

WHITE PAPER

Eliminating the Blind Spots Introduced by Today's Hybrid, Multi-Cloud Environments



Eliminating the Blind Spots Introduced by Today's Hybrid, Multi-Cloud Environments

TABLE OF CONTENTS

Executive Summary

Introduction: Proliferating Cloud Adoption

Visibility Challenges Presented by Cloud Environments

A Modern Solution for Cloud Monitoring

Conclusion

Executive Summary

The adoption of cloud-based services continues to grow more widespread. While this cloud adoption provides dramatic business advantages—it also provides significant challenges for IT and network operations teams. This paper offers a detailed look at the monitoring blind spots today's teams are struggling with, and it reveals how an active monitoring approach can help.

Introduction: Proliferating Cloud Adoption

In response to rapidly evolving market, business, and workplace dynamics, enterprise IT has seen fast, dramatic shifts. One of the most significant impacts is related to the shift to the cloud, which is accounting for an increasing share of IT spending. Gartner analysts estimate that by 2025, 51% of IT spending will have shifted to the public cloud. When it comes to application software, the number is even higher, with spending in the cloud expected to grow to 65.9%¹.

Now, hybrid, multi-cloud approaches are the norm. Organizations are running a mix of on-premises infrastructure and multiple cloud offerings. This hybrid approach provides business leaders with enhanced flexibility. Now, leaders can choose the approach that's optimally aligned with specific workload characteristics, security and performance requirements, budgetary objectives, and more. Through multi-cloud approaches, teams can achieve such objectives as avoiding vendor lock-in, increasing resilience, and reducing costs.

¹ Gartner, "Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025," February 9, 2022 <https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>

VISIBILITY CHALLENGES PRESENTED BY CLOUD ENVIRONMENTS

For IT and network operations teams, the impact of these transitions has been significant, introducing mounting challenges. While reliance upon these dynamic, hybrid and multi-cloud environments continues to be increasingly business critical, operations teams continue to contend with dwindling resources, decreasing visibility, and a lack of control.

In the wake of these transitions, the role of IT has evolved and expanded. Now teams must do cloud monitoring, and they must gain visibility into the network delivery paths between users, managed infrastructure, cloud environments, and business-critical applications. The sections below outline some of the key challenges teams confront as they seek to address these requirements.

What is Active Monitoring?

Traditional monitoring is passive. It relies on aggregating metrics drawn from owned devices. SNMP and flows are the primary ways to capture this data. More modern tools can also gather Border Gateway Protocol (BGP) data from public sources. In contrast, active monitoring sends test packets out periodically over the network (whether owned or third party) and measures the responses to understand performance. Active monitoring can be configured in a single-ended or dual-ended fashion. With single-ended approaches, you have a source of monitoring, typically behind your firewall, and you test connections to a target. In dual-ended configurations, you deploy monitoring software or hardware on both ends, provided you can deploy them there. With this approach, you can gather data for both outbound and inbound routes.

North-South Dependencies

Now, users are commonly either accessing apps running in public clouds or third-party SaaS apps. Given this reality, IT teams must typically first contend with so-called “north-south” dependencies. These are commonly associated with scenarios in which users are accessing applications or services that are located in the cloud. To do so, they rely on network delivery paths that consist of the end-user environment, ISP and transit provider networks (which are increasingly running technologies like SD-WAN), and network routing within the actual cloud environment. The reality is that much of that delivery path lies outside of IT’s control. However, the burden of troubleshooting availability, performance, and end-user experience issues still falls on IT.

When performance issues arise, IT teams encounter significant challenges in trying to pinpoint where the issues are. Often, they spend an inordinate amount of time trying to determine whether the cause is related to an application or the network. They are tasked with solving issues for apps and infrastructure they don’t own or control. Even when apps are running smoothly, third-party network delivery chains can still represent a black box. It is only when IT teams determine where the issues are occurring that they can understand who can fix them.

When application status pages and passive device monitoring tools indicate that everything is performing adequately, teams need to be able to isolate the specific network hop in which the issue is arising, including if it occurs in a third-party ISP or cloud network. This includes the last-mile network operators that IT teams don’t have any formal relationship with. Traditional monitoring approaches can’t offer this visibility. Fundamentally, the only way to achieve this is through an active approach to monitoring.

VISIBILITY CHALLENGES PRESENTED BY CLOUD ENVIRONMENTS (cont.)

Monitoring East-West Performance

As the use of cloud services evolves, IT teams often must contend with a new challenge: understanding the reliance on network connections between cloud environments, which is commonly referred to as “east-west” traffic. This east-west traffic occurs when data is being passed between cloud-based apps or when end-customer facing apps are built on a multi-cloud architecture. In either case, IT is often involved in troubleshooting issues that arise.

Every cloud provider has interconnects, which are often composed of dynamic routes and short-lived infrastructure. The routes in use or available between cloud providers are also changing minute to minute. Trying to stay on top of the performance of these interconnects is simply too time consuming for internal IT teams. IT teams don’t own any of the infrastructure associated with this east-west traffic. That is why active, bi-directional monitoring becomes critical.

For east-west network monitoring, an active approach is the only way to truly understand the application or end-user experience. Passive monitoring methods are limited to the endpoints managed by the enterprise. In addition, they’ll likely limit the metrics available to throughput and packets received and sent.

Regardless of your dependencies, the nature of cloud monitoring is changing rapidly. In order to be able to react quickly and effectively when issues arise, your operations teams must be able to observe the full breadth of the enterprise footprint.

ISP Validation

The move to hybrid working environments, decreased costs, and increasing capacity demands have led most organizations to move from MPLS to ISP networks. The swift connectivity and ease of use offered by ISPs has made this an increasingly clear-cut decision with organizations able to spin up new locations in a fraction of the time. However, while this move means teams can avoid the traditional wait times and low bandwidths of MPLS connections, it also means teams lose the guarantee of performance those old connections came with. Without guarantees, IT operations must take responsibility for understanding when ISP connections are not meeting their performance SLAs.

VISIBILITY CHALLENGES PRESENTED BY CLOUD ENVIRONMENTS (cont.)

SD-WAN Validation

While technologies like SD-WAN have provided resilience by pairing connections together, there is still little IT teams can do without actively monitoring connectivity from enterprise locations. By actively monitoring overlay and underlay networks, IT teams can validate the SD-WAN solution is performing as configured, and they can identify where in the underlay network issues are occurring that may be triggering failovers.

Hybrid Work Monitoring and Troubleshooting

In supporting hybrid work users, IT teams inherently lack visibility into residential and last-mile ISP networks. Consequently, it takes tremendous amounts of time to monitor and troubleshoot issues. Active monitoring is therefore critical.

A MODERN SOLUTION FOR CLOUD MONITORING

Complete Visibility for Any Network

You are moving your infrastructure, apps, and workloads to the cloud for a reason, but losing visibility isn't one of them. Let Broadcom provide the application, user, and network visibility that gives you confidence in your operations. NetOps by Broadcom is device and deployment agnostic, using active and passive monitoring technology from purpose-built AppNeta Monitoring Points. The solution provides performance monitoring for any cloud architecture and over any network, so you can enhance network visibility across your organization. Place our Monitoring Points on premises, inside virtual hosts, on end-user workstations, or next to the code.

Public Cloud

Use the cloud that suits your business best. Rest assured that AppNeta can offer unparalleled network visibility into AWS, Azure, Google, or any other cloud environments. Using any public cloud provider, your traffic will pass through hops on the open internet and then hit the firewall of the provider. What happens beyond that firewall is a mystery to BGP-based solutions. AppNeta can show you where your data goes when it traverses any cloud provider's networks, including those that are software defined.

A MODERN SOLUTION FOR CLOUD MONITORING

(cont.)

Hybrid Cloud

Monitor all networks, from offices to traditional data centers to the cloud. AppNeta offers bi-directional monitoring for any connection to identify congestion between your users, data, and locations. With applications split between data centers, cloud providers, and remote locations, you need better visibility into what your users are experiencing. Congestion, delays, and jitter can kill business-critical applications. If you are not looking at the whole picture, end to end, then you'll waste precious hours troubleshooting the root cause of performance issues.

Private Cloud

SNMP can tell you if an app or network is running, but AppNeta ensures that it's running smoothly and enables IT to deliver digital experiences that drive your business forward. Complex private cloud deployments need active network monitoring between hosts, data centers, and office locations. Moving your data out of your office and into a data center adds physical and logical distance between your apps and your end users. Latency will increase, but with AppNeta you can ensure that the end-user experience doesn't suffer.

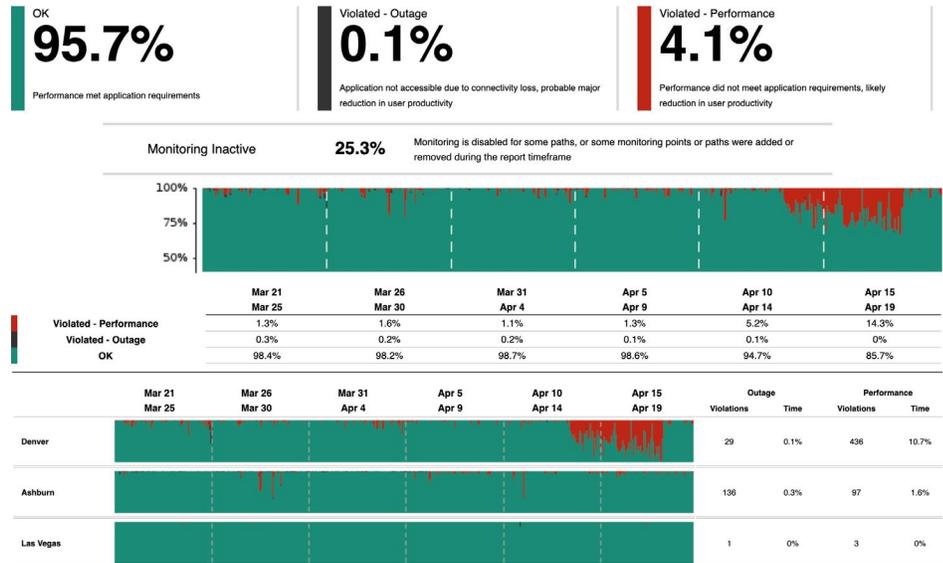
ISP Validation

NetOps by Broadcom provides insight into the performance of hybrid workers' local networks and last-mile ISPs, helping IT quickly understand the location and root cause of performance issues.

As an example, a large cell phone provider in the US is working with AppNeta to validate availability and network capacity across thousands of retail stores. By using active monitoring to continuously test the network, their IT team can identify which ISP is in use at any single store that is experiencing issues. Further, they can look at historical records of availability and capacity metrics to isolate overall performance against the contract for that store. The solution offers dashboards that show regional performance. Given the wide territory the IT team must cover, this visibility is essential in helping them focus their efforts on the most business-critical issues, instead of the areas generating the most alarm noise.

A MODERN SOLUTION FOR CLOUD MONITORING

(cont.)



Flexible Cloud and On-Premises Deployment

Modern infrastructures are virtualized, flexible, and complex. We offer options that make sense in your environment so that you can tailor your monitoring deployment accordingly.

AppNeta can be delivered as a service that is accessed from our public cloud. Alternatively, customers can deploy the solution in their own environment. Deployments consist of Monitoring Points and the AppNeta service.

When you're implementing AppNeta, you'll get access to our full array of monitoring and testing capabilities. AppNeta will consult with your teams to help you deploy in the best network locations possible. We can help ensure you gain the most comprehensive coverage, both in the near term and as your network evolves.

Our platform makes it easy for you to monitor business-critical applications in public, private, or hybrid cloud infrastructure. The server is continuously fed performance data from any number of Monitoring Points deployed across your data center, office, or home office environments. Each Monitoring Point can monitor business critical apps and services, and it can track traffic to and from other locations. Licensing is simple, and is based on deployment locations and business-critical applications monitored.

A MODERN SOLUTION FOR CLOUD MONITORING

(cont.)

Secure Deployment

AppNeta uses industry-accepted best practices to secure deployments. The solution features security groups, firewalled ports, SSH-key-based machine logins, and key rotation. Data access is restricted solely to specific Broadcom employees, all of whom are under strict confidentiality agreements. Only key engineers may access production data, and then only as a last resort for debugging data-related issues. In addition, support engineers may access your web console to provide guidance as a result of specific incidents or requests. AppNeta uses standard encryption practices to make sure that the information held in your packet captures is securely transmitted and stored. Captures must be decrypted using the symmetric key created from the passphrase established.

CONCLUSION

For any given user, at any given minute, many different networks may be relied upon—and many environments are outside of your internal IT team's control. AppNeta provides the active monitoring capabilities that teams need today to contend with these new realities. By employing AppNeta, your teams can gain the timely intelligence they need to streamline troubleshooting, speed remediation, and boost service levels—no matter where your users are based or which networks they are relying upon.

To learn more, you can **request a demo** to see how AppNeta can give you control of your cloud performance.