

Monitis focuses on the end-user experience with a combination of website uptime monitoring, full-page load, synthetic transaction monitoring, and web stress testing. The product simulates an end-user's interactions with your company's websites as well.

Server Monitoring

Users can protect the center of their IT service with Monitis' Agent-based Server and Device Monitoring. The feature is available for Windows and Linux; providing monitoring for CPU, memory, disk, network, bandwidth, TCP and more.

Bottom Line

Monitis monitors networks, the cloud, applications, and servers. The product also supports custom functionality through a modifiable API, allowing administrators with unique monitoring needs to set up monitoring for any device or app they desire. Since the service is completely web-based, downtime on the company's part will impact your monitoring of local resources. However, its pricing options are attractive to organizations that want to ensure the tool can scale with their needs.

OPMANTEK
Network Management and IT Audit Software

Opmantek NMIS Professional is an intelligent network management and infrastructure monitoring tool. It serves as the enterprise version of Opmantek's suite of open source network management solutions. In addition to its core product, Opmantek offers a number of commercial add-on modules, managed service provider solutions, and customizable support and assistance packages. The NMIS Professional edition contains the vendor's Network Management Information System for network monitoring as well as charting (opCharts) and reporting (opReports) tools.

Opmantek
156 2nd St
San Francisco, CA
United States
+1 (415) 315-9859
www.opmantek.com

Key Features

Network Management Information System

Network Management Information System is a scalable, flexible network management solution that classifies events based on business impact. The tool can be augmented with several modules that Opmantek offers.

opCharts

opCharts allows users to create, customize, and manage geographic, network, and topological maps. The solution features interactive dashboards, detailed graphs, business service monitoring, and nested maps to help administrators see actionable insights into their network.

opReports

opReports, automates the creation and distribution of operational and executive-level reports, letting users set custom rules and conditions for the solution to examine and analyze NMIS data for its potential business impact.

Bottom Line

Opmantek NMIS helps organizations detect faults, review current and historical network performance, and predict where future failures are likely to occur. The solution supports two open-source products, NMIS and Open-AudIT, as well. It also features a suite of commercial tools that bring additional features and capabilities to the software. Opmantek is node-based, so engineers who are used to analyzing network performance from a data standpoint will need to adjust accordingly.

PAESSLER PRTG NETWORK MONITOR

Paessler PRTG Network Monitor is a network monitoring solution that allows administrators to stay ahead of IT infrastructure issues. The product primarily offers fault and flow analysis and packet sniffing, though other services like cloud, database, and bandwidth monitoring are also supported. The company touts and continues to release a consistent stream of vendor-agnostic network monitoring sensors as well. Paessler also includes unified monitoring via a powerful dashboard that gives network administrators complete visibility of their entire IT suite.

Paessler
Thurn-und-Taxis-Str. 14
Nuremburg
Germany
+49 911 93775-0
www.paessler.com

Key Features

Full Network Monitoring

Paessler PRTG monitors networks using a range of technologies to assure the availability of network components and measure traffic and usage. Its web interface is based on AJAX, and features high security standards and responsive design.

Bandwidth Monitoring

Paessler connects network monitoring and network mapping by displaying all network devices and all properties at a glance in a unified network map, creating interactive maps of your network and alerting you to problems before they occur.

Network Mapping

Paessler connects network monitoring and network mapping by displaying all network devices and all properties at a glance in a unified network map, creating interactive maps of your network and alerting you to problems before they occur.

Bottom Line

With Paessler's rapid development stream, sensors are updated and released on a monthly basis. This vendor primarily markets to mid-sized enterprises and small to medium-sized businesses. While PRTG is capable of examining servers, options for monitoring them are more limited. PRTG's view can be customized to provide different views for each team member depending on their needs as well. Paessler also offers PRTG as a hosted solution, which may appeal to some organizations.

Plixer

Plixer Scrutinizer is a network monitoring and network traffic analysis system that gathers network flow data and metadata from every network conversation. Scrutinizer works as a network forensics and security tool as well. The product alerts network teams about traffic patterns, offers DNS integration, and provides full visibility into network information that typically stays hidden. Scrutinizer also allows administrators to peer deep into their network to see where threats are originating and how the network is being used.

Plixer
68 Main St
Kennebunk, ME
United States
+1 (207) 324-8805
www.plixer.com

Key Features

Enriching Data Context

Plixer correlates network data with metadata from various network locations to provide better context for network events. The tool features integrations with companies like Cisco, Palo Alto Networks, and VMware as well.

Visibility Across Environments

Plixer promotes visibility across physical and virtual network environments, ensuring that network teams don't lose any traffic visibility. Through partner integrations with VMware operating systems, Scrutinizer can deploy details on virtual appliances.

Scalable Data Collection

Plixer's network monitoring solution can scale to millions of flows per second through its hierarchical deployments. The company offers three different pricing plans for Scrutinizer, with its free solution collecting up to 10,000 flows per second.

Bottom Line

Scrutinizer is vendor agnostic and handles flows like sFlow, Netflow, JFlow, and IPFIX. The solution is scalable, with easy integration for existing network environments. Plixer was designed primarily for large enterprises, so proper scaling for smaller companies might be a bit less reliable. Nonetheless, Scrutinizer features notable partner integrations with other network monitoring vendors, network hardware providers, and applications as well.

PICO

Corvil Anayltics, a Pico product, is a network monitoring and analysis suite designed for financial institutions. Analytics is one of three main offerings that Corvil provides, the others being Corvil Center (for collecting and timestamping data) and Corvil Intelligence Hub (for applying machine learning and intelligent anomaly detection). The provider currently offers over 500 different plug-ins for analytics that are bundled into solution packs; each plug-in helps financial businesses decipher information from specific network protocols and applications.

Pico
32 Old Slip
New York, NY
United States
+1 (646) 362 4420
www.pico.net

Key Features

Packet Capture and Exporting

With Corvil Analytics, users can analyze raw packet data from their network and discover real-time insights. The solution allows network managers to instantly capture and store packets. These packets can also be exported and retrieved across your network.

Analytics Plug-Ins

Corvil offers a large number of Analytics plug-ins that are bundled into solution packs, which are compiled to fit the needs of specific industries and use cases. Packs include Electronic Trading, Market Data, and Enterprise & Security.

Network Capture

Corvil Network Capture is a service offered through Corvil Classic that ensures complete and reliable packet capture for trading networks. The service utilizes packet capture to prevent loss through sudden large or extended traffic bursts.

Bottom Line

Corvil Analytics reports granular behavior of network traffic, right down to individual packets and transactions, providing a more comprehensive overview of the network. Corvil was acquired by financial technology vendor Pico in 2019; the tool's focus appears to now be predominantly on finance use cases. While this will not appeal to other businesses, it makes Corvil an excellent consideration for financial institutions looking to improve business performance and security.

Progress WhatsUp Gold is a comprehensive monitoring software suite that covers infrastructure monitoring, application performance management, and network monitoring. WhatsUp constantly checks for network uptime and downtime, predicting connectivity problems before they happen. With WhatsUp, users can ensure that product installation and deployment is as quick and easy as possible. Progress offers both a web-based user interface and a traditional Windows application for managing different aspects of the program.

Progress
14 Oak Park Rd
Bedford, MA
United Sattes
+1 (781) 280-4000
www.progress.com

Key Features

Distributed Monitoring

WhatsUp Gold's network monitoring capabilities can be extended to multiple remote networks, allowing for a central installation. The tool also allows several remote installations to be monitored from the same centralized dashboard.

Cloud Monitoring

Progress Cloud Monitoring dashboards allow users to track resource usage and billing of their cloud environments, providing cost-justification to management. The solution automatically discovers, maps, and monitors cloud deployments, including for AWS and Azure.

Configuration Management

WhatsUp streamlines the configuration of backup, archiving and restoration. Users are alerted to any changes to network device configurations and receive compliance reporting from out-of-the-box templates and automated policy enforcement as well.

Bottom Line

With a breadth of network monitoring functionality (APM, NPM, and infrastructure management) wrapped up in one piece of software, small and medium-sized businesses should take note of this product. While the vendor's monitoring bundle manages to compete with a number of the other comparable products in the space, Progress may not provide as much specialization. Progress offers excellent customer service and support guidance for VMware virtual machines, however.

riverbed

Riverbed SteelCentral is a network monitoring and application performance monitoring tool that offers full network visibility, analytics, troubleshooting, and user monitoring. The solution is divided into two platforms based on company size. Riverbed also provides its customers with four distinct levels of support based on how quickly they need replacement equipment shipped in the event of a network failure. Riverbed's network performance management acts as a repository for its complete suite of related products.

Riverbed
680 Folsom St
San Francisco, CA
United States
+1 (877) 483-7233
www.riverbed.com

Key Features

AppResponse

SteelCentral AppResponse offers continuous full packet capture for on-prem, virtual, and cloud environments, with analysis modules for network forensics, application, web transaction, unified communications, and database analysis.

NetProfiler

SteelCentral NetProfiler provides flow-based analysis for monitoring the global health of enterprise hybrid networks. Riverbed also offers an Advanced Security Module for flow-based network security analytics for cyberthreat hunting and DDoS detection.

UCExpert

SteelCentral UCExpert is Riverbed's solution for managing multivendor unified communications from Cisco, Microsoft Skype for Business, and Avaya. UCExpert includes configuration management, proactive testing, and performance monitoring capabilities.

Bottom Line

Riverbed SteelCentral provides high visibility across a network, no matter how large it is. Users have noted the particularly strong APM capabilities included, so developers will gain the added bonus of being able to examine the performance of their applications as they see fit. While users that act strictly on the operational level may find the solution's system unfit for their architecture, companies that develop applications would be wise to consider Riverbed.

SevOne

The SevOne Data Platform is a network monitoring and analytics solution. The product provides a collection of comprehensive network performance metrics. SevOne is best suited for infrastructure monitoring and flow and log monitoring. The tool supports live network maps, infrastructure orchestration, SD-WAN, hybrid cloud, and carrier network virtualization solutions as well. SevOne's Data Insight allows for customizable visualizations and reports on a network's performance, alongside flexible workflows that allow for configurable delivery.

SevOne
800 Boylston St
Boston, MA 02199
United States
+1 (888) 970-0567
www.sevone.com

Key Features

Monitoring Collection

SevOne works on a collection of network performance metrics and flow data. The solution supports over 10,000 different network devices, with support for new SNMP devices coming within 10 business days.

Modern Visualization and Analytics

SevOne allows users to create scalable, reusable, and sharable visualizations and workflows. The solution can isolate specific user and tenant visualizations with a series of multitenant administrative and reporting features as well.

Unified Dashboard

SevOne maintains a year's worth of data for highly granular historical performance views. Through its report wizard, users can select which resources, settings, time frames, visualizations, and summary information they need to see in the dashboard.

Bottom Line

SevOne's cluster architecture allows for monitoring to handle the high volume and variety of data found in many networks. While the company primarily markets itself to large enterprises and the service provider market, smaller organizations are still likely to find some features that will catch their interest. Though some users wish that its documentation and user guides were better, SevOne is noted for its ability to handle performance monitoring data with ease.

SolarWinds Network Performance Monitor is a network monitoring solution that, alongside its other network products, provides a wide range of performance analytics and management capabilities. With the SolarWinds solution portfolio, users can identify dead zones and improve their wireless network coverage. Its products can also generate out-of-the-box wireless reports for wireless availability and rogue access points. SolarWinds offers all of its services individually, but also provides bundles for companies looking to integrate a wider solution base.

Solarwinds
7171 Southwest Pkwy
Austin, Texas
United States
+1 (866) 530-8100
www.solarwinds.com

Key Features

Network Availability Monitoring

SolarWinds analyzes network availability, fault, and network performance issues. This helps to ensure that users reduce network downtime and quickly resolve network connectivity issues.

Network Path Analysis

SolarWinds offers full network path analysis features through NetPath, which provides visual analysis and problem solving for hybrid IT. The solution delivers hop-by-hop analysis along critical network paths for on-premise, cloud, and hybrid environments.

Intelligent Network Alerting

Users can reduce the flood of unnecessary network alerts by creating alerts based on simple or complex nested trigger conditions, defined parent/child dependencies, and network topology.

Bottom Line

SolarWinds has achieved significant name recognition over the years. Its network monitoring suite is scalable and customizable, which is ideal for organizations with constantly changing needs. SolarWinds offers a basic packet monitoring solution through its QoE agents, though the feature doesn't appear to be known among its customer base and hasn't seen significant investment. SolarWinds' topology mapping and configuration management features are top-notch.

Statseeker

Statseeker offers a network monitoring product that monitors every physical, virtual, and logical interface across an organization. The product features quick and simple deployment and can scale horizontally and vertically. Statseeker touts three distinct licensing options based on budget, user persona, and required functionality. Statseeker scales from 10,000 to 1,000,000 interfaces on a single server with minimal requirements. Based in Carlsbad, California, Statseeker was acquired by Techniche in January of 2019.

Statseeker
5857 Owens Ave
Carlsbad, CA
United States
+1 (844) 782-8757
www.statseeker.com

Key Features

Network Visibility and Coverage

Statseeker uses SNMP discovery to locate devices, interfaces, and other SNMP-enabled components. Users can direct the discovery process toward specific devices that they want the software to generate reports for.

Anomaly Detection

Statseeker provides anomaly detection by comparing current network data to historical patterns. This highlights variance from normal behaviors and provides an early warning system to alert users to potential problems before they become an issue.

Analytics and Forecasting

Statseeker delivers actionable insights into a user's network behavior using granular 60-second polling data. This establishes an initial baseline within two weeks that becomes more accurate over time.

Bottom Line

Statseeker is recommended for businesses looking to upgrade or renew their maintenance contract for an existing network or do a full cost and capabilities check-up. The company's support teams are quick to respond to questions or problems, and deployment has been cited by reference customers as easy. Though some users report lag time on feature updates and product enhancements, Statseeker's network monitoring portfolio provides a solution suite for organizations of any size.

ThousandEyes Network Intelligence is a cloud-based network monitoring solution that allows IT teams to diagnose performance issues with both network infrastructure and applications. ThousandEyes is able to identify network problems across an organization by collecting topology information and using it to depict the paths taken by network traffic from the source to the destination. The product uses agents to generate synthetic traffic that is used to probe network patterns and flows. ThousandEyes has raised more than $110 million in funding since its founding in 2010.

ThousandEyes
201 Mission St
San Francisco, CA
United States
+1 (800) 757-1353
www.thousandeyes.com

Key Features

Network Data

ThousandEyes users can capture unique insights across every portion of the network via smart agents. Smart agents are located across the internet and inside the enterprise, and collect detailed forensiv data of network topologies, dependencies, and behavior.

Visual Analytics

Administrators can rapidly analyze performance with purpose-built visualizations across multiple layers of network data. The solution's network intelligence analysis helps diagnose diverse infrastructure, service, and app issues.

Shared Intelligence

ThousandEyes' Shared Intelligence lets users share knowledge on network issues with internal teams, vendors or clients to foster collaborative problem resolution. They can also integrate data and insights directly into existing workflows and systems.

Bottom Line

ThousandEyes offers a clean and easy-to-use interface and features network insights using a clear visual approach. Though their end-user experience monitoring capabilities are weaker than other services since ThousandEyes, users can deploy their own sensors, giving them more control over their network. Cisco announced its intention to acquire ThousandEyes and adopt the vendor into its networking portfolio in May 2020; it remains unclear how this will affect ThousandEyes' operations.

The VIAVI Solutions Observer platform, comprised of Apex, GigaStor, and GigaFlow, delivers network visibility to NetOps and SecOps teams to help manage daily IT operations, mitigate risks, and solve performance and security issues. VIAVI is a veteran network monitoring vendor, delivering wire data capture with its GigaStor appliance. Recently, VIAVI also has added flow-based analysis with its GigaFlow solution to help organizations gain insights into network infrastructure devices and corresponding IP addresses, MAC addresses, and usernames.

Viavi
6001 America Center Dri
San Jose, CA
United States
+1 (844) 923-1781
www.viavisolutions.com

Key Features

End-User Experience Scoring

VIAVI delivers an end-user experience scoring model that identifies issues with scope and impact context, isolating the problem domain. Users can drill down from dashboards to complete wire data transactions, reducing mean-time-to-resolution (MTTR).

Enriched-Flow Records

VIAVI stitches together enriched-flow records that aggregate flow, SNMP, user identity and session syslogs. These insights yield let a customer drill into network device types, IP to MAC to User relationships, interface information, and usage patterns.

Third-Party Validated Wire Data Capture

VIAVI's third-party validated wire data capture delivers stream-to-disk speeds and metadata production to give an organization complete packet forensic visibility into their network activity. This provides companies with essential data for analyzing network security incidents.

Bottom Line

By combining wire data and flow-based analysis with its Observer platform, VIAVI offers SecOps and NetOps teams with comprehensive visibility into their network. VIAVI provides the customer with an end-user experience score with the ability to deep dive into any issues to the network conversation level. To get the full effect of VIAVI's tools, it is recommended that you implement them all at once; companies only looking to integrate one or two may not be satisfied.

ZABBIX

Zabbix is an open source network performance monitoring solution available as a software and virtual appliance download. Zabbix is designed to be scaled from small business environments to large enterprises with ease. This scalability is made possible through intelligent algorithms that take advantage of modern hardware and software modularity. Zabbix is optimized for high performance monitoring of operating system and application-specific metrics. Zabbix also offers server, cloud, application, and services monitoring.

Zabbix
Dzelzavas 117
Riga, LV-1021, Latvia
+371 67 784 742
www.zabbix.com

Key Features

Configuration Changes

Zabbix observes every configuration change (including added or removed devices, upgraded firmware, and changes in device serial number) to ensure network configurations aren't adversely impacting the network.

Network Health

Zabbix's network health monitoring alerts you when a link is down, system status is in a critical state, device temperature is too high or low, power supply is running low, or there isn't enough disk space.

Web Monitoring

Users can monitor the availability and performance of web-based services over time. This function enables Zabbix to log into a web application periodically and run through a series of typical steps being performed by a user.

Bottom Line

Zabbix web monitoring lets organizations audit the availability and performance of web-based services. One common complaint about Zabbix is that it lacks real-time tests, as well as complex templates and alerting rules. Because Zabbix's tools are open source, users with technical knowledge can fit Zabbix's capabilities to suit all their needs. While this will require training, it also allows user access to the Zabbix community of developers and support team members.

ABOUT SOLUTIONS REVIEW

Solutions Review is a collection of technology news sites that aggregates, curates and creates the best content within leading technology categories. Solutions Review mission is connect buyers of enterprise technology with the best solution sellers.

Over the past three years, Solutions Review has launched ten tech Buyer's Guide sites in categories ranging from Cybersecurity to Wireless 802.11ac as well as Mobility Management and Business Intelligence, Data Analytics, Data Integration and Cloud Platforms.

Information for this report was gathered via a meta-analysis of available online materials and reports, conversations with vendor representatives, and examinations of product demonstrations and free trials. Solutions Review does not endorse any vendor, product or service depicted in this publication and does not advise technology users to base their vendor selection entirely on this research. Solutions Review disclaims all warranties, expressed or implied, regarding this research, including any warranties of merchantability or fitness for a particular purpose.