WHITE PAPER

Blinded by the Cloud – The Real Cost of Moving Applications to the Cloud

Moving to the Cloud is a Business Decision

When business teams meet, it often seems like the cloud will solve all of the company's problems. For instance, you will supposedly be able to easily spin new applications up and down, the system will always "be on", and business applications will seamlessly melt together in harmony.

Unfortunately, real business experiences don't match the hype. As an example, Dimensional Research found in a study they conducted (documented in this Keysight white paper Top Four Considerations When Migrating to Public Cloud, Figure 1) that 9 out of 10 companies moving to the cloud experience security and performance problems. This includes application and network troubleshooting and performance issues, as well as delays in resolving security alerts stemming from a lack of visibility.

An analyst company, Enterprise Management Associates (EMA), found similar problems in their 2022 research report (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise). The EMA study found that 46% of companies moving to the cloud realized that the migration to the cloud had created blind spots, i.e. places where IT personnel are unable to collect data for performance and security analysis, in their architecture.

Other cloud-related problems include 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 — making the migration to the cloud far more expensive than most think.

When moving to the cloud, make sure you have all of the facts before you make the leap — as you Do Not want to be blinded by the cloud. For instance, you will want to look out for the following potential problems:

- Security concerns
- Performance issues
- Single vendor lock in
- Complexity due to use of a multi-cloud architecture
- The actual cost may be much higher than you were quoted

The following white paper will give you a good overview of the issues involved with cloud visibility.

To Leap or Not to Leap?

One common misconception is that everything in your physical network has a cloud equivalent. This is not the case. You are moving from an environment (physical on-premises) where you have full control to an environment (public cloud network) where you have limited control. This situation is akin to moving from ownership of a house to rental of a house. You may still be living in a house, but you are now subject to someone else's rules and whims while you pay them money.

Performance monitoring, data security, and business continuity remain key issues for the IT team. However, once you make the leap to a cloud environment, you may find that you no longer have the types of information that you used to.

For instance, a Keysight cloud report (The State of Cloud Monitoring) based upon survey data collected by Dimensional Research showed that as companies moved to the public cloud, less than 20% had the data they needed to properly monitor their networks. Comparing this to on-premises networks, 82% of IT professionals in those environments had the data they needed.

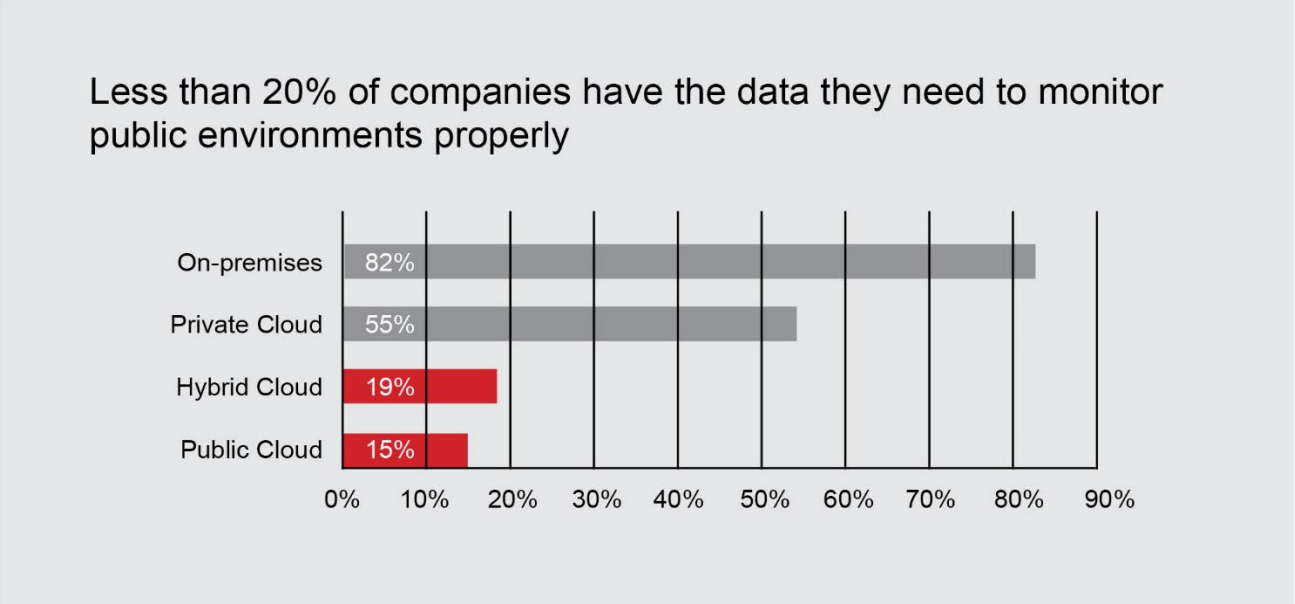

Figure 1: In which environment do you have complete and timely access to network packets?

Additional data from that report showed that many IT professionals are disappointed with their leap to the cloud. The survey showed that 9 out of 10 respondents have seen a direct negative business impact due to lack of visibility into public cloud traffic. This includes application and network troubleshooting and performance issues, as well as delays in resolving security alerts stemming from a lack of visibility.

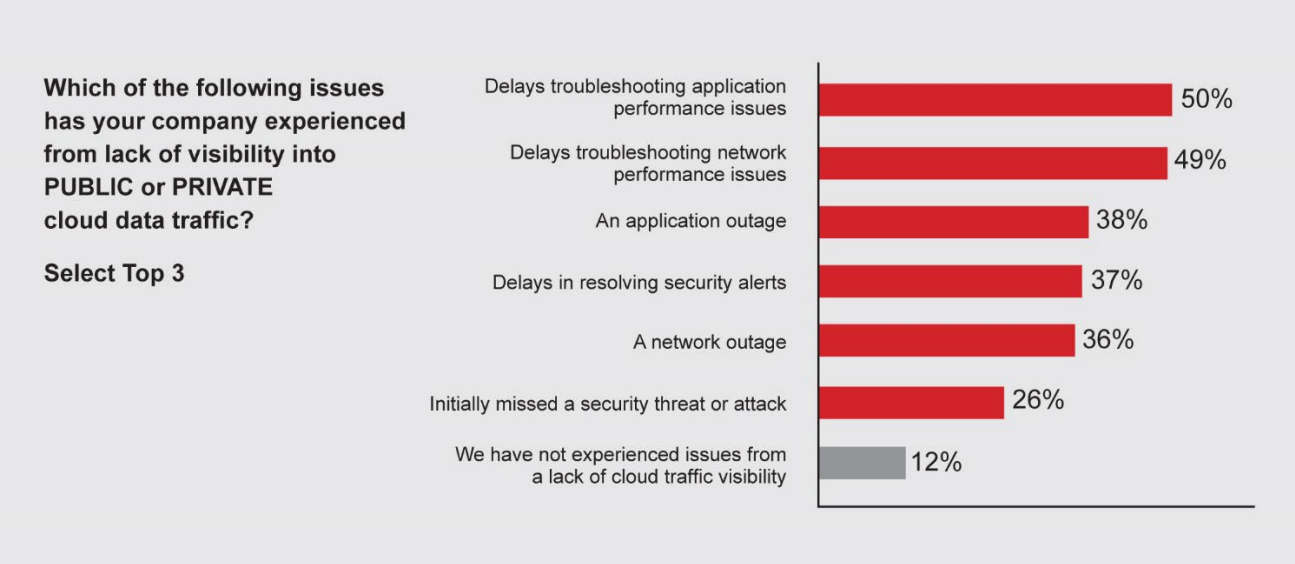

Figure 2: 88% of users experienced issues from lack of visibility into public cloud data traffic

Let's look at five specific problem areas.

Cloud Security Concerns

The ultimate security challenge in the digital realm is how to protect yourself from danger that you can't see. After all, hackers don't knock at the door and wait. They breach, they hide, or worse, they masquerade in plain sight, pretending to be something they're not. No matter what the technology though, you still have to defend against the threat(s).

This is where you need network visibility. You can't defend against what you can't see. The Keysight cloud report found that less than 20% of participants say they have the data they need to monitor public cloud environments accurately and that 87% were concerned this lack of visibility was masking security threats. The EMA report found that 34% of surveyed companies had suffered a security breach, which made them reprioritize data visibility solutions. The Keysight cloud report had similar findings where 59% of the respondents believed that visibility enables threat protection solutions to identify malicious traffic by source and 57% believes that visibility allows security monitoring solution to detect 'indicators of compromise' (IOC).

While there are many security threat vectors in a cloud environment, here are three security risks that tend to surprise IT teams moving to a public cloud network:

- Enhanced security threat due to native cloud mirroring combined with compromised credentials
- Increased API attacks
- Reduced ability to secure the infrastructure

A new security risk for previously on-premises based IT teams is native cloud mirroring. Data once secured in private data centers can end up moving between virtual cloud servers on geographically-dispersed hardware, as cloud providers strive for operating efficiency. Traditional security practices cannot be applied in such an environment. Many large enterprises have had sensitive data stored in the public cloud compromised due to inadequate testing of web-based applications and configuration mistakes. In one high profile case, Deloitte had its cloud-based global email server breached, and thousands of emails with sensitive data were potentially exposed.

API attacks is another, "new", attack vector. The rise of cloud computing has increased the possibility of API attacks. By definition, APIs allow external people, applications, or services access to your internal systems, data, or other resources. Most applications today use APIs to increase flexibility and enable integration, and this is particularly true for cloud applications. In fact, integration with other services is often a reason for migrating to cloud in the first place. These interfaces, however, also increase the risk of an unauthorized person accessing your network by exploiting an unprotected API. Security researchers are focusing more on the vulnerabilities associated with APIs.

The Open Web Application Security Project (OWASP) even has a Top Ten list just for APIs due to the importance of this category. According to 451 Research in their 2022 API Security Trends Report, 41% of surveyed companies suffered an API related security incident and 63% of those involved a security breach or data loss during the last year.

A third key security issue is that while the cloud provider is responsible for protecting the network, security for each individual customer's environment is typically controlled with access lists. Most data centers have already abandoned an "access list only" method of security as it has been proven to be insecure. This is why on-premises security teams implemented inline security techniques like intrusion prevention systems and other appliances to inspect data before it enters your network. While this was never 100% effective, swatting down 80 to 90% of incoming threats at the perimeter is very beneficial to stopping security attacks, as it means that there is less threats you have to stop further on within your network. This is relevant to whatever security architecture you have, including Zero Trust.

Cloud IT teams need to be prepared that once they move to the cloud, they can't simply depend upon the service provider to secure everything. If that were true, there would never have been any cloud networks breached over the last few years.

Cloud Performance Concerns

Performance is another issue to be concerned with. Data processing in a cloud network doesn't always work the same as an on-premises system. The cloud uses a distributed system with functionality spread across multiple servers and serverless processes that can, and probably are, geographically separated from each other. This can lead to transmission delays and service slowdowns. Other issues can include device malfunction, OS failures, and cloud server reboots.

If we refer back to the Keysight cloud report, the Dimensional Research survey found that nearly half of companies experience performance issues.

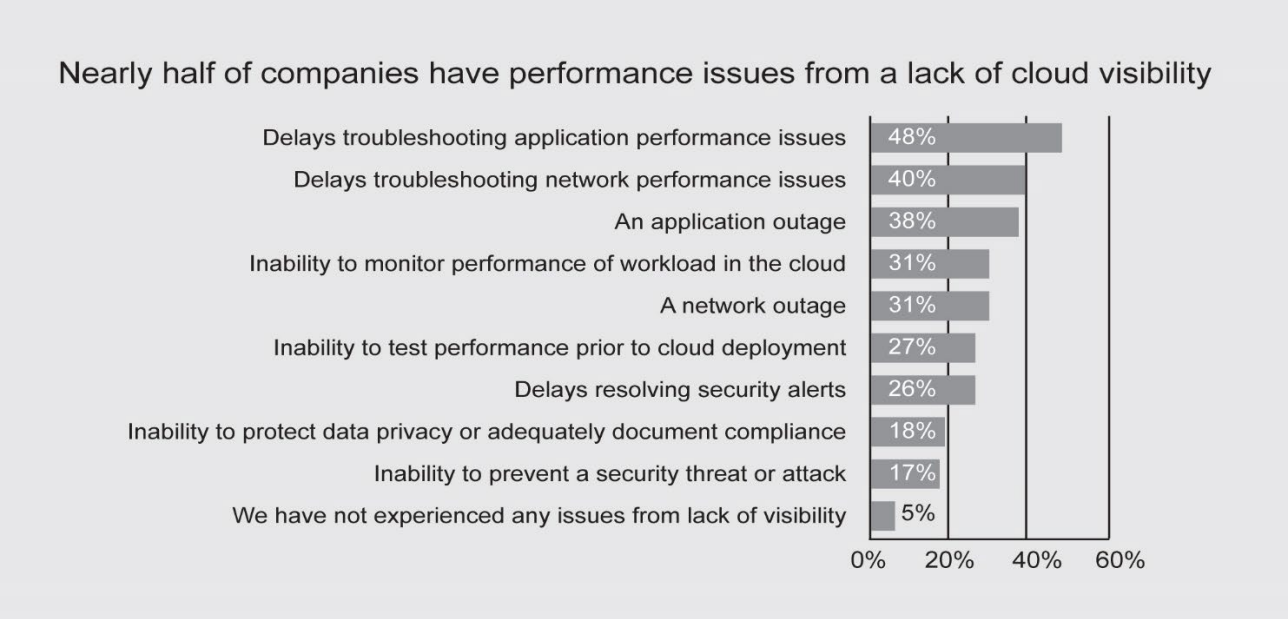

Figure 3: In the last 12 months, which, if any, of the following issues has your company experienced from a lack of visibility into the Public or Private clouds?

This lack of visibility into performance problems is another driver in the need for cloud visibility solutions. The EMA report found that 19% of surveyed companies had such a severe problem that it made those companies reprioritize data visibility solutions.

Another important question to answer is how do you plan to accurately gauge the impact of poor network performance on your cloud-based application workloads? As demonstrated earlier, performance issues are a real consideration for new cloud networks. Once you migrate to the cloud, and during the migration process, you will not have clear network performance data within your environment. It is up to you to implement this, if you want this visibility. Specifically, this means that you cannot natively tell how your applications are truly performing or even how your cloud instance is performing. Is it meeting or exceeding the service level agreement (SLA) that was put in place? Your cloud vendor will probably tell you that it is, but you have no independent data for a “check and balance” strategy on what they are, and are not, delivering.

Addressing Single Vendor Lock in

A third fundamental concern 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. Unfortunately, a cloud network is not as easy to set up as vendors may tell you. There is time and effort, which means cost, to set up a cloud network and then more time, effort, and cost to maintain it. You can’t just switch to a new technology at will.

Some companies try to overcome vendor lock in by using a multi-cloud approach. They replicate the same network configuration and data storage across 2 or more public cloud vendors. As a case in point, the EMA report found that 56% of companies surveyed had 2

public clouds, 19.5% had three clouds, and 7% had four more clouds. Unfortunately, this adds lots of complexity (in addition to lots of additional cost), as the business tries to replicate and synchronize data across multiple cloud networks. As a specific example, a service or tool that's natively available from one cloud vendor may not be available from another vendor. This makes it very difficult for application developers who intend to leverage multi-cloud redundancy.

The New Complexity Problem

As was just mentioned, complexity of your network design is a fourth concern that you will want to address. While one of the inherent problems with IT networks is complexity, the market appears to be telling enterprises that they need to move everything to the cloud and it (complexity) will all be better. However, complexity isn't being reduced with cloud deployments. The EMA report shows that complexity is actually increasing as cloud deployments increase.

Part of the increased complexity is to overcome vendor lock in by using a multi-cloud approach and the replication and synchronization of data across multiple cloud networks. While just the set-up and maintenance of this scenario is complex, afterwards the IT personnel don't have the tools, expertise, and visibility to manage a network across multiple cloud providers.

Other drivers for complexity include traffic growth that is forcing upgrades to tools and networks as IT networks move to faster network speeds, like 40 and 100 GE. The COVID-19 pandemic has also obscured the network edge. This means that IT personnel don't have the insights that they used to have.

Another fundamental 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.

However, you end up at a point of high complexity, you will definitely want to address the issue. Complexity leads to two outcomes — additional performance problems and configuration problems (i.e. headaches) along with unnecessary and expensive costs.

What Happened to My Cost Savings?

It's an interesting dichotomy that 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 according to the EMA report, 46% of companies moving to the cloud said the cloud created blind spots. Others experienced performance and security problems and rolled back parts of their operation to their on-premises systems.

As mentioned earlier, 83% of the companies that were surveyed in the EMA report had two or more clouds. This means double, triple, or quadruple the costs for your cloud network — i.e. no volume discount for buying more cloud networks. Again, it's not just the setup costs here but ongoing maintenance and data replication costs that are painful as well.

In case someone may think this discussion is just hyperbole, there are actual experiences from companies that tried to make the leap to the cloud and were unsuccessful. For instance, there is an interesting viewpoint from David Heinemeier Hansson who wrote a blog about his foray into networking and his return from the abyss. He noted that the cloud is good for low usage or wild swings but not those in the middle. Specifically, he found that, "Renting computers is (mostly) a bad deal for medium-sized companies like ours with stable growth. The savings promised in reduced complexity never materialized."

Mr. Hansson found that operational costs for cloud networks seem to be about the same as on-premises. However, computing costs to "rent" public cloud networking computers for him came to about half a million dollars for one year. When compared to the amount of servers that he could buy for an on-premises system for that annual cost, the economics were just not there.

Conclusion

When it comes to making the leap to the cloud, IT engineers and architects need to keep in mind that there is a fundamental challenge due to inherent differences in cloud and on-premises architectures. The security and performance controls you had with on-premises solutions don't work with cloud networks that you lease. According to the EMA report, 66% of companies are struggling with visibility architectures due to the impacts of cloud migration, increased network complexity, tool complexity, and lack of qualified personnel.

This doesn't mean that you should ignore the cloud. The secret to success is to plan your migration strategy out. For instance, maybe don't move everything to the cloud, just what makes sense. You may very well find that a hybrid scenario using both physical on-premises AND a public cloud network is the right choice to optimize both cost and functionality.

Next, make sure that you integrate solutions into your architecture that give you visibility into both on-premises and cloud networks. This allows you to integrate solutions for 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 report found that 55% of those respondents are investing in visibility solutions to support their hybrid and/or multi-cloud networks. Improved visibility enables you to accurately address security, performance, complexity, and cost controls in the best possible way.

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 they can show you how to optimize your public cloud and hybrid cloud solutions.

Learn more at: www.getnetworkvisibility.com.