Network Security Monitoring Tools

1. **SolarWinds Network Performance Monitor (NPM)**

Function: This robust and reasonably priced network monitoring software helps you to promptly identify, assess, and fix issues with network performance and disruptions.

Use Case: accelerates troubleshooting and lowers downtime while raising service levels. sophisticated network troubleshooting using critical path hop-by-hop analysis for cloud, hybrid, and on-premises services.

Open Source/ Paid: Paid

Pros	Cons
● Custom reports building. ● Alert management with conditions constructor. ● A huge variety of data sources.	● Web console requests cashing works quite slow ● Network elements virtualization and clustering monitoring do not satisfy the contemporary requirements (has to be more functional and provide a wider list of vendors). ● WiFi heatmap is available for Cisco Meraki equipment only.

2. **Auvik**

Function: It captures and manages device configurations, monitors network performance, notifies you of potential network issues, and updates network maps and documentation in real-time.

Use Case: This cloud-based solution for network management and monitoring is vendor-neutral and offers automated network discovery. Both new and current users

can receive onboarding and training from it, and it doesn't require any service hardware or interruptive maintenance cycles.

Open Source/ Paid: Paid

Pros	Cons
● Efficiency ● Reduced Risk ● Configuration Backup ● Lower cost ● Greater Security	● Steep learning curve ● Initial cost

3. Datadog Network Performance Monitoring

Function: It gives you access to information about network traffic flowing through availability zones, containers, services, and any other tag in Datadog. Once NPM is enabled, you can set up an NPM monitor to receive alerts whenever a TCP network metric exceeds a predetermined threshold.

Use Case: With the help of Datadog NPM, you can identify unforeseen or latent service dependencies by seeing your network traffic between services, containers, availability zones, and any other tag in Datadog.

Open Source/ Paid: Open Source

Pros	Cons
● Comprehensive monitoring across systems ● Real-time data views ● Wide integration with other tools ● User-friendly interface ● Effective alerting and	● Can be expensive, especially for large deployments ● Setup can be challenging in complex environments ● Data storage and retention limitations

troubleshooting	• Some customization difficulties

4. Paessler PRTG Network Monitor

Function: PRTG is a unified monitoring tool that can monitor almost any object that has an IP address. It is composed of one or more probes and the PRTG core server: Configuration, data management, PRTG web server, and other tasks are handled by the PRTG core server. Through the use of sensors, probes gather data and keep an eye on device operations.

Use Case: PRTG is used primarily in the infrastructure domain to monitor various IT technologies. There are numerous important applications: Monitoring of devices (power, servers, telephony, security, and network)

Open Source/ Paid: Paid

Pros	Cons
• Intuitive Interface • Out-of-the-box monitoring • Automatic Device Discovery	• Steep Learning Curve • Expensive Pricing Structure

5. ManageEngine OpManager

Function: OpManager uses the SNMP and CLI protocols to monitor network devices, including wireless access points, firewalls, load balancers, routers, switches, and more. Performance indicators like CPU, memory, interface traffic, errors and discards, packet loss, response time, and so on are tracked by it.

Use Case: This software monitors networks, servers, and virtualizations, aiding SMEs, large enterprises, and service providers in managing data centers and IT infrastructure efficiently and cost-effectively. It features automated workflows, intelligent alerting engines, configurable discovery rules, and extendable templates. IT teams can set up a 24x7 monitoring system within hours of installation.

Open Source/ Paid: Open Source

Pros	Cons
● Easy to use Interface ● Cost-effectiveness ● Comprehensive Network Visibility	● Challenges with Configuration ● Lack of notifications for updates ● Integration Limitations

6. Checkmk

Function: It can monitor servers in cloud environments, virtualized servers, hypervisors, and all known operating systems. It also offers agents for these platforms.

Use Case: Servers, Networks, Applications, Databases, Cloud, Containers, Storage, IoT Monitoring, Docker, SNMP Monitoring, Open Source Monitoring, CPU Monitoring

Open Source/ Paid: Open Source

Pros	Cons
● Customization options ● Distributed monitoring approach ● User-Friendly Interface	● Lack of Stability and Quality Assurance ● Need for Better Documentation

7. Nagios

Function: It is an event monitoring system that provides servers, switches, apps, and services with monitoring and alerting capabilities. Users receive alerts when something goes wrong and another alert once the issue has been fixed.

Use Case: Server Monitoring, Network Monitoring, Service Availability, Resource Utilization, Performance Metrics and Trend Analysis, Log File Monitoring, Alerting and Notification, Application Monitoring, Database Monitoring, Cloud Infrastructure Monitoring

Open Source/ Paid: Open Source

Pros	Cons
● Flexibility and Configurability ● Intuitive User Interface ● Extensibility through Plugins	● Reliance on Community-Driven Plugins ● Steep Learning Curve

8. Zabbix

Function: This software keeps an eye on a variety of network parameters as well as the functionality and security of servers, virtual machines, software, databases, websites, servers, services, and more.

Use Case: Performance Monitoring, Availability and uptime monitoring, Capacity planning, Application troubleshooting, Security monitoring, Compliance reporting, Root cause analysis, Automated alerting and notifications

Open Source/ Paid: Open Source

Pros	Cons
● Simple deployment in non-virtualized environments with scalable typical server hardware. ● Easily configure triggers and integrate with collaboration tools; fast email delivery. ● Excellent reporting with detailed graphics and diverse notification options (email, SMS, Teams).	● Some vendors don't provide SNMP templates, requiring discussion with the Zabbix community. ● Migration between versions is difficult and lacks multiple MFA authentication. ● Initial setup can be challenging due to complex alert workflows.

9. Icinga

Function: Icinga is a monitoring system that verifies the availability of your network resources, alerts users to outages, and produces performance data for reports. It is scalable and extensible, enabling it to monitor vast, complicated environments at various locations.

Use Case: used for monitoring network services, host resources, and server performance, providing comprehensive insights into IT infrastructure. It supports advanced alerting and reporting, helping IT teams identify and resolve issues promptly. Additionally, Icinga's extensible framework integrates with various tools and systems, enhancing overall IT management efficiency.

Open Source/ Paid: Open Source

Pros	Cons
● User-Friendly Configuration Language ● Scalability and High Configurability ● Beautiful Web User Interface	● High Learning Curve ● Limited Customization Options

10. Dynatrace

Function: With the DAVIS AI engine, Dynatrace automatically evaluates Azure Functions, finds and diagnoses issues in real-time, and locates the core cause even before your customers are impacted.

Use Case: DQL, Security data analysis and reporting, Threat hunting and forensics, CSPM Notification Automation, Instant Intrusion Response

Open Source/ Paid: Open Source

Pros	Cons
● Application Monitoring ● Real User Monitoring	● Network Monitoring ● Troubleshooting