NETWORK MONITORING TOOLS: APPLICATIONS FOR DETECTING SUSPICIOUS NETWORK ACTIVITIES (2025)

Monitoring network traffic is essential for identifying suspicious activities, detecting intrusions, and maintaining the overall security of your IT environment. Below is a detailed list of leading network monitoring tools and their key features for 2025.

TOP NETWORK MONITORING TOOLS

TOOL NAME	KEY FEATURES	BEST FOR
Wireshark	Deep packet inspection, real-time/retrospective analysis, protocol decoding	Detailed traffic analysis, forensics
Nagios	Real-time alerts, host/system monitoring, customizable notifications	Live monitoring, infrastructure
Snort	Real-time traffic monitoring, intrusion detection, protocol analysis	Intrusion detection, traffic analysis
Splunk	Real-time/historical data analysis, alerting, dashboards, threat intelligence integration	Security analytics, SIEM
Auvik	Automated network discovery, mapping, resource utilization alerts, config management	Multi-site/WAN monitoring
Paessler PRTG Network Monitor	SNMP, packet sniffing, bandwidth monitoring, customizable maps, threshold-based alerts	SMEs, large enterprises
SolarWinds Network Performance Monitor (NPM)	Agentless monitoring, automated mapping, real-time dashboards, SNMP support	Large enterprises, Windows networks

ManageEngine OpManager	Real-time monitoring, workflow automation, config management, bandwidth analysis	Small/mid-sized organizations
Nexpose	Vulnerability scanning, real-time risk scoring, prioritized remediation	Vulnerability management
Forcepoint	Cloud activity monitoring, suspicious behavior alerts, data protection	Cloud-centric organizations
Checkmk	Scalable monitoring, lightweight agents, BI integration, hybrid/cloud support	Large, heterogeneous environments
LibreNMS	Automatic discovery, custom alerting, API access, mobile UI	Community-driven, open-source
Dynatrace	AI-powered root cause analysis, full-stack monitoring, real-time topology, cloud-native	Cloud/hybrid environments

KEY FEATURES TO LOOK FOR

- **Real-Time Traffic Analysis:** Immediate detection of unusual or unauthorized activity.
- **Automated Alerts:** Instant notifications for suspicious events or threshold breaches.
- **Deep Packet Inspection:** Ability to analyze the contents of network packets for detailed threat detection.
- **Network Mapping & Visualization:** Visual representation of devices, connections, and traffic flows.
- **Integration with SIEM:** Aggregates logs and alerts for advanced security analytics.
- **Customizable Dashboards & Reports:** Tailor monitoring to your organization’s needs.

SPECIALIZED TOOLS FOR SUSPICIOUS ACTIVITY DETECTION

- **Snort:** Open-source intrusion detection and prevention system (IDS/IPS) that analyzes real-time traffic for malicious patterns.
- **Wireshark:** Captures and inspects network packets, useful for forensic analysis and troubleshooting.
- **Splunk:** Aggregates and analyzes network data, maps alerts to cybersecurity frameworks, and provides automated threat intelligence updates.
- **Nagios:** Monitors hosts, services, and network protocols; sends real-time alerts for unauthorized network activity.
- **Auvik:** Cloud-based, automates network discovery and provides visual mapping with resource utilization alerts.

EMERGING TRENDS (2025)

- **AI/ML Integration:** Tools like Dynatrace leverage AI for root cause analysis and predictive threat detection.
- **Cloud & Hybrid Monitoring:** Solutions like Forcepoint and Dynatrace offer robust monitoring for cloud-native and hybrid environments.
- **Automated Documentation & Mapping:** Tools such as Auvik and SolarWinds provide automated network mapping and configuration tracking.

SUMMARY TABLE

Tool	Real - Time Alerts	Deep Packet Inspection	Intrusion Detection	Cloud/Hybrid Support	Visualization
Wireshark	✓	✓	—	✓	✓
Snort	✓	✓	✓	✓	—
Nagios	✓	—	✓	—	✓
Splunk	✓	—	✓	✓	✓
Auvik	✓	—	—	✓	✓
PRTG	✓	✓	—	✓	✓
SolarWinds NPM	✓	✓	—	✓	✓
OpManager	✓	—	—	✓	✓
Dynatrace	✓	✓	✓	✓	✓

SUMMARY:

Top network monitoring tools in 2025 include Wireshark, Nagios, Snort, Splunk, Auvik, PRTG, SolarWinds NPM, and Dynatrace. These applications provide real-time monitoring, deep traffic analysis, automated alerts, and advanced visualization to help organizations detect and respond to suspicious network activities effectively.