MODERN CSPS NEED UNIFIED VISIBILITY ACROSS HYBRID CLOUD

As consumers demand new and better services, communication service providers (CSPs) are under pressure to deliver more services without charging more. In response, network operators are moving to adopt software-defined, hybrid cloud infrastructures and autonomous networks as a way to increase agility at scale while still controlling cost. But while the vision is a sound one, its practical reality is pushing traditional network inventory and asset management approaches to the breaking point. To deliver the transformation their business demands, CSPs need to break down silos between network and cloud domains, remove operational friction, and use data effectively to make better decisions, faster.

Lines blur between network and cloud

Traditionally, telecommunications networks and IT infrastructure represented two different worlds. Even within the operational network, telcos often ended up with dedicated silos for fixed-line service, mobile, carrier, transport, and so on—each with its own domain-specific network inventory and topology tools. The IT applications and services delivered on top of the network required their own dedicated management technologies, as well. This fragmentation was far from ideal in terms of efficiency, but as long as operators relied on relatively static, monolithic environments, the challenges it posed remained manageable.

In today's fast-moving markets, however, CSPs are turning to virtualization and cloud as a way to increase agility, resiliency, and redundancy while reducing cost. To escape the constraints of

physical network infrastructures, they're delivering virtualized network services (VNS) and converged network services (CNS) over Kubernetes and virtual machine (VM)-based hybrid cloud infrastructures. Hardware devices—from routers and switches to packet gateways, radio access network (RAN) controllers, and mobile network cores—are being replaced with software. Open-source cloud-native network functions (CNFs) and commodity telco clouds offer faster ways to add services and respond to changes in demand while managing resources more efficiently.

As a result of this shift to software, the traditional separation between network and IT is now blurring. For network operations teams, which brings endless new challenges. If a problem arises with a virtualized network function being delivered over VMWare or OpenStack on hybrid cloud, for example, the network team's remediation efforts can be hampered by a lack of visibility and insight into the dynamic elements of this converged infrastructure. Without access to complete data across both IT and network domains, it's difficult or impossible to understand the dependencies between the two—especially when services depend on assets in a Google, Azure, or Amazon Web Services (AWS) cloud. Service assurance becomes slow, costly, and complex, putting customer experience at risk.

And reactive problem-solving is only part of the problem. Given customer expectations for flawless service at all times, CSPs need to proactively prevent issues in the first place, and to adapt quickly to demands that change by the minute. However, without the tools, data, and understanding they need to manage increasingly dynamic and elastic virtualized services, network operations teams struggle to be agile or effectively use automation. The challenge is compounded when operators acquire smaller companies, inheriting their technology environments, and do not have holistic insight, which further complicates an already arduous integration process. The rapid rise of cloud-native development also makes it too easy for business units to build and deploy their own applications without the knowledge of or visibility into network operations, incurring the security and compliance risks of shadow IT.

New rules around telecommunications cybersecurity, such as the U.K.'s Telecommunications (Security) Act (TSA) 2021, the Security of Critical Infrastructure Act 2018 in Australia, and similar U.S. legislation, are making these data silos and blind spots a matter of regulatory risk, as well. With assets spread across proliferating repositories located on-premises and in the cloud, CSPs face an urgent need for unified visibility to ensure compliance and protect their business from threats.

Converged infrastructure calls for converged discovery

As CSPs adopt network virtualization and a hybrid cloud infrastructure that includes telco clouds, they need to ensure full visibility, understanding, and data integration across both domains. In other words, they need a cloud-native, converged platform to discover the dynamic elements that make up their network, the underlying hybrid cloud infrastructures, and the dependencies among them. The idea isn't to replace traditional network inventory tools—which will remain essential—but rather to augment them with new discovery capabilities tailored to the more agile, dynamic nature of environments transformed through cloud-native development and software-defined networking.

With this foundation of unified visibility and understanding, CSPs can evolve toward the unified service management of its IT and network technologies that is demanded by the dynamic and elastic nature of modern telco clouds. Both network service management platforms and AIOps platforms can be provided with complete data to enrich, automate, and contextualize workflows, predict faults more accurately, and remediate problems more quickly and efficiently. Dynamic

application topologies, enriched with data ingested from application performance monitoring (APM) and other systems of management, can help network teams better predict the customer service impact of problems and changes and construct new service topologies more easily.

For customers, the impact of this unified approach can be dramatic. Network operations teams are better able to predict and prevent problems affecting service wherever they might occur, and when problems do arise, they can be diagnosed and repaired faster. For both network and IT teams, shared visibility and understanding removes friction and enables better collaboration. And for the business, converged asset discovery across hybrid cloud infrastructures helps improve security and regulatory compliance.

Toward zero-touch, zero-trouble networks

While converged discovery is an essential capability for the modern telco cloud, it's only one element of a larger vision. The next step is for CSPs to put this single trusted source of asset data to work to enable both AIOps-powered service assurance and network service management. In the next two blogs in this series, we'll explore each of these transformations and the benefits they enable for CSPs and their customers.

To learn more, read the first two blogs in this series, Zero Touch, Zero Trouble Starts with AIOps-Enabled Service Assurance and Demanding Markets Drive CSPs to Transform Network Service Management.

To learn more about our BMC Helix solutions for AIOps, visit https://www.bmc.com/it-solutions/observability-aiops.html