Lack of Visibility is a Killer for Cloud Deployments

A recent Enterprise Management Associates survey (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise) found that 46% of IT professionals admitted that their migration to a cloud-based network created blind spots. Furthermore, the number of blind spots increased directly with the increase in the number of cloud networks deployed, i.e. two, three, or more.

So, what does this mean? Essentially, you could be hit with perpetual performance and security problems without warning after you move to the cloud. In the best-case scenario, these issues will be bearable but irritating. Worst case — your company could suffer a massive security breach that causes significant monetary and reputation harm. However, this is a solvable problem.

What Are Blind Spots?

Blind spots are places where IT engineers and operations personnel are unable to collect monitoring data for performance and security analysis. Obviously, this is bad. If you can't see a problem — how do you know it exists or even what it is? It's also much easier to fix a problem that you CAN see.

Here are just a few common sources of blind spots:

- Silo IT – IT and business organizations deploying independent solutions
- Use of virtualization technology – Lack of visibility into East / West traffic
- SPAN port overloading – For physical on-premises / hybrid cloud deployments
- Mergers and acquisitions – The blending of disparate equipment and systems
- Rogue IT – Users adding their own equipment and networks
- Network complexity – Either due to network design or technology choices

How Do Blind Spots Affect My Cloud Network?

Blind spots directly correlate to network problems and outages, increased network security risk, and potential regulatory compliance issues. In fact, the EMA survey mentioned above found that 97% of companies have experienced at least one significant problem due to the network blind spots introduced by their migration of applications to the public cloud.

Here are some specific problems they encountered:

- 49% of companies experienced a violation of a security or compliance policy
- 46% experienced extended application downtime or performance problems
- 45% experienced a security breach
- 44% experienced cloud cost overruns

Overcoming Blind Spots

There are typically two ways to respond to the blind spot issue — either in a proactive or a reactive manner. The reactive approach is straight forward, just wait until something happens and then go fix it. While it's the simplest approach, it's also usually the costliest in terms of locating exactly what issue the blind spot caused (which usually increases your mean time to repair and the chance of a security beach).

For a proactive approach, the best solution is to design a visibility architecture. This involves more upfront cost and planning but also pays for itself very quickly. The visibility architecture is a plan you create for organizing exactly how you want your monitoring tools to connect to the network and the data they receive. This involves how they connect (cloud tap, physical tap, or SPAN ports or RSPANS), where they connect (edge, core, multiple clouds, etc.), and how you treat the monitoring data before you send the stream to a tool (packet filtering, application filtering, deduplication, packet trimming, decryption, aggregation, etc.).

To end blind spots in your network, you need to be able to see everything. Unknown issues and "soon to be problems" exist in every network to some degree. To achieve the goal of ending blind spots in your network, you'll need to implement a visibility architecture. It's not hard or complicated, but it does require some planning. At the same time, the sooner you can accomplish this step, the faster you can integrate a visibility architecture within your cloud or hybrid cloud network. And the sooner you can realize cost and productivity savings.

Reach out to Keysight Technologies and they can show you how to save money by optimizing your security and monitoring solutions with the best line of cloud taps and packet brokers on the market.