WHITE PAPER

Evaluation Guide:

How to Choose a Network Monitoring Tool

PARK PLACE TECHNOLOGIES

ParkPlaceTechnologies.com

Table of Contents

PARK PLACE TECHNOLOGIES

Why Invest in Network Monitoring? Benefits of Monitoring in a Risk-Laden, Customer-First Business Environment.

For all businesses, making certain that the network is up, running, and supporting business services is beyond necessary – it's the enabler of daily operations, from the productivity of staff to customer service. Employees and customers must have access to services, efficiency, and overall quality. This is especially relevant in today's remote work-dominated environment, largely brought about by the COVID-19 pandemic. For this reason, every business needs tools that provide network status and keep services operating while ensuring sufficient capacity.

> **"Your network is the foundation of digital business today. When the network performs, business performs. If it doesn't work, your business grinds to a halt. Network monitoring tools help prevent that."**
>
> - Lee Walker, CTO, Park Place Technologies

In the context of network monitoring, it's also important to acknowledge that in many businesses, there's often an IT group for nearly every function of technology: hardware, installation, configuration, application implementation, and security. Furthermore, technology assets are commonly spread across data centers, colocated environments, and the cloud. As a result, IT is more complicated, creating the need for a more unified view of network operations. Without robust network monitoring software, businesses are open to a wide array of risks and vulnerabilities.

However, the truth of the matter is that sometimes risks become network events, and network events become outages. Even with the most advanced technology and built-in redundancy, IT is still working with imperfect systems.

Often, downtime is caused by relatively simple mistakes:

- Lack of network documentation
- Limited information on network configurations
- Ineffective means for identifying and tracking devices on the network
- Inability to identify ISP connections
- Lack of visibility into performance
- Inability to identify root causes

> **"The failure is going to occur, the downtime's going to happen, but what you do next is what defines whether it was a big downtime or a blip. Network monitoring gives you the power to respond."**
>
> –Jordan MacPherson, Enterprise Operations Center Program Manager Park Place Technologies

Ultimately, the greatest consequence of downtime in today's digitally driven climate is the inability to recover as a business, although the impetus can vary. Perhaps an organization lost employees due to the inability to pay staff on time because IT systems were down. Or maybe the service offered wasn't delivered in time because systems aren't available or performant. Other consequences include but are not limited to loss of productivity, lost revenue, and costs that cannot be quantified such as abandoned IT initiatives, damaged IT morale, and lost opportunities in the market (Mission Critical Magazine).[1]

- According to a report from the Federal Emergency Management Agency (FEMA), 40% of businesses do not reopen following a disaster. On top of that, another 25% fail within one year.[2]
- The United States Small Business Administration found that over 90% of companies fail within two years of being struck by a disaster.[3]
- According to an ITIC study, an overwhelming majority (98%) of organizations report that a single hour of downtime costs them $100,000 or more, and 81% state that the hourly cost is $300,000 or more.[4]

Every organization needs visibility into the network and actionable intelligence to make appropriate decisions. Resource planning, performance adjustments, and security measures are all consequential safeguards against downtime. For instance, if a company plans to add resources such as a new productivity application, anticipating the appropriate amount of bandwidth the application will demand is extremely difficult. This kind of delay in such a fast-paced, customer-first business environment can severely limit an organization's growth and agility potential. However, with the right network monitoring system, it becomes possible to effectively monitor status, resources, and performance for applications and services.

In essence, IT is built on top of the network; everything requires network connectivity to function. Without network visibility, performance management, or analytics, there's no way to make connections between the network and everything it's attached to.

1. https://www.missioncriticalmagazine.com/articles/92664-what-unanticipated-downtime-means-for-your-business
2. https://www.fema.gov/
3. https://www.sba.gov/
4. https://itic-corp.com/blog/2016/08/cost-of-hourly-downtime-soars-81-of-enterprises-say-it-exceeds-300k-on-average/

The Network Monitoring Market: Three Primary Types of Solutions

There's no infallible way to avert hardware failures or stop hackers, but all businesses can take proactive measures to defend the network. Network monitoring solutions are often the first line of defense against problems before they become disastrous.

It's important to note that the tools available on the market today are generally not one-size-fits all. Every network is configured uniquely and therefore comes with different challenges. Let's look at the primary types of network solutions that are available today.

1. **Traditional Network Monitoring**
   The A1 way to monitor is to go out, discover your network, and poll for information. This is referred to as traditional network monitoring. Generally, these types of solutions find the assets that exist on the network, how they're connected, how businesses services depend on the network, and then continuously poll the infrastructure for status updates or changes.

2. **Flow Analysis Tools**
   There are also monitoring products designed to "sit and listen" rather than discover the network and wait for various devices to send information to them directly, also known as flow analysis tools. The information gathered provides insights such as who's talking to who, amount of bandwidth on links, whether there are many sources trying to connect to one target, etc. Flow analysis tools provide a sense of security without regular polling.

3. **Application Dependency Mapping and Application Performance Tools**
   Application dependency mapping and application performance tools are not as focused on the infrastructure, offering very little visibility. Instead, they connect directly to servers and find out which applications are running on them. From there, these tools identify dependencies between applications, though multiple applications typically go together to comprise a service.

   These kinds of tools tend to focus on application response times. Typically, dependency mapping and application performance tools come with the ability to instrument web pages, providing information to administrators such as how and what sort of requests users are making and how long it's taking to service requests, offering a detailed picture of user experience.

How can an organization decide which type is right for their needs?
To put it simply, it's best to cover all three areas; no one solution is a replacement for the other two because they work in tandem. One way to minimize complexity and avoid disparate tooling is to select a comprehensive network monitoring product that will allow the IT team to replace several tools with one complete solution.

ENTUITY SOFTWARE™

When we are supporting a client that is having a performance problem, the ability to go to a single console to see all the network views that we care about (instead of half a dozen different products) goes a long way to reduce the time to resolution. Then on top of that are all the event management rules we can leverage to control unwanted noise and out of the box integration to our preferred enterprise management tool.

–Sean O'Brien, Senior Manager of Global Platform Engineering for Monitoring | Ensono

PARK PLACE TECHNOLOGIES

Network Monitoring Features Admins Can't Do Without

While the network monitoring solutions on the market today have some shared qualities, they're all different. As your IT team sets out to select a network monitoring tool that will adequately address your requirements, it's helpful to be prepared with a general idea of the features that are indispensable.

- **Visibility into the Entire Infrastructure Estate**
  What assets do you have? How are they connected? The answers to these questions support your network teams' collective ability to monitor the infrastructure. As a result, your network monitoring tool of choice must provide total visibility into your entire estate. Look for recurring, automatic topologies.
- **Management of all Discovered Assets**
  Being able to discover assets is one thing, but how do you manage them, especially in large environments with hundreds of thousands of assets? Network monitoring tools should categorize and visualize assets in terms of business services rather than applications. This enables the ability to model business services and visualize underlying assets that power them. In the event of a network issue, a tool with comprehensive management capabilities will make it easy to identify the root cause. To further time savings and simplicity, consider solutions that offer automation by identifying all dependences between endpoints for applications.
- **Quality Incident Management and Remediation Capabilities**
  Quality incident management and remediation capabilities come down to event noise reduction and highlighting the incidents that network administrators need to focus on in a user friendly fashion.

Ultimately, IT personnel want to make sure business services are kept up, running and operating at their best. This means monitoring and listening for events across the entire estate, as well as reducing noise in such a way that makes it easy to identify important, actionable events.

DID YOU KNOW?

Entuity Network Analytics offers one of the deepest recurring, fully automatic topologies of network monitoring products out there, extended to cover servers, storage, applications, and more.

ENTUITY SOFTWARE™

DID YOU KNOW?

Out of the box, ENA reduces event noise by 90% with simple, but effective rules that are completely customizable by end customers. Extending rules to reduce noise further relative to business needs is easy.

ENTUITY SOFTWARE™

- **Excellent Support and Professional Services**

  Support and professional services are often overlooked from the outset because they're not considered traditional network monitoring features, but they're rarely undervalued when utilized.

  Support and professional services boil down to total cost of ownership. Typical, free tools may appear cheap in the beginning, but they become costly in the long term. Think of it this way: does it make sense to task your IT team with handling deployment, integration, support, and maintenance when there are high-quality monitoring products available that focus on those objectives exclusively? The answer is not usually, and it's often best to choose a comprehensive solution that enables the network team to focus on business.

  The nature of the support relationship matters, too. Be sure you're getting a solution that's supported by human beings who truly care about your outcomes. Your network admins shouldn't have to talk to a different person with limited experience every time they call support. Further, the best network monitoring solutions will maintain close relationships between support and engineering, making it easy for you to solve technical issues quickly.

- **Scalability**

  A network monitoring solution must cover the entire infrastructure – and that doesn't mean deploying hundreds of servers, each with their own separate interface. There should be a single interface to cover the entire estate, even if there's hundreds of thousands of network devices

  Technology coverage is particularly critical because in addition to the traditional networking kit (routers, switches, firewalls, load balancers), servers, and storage, there's different types of cloud, virtualization, and hybrid IT environments to consider, and they're growing massively. Compounding the intricacy are software-defined technologies, some of which allow users to make on-the-fly software configuration changes. Many vendors are consolidating asset management into their own cloud solutions. Because of the widespread, complex nature of modern IT environments, network monitoring tools must support all these technologies.

- **Machine Learning and Artificial Intelligence – Hype, or a Need-to-Have?**

  If you're involved with the network at all, you know that machine learning and artificial intelligence are being touted as rich, innovative new feature sets among many of the network monitoring tools available on the market today. Frankly, currently there's more hype around ML and AI than actual value. To be clear, network monitoring tools that integrate ML and AI are on their way – but not today. Focus on solutions that reduce network noise out of the box without overemphasizing the role of AI.

DID YOU KNOW?

ENA allows you to deploy many servers and consolidate all information through a single user interface. Essentially, it looks and works like one giant server.

ENTUITY SOFTWARE™

Preparing for the Buying Process: How to Choose a Network Monitoring Tool

Choosing a network monitoring solution is an individualized process depending on your business needs, but the goal is the same: delivering a centralized, unified view of network services operations. Your network admins should be able to see the detailed activities of network operations from a holistic viewpoint and use a unified method for identifying anomalous events.

Effective Network Monitoring Delivers:

- Smarter monitoring
- Enhanced analytics capabilities
- Faster identification of anomalies
- Optimized IT operations

To help you as you set out on your path to find a network monitoring solution that will effectively prevent unforeseen IT events, we've put together a detailed, practical checklist you can use to evaluate possible solutions in the market.

PARK PLACE TECHNOLOGIES

Network Monitoring Solution Checklist

- ❑ **Does the monitoring solution provide the features that I need?**
  - ❍ Asset discovery, component modelling, and automatic topology
  - ❍ Business service modelling
  - ❍ Realtime health monitoring
  - ❍ Network performance monitors, capacity planning, and trending
  - ❍ Configuration management, backup, change detection, compliance, and automation
  - ❍ Network traffic flow and bandwidth analysis
  - ❍ Application monitoring and network path analysis
  - ❍ Powerful, customizable reporting
  - ❍ Event and incident management system to reduce event noise and speed up root cause identification/remediation of issues
- ❑ **Does the system support all technologies in use within the company, both now and in future plans?**
  - ❍ Does it provide support for traditional, software defined, and cloud-based assets, as well as servers, storage, and end devices?
- ❑ **Does the system deliver a fast, responsive, and intuitive user experience?**
  - ❍ What data is collected? Is it presented in a clear, concise, and usable form?
  - ❍ Does the system focus on highlighting areas that need attention while offering drill down for further investigation?
  - ❍ Does the system offer contextual dashboards, interactive charts, powerful filters, practical grouping of assets, seamless and consistent navigation to maximize user efficiency?
  - ❍ Can the system be easily configured to present different capabilities to different users, e.g., based on role, or service levels?
  - ❍ Can the system be accessed from anywhere via a desktop or mobile device?
- ❑ **Will the software scale to meet the size and geographical distribution of my network infrastructure?**
  - ❍ How many servers will be needed to host the system? Is this number reasonable for my IT team to manage?
  - ❍ Does the system support seamless management of remote locations anywhere in the world?
  - ❍ Can I view and manage my entire infrastructure through a single, consolidated user interface?
  - ❍ Is the user experience maintained at scale?
  - ❍ Is there a long-term data archive providing the foundation for long-term trend analysis?

Network Monitoring Solution Checklist (Cont.)

- ❑ **Does the system provide full reporting capabilities with ability to access and slice & dice all data collected?**

- ❑ **Does the system provide comprehensive OOTB event handling to reduce event noise and speed up root cause identification and remediation of issues?**
  - ❍ Can the system be customized to better match business needs and further reduce noise?
  - ❍ Does the system support maintenance windows for groups of assets to avoid false alarms?
  - ❍ Can the system be configured to alert the right people based on incident context, time, severity, and other data?

- ❑ **Does the solution provide strong and flexible security?**
  - ❍ Does the system follow industry best practices for security?
  - ❍ Does the system support local, centralized (e.g., LDAP), and multi-factor authentication?
  - ❍ Can I define different access permissions for different users so they can only see and do what they need to?

- ❑ **Can the system be customized and/or extended to meet my business' specific needs?**
  - ❍ Can I customize dashboards, reports, automation, CMDB schema and data polling, service modelling, event and incident rules, etc.?
  - ❍ Can the system be easily integrated with other systems in my business?
  - ❍ Does the solution provide OOTB integrations to key third-party systems, such as ITSM and ML/AI data processing, e.g., ServiceNow, Splunk, Moogsoft, etc.?
  - ❍ Does the product provide APIs for easy integration and automation, e.g., REST API?

- ❑ **Is the solution offered as an on-premises and/or SaaS solution?**
  - ❍ Which one best suits my budget and internal IT capabilities?
  - ❍ Can I try before I buy?

- ❑ **What is the TCO of the system?**
  - ❍ How easy is the system to deploy and maintain?
  - ❍ Is the product ready to go OOTB, or does it require lots of manual configuration, either one off or ongoing?
  - ❍ Can the system be hosted in the cloud?
  - ❍ How easy is it to upgrade the system?
  - ❍ Will the system allow me to consolidate/reduce my current toolset to achieve lower maintenance, tighter integration, improved usability and workflow efficiencies, and lower overall cost?

Network Monitoring Solution Checklist (Cont.)

- ❑ **What level of support will I get?**
  - ❍ Can I expect personalized, 24/7/365 telephone support?
  - ❍ Does the vendor offer full system training?
  - ❍ Does the vendor offer professional services to help with deployment, configuration, and custom extensions?
  - ❍ Will the vendor listen to my requests for enhancements and roadmap improvements?