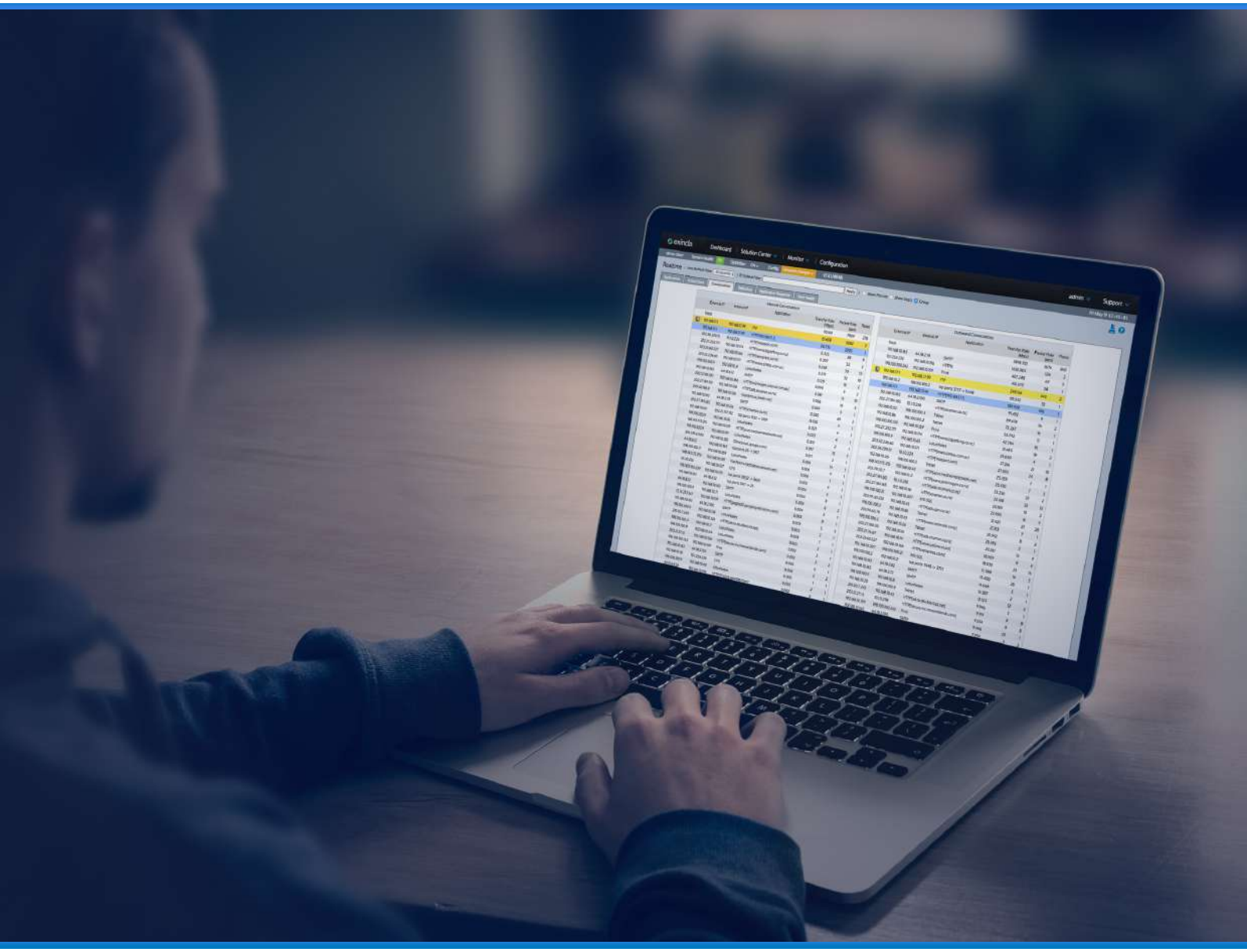
WHITEPAPER

7 reasons why you need a network assessment



GFI Software™

Table of Contents

Introduction

Networks are critical IT resources in every organization. They are the key “connector” that brings together the devices, applications, data and people within the company. Accordingly, networks have become larger and more complex because of the ever-increasing number of devices and apps organizations use. Over 120 devices are added to the Internet each second; by 2020 there will be over 20 billion IoT devices alone.

Every organization will be touched by this phenomenon whether they actively or passively engage with IoT, AI or other new technology waves. The corollary to this growth is there are an increasing number of things that can go wrong in such a complex network. The repercussions of this fault or failure can be huge for your organization.

Network failures are often due to lack of oversight or monitoring capabilities. When network issues are detected early, it can take perhaps a few hours to fix them with little to no impact on the end-user. When issues are not identified early, they can balloon quickly—multiplied by the complexity and foundational importance of your network—into a catastrophe with major financial and operational loss potential for the organization.

Network issues

Network issues can crop up at any time, from any part of your network, and when you least expect it. These issues can set your operations back by a few days to a few years, depending on the severity of its impact.

Common network issues that may have a severe impact on your organization follow.

- **Security vulnerabilities -** One of the most common sources of network issues is security or rather, lack of security. Networks are the gateway to your resources and assets. If hackers can compromise your network, they can gain access to your data, assets, and other resources.

  According to the Ponemon Institute, two-thirds of all data breaches are due to network glitches, human errors, and negligence. Network issues increase the risk of an accidental breach caused by insiders. Employees will often take matters in their own hands and make decisions about how to protect data during a network failure. This could lead to inconsistencies in data handling and worse, open up security vulnerabilities that are hard to identify using manual processes.

  Continuous, automated network monitoring tools counter these issues by making it easy to identify and fix security loopholes before someone can take advantage of them.

- **Configuration changes -** Network and configuration changes are essential when you add or remove devices, bring in new capabilities, migrate systems, or make any significant change to existing applications. You should check the network for performance and vulnerabilities after making such major changes.

  Unfortunately, few organizations do this check. Those who do tend to rely on manual processes, which make it difficult to detect anomalies.

  A study by Veriflow shows that 69 percent of organizations rely on manual processes, 47 percent use internally developed tools or scripts, and 7 percent don't verify the network's functionality after every change. These are all scenarios that lead to network failure.

- **Not prioritizing critical applications -** Streaming video and audio apps like Netflix or YouTube may consume a substantial part of an organization's bandwidth. This can leave

- little bandwidth for mission-critical applications. Your important business-centric applications may be slow to load or freeze while working. The result—lost data; lost productivity; frustrated users.

  Networks are increasing in size due to the prevalence and maturity of BYOD (bring your own device) initiatives or as organizations that offer more open access have multiple devices per person accessing bandwidth. Quickly, you can see your network overwhelmed and grind to a halt.

- **Human error -** Human error is one of the most common causes of problems for networks. Over 95 percent of participants in a survey of midsize and large enterprises indicated human error as a cause of network outages. Human error occurs due to lack of knowledge or training, communication gaps, inability to understand or fix the problem, lack of oversight, lack of time, shortage of people resources.

  For many organizations, these causes compound each other. A lack of people to manage a network coupled with lack of knowledge is a risky combination.

- **Reduced innovation and competitiveness -** Manual management and interventions, ineffective network practices and processes, and incomplete visibility into network ops and performance can reduce your organization's innovation and competitiveness. A study by Forrester shows that most companies spend about 70 percent of their IT budgets to maintain and operate existing systems while about 30 percent is invested in new projects.

  A majority of companies are treading water when it comes to managing and honing one of their most significant sources of competitive advantage—the data, internal systems, and people's efficiency and effectiveness enabled by their networks. An innovation gap can open up if your competitors are spending more on understanding and optimizing network-based applications and performance.

NEXT PAGE

7 reasons why you need a network assessment

7 reasons why you need a network assessment

Regardless of the underlying cause, network inefficiency, slowness, and downtime may cost companies huge amounts of money, introduce unnecessary security or compliance risks, and may slow your growth or affect competitiveness.

To avoid these issues, always stay on top of the health of your network. Just as people benefit from medical checkups to ensure ongoing good health; networks need frequent, consistent assessments to ensure they continue to work at optimal levels.

You can identify and address the above network issues through continuous network assessments. This allows you to get at the root cause of a problem at the earliest possible moment.

The following are seven concrete reasons to assess your network and to stay on top of its performance.

1 Employee productivity

When your network stalls or comes to a standstill, so does your employees' productivity. We depend on our organization's network and the applications it supports for our everyday work. A study by Ireland-based ERS IT Solutions compiled recent data points about networks and productivity. For example, businesses experience 14.1 hours of network downtime per year. When you consider typical small and medium business sizes and their numbers of employees, this downtime can represent about 545 people-hours of lost productivity.

The same study shows that companies spend an average of 200 minutes per downtime incidence to resolve the problem; employees spend about 30 minutes every week to fix PC and network-related problems.

2 At your finger-tips reporting

When you want a snapshot of your network and its performance at any given point in time, network assessment tools are your best bet. Reports are necessary to monitor changes, identify opportunities, demonstrate compliance, and reduce risk. Most network tools come

with advanced reporting features to make network visibility and understanding easier. Out-of-the-box templates that you can customize deliver reports to meet your organization's varying needs.

3 Real-time picture

Your network changes as your businesses grows and changes. A network assessment gives a detailed and real-time picture of the effect of these changes. Understanding this impact helps minimize potential problems and prevent productivity/monetary loss.

This real-time picture (like an MRI in our health metaphor) also helps to identify system upgrade and replacement requirements. A network assessment delivers a real-time SWOT (strengths, weaknesses, opportunities, and threats) analysis of your network. It helps you prioritize, plan, and budget for new projects. It also lets you check if existing IT processes are being followed in your organization so you can take any necessary actions to improve them.

4 Financial loss

Lost employee productivity is one cost; but networks are also revenue generators. Gartner reports that the average cost of network downtime is $5,600 per minute. You may directly lose sales with a downed network. A slowed network may convince potential customers to go elsewhere. Your customer-facing staff may be unable to serve clients in front of them who may then walk or click away.

Over 80 percent of companies set 99.9 percent uptime—or 0.1 percent downtime—as their network standards. However, the average downtime of 14.1 hours per year represents an almost doubling of this downtime threshold.

Even if network issues are fixed within a few hours, the cost could run into hundreds of thousands of dollars or more.

Continuous network assessments catch issues before they lead to downtime. This preventative approach translates into bottom-line benefit on your balance sheet.

5 Managing network complexity

Today's networks are complex and continue to grow more complicated. The plethora of servers, workstations, and personal devices make networks large and unwieldy. Complexity makes it difficult to spot exact fault points along the network if you are using manual monitoring.

Automated network assessment tools continuously scan your network. They are scalable, growing with network complexity without requiring additional staff to manage. They can help identify the precise cause of a problem and do so much sooner.

6 Being proactive rather than reactive

Investigating the cause of network problems after an outage is reactive. The damage is done—lost productivity, revenue, customer trust, customer service. Your work is to find the root to ensure it doesn't happen again and while mitigating the current impact. Being proactive, on the other hand, means you identify and fix problems before they affect end-users.

A network assessment before launching a new application or before migrating a legacy system is a proactive way to identify potential problems and fix them before changes are rolled out.

Automated network assessments are by nature proactive rather than reactive, helping you avoid financial loss and other implications that come with network failures.

7 Ensuring optimal performance and capacity

A poor network undermines the performance of new applications or technology migration you undertake. For example, if the network doesn't have enough bandwidth, end-users will not be able to access all the features of the new application.

Well-managed companies perform network assessments before any major additions or changes to the IT system. You then know if you have the appropriate capacity, latency, bandwidth, storage or other network performance. You can identify if the network needs changes or upgrades for a smooth implementation of any new application.

How to do a network assessment?

These seven reasons make the case for continuous network assessment to ensure network health.

Organizations may turn to other approaches to managing their networks:

- Bringing more redundancy into your network
- Keeping spare pieces of equipment on hand to quickly replace equipment when they fail
- Making the most of premium support offers from vendors
- Improving hiring processes and train employees to handle network problems in the best possible way
- Using backup processes that are independent of Information and Communications Technology systems.

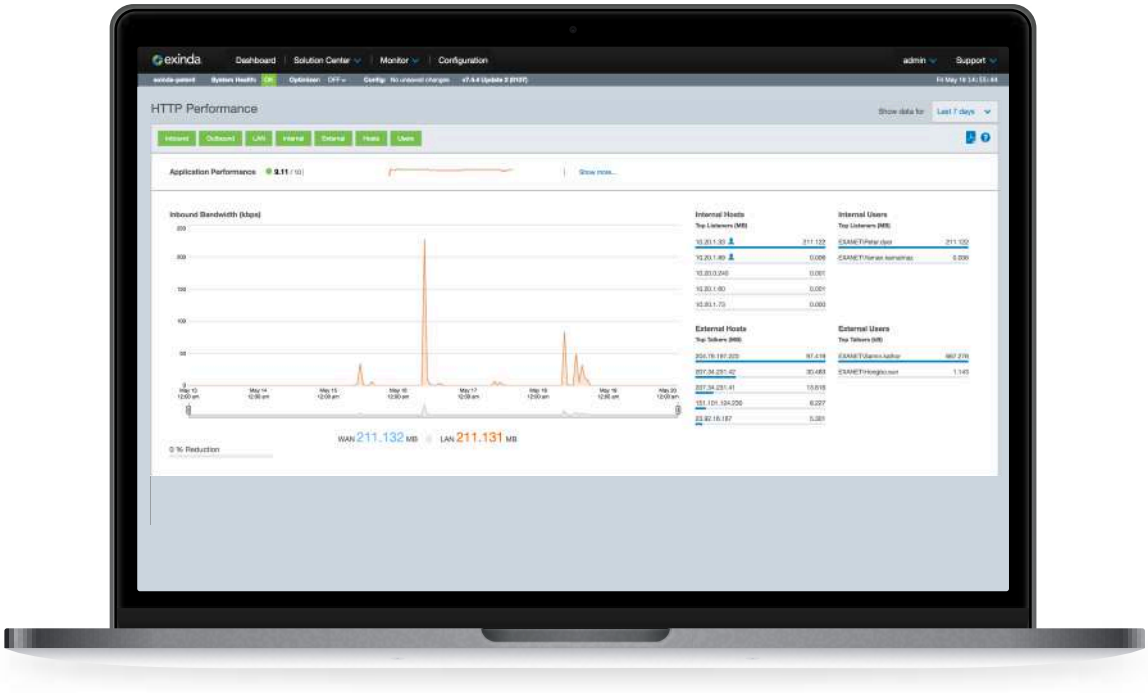
While the above options may work, they don't work well in isolation. These strategies also require manual intervention. Manual intervention is error-prone, non-scalable, and ultimately more expensive. You'll have to hire more people to monitor your network manually as you grow.

Mitigating network problems by doing regular network assessments is the key to avoiding network downtimes and security vulnerabilities.

Automated network monitoring tools monitor different key metrics of your network while you do other work. They notify you when any metrics breach set thresholds. Since these tools run around the clock, you can proactively find and fix problems. Typically, these tools present information about threats, risks and opportunities in a visually appealing way to make it easy for network administrators to share.

In a recent IHS study of 400 midsize to large companies in North America, more than 64 percent of respondents said they had already implemented, or they are in the process of implementing, network monitoring and assessment tools to stay on top of their network's health and performance. These companies have realized that such tools are necessary to remain competitive in today's dynamic business environment.

Network problems abound. And they will increase as we grow and put more demands on networks for business. Automated network assessments become your early warning system for network issues... rather than complaints from your customers or problem logs from your employees.



Request a demo

GFI Software™