Geek-to-Guru Guide:

PROACTIVE NETWORK MONITORING

KEYSIGHT TECHNOLOGIES

INTRODUCTION

“Good Enough” is Not Enough

Your network is changing. Hybrid deployments offer speed, scale, and savings — but all that complexity makes them more challenging to maintain consistent quality of service. When customers and employees demand 24/7 access to critical applications, service outages and latency can delay time-to-market, jeopardize customer loyalty, and erode your competitive advantage.

As you read through this guide, you’ll discover the benefits of a proactive approach to network performance monitoring. Whether you’re looking to prevent service interruptions from causing downtime, troubleshoot issues faster, or see your network from your users’ point of view, you’ll get the insights you need to maintain peak performance.

CHAPTER 1

See It Before They Do

Why NetOps Teams are Embracing Active Monitoring

Your network is more than an information delivery system. It's the heartbeat of your business. That's why so many NetOps teams are embracing a more proactive approach to network monitoring.

CHAPTER 1

See It Before They Do

Why NetOps Teams are Embracing Active Monitoring

Your network is more than an information delivery system. It's the heartbeat of your business. Bottlenecks and service outages are more than annoyances; they spoil your users' experience. And you know what that means: reduced revenue, delayed time to market, impaired productivity, and — worst of all — lost customer loyalty.

At the same time, sustaining your network is more difficult than ever. Active monitoring offers a well-established method to monitor user experience, but many in IT have seen it as more of a luxury than an essential tool. But that's all changing. The shift to remote work has spurred a sea change in network deployment models. Scalable, cost-effective solutions such as SD-WAN, cloud, and virtualized infrastructure help address some of these challenges, but they also make networks more complex — and difficult to monitor.

Next-generation networks demand next-generation performance monitoring. That's why so many enterprises are adding active monitoring solutions to their network tool stack. From its hybrid-friendly nature to the predictive insights it provides, here are some of the most important reasons network operations teams are making the switch.

See it before they do

Traditional performance monitoring tools are reactive. They alert you when network speeds fall short, which is helpful for understanding if your equipment needs upgrading or if signal conditions are causing performance degradation. But by the time passive monitoring tools detect a problem, your customers are already frustrated — and potentially evaluating the competition.

When the quality of your customer experience can make or break your business, you need to get ahead of issues to maintain quality of service (QoS). That's why network operations teams are embracing a more proactive approach. With active monitoring, it's easy to detect, diagnose, and remediate issues before they impact your end users and cause costly service interruptions.

Monitor distributed networks with ease

Network perimeters are vanishing. SD-WAN, cloud, and edge computing are replacing the clearly defined corporate data centers of the past. These technologies offer considerable cost savings and flexibility, but they also make it challenging for traditional network monitoring tools to measure QoS effectively. Since organizations no longer house most network infrastructure on premises, directly monitoring certain types of traffic and equipment is considerably more complex. Modern hybrid networks demand a more flexible, lightweight solution. Otherwise, you risk blind spots that can hamper your ability to identify, troubleshoot, and ultimately resolve performance problems.

Active monitoring tools, like Keysight's Hawkeye, offer an ideal solution to manage performance across distributed, hybrid networks. These tools simulate traffic by sending synthetic packet data to various hardware- and software-based endpoints across your network — eliminating the need to access physical infrastructure. Whether you want to monitor a remote site, software-as-a-service (SaaS) application, cloud deployment, or corporate headquarters, you just need to install an endpoint and you're ready to go.

Measure QoS from your users' perspective

User experience is the metric by which your network is measured. However, when you shift to an active approach, you can track how traffic moves through the entire network topology. You get a look at network performance from your end users' point of view. Since you have visibility to what your users are seeing, you can track key performance metrics on connectivity, network infrastructure, network services, calls out to the internet, and communications with cloud-based applications and service providers.

Answer your most vexing questions

Uncertainty is a persistent problem for network operations teams. What happens to performance if you introduce a new application or expand your use of an existing one? Will unforeseen issues trigger a bandwidth crunch and leave your users facing latency and performance bottlenecks? Questions like these can be difficult to answer, but incredibly important.

However, active monitoring gives you an advantage. Since these tools rely on realistic traffic simulations, you can construct models that closely mimic what you expect to see moving across your network and run "what-if" analyses to test various scenarios. You can even test and validate more complex deployments such as SD-WAN. With the insights gained from traffic simulation, you can explore how your network performs under various conditions and test the impact of potential fixes. Instead of waiting for the unexpected, you can proactively take control of the future.

See your network through a single pane of glass

No one likes flipping through multiple dashboards — it's clunky and wastes precious time. That's why robust tools, like Keysight's Hawkeye, consolidate application and performance insights into a single pane of glass. From core to edge, from your headquarters to your remote users, you can see everything at a glance. With a clear view of your network's behavior in real time, you can prevent downtime, maintain QoS, and take unprecedented control of user experience with fewer obstacles.

Be ready for whatever the future holds

Nothing is certain in the future. However, it's safe to assume networks will continue to evolve, and user expectations will only grow more stringent. That's why it's critical to future-proof your network now with a scalable solution like active monitoring. Lightweight, easy-to-deploy endpoints make it simple to expand your coverage while synthetic traffic is versatile enough to monitor all phases of hybrid network environments.

Your business depends on peak performance. Passive monitoring has its place. But as complexity grows and expectations rise, your approach to monitoring your network must also evolve. Add active monitoring to your toolkit to ensure a network that delights your users, no matter what the future throws at you.

CHAPTER 2

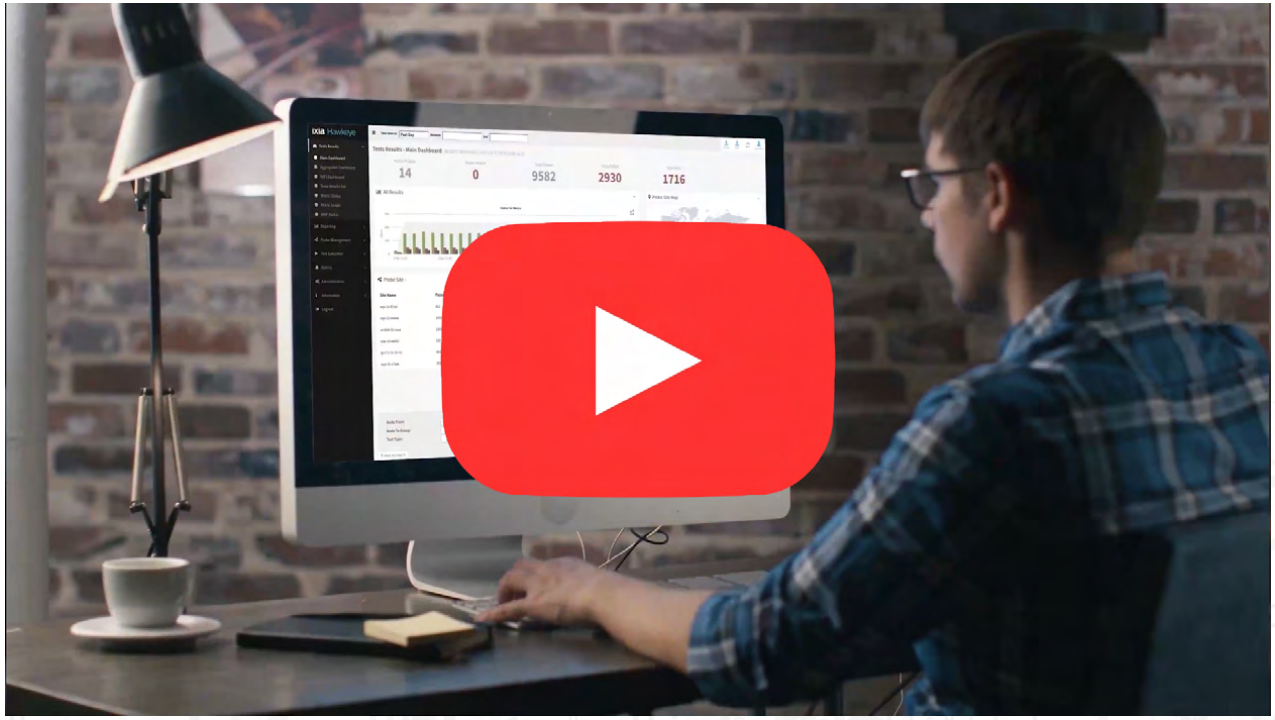
What is Active Monitoring?

Tech Tips with Packet Boi

When it comes to minimizing bottlenecks and service outages, you need to get ahead of network performance problems. Watch this short video to discover how active monitoring can help.

CHAPTER 2
What is Active Monitoring?

Tech Tips with Packet Boi



Source: https://youtu.be/aBSPzKMgTeo

CHAPTER 3

Take Five

Keysight's CIO Talks User Experience and Digital Transformation in IT

A conversation with Dan Krantz, Keysight's chief information officer, on monitoring distributed networks, leading network operations teams, and the evolving role IT plays in digital transformation.

CHAPTER 3

Take Five

Keysight's CIO Talks User Experience and Digital Transformation in IT

A lot has changed over the last few years. Remote work is here to stay, and hybrid architectures are shaking things up. But despite all that upheaval, one constant remains: user experience is as important as ever. That's why we sat down with Dan Krantz, Keysight's chief information officer, to get his thoughts on monitoring distributed networks, leading network operations teams, and the evolving role IT plays in digital transformation.

Dan Krantz
Chief Information Officer

1 Organizationally, how much importance do you place on user experience? In your opinion, how much effect does it have on the business as a whole?

We put a lot of focus on user experience in IT. In fact, two years ago, I started an employee recognition program called the Smarter IT Awards, where we hand out little Yoda statues because we're "battling the Dark Side" of bad user experience. The goal is to incentivize people to come up with new, Yoda-worthy ways to improve user experience through fewer clicks, faster response times, or clever automation. We have both a peer recognition award and one selected by management — and I always highlight the winners at my quarterly all-hands meetings. Then, at the end of the year, I present a Jedi Master award to someone who is not only battling the Dark Side of bad user experience but is also teaching others to do so as well.

User experience is so important, in my opinion, because bad user experience leads to wasted time. Time is the one resource we share with our competitors, and none of us can get more of it. So, the more time I can get people in Keysight to spend doing something productive, the more competitive we're going to be. Conversely, if people are less productive — wasting time on bad user experience or bad IT interactions — we're just going to be less competitive. I always tell people on my team, it's not really about people liking the systems and applications — or even liking IT, for that matter. If something looks and feels really cool but takes just as long to navigate through, it's not worthwhile. For me, the business value of user experience is all about time compression — and how much faster someone can get something done.

For example, as we help Keysight achieve its own digital transformation goals, our IT department is undergoing its own transformation. Whether an employee has an issue with a PC, wants to order a headset, or needs a user account on a reporting platform, we want to automate every one of those requests and fulfill them through an artificial intelligence (AI) engine. That way, if you put in a request and approval is needed, it's automatically routed to your manager — who simply needs to say "yes" or "no" before the action is autonomously fulfilled on the back end. Instead of taking days, it'll take hours or minutes. It's a real game changer. It's going to require everyone in IT to tackle things differently, automate a lot of stuff, and essentially turn us all into software engineers.

2 What are some of the most common challenges you've experienced with network monitoring and maintaining consistent quality of service?

The biggest challenge with network monitoring is trying to go beyond the basics. We are emerging from a place where we were very human-driven, relying on our outsourced partner to manually monitor and react to each switch, each router, and each circuit in our global network. To scale our growth, we've moved this in-house and begun automating. We want our systems and tools to inform us when there's an issue and, ideally, self-correct if they can. It's been hard enough to set up the basic, automated up / down tracking, but I really want to go beyond that. I want to measure performance at the raw level — like throughput, megabits per second, or latency — and measure the real user experience.

The other challenge is filtering out the noise, like false alarms. Now that we've moved past the human approach to a systems-based approach to monitoring, you have to get things configured properly. Otherwise, you can easily drown in meaningless alerts — and have to revert to people making sense of all the data that's coming in.

3 In your opinion, how do synthetic monitoring tools fit into a NetOps tool stack? Do they work well in concert with more passive tools, like packet-fed application and network performance management platforms?

Synthetic monitoring tools are where an organization needs to be. You want to get to the stage where you can really see the true user experience, but you need to make sure you have your basic table stakes monitoring in place first. Network monitoring is a stack, and synthetic monitoring tools are the next layer up. If you don't have a solid foundation — like your basic monitoring of availability, for example — who cares? You've got to get the basics right first and then implement synthetic monitoring for insights on user experience.

The challenge I see with synthetic monitoring tools is our new work-from-anywhere / cloud-connect-to-anywhere mode. As employees, we might be accessing systems on our corporate network, such as our data center, or maybe it's in a lab environment or systems in a manufacturing line. We might also need to access something in the cloud or a software-as-a-service (SaaS) application. But then you take your laptop, leave the office, and need to work from home for a while. Instrumenting synthetic monitoring there gets tricky because you need it on the endpoints. That's what users are taking whenever they connect to access things on the corporate network, in the public cloud, or through SaaS applications. The one constant is the endpoint. You need monitoring beyond your corporate network if you really want full resolution into the user experience.

For example, when everyone was working from home last year, we were fielding lots of escalations about individual applications not performing well. But the problem wasn't our network — it was employees' internet service providers (ISPs) or home Wi-Fi. One time, we were trying to play a video in an important virtual meeting, and it started glitching and freezing up. We'd tested it multiple times, but it turns out the person who was trying to play the video had suffered an internet outage in their neighborhood right at the same time. That's the real challenge right there. Even as we go back into the office, I think the idea of working anywhere is here to stay. So how can we use synthetic monitoring to understand the "real" user experience when people are transiting across all of these networks that we don't own?

4 With the proliferation of things like SD-WAN, edge computing, virtualization, and cloud, what challenges do you foresee in monitoring increasingly hybridized networks? How do you think organizations will evolve to meet these new challenges?

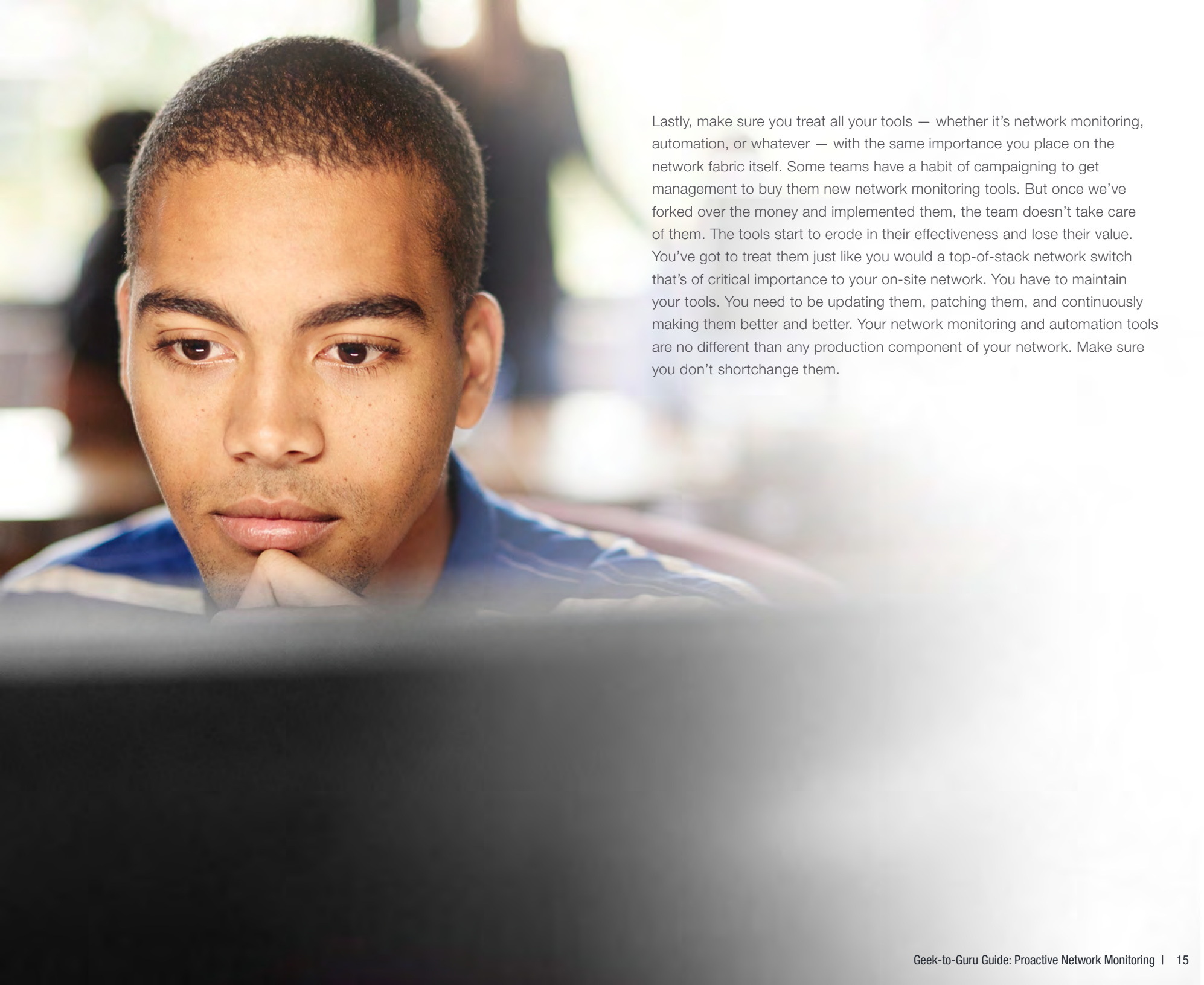
Since so many companies are stitching together various network providers, I'd love to see those providers start instrumenting their networks with APIs [application programming interfaces]. That way, companies like Keysight could tap into them to get insights and visibility into what's going on. Rather than just going to an ISP and seeing the standard red, yellow, and green network statuses, it would be really cool if they enabled companies like us to tap into the APIs of their network monitoring tools, so we could federate performance data across the ecosystem. Even if it were monetized, we might be willing to pay all the ISPs our employees use to tap into their APIs to see the performance of their networks. That way, we could better serve our employees who rely on those ISPs to do company work.

The other piece of the puzzle is the endpoint. Now we have to toy with the endpoint agent side of things. That's one of the ways we are getting at this problem here at Keysight. We're putting a small, unobtrusive AI agent onto all computers that tries to anticipate issues before users observe them. That way, we can utilize the agent's machine learning algorithms to predict problems before they occur — including in the network space — widening our aperture into what's going on from a performance perspective. In other words, we're coming at network performance from the endpoint versus from the network switch or infrastructure. Since we no longer own the physical network in all cases, we have to come at it differently.

5 If you could give a network operations team any piece of advice, what would it be?

To run a global network — where you have interconnected switching, routing, and fabric at each site — the only way to make it scale and run effectively is to start with consistency and standardization. For example, when Keysight acquires a company, we typically rip out whatever network they had and put in our network. Even if it works fine or better than ours, it's not the same. And for us to be able to scale and run a global network, it needs to have the exact same model of network switches and routers as us so we can standardize changes. That way, when we're going to make a small update and push it out, hundreds of devices are all going to take that change at scale. That's the way to run a network — making sure there's consistency and standardization across the board.

Then, when you have all that, you can start to build automation. So, instead of manually making changes — which can ruin a network engineer's weekend by forcing them to log on to hundreds of network switches and update each one individually — you need to have a way to just press a button and push out the change, so it propagates automatically. At the same time, that automation needs to be smart, so you have a way to roll things back if there's a mistake. I've seen issues where a company rolled out an application change that caused outages on our network. However, that same company showed us how, when they push out code changes, they don't just send it out to everyone at the same time. This particular application has over 130 million users at any given time, so they send out updates in what they call "rings." The change first goes to ring 1, then ring 2, ring 3, and starts to scale out. That way, if they detect a problem, they can contract it back in reverse order.



Lastly, make sure you treat all your tools — whether it's network monitoring, automation, or whatever — with the same importance you place on the network fabric itself. Some teams have a habit of campaigning to get management to buy them new network monitoring tools. But once we've forked over the money and implemented them, the team doesn't take care of them. The tools start to erode in their effectiveness and lose their value. You've got to treat them just like you would a top-of-stack network switch that's of critical importance to your on-site network. You have to maintain your tools. You need to be updating them, patching them, and continuously making them better and better. Your network monitoring and automation tools are no different than any production component of your network. Make sure you don't shortchange them.

CHAPTER 4

In Cyberspace, No One Can Hear You Scream

6 Reasons Why Your Users Might Be Suffering Silently

Network quality of service can make or break your business. Here are six of the most common factors can jeopardize user experience — and the practical steps you can take to prevent them.

CHAPTER 4

In Cyberspace, No One Can Hear You Scream

6 Reasons Why Your Users Might Be Suffering Silently

As technology and business intertwine in more and more complex ways, networks are becoming more than information delivery systems: they're strategic business assets. However, users are asking more and more out of the networks they use. When customers and employees alike demand unfettered access around the clock, surprises like service interruptions, downtime, and performance drags can be costly.

If you're not aware of your network's performance, your users could be suffering silently. It's only a matter of time until that problem comes back again. From lost revenue to declining productivity and eroding customer loyalty, the consequences of network issues are steep. The quality of your customer experience can make or break your business. You need to get out ahead of issues to maintain quality of service, but that isn't always easy.

Here are six of the most common factors that undermine user experience — and the practical steps you can take to prevent them.

1. Your Tools Aren't Seeing the Whole Picture

To say modern networks are "complex" is an oversimplification. Between cloud deployments, SD-WAN, edge computing, virtualization, and an increasingly mobile workforce, keeping tabs on network quality of service (QoS) introduces a significant level of additional complexity and cost. Since most traditional application performance monitoring (APM) and network performance monitoring (NPM) tools rely on packet data, you need to deploy the requisite infrastructure to capture it. Otherwise, you face a host of blind spots that can leave you unaware of service interruptions and performance bottlenecks.

However, challenges still abound. Deploying the necessary infrastructure to capture packets across your clouds, data centers, and branch locations is hard enough — and just the tip of the iceberg. First, you must secure any data sent back to your tools for analysis. Second, you must correlate that data across diverse network segments. Lastly, you risk budget and schedule overruns deploying passive probes in remote locations since there is no way to test remote access before going live.

ProTip

Be your own worst enemy

Unlike packet-based monitoring solutions, active monitoring tools make it easy to measure performance across your hybrid network infrastructure. For example, Keysight's Hawkeye uses lightweight hardware and software endpoints that can be deployed at the network edge, on client PCs, or in the cloud. With an array of monitoring endpoints deployed across your network, it's easy to simulate end-user behavior between cloud applications, data centers, branch locations, and more.

By shining a light in these hard-to-reach places, you can get a holistic view of user experience from a single tool. No costly infrastructure or complex deployments required. Moreover, since your network operations team is no longer exclusively dependent on live user traffic, you can conduct continuous monitoring simulations between any two locations or endpoints in your network.

With active monitoring, you get time-based data on uptime, throughput, delay, packet loss, and other indicators, so you can quickly spot trends and deviations. Actionable insights like these make it easy to fine-tune your network and keep things running smoothly.

2. You Aren't Looking at Things from Your Users' Point of View

Traditionally, network operations engineers collect data from network devices and management systems to assess uptime. Downticks may tell you it's time to upgrade equipment or indicate performance degradations. However, these metrics only reflect the availability of the polled element — not the overall user experience.

If you really want to see what your users are seeing, you need a different approach. Instead of passively collecting data, you need to regularly probe network elements using network- and application-layer tests that form a "heartbeat" to track responsiveness. These heartbeats monitor availability from an end-user perspective, rather than from your equipment. To achieve this, you need to monitor the same types of network behaviors as your users — enabling you to detect issues that impact them more accurately. Unfortunately, this is not feasible by probing individual components alone.

ProTip

Simulate real user traffic

While "what-if" scenarios like these aren't possible with traditional passive monitoring tools, they're quite simple to perform with active monitoring platforms. Because you're simulating real user traffic instead of waiting on it, you can see how network traffic volume, type, mix, or geographic location affects user experience. Since you can see how traffic moves through your entire network topology, you can measure user-centric key performance indicators (KPIs) on connectivity, network infrastructure, network services, calls out to the internet, and communications with cloud-based applications and service providers.

3. Your Network Operations Team Is Relying on Too Many Passive Tools

Traditional network monitoring is reactive. Your tools gather data from your production network and alert you when performance falls short. In the best case, you identify and resolve an issue before it affects end users. More often than not, however, users notice a problem before you do. You end up rushing to figure out what happened and get a fix in place.

Unfortunately, passive tools also fail to help you assess network readiness — which is critical to the success of new services and applications. For example, you know that migrating to the cloud will change traffic flow considerably, but how do you know for sure if you need to upgrade your network equipment? With a limited budget, it can be challenging to make that decision without having the data to back it up.

ProTip

Arm yourself with predictive intelligence

Active monitoring tools help you get ahead because they don't rely on real users to stumble across problems. Instead, continuous traffic simulations enable you to see what happens as network conditions change to pinpoint potential problems before they cause downtime. Armed with this predictive intelligence, you can proactively make changes to your network to prevent bottlenecks and latency from occurring — reducing the risk of downtime, application outages, and frustrated customers.

4. You Aren't Monitoring Bandwidth Proactively

Every day, your users use resources hosted across various cloud providers and on-premises data centers — all via the same access link. However, because those users span cities, countries, and continents, maintaining a consistent, high-quality user experience is increasingly difficult. Just as uplink and downlink speeds vary per location, so do service level agreements (SLAs) from different internet service providers.

Without adequate quality of service (QoS), your business applications suffer — especially those that handle voice and video. But that's only the start. Lost time causes operational inefficiencies, frustration, and lost productivity — which is especially true for users working from home because they lack direct IT support.

However, that does not imply that you cannot take back control. By measuring active bandwidth around the clock, you can be the first to know if any services are not getting enough bandwidth. Not only does this help you hasten troubleshooting with internet service providers (ISPs), it enables you to ensure the ISPs are meeting their SLAs, and you're getting the speeds you paid for.

ProTip

Set up continuous bandwidth monitoring

With realistic traffic-simulation capabilities, active monitoring platforms make it easy to take a predictive approach to bandwidth monitoring. By maximizing uptime and troubleshooting issues faster, you can ensure a consistent, high-quality user experience — for on-premises and remote users alike.

For example, here's how we recommend setting this up with Keysight Hawkeye.

- Create specific bandwidth checks for each site or location, with specific uplink and downlink targets to monitor QoS.
- Deploy hardware-, software-, or cloud-based endpoints anywhere in your network.
- Measure bandwidth on automated schedules, creating pass / fail thresholds for clear insight into bandwidth availability 24 / 7.
- Set up alarms to alert network operations and existing remediation systems.
- Track historical metrics and trends to identify potential causes of network bandwidth overconsumption, such as network changes or services.

5. You Aren't Monitoring Voice and Video Quality in Real Time

VoIP and video solutions offer significant savings for global organizations. These collaborative applications are critical for day-to-day business — both internally and externally — and you need to protect them at all costs. Not only must you ensure that services run continuously and with good quality, but you also must be able to proactively detect issues that can potentially affect end users.

Quality requirements for voice services are more demanding than standard data applications. These requirements make it harder for IT to maintain consistency, address drops in quality, and prevent service interruptions from jeopardizing user experience. Moreover, supporting a broad base of remote users can make things even more challenging. Without access to network infrastructure or SLAs with the service providers that supply their connectivity, you'll find that troubleshooting issues are often lengthy and painful.

ProTip

Actively validate service quality for VoIP and Video

Fortunately, active monitoring tools offer a cost-efficient solution. By deploying endpoints across all relevant network locations — such as headquarters, remote sites, and data center hosting gateways — you can validate service quality by continuously simulating VoIP calls and video traffic between sites. Plus, with real-time metrics such as mean opinion scores and pass-fail reports, you can quickly identify issues, troubleshoot them, and prioritize fixes.

6. Your Tools Aren't Doing Enough Heavy Lifting

As the volume and velocity of raw network and application data continue to increase, it's getting more difficult to identify when user experience is suffering. Basic equipment polling will tell you if something is online or offline, but problems are rarely that straightforward anymore. Even if you're conducting thorough user experience simulations, it can be hard to correlate raw performance metrics with actual network problems.

After all, there are only so many alerts a team can reasonably respond to, investigate, and prioritize. Unfortunately, with so much information coming from so many places, it's easy for even the most seasoned network operations teams to get overwhelmed.

ProTip

Leverage the power of automation and AI

You need to cut through the clutter. So let your tools do the hard work for you. With specific active monitoring tools, you can do just that. For example, Keysight's Hawkeye uses machine learning to help network operations teams make sense of their increasingly complex networks. With automatic threshold and outlier detection, you get immediate notifications to any potential problems. An outlier dashboard enables fast drill downs and root-cause analysis, while flexible sensitivity criteria make it easy to customize alerts to match specific quality thresholds.

It's Time to Stop Fighting Fires — and Start Preventing Them

Whether you are a network engineer or a CIO, driving change in IT is never easy. As budgets tighten and the business presses for faster fixes and better performance, reacting to problems is not sustainable. You need to get ahead of network issues. That's why it is so important to take a proactive, user-centric approach to network performance monitoring. As legacy infrastructures continue to integrate with new technologies, networks will only get more distributed and complex — underscoring the need for a versatile, hybrid-friendly solution.

At the end of the day, your users' expectations are clear. They want a network that works — providing consistent QoS with minimal service interruptions or latency. However, that's easier said than done, and pushes passive monitoring tools past their capabilities. That's why an active monitoring solution is critical to keeping your network in good health. Instead of worrying about downtime and outages that could bring your systems to a standstill, you can detect, identify, and remediate potential problems long before anyone outside of your department even knows they existed. By contrast, the only thing your users will experience is sublime satisfaction.

Information is subject to change without notice. | 7121-XXXX.EN © Keysight Technologies, 2020 - 2021 | Published in USA, June 24, 2021 | keysight.com