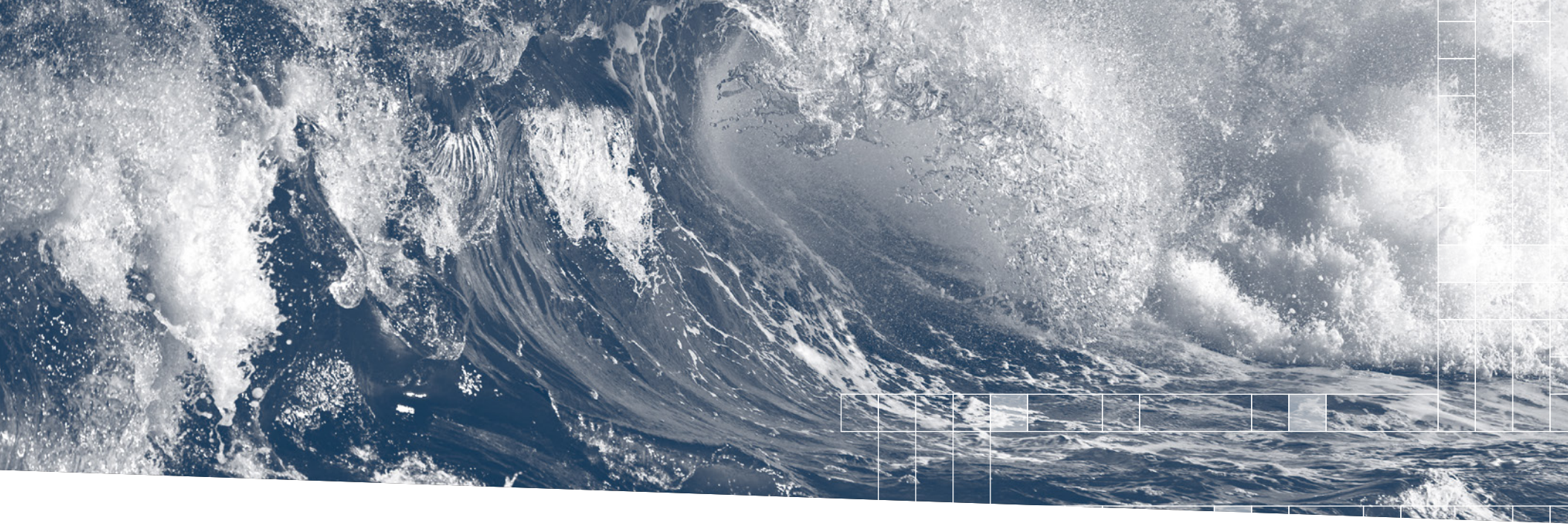
Why You Need Independent SD-WAN Visibility

sinefa

Introduction

SD-WAN is an inevitability for most enterprise networks as organizations undergo digital transformation. As SD-WAN matures in the market, end-user organizations, and the Managed Service Providers (MSPs) that many of them rely on for wide area network service management are realizing the need for new forms of network visibility. The reason is simple. SD-WANs enable new network architectures that feature heavy use of the Internet, an uncontrolled and unpredictable infrastructure. The Internet creates new blinds spots that traditional monitoring solutions don't adequately address. And those blind spots mean that your SD-WAN deployment, application performance, user experience, and business outcomes are at risk of disruptions that you won't be able to resolve effectively. That is unacceptable for IT leaders and a nightmare for network managers.

SD-WANs require a new type of visibility to cover these blind spots. In this ebook, we'll cover five critical aspects of SD-WAN visibility that can ensure the success of your planning, deployment, and ongoing network operations.



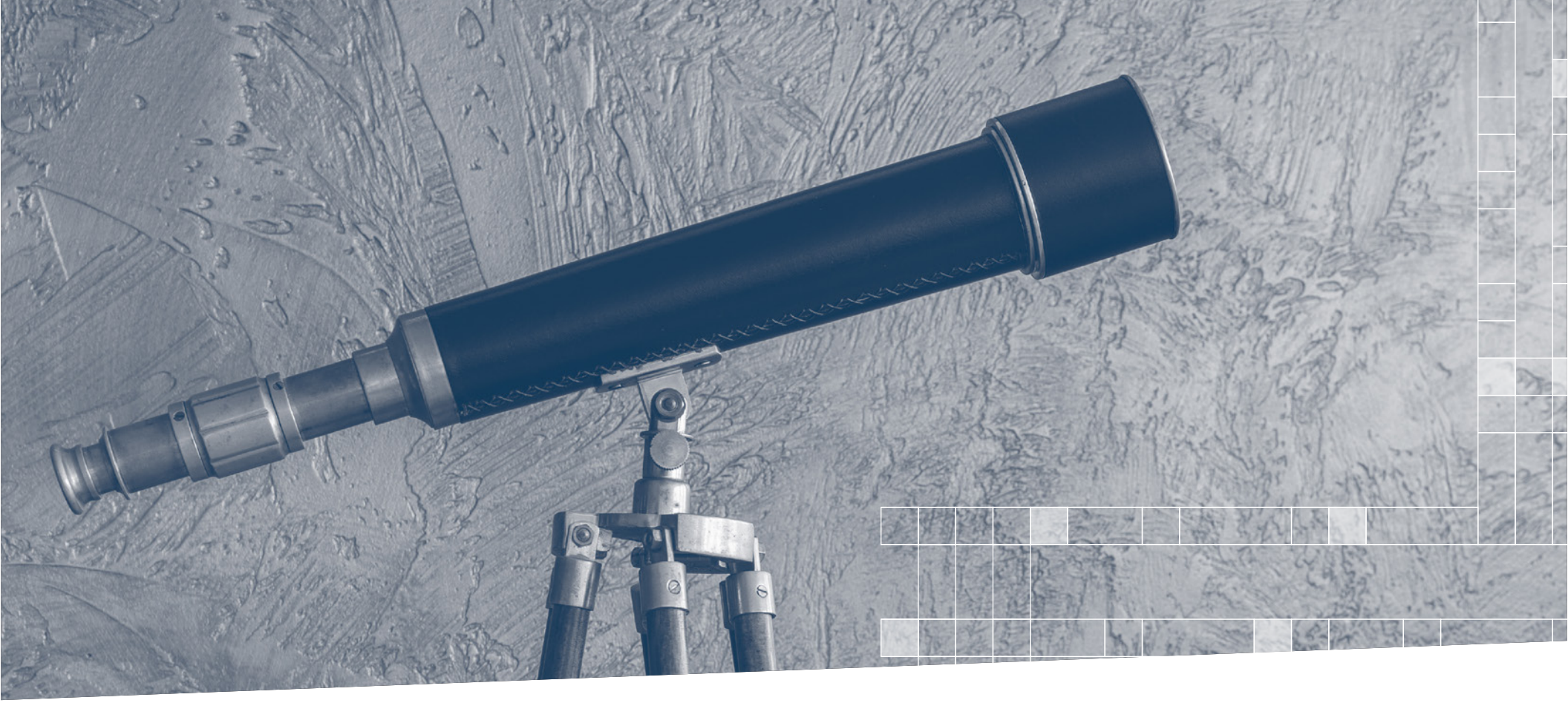
The inevitability of SD-WAN

According to many industry analysts, one of the things that has become clear is that there is literally nobody they're talking to who isn't turning to SD-WAN solutions from Cisco, VMWare, and others. Modernizing the enterprise WAN edge using SD-WAN technology has taken hold for a variety of reasons. First is the opportunity for steep cost savings by moving off MPLS circuits to lower-cost Internet connectivity. Second, Direct Internet Access (DIA) from branch offices improves cloud SaaS application performance. The reason is, instead of paying a latency penalty from backhauling traffic through data centers, connectivity can go straight to increasingly built-out cloud provider network edges. DIA connectivity makes a ton of sense, given how enterprises have increasingly moved to a SaaS and multi-cloud world. Third, SD-WAN orchestration provides an automated approach to traffic steering across various links. For example, sensitive and critical applications like inter-office VoIP RTP streams could be steered and given priority QoS treatment over MPLS links, while Office 365 goes via DIA. This automation makes network operations more effective and efficient. Finally, SD-WAN is proven. Voluminous case studies showcase enterprises that have deployed SD-WAN technology, and who have found it to be effective at meeting their connectivity use cases.

SD-WANs don’t control the Internet

Despite their benefits, SD-WANs do come with a significant catch--reliance on the Internet. The Internet is vast, comprised of thousands of service provider networks connected in a continuously changing fashion. Internet routing can change unpredictably and cause sub-optimal network paths that pull application traffic around the world rather than across the street. Unlike MPLS services, the Internet doesn’t offer you an SLA. You will only have direct relationships with a subset of the providers your application traffic crosses. So it’s your responsibility to make sure you can manage that complexity.

Overlay tunnels do a nice job of simplifying how all that complexity looks to SD-WAN policy engines. However, the Internet, as an underlay transport, is highly diverse, complex, and unpredictable. SD-WAN orchestration can temporarily choose one path over another in the case of a glaring performance disparity. But if you have ongoing Internet performance issues, SD-WANs can’t help you resolve those because they simply can’t see details of the Internet underlay.



Legacy network performance monitoring doesn't cut it

A central economic and performance premise of SD-WANs is to take advantage of Internet connectivity to data centers and cloud services. If we accept that the Internet lies outside of the realm of IT controls, then by definition, network monitoring that only focuses on IT-managed infrastructure leaves a considerable visibility gap. Trusting your critical applications to hundreds of different provider networks (including ISPs, SD-WAN, cloud-based network security, and SaaS providers), without any way to troubleshoot and find the root cause of problems, is putting your business at risk.

SD-WAN visibility must be independent

One of the misperceptions about SD-WAN visibility is that the reporting tools included within SD-WAN solutions are sufficient for network operations. Let's be clear that what we mean by "independent" is an overlay of visibility that includes but goes well beyond the measurements and metrics used by SD-WAN solutions to power their control planes and provide performance reporting.

There are three main reasons why you need to take visibility beyond SD-WAN monitoring and SD-WAN vendor tools.

Transport visibility:

You need an independent way to understand the behavior and performance of SD-WAN transport--most importantly, Internet connectivity and network paths.

User experience:

SD-WAN visibility must go beyond network performance metrics and take into account application visibility and user experience insights because all the cost savings in the world won't matter if your employees can't be productive. Now, this may seem a bit controversial because many network teams and service providers focus primarily on network performance metrics. But increasingly, any IT investment has to have a line of accountability to business outcomes. Due to digital transformation, user experience is a critical business outcome.

Full service delivery chain:

Visibility must cover all the most essential pieces of the delivery chain from users to apps. It's not enough to monitor from WAN edge to WAN edge. You need to see from end-user devices, through wifi connectivity and local branch office or home LANs, across overlay tunnels, over underlay transport including the Internet, to applications. SD-WAN vendors can't give you the depth of metrics and comprehensiveness you'll need to ensure success.

MSPs need independent visibility to deliver on their SLAs

Globally speaking, MSPs will provide the majority of SD-WANs, and MSPs generally offer more than one SD-WAN solution. If you're an MSP, you'll want to have an independent way to ensure service delivery, no matter which SD-WAN vendor is in play. Furthermore, as an MSP, you're on the hook for service performance, even though you depend on many third-party providers to transport your clients' traffic. Without a fast, independent way to establish your network's innocence and find the root cause problem domain, you will likely get the blame for tons of problems that are not your fault, with no way to help clients resolve them. But in-depth visibility isn't just a defensive move. It's a value-added offering that customers will recognize is worth paying for as part of their service assurance strategy to offset the risks of depending on lower-cost Internet transport.

5

SD-WAN visibility keys

Here are five essential aspects
of SD-WAN monitoring:

1 Overlay and underlay network path visibility

Network path monitoring is simply a must for SD-WANs. Network path monitoring means synthetically measuring on a scheduled or on-demand basis from branches or end-user devices, hop-by-hop through every Layer 3 network device in every network domain, and seeing end-to-end and per-hop network performance metrics. With network path visibility, you can get a visualization that will tell you whose network is having the issue: your internal network, an ISP, or the SaaS provider. This speeds Mean Time To Innocence (MTTI), shows you which provider to escalate to, and gives you the data you need to solve problems and reduce Mean Time to Repair (MTTR).

Some simple math can help illustrate the need. Let's say you have twenty branch offices, two data centers, and ten essential SaaS apps. So 20 branches x 12 DCs and SaaS providers = 240 network paths that matter to your business. Let's assume that for each branch office to DC/SaaS path, traffic crosses an internal network, 3 ISP networks, a cloudnetwork, or six networks in total.

240 network paths x 6 networks = 1440 networks that you're relying on to deliver excellent user experience. Let's say you have traditional network monitoring, so you can only collect information from within your 20 branch offices, and you can't see both overly tunnel paths and the underlay transport paths on a hop-by-hop basis. That means you're dealing with 1420 networks that could impact your business, for which you're completely blind.

Remember that network paths change within the Internet in unpredictable ways. You can't just take a one-time snapshot of your network paths, draw them in a Visio diagram, and think you're equipped to troubleshoot problems because that snapshot will be irrelevant in no time flat. You need to see the paths in real-time, as they change, so you can figure out where packet loss, latency, and jitter are occurring when your users are being impacted. So let's say that over a month that you're going to see a 20% rate of change in your network paths. 1420 invisible networks x 150% = 1704 networks per month that you may need insight into to solve problems, for which you're blind. Does that sound like a recipe for successful network operations? If you don't think so, then you'll agree that network path monitoring is a necessity for SD-WAN operations.

2 Real-time, real user traffic visibility

Network path monitoring is critical, but don't forget that you still have branch offices, data centers, and cloud VPC networks. Combining network path visibility with on-premises insights into app experience and network performance means that once you isolate the network problem domain, and your internal network is where the problem is occurring, you can go deep and discover the root cause. The way to do this is by analyzing real user traffic in real-time. Is there a congestion issue in a branch office? Being able to see exactly what or who is consuming that bandwidth rapidly allows you to catch intermittent problems that can bedevil user experience. Synthetic monitoring is critical, but monitoring isn't complete without looking at real - and real-time - user traffic.

3 Visibility from the end-user

SD-WANs may primarily serve edge-to-edge connectivity, but user experience doesn't start or end there. The goal is to ensure that the WAN serves the user experience and productivity needs of your employees. So, you need to see from the perspective of individual users because their devices, wifi, and LAN performance all can impact the user experience. It does you no good to declare that the "WAN is fine" and "all the lights are green" when users can't do their work. Is there an issue with OS version non-compliance that's potentially causing problems? Are metrics like memory, CPU, and storage indicating an issue on the device itself? Is there a wifi signal health issue in the office or at a home office? Is a home user's wifi signal just fine, but the path from that end-user to an app clearly shows that their home broadband gateway is dropping packets, perhaps because of conflict with Netflix or gaming youths? You need to see all of these issues.

The focus on remote worker user perspective may seem a bit strange because SD-WANs are typically thought of as solely connecting branch offices. However, SD-WANs often pair with cloud-based security from companies like Zscaler, Netskope, and Palo Alto Networks. Those cloud-based security schemes include ways for both branch offices and remote users to connect securely (via overlay tunnels) to cloud apps and services. Your overall SD-WAN architecture is increasingly encompassing home and remote workers, which means you need visibility from every user device from any location.

4 App experience visibility

Delivering great user experiences for every vital application is the goal of IT today. So an SD-WAN monitoring scheme must go beyond troubleshooting network conditions and place user and app experience as a central focus. That means that you should be able to easily track experience scores for the applications that matter the most to your organization. You should be able to scan your user locations and experience scores geographically, in lists, in heatmaps, and other visualizations to make sense of patterns. You should be able to organize app group dashboards that correspond to key stakeholders. For example, your call center uses a particular set of applications, and any degradation in those will impact customer service, which can damage brand loyalty and long-term revenue. Track those call center apps and give an overall score to them so you can see how you're delivering.

Again, a focus on app experience isn't typical for the way most network teams have been guided to think. But digital transformation means that every part of the IT organization needs to focus less exclusively on the assets that they're managing and put more attention on the user and business outcomes.

Finally, understanding your app experience scores should be easy. You should be able to see how scores are changing over time. But how do you know if your range of scores is "good?" You should also be able to compare your experience scores to industry or collective benchmarks on an app-by-app basis so that it's easier to judge where you stand vis-a-vis your peers.

5 The user needs to be at the center of IT service delivery

SD-WANs aren't just about the end-user, branch offices, and SaaS applications. They also connect your data centers and public cloud instances where you host critical employee-facing applications. Modern applications are composed of distributed microservices. If communication between those microservices gets disrupted, applications break down. In a sense, those microservices are also "users" of your SD-WAN, and one microservice may play the role of an "app" to another microservice. So, you need to see the "experience" that microservices are getting from other microservices.

Let's take the example of a scheduling system to dispatch service technicians. The front-end is built in AWS or Azure. The back-end runs in a data center, accessing proprietary records sitting in your supply chain system. API calls from your data center to Salesforce tie in customer data. Other API calls tie in mapping and weather information. If your front-end can't reach the back-end over an SD-WAN tunnel between AWS and your data center, or if the back-end can't reach the Salesforce API to look up customer data for example, then the service call and dispatch process break down. Without sufficient visibility across those inter-service communication paths, you'll be lost and unable to resolve the issue and restore the service.

That's why you should monitor network paths between data centers, cloud VPCs, and third party API endpoints for critical services (like CRM or other integrations). This way, if something breaks down within that path, due to an ISP or SaaS provider network issue, you can find and fix things fast and keep your mission-critical applications running.

Again, it may be easy to ignore this scenario when looking at SD-WAN visibility. However, if you have mission-critical, internal applications that depend on your WAN, possessing in-depth visibility will make a material difference to the business.

Sinefa: holistic SD-WAN visibility

Sinefa offers comprehensive digital experience monitoring (DEM) visibility into SD-WANs. Our approach includes probe-based real user traffic analysis and synthetic network path monitoring from branches, DCs, and cloud VPCs. It adds Endpoint Agents that deliver real-time end-user experience insights into device and wifi health, plus on-demand network path monitoring to see whether local LAN, upstream ISP, Internet, or cloud networks are causing issues. You get visibility into user experience no matter where users sit. Learn more about our Digital Experience Monitoring solutions and request a demo today at www.sinefa.com.

sinefa

2445 Augustine Dr, Suite 150
Santa Clara, CA 95054
+1 (650) 618 0183

www.sinefa.com

About Sinefa

Sinefa is a digital experience monitoring platform that delivers visibility into the entire service delivery chain from endpoint devices across internal and external networks, through applications and APIs, enabling you to plan smarter, deploy easier, resolve issues faster, and run your business smoother.