

CASE STUDY

Kyndryl Boosts Monitoring Scale by 50%, Optimizes SD-WAN Performance and Patient Care

Kyndryl

CLIENT PROFILE

Company: Kyndryl

Industry: IT infrastructure services

Employees: 90,000

Annual revenues: \$17.0 billion

CHALLENGES

Ensuring optimized user experiences, even as user traffic gets increasingly reliant upon a complex mix of legacy infrastructure, SD-WAN, cloud, and ISP networks.

SOLUTION

Combining DX NetOps with AppNeta, the team is able to monitor connections between data centers and cloud services and between hybrid workers and cloud environments.

BENEFITS

- Reduced alarm noise
- Accelerated root cause analysis and resolution
- Improved monitoring scale by 50%

Business

Kyndryl is the world's largest provider of IT infrastructure services, serving thousands of enterprise customers in more than 60 countries. The company has 4,400 customers, including 75 of the Fortune 100.

The company designs, builds, manages, and modernizes the complex, mission-critical information systems that the world depends on every day. Kyndryl was formed when IBM spun off its Global Technology Services division in 2021.

The company features six globally managed service areas, including network and edge computing. Customers are highly reliant upon these outsourced network operations. Given the business-critical nature of their outsourced network services, Kyndryl establishes strict SLAs with clients. These SLAs hold Kyndryl's team accountable for service levels, and, if issues arise, the team can be exposed to financial penalties and other negative ramifications.

Challenges

Modern networks have introduced fundamental new realities for the IT operations team at Kyndryl. Following are a few of the key shifts that have occurred:

Work from Anywhere

Early on in the pandemic, the IT operations team had to rapidly adapt to approximately 20,000 of the organization's employees starting to work remotely.

Cloud

In recent years, clients and teams across Kyndryl have continued to adopt cloud services for a range of workloads. As a result of this move, users have increasingly become reliant on many networks that the IT operations team doesn't own or manage. This introduced an entirely new level of complexity to troubleshooting.

"With the move to the cloud, pinpointing network issues started to feel like trying to find a needle in the haystack," said one of Kyndryl's senior infrastructure architects.

“With the move to the cloud, pinpointing network issues started to feel like trying to find a needle in the haystack.”



Software-Defined Networking

In recent years, Kyndryl has expanded its adoption of software-defined networking technologies, including SD-WAN. For example, for one of their healthcare clients, they now have implemented SD-WAN to provide secure, cost-effective connectivity between nine data centers and hundreds of medical clinics.

The team had previously relied upon traditional monitoring approaches and tools from technology vendors, including SD-WAN vendors. With these tools, teams were left with blind spots, and couldn't track end-to-end delivery paths of user connections. Further, the team has been contending with spiraling volumes of alarms.

Given all these trends, user experiences are now reliant upon a dynamic, complex set of internal network infrastructure and third-party ISP and cloud networks. This has left the team increasingly exposed to downtime and performance issues.

Solution

DX NetOps

To monitor the large, complex networks of clients and the business, the IT organization turned to DX NetOps by Broadcom more than 10 years ago. Over that time, the team has continued to grow increasingly reliant upon these capabilities:

- **DX NetOps Fault.** DX NetOps Fault provides Kyndryl with enhanced stability for monitoring and alerting. In addition, the team leverages the solution's capabilities for network event correlation, topology views, and reduced alarm noise.
- **DX NetOps Performance.** DX NetOps Performance provides network performance analytics that deliver advanced visibility into customer SLAs, so the team can intelligently track how Kyndryl is adhering to contractual agreements for network availability.
- **DX NetOps Flow.** DX NetOps Flow equips Kyndryl with enterprise-wide visibility into application traffic on every link and enables early detection of abnormal traffic patterns.
- **DX NetOps SDN.** With DX NetOps SDN, the IT organization reduced the challenges and risks associated with delivering services over their SD-WAN environments. This includes critical services for healthcare clients, whose medical staff and patients are now highly reliant upon SD-WAN-based networks. It also provides differentiated capabilities for correlating underlay and overlay metrics, automating SD-WAN configurations, and doing zero-touch provisioning.

With these capabilities, the team can quickly identify the source of performance problems, validate the impact of planned and unplanned changes within the network, and avoid unnecessary WAN costs.

AppNeta

DX NetOps provides visibility into the network underlay and overlay within their data centers. In addition, to gain a clear picture of end-to-end network performance, the team also needed to expand this coverage beyond the network edge, and gain visibility into ISP and cloud

“The team had previously relied upon traditional monitoring approaches and tools from technology vendors, including SD-WAN vendors. With these tools, teams were left with blind spots, and couldn’t track end-to-end delivery paths of user connections.”



environments. They also needed to see how the SD-WAN platform itself was performing, tracking CPU utilization and whether it is dropping packets or exceeding performance thresholds.

To gain the required visibility, the team has started working with AppNeta by Broadcom, completing a successful implementation in their healthcare client’s SD-WAN environment.

Combining DX NetOps with AppNeta, the team is able to monitor connections between data centers and cloud services and between hybrid workers and cloud environments. AppNeta provides hop-by-hop visibility across cloud environments, enabling the team to get essential visibility into application response, network response, and retransmission time.

By combining this overlay and underlay visibility, the team is able to get a unified picture of how the environment is performing. This visibility provides a number of advantages.

“Broadcom helps us intelligently focus our triage efforts and enables us to confidently validate SD-WAN performance,” a senior infrastructure architect explained.

Unified Visibility

With AppNeta and DX NetOps, the team at Kyndryl established what are internally referred to as site pages, which are unified SD-WAN dashboards that present all the relevant network metrics being collected. These site pages provide teams with actionable insights into the performance of their SD-WAN networks and the quality of the user experience.

They have views defined for multiple data centers and remote sites. In one unified operational dashboard, they can view these remote sites and key connection paths.

Any time someone complains about slow response or downtime, operators can come to these pages to investigate whether the issue is in their domain or in a network managed by a third-party ISP or cloud provider. With Broadcom solutions, the team has correlated visibility of both the overlay and the underlay. Following is more information about the views in each section.

Underlay Section

In this section, administrators can track these aspects:

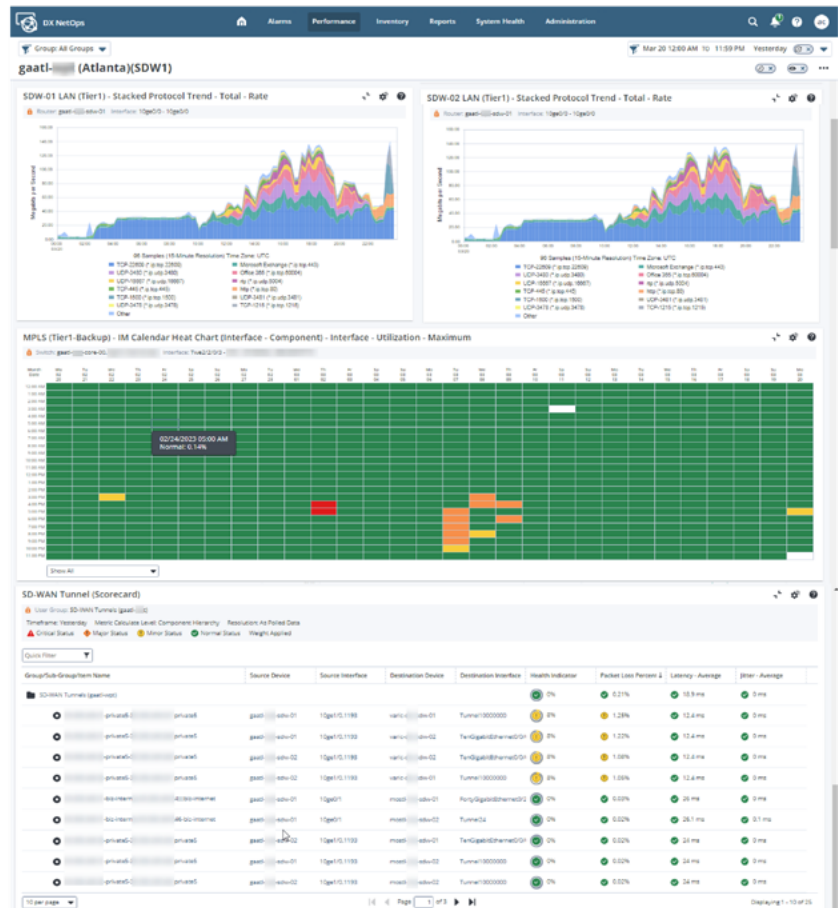
- **Interface utilization.** Teams can track utilization on interfaces that connect to SD-WAN vendor circuits, including MPLS and broadband. This visibility is essential because SD-WAN invokes routing policies by SLAs and QoS metrics, rather than just OSPF or BGP routing protocols. For example, a platform may shift traffic from circuit A to circuit B because circuit A is violating a policy. This happens automatically, without anyone being notified. The team now can see when these changes are happening, and, in this scenario, find out why circuit A is violating the policy. Through this view, the team can also see how much traffic there is, when traffic is spiking, and whether thresholds are being exceeded.

Monitoring Scope: Customer SD-WAN Environment

Overlay:

- 9 data centers, with 400,000 SD-WAN elements, including 80,000 SD-WAN tunnels and 320,000 SLAs

All told, they're continuously monitoring around 1.5 million underlay and overlay network elements.



- **Heat charts.** The team can view heat charts that provide insights into the cyclical behavior of utilization. For example, teams can track behavior over the past month, with color-coded dashboards that reflect relative levels of utilization.
- **Netflow analysis.** By pulling in data from SD-WAN routers, administrators can see traffic by applications and ports. For each view, users can drill down to see which apps are driving traffic to a router, track top talkers, and identify if someone is using too much bandwidth or violating usage policies. These views are highly customizable. Teams can set granular policies and thresholds. For example, the team has a backup MPLS interface. They want to know immediately if any traffic starts to run on it, so they've established very low thresholds for this interface.

Overlay Section

The overlay section features these elements:

- **SD-WAN tunnels.** The organization has established integrations so SD-WAN data is continuously flowing into the system. Teams can track scorecards for the SD-WAN tunnels that support their clients' major data centers. Clients are running complex mesh networks, so it was important to narrow their focus on the most critical connections. Through these views, teams can see traffic per tunnel, destination device, and destination interface. They can also view packet loss, latency, and jitter for each tunnel.

“Broadcom helps us intelligently focus our triage efforts and enables us to confidently validate SD-WAN performance.”



- **SLAs.** The IT organization has established views for tracking ongoing performance against SLAs. Teams can track SLA performance against established thresholds and see actual performance, packet loss, latency thresholds, and more.
- **IPSLA.** Through a core switch, the team runs IPSLA for each remote site. They use this visibility to track connectivity to primary data centers, monitoring mean opinion scores (MOS). IPSLAs emulate business-critical voice and data traffic. Synthetic transactions are run every 60 seconds, with 10 packets sent at 10ms intervals. They can monitor round trip time, and see how well IPSLAs are performing.
- **Device-level stats.** Teams can get detailed device visibility, with views that feature IP address, CPU utilization, memory utilization, interface feed, traffic in and out, and more. They can also readily track bits per second on interfaces as well as average bits per second. They can easily detect any interfaces that have errors.
- **Alarm and event views.** The team has one dashboard that displays all DX NetOps events. Often, these events are created when DX NetOps identifies a configuration change and makes needed updates to polling to align with the new configuration. Events are also generated when thresholds are exceeded.

“With the solution, the team has been able to realize dramatic reductions in alarm noise and enhanced root cause analysis, so it can speed mean time to resolution.”



Results

Through their implementation of Broadcom solutions, the IT organization has realized a number of key benefits.

Improved Monitoring Scale

Broadcom solutions have enabled the team to effectively scale to meet the monitoring demands of a large, and rapidly growing SD-WAN estate. Native monitoring tools lacked the scale and underlay/overlay correlation the team needed. By employing Broadcom solutions, the team was able to boost monitoring scale by 50%.

Currently, the organization has 80,000 SD-WAN tunnels, and 320,000 SLAs to manage based on those tunnels. As a result, on 10-minute increments, they’re monitoring over 400,000 different elements—and that’s just in the overlay. All told, they’re continuously monitoring around 1.5 million elements.

Improved Mean-Time-to-Innocence Metrics

For the IT organization, speeding mean time to innocence (MTTI) is a key imperative.

“When issues arise, determining innocence, that is, proving that our infrastructure isn’t the issue, is important,” said the senior infrastructure architect. “But what’s even more critical is making sure we’re getting the right teams engaged to focus on the problem.”

With Broadcom solutions, the team at Kyndryl is able to correlate individual device performance with end-to-end network monitoring, across both internal environments and externally managed networks. As a result, they can quickly pinpoint the location and root cause of issues, speeding MTTI.

Accelerated MTTR

With the solution, the team has been able to realize dramatic reductions in alarm noise and enhanced root cause analysis, so it can speed mean time to resolution (MTTR). Broadcom solutions deliver improved visibility into managed and unmanaged networks that customers count upon. With this comprehensive visibility into networks and the user experience, the team can identify and resolve network issues in minutes—not hours.

Enhanced Brand Protection and Customer Satisfaction

By ensuring network services are reliable and responsive, the team at Kyndryl is able to better ensure optimized user experiences, helping improve customer loyalty and protect the company’s brand.

For more product information, please visit broadcom.com/netops.

About Broadcom

Broadcom Inc. (NASDAQ: AVGO) is a global technology leader that designs, develops and supplies a broad range of semiconductor and infrastructure software solutions. Broadcom’s category-leading product portfolio serves critical markets including data center, networking, software, broadband, wireless, storage and industrial.

For more information, go to broadcom.com