RapidFireTools®
A Kaseya COMPANY

A Buyers Guide to Network Assessment Tools

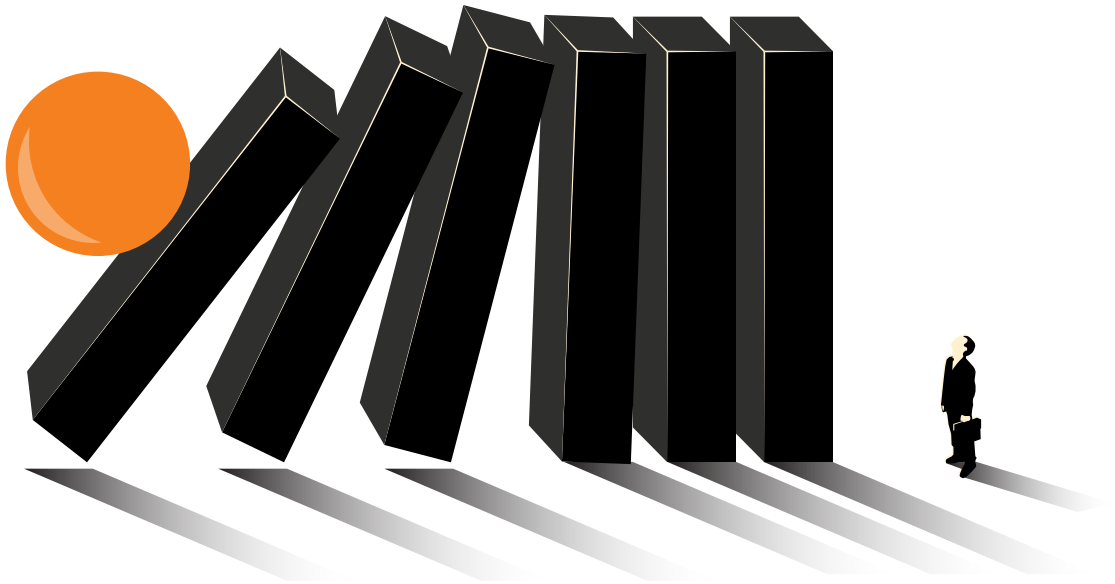
Introduction: You Don't Know What You Don't Know

With cybersecurity risks continuing to grow in number and sophistication, IT technicians responsible for managing security need specialized tools to identify threats across their network, prioritize them and develop remediation strategies to resolve them.

Cybercriminals have grown incredibly creative and innovative, deploying powerful spyware, malware, viruses and social engineering to compromise daily business workflows. Even the most robust antivirus and malware protection software do not provide 100% protection, nor can the most sophisticated firewalls. And if you're not regularly checking for new issues and vulnerabilities that can be exploited — both by hackers and bad actors inside your organization — you put yourself, and your business, at great risk.

Simply put, what you don't know can hurt your enterprise. **And, without the right tools to carry out timely, scheduled assessments, you won't even know what you don't know.**

In this buyer's guide, we'll explore the difference between network audits and network assessments, the benefits of network assessment tools and the key features to look for when selecting a network assessment solution.



Network Assessments vs. Network Audits

Network assessments examine an organization's IT infrastructure and identify the areas that require immediate attention, prioritize or score security concerns, and generate a risk management plan to address the discovered issues. Regular network assessments are essential to minimize the risk of a breach and keep IT assets optimized and available. These assessments are also critical for maintaining privacy protocols, where personal identifiable information (PII) is collected, processed or stored. In addition, network assessment reports can be used to improve network performance, increase network security and reduce costs — all with the goal of maximizing an organization's IT infrastructure and underlying network.

Similarly, a network audit requires the collection and consolidation of a massive amount of IT data. However, the purpose is quite different. Network audits are conducted to manage inventory and validate the presence and types of network assets, configurations, users and systems to ensure they align with an organization's records and requirements. Network auditing also helps IT professionals and the C-suite understand how compliant they are in meeting their own IT requirements, as well as those imposed on them by their government, industry or business partners.

Network Assessments Keep You in the Know

A true, purpose-built network assessment tool does more than just collect data from various parts of the IT infrastructure. It also organizes and analyzes the data it collects. It scrutinizes an organization's existing network health by assessing networking devices, network performance and security threats, all of which help frame a reliable network management strategy. Companies can use network assessments to identify areas to improve the efficiency of the IT infrastructure as well as vulnerabilities that need to be addressed.

Unlike remote monitoring and management (RMM) software, which continually monitors network conditions and only provides alerts that they are programmed to flag — network assessment software runs at periodic intervals and takes comprehensive "snapshots" of the entire network. Viewing these snapshots over time and comparing them against each other helps identify patterns and behaviors that can troubleshoot problems and predict a breach. It's a more proactive and holistic way to support network security programs.

Network assessments can be extremely broad and comprehensive, or they can be specialized for specific purposes, including security health checks, asset aging, network change reports, etc.

How To Implement an Effective IT Assessment Strategy

Network assessments expose security loopholes in your local network, cloud and on devices that connect remotely. An automated network assessment allows you to regularly monitor everything important to you, enabling you to optimize network health and defenses. Here are some practices to help you get started on your IT assessment.

- **Automate Your Data Collection**

  It's important to automate your data collection to reduce the workload and ensure that scans are properly performed.

- **Collect Security Data**

  Be sure to collect security data from all environments — on-premise, cloud and remote users and machines.

- **Schedule Your Data Collectors**

  Consider scheduling your data collectors to run regularly, in line with the cadence of typical changes.

- **Keep Your Network Accessible**

  Ensure your teams have immediate web access to all the network data to troubleshoot issues quickly.

- **Prioritize Remediation Tasks**

  Focus on remediating the most important risks and issues first, based on the guidance from your software.

- **Double-Check Your Work**

  Run a follow-up assessment after you perform remediation to ensure the issues have been resolved.

- **Share The Learnings**

  Share clear and concise summaries of critical issues with the entire IT team

- **Deliver Summaries to Management**

  Showcase the health and performance of your network to corporate leadership with executive summary reports that justify continued investment in IT.

The Benefits of Using a Network Assessment Tool

Listed below are the security benefits you can expect from an effective network assessment solution.

- **Identify network performance issues**

  Identify performance bottlenecks that can impact network performance. This information can be used to create a plan to optimize, consolidate, automate and simplify some aspects of your IT system. You can also identify ways to make your IT system more cost-effective.

- **Detect security vulnerabilities**

  Identify security vulnerabilities, such as weak passwords or open ports, that attackers could exploit. By identifying these vulnerabilities, you can implement a strategy to improve security and better protect your network from threats like data breaches, unauthorized users and malware.

- **Improve network reliability**

  Identify configuration errors or other issues that can impact network reliability. By addressing these issues, IT teams can improve network uptime and reduce downtime.

- **Prioritize issues**

  Measure risks as part of a continuous IT management plan. This provides you with an effective system to prioritize and address issues.

- **Plan for network upgrades**

  Gain insight into the current state of the network and identify areas for improvement. This information can be used to plan for network upgrades or expansions, ensuring that the network is able to meet the organization's needs.

- **Reduce costs**

  Determine how much or how little certain assets within the system are used. This will help you save costs on assets that may not be necessary and make other changes that will improve the overall cost-effectiveness of the IT system.

Key Features of an Effective Network Assessment Tool

The ideal IT assessment solution should have the following features:

Network discovery

Identifies all the devices, data or components connected to a network, including servers, workstations, routers, switches, printers and mobile devices.

Performance measurement

Monitors a network's performance metrics, such as bandwidth usage, packet loss, latency and uptime.

Configuration assessment

Assesses the network's configuration, including device configurations, network topology and routing tables.

Vulnerability scanning

Performs external vulnerability scanning to identify potential security threats and vulnerabilities in the network.

Customizable reporting

Has customizable reports that can be tailored to an organization's specific needs. The reports should be easy to understand and provide actionable insights.

Seamless integration with other IT tools

Integrates with other IT tools, such as help desk software, to streamline IT workflows.

User-friendly interface

A user-friendly interface that makes it easy for IT teams to navigate the tool's features and functionalities.

Issues You Can Detect With a Network Assessment

A well-designed IT assessment solution should generate detailed and customizable reports on the following assessment procedures:

- **Inbound Firewall Issues.**
  Evaluate inbound firewall configuration and search for known external vulnerabilities. Ensure that changes made to the external firewall — or exposure of outward-facing applications — are minimized.

- **Outbound Firewall Issues.**
  The SANS Institute best practices for egress filtering points to the vital role the blocking of unnecessary traffic plays in eliminating the spread of viruses, worms and Trojans in the environment.

- **MS Cloud Issues.**
  Evaluate the current configuration of the Microsoft Cloud environment (including Microsoft 365 and Azure) for adherence to Microsoft best practices for security.

- **Misconfiguration Issues.**
  Ensure all configuration changes are known and approved. Misconfiguration, either accidental or malicious, may compromise the security of the Microsoft Cloud environment.

- **Patch Management Issues.**
  Evaluate the effectiveness of the current patch management tool, and confirm that all known and available patches have been deployed.

- **End-Point Protection Issues.**
  Evaluate antivirus and anti-spyware deployment.

- **Access Privilege Issues.**
  Validate the list of users with administrative privileges and which users have access to critical business data.

- **End-User Behavior Issues.**
  Anomalous login detection for suspicious logins. Review users, computers and layer 2/3 detail to identify possible defunct or rogue users and systems.

- **Security Policy Issues.**
  Security Policy Assessment default review of Group Policy and applicable Local Security Policies for consistency and alignment with best practices.

- **Back-up Issues.**
  Evaluate and report on back-up requirements and effectiveness.

Factors to Consider When Selecting a Network Assessment Tool

The ideal IT assessment solution should have the following features:

- **Budget**
  Network assessment tools can vary in price. That's why it is essential to consider your organization's budget when selecting a tool. Check for restrictions on the number of sites/locations, assets and users.

- **Scalability**
  The network assessment should be able to scale with your organization's growth and changing network requirements.

- **Compatibility**
  The network assessment tool should be compatible with your organization's existing IT infrastructure, including hardware, software and network devices.

- **Vendor support**
  The network assessment tool should have a reliable vendor support system that can assist with any issues or questions.

- **Security**
  The network assessment tool should have robust security features to protect your organization's network data and prevent all unauthorized access.

- **Ease of deployment**
  The network assessment tool should be easy to deploy and not require extensive installation and maintenance of IT resources.

Summary

A network assessment tool is a software solution that helps IT professionals streamline and automate network assessments. It is used to analyze various aspects of an organization's IT infrastructure, including hardware, software and network resources, to identify opportunities for improvement. Organizations can use network assessments to improve decision-making processes across the enterprise regarding network performance and security.

Features of an IT assessment solution should include the collection of detailed information on all network assets. This includes assets not physically connected to the network; the ability to identify risks from misconfigurations, network vulnerabilities and user threats; the ability to support all environments, such as on-premise, remote and cloud; and the ability to produce highly customizable, value-proving reports.

Network Assessment Tools Available Today

There are a variety of professional-grade tools that IT professionals can use to conduct both ad hoc and recurring Network Assessments. However, most of these tools bundle the Network Assessment functionality with other network management and security functions that drive up both cost and complexity. For example,

- ManageEngine

A product called **ManageEngine**, from Zoho Corporation, is an enterprise class solution offering a complete range of IT Management tools. The company offers more than 120 products, from network and device management to security and service desk software, each module costing an average of $5000+. To get a full set of IT Assessment tools covering every device on the local network, in the cloud, and remote device would require a consultation with the company to determine the best mix, with an average starting price of $20,000-$25,000 per year.* (Based on prices published in the ManageEngine online store). Visit manageengine.com for more info.

- netwrix

Netwrix is another company offering a Network Assessment solution. Unlike ManagEngine, which bundles in many un-related functions, Netrix goes in the opposite direction and breaks apart its network assessment solution into a variety of specialized network assessment products. For example, Netwrix Auditor for Active Directory is a small piece of the much larger Netwrix Auditor Suite, and has a starting price of $1,549. However, for a full 360-degree IT assessment you would also need to purchase separate products for: Network Devices, Microsoft 365, Windows File Servers, SQL Servers, SharePoint, Dell Computers, Oracle Databases, Azure AD, and VMware. Again, the full Network Assessment suite alone could average $20,000-$25,000 per year.* (According to the company's last published pricing). In addition, the company charges an extra fee for basic support and updates. Visit netwrix.com for more info.

NETWORK DETECTIVE PRO™

By contrast, **Network Detective Pro** by RapidFire Tools was purpose-built to do comprehensive end-to-end, highly automated IT assessments at a fraction of the price of competing products. Several years ago, the company bucked the industry trend and consolidated its various IT assessment products into a single integrated solution that includes: Full Network Assessment (including Active Directory and all types of endpoints), Security Assessment, SQL Server Assessment, Exchange Assessment, MS Cloud Assessment (Including SharePoint, OneDrive, and Teams), plus AWS infrastructure. It also includes a wide range of scanning techniques, from non-invasive executables that scan with no software installs or probes, light weight computer discovery agents, and cloud-based scanners. It also includes automate scheduling of scans, and automated report generation and delivery. All for an average price of $5000 per year. The company does have a modest onboarding and training fee, but basic support and all updates are free.

To learn more and schedule a demo, visit:
https://www.rapidfiretools.com/products/network-assessment/demo/