WHITE PAPER

Essential Guide to Active Monitoring

The Business Value of Being Proactive

KEYSIGHT

Introduction

The bigger the network, the harder it fails. When your employees and customers rely on round-the-clock access to business-critical applications, the effects of service outages and downtime can be wide-ranging and catastrophic:

- wasted revenue
- delayed time to market
- lost productivity
- declining competitive advantage
- eroding customer loyalty

Unfortunately, these kinds of issues are getting harder to prevent. Networks are growing more complex, making it harder to identify bottlenecks and maintain quality of service.

When your business depends on peak performance, you cannot afford costly surprises bringing your system down. You need to get ahead of the curve. And that's why an active monitoring strategy is so important. It enables you to detect, diagnose, and remediate issues before they cause costly rework and leave a lasting impact.

In this white paper, you will learn everything you need to know about active monitoring:

- the critical role it plays in your network performance monitoring portfolio
- how it differs from passive approaches
- how it benefits your bottom line
- what you can do to start applying it to your network

The Need for Active Monitoring

The last decade has seen a sea change in enterprise networking. The rise of mobile devices and the Internet of Things has helped make people more connected. With near-unfettered access to corporate networks, employees and customers are more efficient, productive, and satisfied than ever before.

However, with increased connectivity comes increased risk. Networks are getting more complex. Critical workloads are migrating from legacy systems to scalable, cost-effective solutions such as software-defined wide area networks (SD-WAN), cloud, and virtualized infrastructure — and that's making it harder for IT to prevent outages and maintain quality of service.

Traditional approaches to network performance monitoring are not enough anymore. You cannot rely on a platform that only tells you when your network is down. You need a new approach — one that enables you to pinpoint problems before they affect your end users.

Key takeaway

Critical outages can cost you as much as $1 million for every hour an application is offline, according to a 2014 IDC study. And that's not even counting the $540,000 you lose for every hour of lost productivity, according to a 2016 report from the Ponemon Institute. With such costly consequences looming, a proactive approach to preventing outages is critical for ensuring quality of service.

> Critical application outages can cost you as much as $1 million for every hour an application is offline — and that's not even counting the $540,000 you lose for every hour of lost productivity.

Different Approaches to Network Performance Monitoring

When it comes to monitoring your network, you have a few options. They all have inherent benefits and limitations, but their approach to data collection is what fundamentally differentiates them. While some can help you troubleshoot after a crash, others can help you prevent crashes from happening in the first place.

- Equipment polling is the easiest way to monitor live traffic, but this passive approach becomes less viable as networks grow more complex.
- Packet data monitoring is a better way to monitor real-time traffic in distributed networks, but a lack of proactive insight is a limitation.
- Active monitoring (aka synthetic monitoring) uses simulated traffic analysis that enables continuous user-experience monitoring and proactive problem detection.

Equipment polling

The most basic monitoring approach, equipment polling gathers data from existing equipment in your data center, such as routers, switches, and servers. Aggregating all that data onto a centralized dashboard makes it easy to see what is happening in your network.

Because live traffic data is useful for analyzing outages after they occur, equipment polling is an excellent approach for advanced troubleshooting. However, this approach will only reveal current problems affecting users and causing downtime — preventing you from taking proactive action and resolving issues before they impact your users.

Furthermore, as networks move to increasingly virtualized workloads, IT organizations have less access to physical equipment than they once did. This decreases the efficacy of this approach and creates a host of blind spots that hamper visibility and increase risk.

Packet data monitoring

As companies lose access to physical infrastructure, packet data is emerging as a viable alternative for passively monitoring applications. Because you can tap packet data in both physical and virtual environments, this approach offers flexibility that equipment polling cannot match.

Granted, because it is a passive technique, packet data monitoring faces the same limitations as equipment polling. While excellent for course-correcting after your systems go down, it does not enable any proactive detection — leaving your team scrambling when something goes wrong.

Packet data monitoring offers a more feasible monitoring approach to distributed networks, but don't take the challenge of gaining packet-level visibility across your entire network for granted. Capturing inter-VM traffic in cloud-based workloads is not as simple as tapping a physical appliance. You limit the scope and efficacy of your monitoring if you cannot access that traffic.

However, these considerations should not imply that packet data monitoring has no place in your organization. Access to real traffic data is critical for a well-rounded monitoring portfolio. Studying such data enables long-term insights about your users and aids root-cause analysis, provided you have the tools necessary to capture it.

Note: For more information on Keysight's industry-leading visibility solutions, check out our complete list of network visibility products. With a full suite of taps, aggregators, regenerators, bypass switches, network packet brokers, and CloudLens — Keysight's proprietary platform for public, private, and hybrid cloud monitoring — you can ensure comprehensive packet-level visibility across your entire distributed network.

Active monitoring (aka synthetic monitoring)

Unlike passive monitoring approaches, active monitoring helps prevent outages by identifying issues before they happen. Instead of relying on live traffic, active monitoring tools simulate traffic by sending synthetic packet data to various hardware- and software-based endpoints across your network. You can pinpoint potential problems long before they reveal themselves under actual loads by proactively probing your network for vulnerabilities.

That proactive analysis is why active monitoring deserves a permanent place in your enterprise IT strategy. Because it does not require an outage to alert you of problems, you can identify issues long before they cause downtime for your end users. This doesn't just save considerable amounts of time and money for IT; it prevents network outages that would negatively impact the business.

Additionally, synthetic traffic generation does not require tapping, making it ideal for distributed networks. You can install the software-based monitoring agents in any physical or virtual environment, helping you start faster without additional complexity.

Key takeaway

So which approach is best — active or passive monitoring? The truth is that you need both. As helpful as active monitoring is, you will never be able to predict every outage. And when one inevitably occurs, you will need real traffic data to investigate and perform root-cause analysis. However, don't underestimate the value of a proactive approach — especially for companies employing highly distributed networks.

Active Monitoring – An Ounce of Prevention That's Worth a Pound of Cure

So, what can you expect when you implement an active monitoring solution? Here's a look at six use cases that detail the wide array of organizational benefits it provides.

1. Avoid costly outages with pre-deployment awareness

Think about the last time your network went down. Everything was going great one second, and then it all came crashing down without warning. Remember how much time you spent troubleshooting — and then, once you finally isolated the problem, how long it took to implement a fix?

Now imagine this: You are about to roll out an update for one of your company-wide systems when your active monitoring tool sends you a warning. It has simulated an average day of network traffic in your test environment and identified significant latency issues at peak load. After a brief investigation, you use your tool's included network path discovery application to quickly pinpoint the culprit and resolve the problem without incident. Instead of lengthy downtime, frustrated users, and squandered revenue, your update is ready to go live with minimal impact on your schedule.

Granted, this is just an example, but you can imagine the possibilities here. Getting ahead of potential problems like these can be invaluable in any of the following scenarios:

- opening a branch office
- deploying software-as-a-service (SaaS) solutions
- migrating to a new data center
- rolling out a distributed application
- load-testing a website before going live

2. Maintain quality of service with end-to-end monitoring

How often do your end users notify you of problems in the network? Whether the Wi-Fi is lagging, Office 365 is running slow, Skype is crashing, or something else is going wrong, your users are on the front lines. They are often the first to alert IT to service issues.

Unfortunately, the information they convey is not always useful. Sure, something went wrong, but all you have is an undependable anecdote that does not help with troubleshooting or root-cause analysis. You need to get ahead of the curve, and active monitoring can help get you there.

With distributed endpoints that can monitor equipment, service providers' networks, and cloud-based applications 24 / 7 / 365, you can identify and resolve issues before your end users ever discover them. Whether you are examining Wi-Fi performance on an employee's device, measuring how long it takes your web server to respond to users, or testing Outlook 365 by sending a sample email, you will always know what is happening across your network.

3. Safely migrate to the cloud without compromising performance

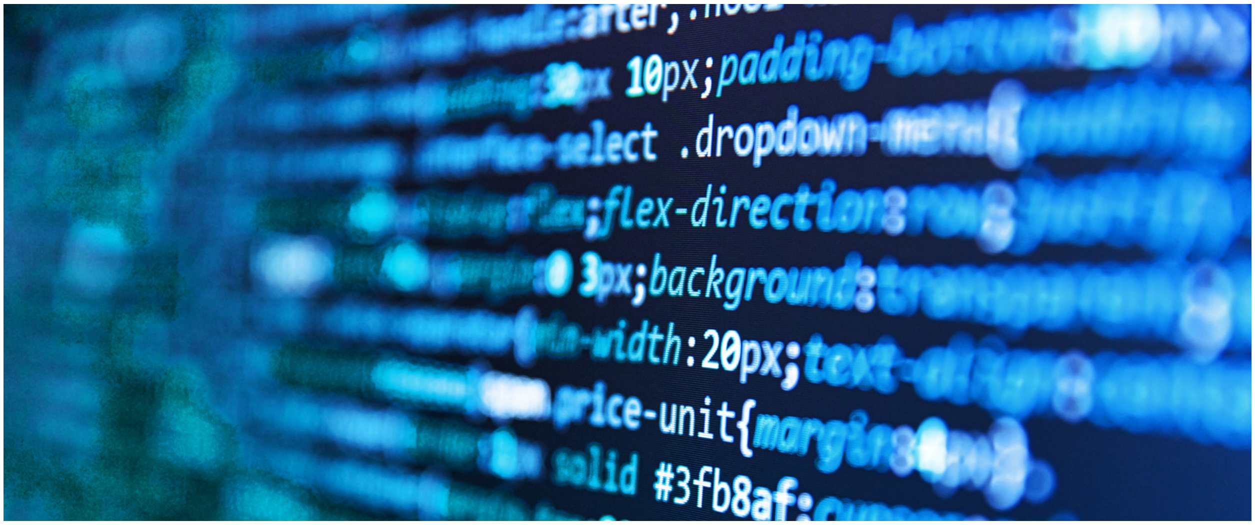
Enterprise workloads are moving to the cloud because it offers companies unparalleled agility, elasticity, and cost benefits. However, migration has one noteworthy drawback: Critical application traffic, which once traversed your controlled physical network, is now traveling over the internet. Where controlled environments offer stability, the internet is less predictable — leaving your applications vulnerable to productivity-killing latency issues.

Active monitoring tools help smooth this transition by giving you the metrics you need to ensure peak performance while keeping abreast of any potential service degradations in the future. Verifying access links from your remote locations and monitoring the performance of cloud applications across hundreds of WAN-based endpoints gives you a clear view of end-user experience during operations.

4. Ensure voice and video reliability with real-time mean opinion scores

As cloud-based VoIP and videoconferencing applications grow ever more vital to your daily operations, you need a viable way to maintain performance. Otherwise, productivity will take a nosedive as communication and collaboration suffer. And remember — that costs your company $540,000 per hour.

Without a reliable way to monitor these critical communications, you are likely relying on reports from your users themselves. Unfortunately, those are inherently subjective and unreliable. But what if you could continuously test thousands of endpoints across your network to get an objective assessment of video and call quality for your entire organization? With active monitoring, you can see mean opinion scores across your network in real time, providing insight the moment something goes awry.



5. Improve SLA management with network path discovery

When it comes to service-level agreements (SLAs), you are supposed to get what you pay for. But what happens when things slow down? Once data leaves your router, it becomes much harder to track. That can lead to lengthy troubleshooting with your service provider. Meanwhile, you are not getting what you paid for — and neither are your users.

With network path discovery, you can see every step your traffic takes in a powerful and intuitive layout. This enables you to quickly identify faulty nodes, so you can show your service provider the specific endpoint that is causing you trouble — shortening your mean-time-to-resolution and ensuring that your SLAs are being met.

6. Track performance at the edge with network packet broker integration

Edge computing has made branch sites more connected than ever before. However, as data flow grows more complex and distributed, the need for visibility on the edge of your network is even more critical. Protecting against threats is not enough anymore. You need to be in full control of your end users' experience, too.

When security and performance matter most, specialized packet brokers like Keysight's Vision Edge 1S, combined with an active monitoring platform, enable complete network visibility and performance monitoring at all your branch sites. Packet-data visibility bolsters your security tools with threat-detection intelligence, while integrated monitoring endpoints give you a clear view of each location's LAN, WAN, Wi-Fi, and cloud performance.

Key takeaway

While the Keysight Hawkeye monitoring platform offers all the features and functionalities mentioned above in a seamlessly integrated, user-friendly package, it is worth remembering that not all tools are created equal. When evaluating solutions, make sure you choose one that offers the same capabilities and performance. If not, you risk missing out on the proactive benefits that make active monitoring so essential in the first place.

Web-Based or On-Premises?

When deploying an active monitoring platform, you generally have two options: a web-based SaaS application or an on-premises solution hosted on a physical server or your cloud infrastructure.

Which is better for you? That depends on the architecture of your environment and your organization's goals and requirements.

Web-based (SaaS)

A web-based active monitoring platform is ideal for highly distributed networks, especially those featuring diverse cloud applications and physical servers. Though they can lack some of the functionalities that self-hosted applications offer, SaaS platforms offer flexibility and a pay-as-you-go subscription model.

Self-hosted (on-premises)

If you want customizability, a self-hosted implementation that installs in your own physical or virtual infrastructure is a more robust option. However, while self-hosted platforms offer additional testing options, increased test coverage, and more detailed metrics reporting, they require a larger investment and lack the flexibility of a monthly subscription.

Key takeaway

Implementation options for specific tools vary. For example, Keysight Hawkeye offers both web-based and self-hosted platforms. Be sure you understand how your preferred choice will integrate with your network.

Stop Fighting Fires and Start Preventing Them

Whether you are a network engineer or a CIO, driving change in IT is never easy. Every day, you face a cacophony of new problems — and there is never enough time (or money) to solve them all. You are continually asked to do more with less. With that kind of pressure, it can be hard to opt for anything other than the status quo.

However, as budgets tighten and the business presses for faster fixes and better performance, reacting to problems is not sustainable anymore. You need to get ahead — and that means preventing those issues in the first place.

Network performance is more vital than ever, and things like cloud, SD-WAN, and edge computing are not going anywhere. As legacy infrastructures continue to integrate with these new technologies, networks will only get more distributed and complex — increasing both technical debt (the implied cost of additional rework down the road) and risk of failure.

No doctor would fight a patient's symptoms while ignoring the disease that causes them, and neither should you. That's why an active monitoring solution is so critical to keeping your network in good health. Instead of worrying about downtime and outages bringing your systems to a standstill, you will be detecting, identifying, and remediating potential problems long before anyone outside your department even knows they exist.

No doctor would fight a patient's symptoms while ignoring the disease that causes them, and neither should you.

Further Reading

Want to learn more about active monitoring? Whether you are looking for technical guides, product information, case studies, or something else entirely, Keysight's in-depth resources deliver the content you need to make the most informed decision possible.

1. Technical guides

- Network Monitoring: Have You Ever Monitored 'What If'?
- Virtual Private Cloud: Are You Getting Your Money's Worth?

2. White papers

- Solve SLA and QoE Problems
- Ensure Optimal SD-WAN Network Performance and Service QoE
- Qualify Net Neutrality with Hawkeye

For more information on Keysight Technologies' products, applications, or services, please visit: www.keysight.com

Published in USA, June 9, 2022, 3119-1154.EN