Are You Ready for the Complexity Train Wreck?

One of the inherent problems with IT networks is complexity. Just by itself, IT networks are growing in complexity as the edge of the network disappears, virtualized servers that were introduced to reduce costs, artificial intelligence and machine learning that were introduced to speed up reaction time and reduce costs, and then constant infrastructure upgrades as bandwidth consumption increases almost exponentially. Once you add on additional complexity due to network security, complexity has dramatically increased over the last five years.

If that wasn't enough, cloud computing is now taking center stage. The market appears to be telling enterprises that they need to move everything to the cloud and it will all be better — but is it? Complexity isn't being reduced with cloud deployments. As a 2022 EMA research study (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise) shows, complexity is actually increasing as cloud deployments increase.

The EMA study revealed the four following reasons for increased network complexity:

- Use of multi-cloud deployments for business continuity purposes
- Unplanned Day 2 operational issues due to cloud networks
- Architectural security and performance issues due to moving from on-premises physical equipment to the cloud
- Lack of visibility into cloud networks is preventing proactive maintenance

A fundamental problem with cloud networks includes vendor lock-in and the fact that when your public cloud provider goes down for hours or days, YOUR network goes down too. Some try to overcome this by using a multi-cloud approach. Unfortunately, this adds lots of complexity as well as lots of additional cost, as the business tries to replicate and synchronize data across multiple cloud networks. The total cost of a cloud migration is far more expensive than most think, possibly even far more than on-premises solution costs.

A second common problem is that when the cloud network is being designed, network engineers are often incented to get things up and running as fast as possible — so they focus less (or dismiss) Day 2 operational problems. It is left to the Operations team to find multi-network, multi-vendor solutions that actually work.

Another fundamental challenge is due to inherent differences in cloud and on-premises architectures. The security and performance controls you had with on-premises solutions just don't work with cloud networks that you lease. According to the EMA report, 66% of companies are struggling with visibility architectures due to impacts of cloud migration, increased network complexity, tool complexity, and lack of qualified personnel.

Lastly, tools and services that cloud providers offer for visibility are often highly proprietary, making it extremely difficult for some companies to create an end-to-end solution for monitoring multi-cloud performance and security. At the same time, 87% of organizations believe it is at least somewhat important to establish a single visibility architecture that spans physical, virtual, and cloud-based networks, according to the EMA report.

So, what can you do about it? After all, complexity leads to two outcomes — additional performance problems and configuration problems (i.e. headaches) along with unnecessary and expensive costs.

Overcoming Architectural Issues With Network Visibility

There are two clear answers to overcoming this unwanted complexity:

- Move only what you need to the cloud
- Create a visibility architecture across public cloud, private cloud and physical on-premises network

First, consider if "Everything" really needs to move to the cloud. Moving to the cloud is a business decision. What makes sense financially in one area may cost you significantly in other areas. For instance, the main business case touted by lots of cloud proponents is that you can spin applications up and down quickly to respond to market conditions. This is very true. However, what you may not know is that 46% of companies moving to the cloud said the cloud created blind spots — places where they are unable to collect data for performance and security analysis. Others experienced performance and security problems and rolled back parts of their operation to their on-premises system. So, instead of moving everything to the cloud, considering only moving what makes sense – sort of like the "right tool for the right job" concept. You may very well find that a hybrid scenario of physical on-premises and a public cloud network is the right choice.

A second, mandatory activity is to create a visibility architecture. This allows you to integrate solutions into your network architecture that give you the visibility into on premises networks, single and multi-public cloud networks, and private cloud networks. With this integration, you get packet level visibility that enables you to accurately address performance, security, compliance, and cost controls in the best possible way. This is why the EMA study reported that 55% of those respondents are investing in visibility solutions to support their hybrid and/or multi-cloud networks.

The good news is that there are purpose-built visibility solutions available to help you. Depending upon your architecture (pure cloud or hybrid cloud), a combination of physical taps, cloud taps, physical packet brokers, virtual packet brokers, and active monitoring solutions that can span both on-premises and cloud networks are available to give you the right tools you need to create visibility across any network.

Reach out to Keysight Technologies and we can show you how to optimize your public cloud and hybrid cloud solutions.

Learn more at: www.getnetworkvisibility.com

Keysight sponsors GetNetworkVisibility.com, a thought leadership website dedicated to the importance of packet-based visibility to power security, performance and network monitoring tools. For more information, contact us at:

www.getnetworkvisibility.com/contact-us/