WHITE PAPER

Top Four Considerations When Migrating to Public Cloud

Are Public Cloud Workloads Good Or Bad?

A common question today is whether moving workloads to the public cloud is a good decision or a bad decision. While this question is understandable, it is the wrong question to ask. Public cloud computing has considerable advantages over physical on-premises equipment solutions, including lower deployment costs and rapid turn-up of new applications. On the other hand, there are drawbacks including security and performance concerns, vendor lock-in, lack of network visibility, and lack of infrastructure control. So, the real question is, "How do I balance all of these factors to achieve the best solution, especially when it comes to network monitoring?"

Public cloud computing has considerable advantages over physical on-premises solutions including lower deployment costs and rapid turn-up of new applications. On the other hand, there are drawbacks including security and performance concerns, vendor lock-in, lack of network visibility, and lack of infrastructure control.

The answer to this question is to make sure that you understand the risk and reward upfront, before you get a shocking surprise. The solution may end up being a hybrid approach using a combination of physical and virtual network capabilities. In the end, whether you deploy a complete public cloud network or a hybrid cloud network, there are four questions you need to consider before you create your new architecture:

- What is the extent and timeframe of your migration strategy?
- How will you handle the decrease in network visibility as you move to the cloud?

KEYSIGHT TECHNOLOGIES

- Will you need to deploy inline security and monitoring tools?
- How do you plan to accurately gauge network performance?

Cloud Monitoring And Visibility Concerns

Let us examine the four considerations in detail. These items present serious challenges for businesses considering cloud deployments. At the same time, there are viable solutions and processes that mitigate these considerations to help make cloud migration as beneficial as possible.

Migration strategy and planning is critical for success

Data from surveys show that many IT professionals are disappointed with their leap to the cloud. A survey performed by Dimensional Research 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.

Sanjit Ganguli of Gartner Research also conducted polling on public cloud migrations at the Gartner December 2017 Data Center Conference and found that 62 percent were not satisfied with the monitoring data they get from their cloud vendor now that they have moved to the cloud. In addition, 53 percent actually said that they were blind to what happens in their cloud network.

A survey performed by Dimensional Research showed that 9 out of 10 respondents have seen a direct negative business impact due to lack of visibility into public cloud traffic.

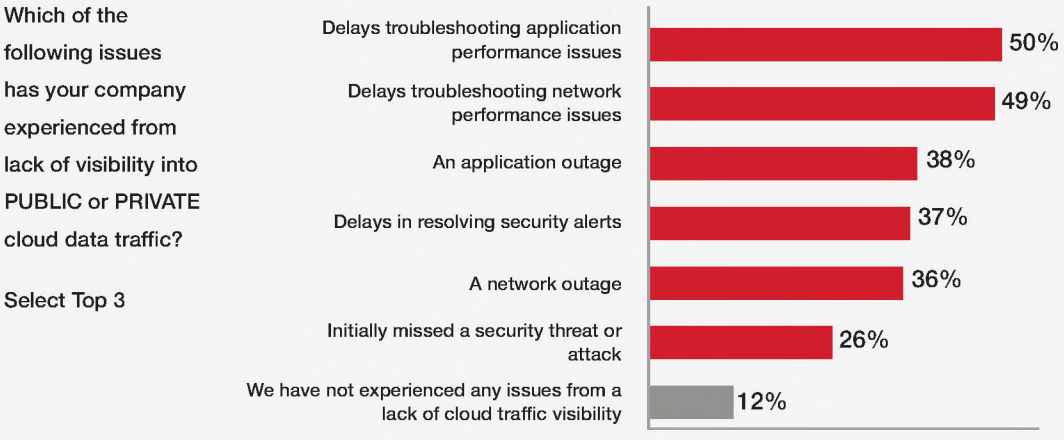

Figure 1. 88% of users experienced issues from lack of visibility into public cloud data traffic

While not all cloud migration problems are avoidable, many can be. Your migration plan should answer this basic question, "What are my network visibility requirements, and how do they fit into my forensic and troubleshooting plans?"

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 where you have full control to an environment where you have limited controls. 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 while you pay them money.

Your migration planning will be a key factor. For instance, do you plan on migrating immediately, over the course of a year, several years, or are you planning on a permanent hybrid model? When making this move, here are four common technical aspects of the solution to consider:

- Do you plan on deploying multi-cloud networks and how will you monitor them?
- Do you plan on implementing orchestration and automation and how does it all work together?
- How will you manage your environment, and can you achieve a "single pane of glass" for visibility?
- Have you performed a true cost analysis that includes your productivity savings and ongoing costs?

Creating a proper financial analysis for migration to the cloud can be tricky. There are a lot of factors that figure into the total cost ownership (TCO). While the cloud computing instance costs are what most people focus on, there are additional troubleshooting and performance management costs that stem from lack of visibility and control within standard cloud environments. In addition, cloud computing vendors have additional services like providing log file data. However, vendors usually charge for these services and log data can be expensive to manage, since you either have to manually sift through those log files to find what you need or buy additional purpose-built tools, which can be expensive.

Instead of buying several brand-new analysis tools for the cloud, existing tools in your on-premises environment may be reusable. However, this requires you to backhaul the requisite data from the cloud to the physical premises. While these costs vary depending upon the bandwidth, typical costs run about $0.10 per GB to export data to the Internet. For a "typical" business that exports 500 GB of data per month, this cost could be about $50. So, this backhaul data cost is very low and is actually a viable cloud option. It is comparable to the cost of adding one extra business phone per month.

Here is a quick summary of the data monitoring costs and benefits for migrating from on-premises to a cloud network.

Cloud networks do not offer native visibility

One common misunderstanding is that a simple "lift and shift" approach will work. It normally does not. In fact, it will actually create network visibility and control issues because cloud and on-premises tools function differently. Visibility is what allows IT to control and optimize the network along with the applications and IT services running

Costs	Benefits
Set-up costs for cloud computing provider	• Productivity increases due to using cloud apps
Recurring annual costs for cloud computing provider	• More OPEX costs, less CAPEX costs
Log data file service cost for cloud computing provider	• Fine-grained application log data
Purchase of new monitoring tools that work in the cloud	
Data backhaul costs (for hybrid networks)	
Additional costs for troubleshooting	
New productivity costs due to performance issues	
Cloud solution and monitoring managerial costs	

Once you migrate to the cloud, and during the migration process, you will not have clear visibility into the network layer. You will only be able to get information about the cloud network and some parts of the operating system from cloud-based service providers.

on it. This is why network, application, and security visibility are absolutely vital for any IT organization to accomplish its job. Without visibility, IT personnel can only operate reactively to problems and are never truly effective at eliminating those problems.

Once you migrate to the cloud, and during the migration process, you will not have clear visibility into the network layer. You will only be able to get information about the cloud network and some parts of the operating system from cloud-based service providers. They provide summarized metadata on cloud-centric information (network, compute, storage). This includes high-level cloud data (e.g. CPU performance, memory consumption, etc.) and some log data.

What the cloud providers and other cloud tools do not provide is network packet data. This data is absolutely necessary for security forensics and troubleshooting using root cause analysis. Data loss prevention (DLP) tools and most application performance management (APM) tools are dependent upon the packet data for problem analysis.

Typical cloud tools provide limited data that is often time-delayed which can dramatically impact tool performance. For instance, tactical data loses 70% of its performance monitoring value after 30 minutes of time delay, according to Nucleus Research.

Cloud tools primarily provide summarized flow data (like VPC flow logs) which has some use for general information but contains none of the details that are necessary for troubleshooting and deep packet inspection for threats. For instance, Amazon Web Service (AWS) flow log data will not include the following information:

- Traffic to Amazon DNS servers, including queries for private hosted zones
- Windows license activation traffic for licenses provided by Amazon
- Requests for instance metadata
- DHCP requests or responses

In addition, cloud providers also do not provide user experience data or the ability to watch conversations. Specifically, this means that you cannot accurately gauge customer quality of experience based upon cloud provider delivered data. In addition, the flow data provided lets you see who the talkers are but does not contain anything about the details of the conversation.

An easy remedy for this issue is to add cloud-based monitoring data sensors (also called virtual taps) to your cloud network. These sensors can replicate copies of the desired data packets and send them to your troubleshooting, security, and or performance tools. This gives your tools the data they need to perform their functions.

One key factor though is that the data sensors need to have the ability to scale automatically as needed. The whole reason you have decided to move to the cloud is to take advantage of its elastic nature. As cloud instances get spun up, the sensors capability needs to be able to scale sufficiently as well. As your cloud solution scales, your visibility solution needs to scale with it, automatically and programmatically. Avoid virtual tap solutions that require manual intervention to load licenses or add instances of the virtual taps, as this is a productivity killer.

Inline on-premises security and monitoring tools do not work the same in the cloud

Some of the cloud vendors will tell you that cloud network security is just as safe as the data center you currently own. This is not correct. While the cloud provider is responsible for protecting the network, security for your 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. Bad actors can, and will, bypass this security mechanism. You will need an additional security solution.

Due to the nature of public clouds, inline tools are not an option. Public cloud vendors do not allow customers access to their network and system layers to deploy any inline security (e.g., intrusion prevention system (IPS), data loss prevention (DLP), or web application firewall (WAF)) tools, as this can create a security risk to their network. So, if you plan to deploy inline security protection, you should understand that it won't be a "bump in the wire configuration" that you are used to for on-premises devices, like a typical IPS. When planning your security architecture, make sure you talk to a security vendor that understands how the cloud architecture needs to be configured.

Lack of inline tool deployment obviously creates a risk to your cloud instance that you will need to address. So, how do you secure your environment now? First, you need to deploy an architecture that enables you to be proactive and stay ahead of the bad guys. This includes visibility components (like sensors) that allow you to capture security and monitoring data of interest for analysis.

If your cloud vendor does tell you that you can deploy inline security tools, verify what that architecture will, and will not, do and then make sure that the IPS (or other device that will take an active role in deciding the fate of a packet) can have a dedicated IP address and be a router or gateway device. This will allow you to control the packet routing. The IPS, or other device, will also need to support an EC2 instance capability, if you're in an AWS environment for instance.

A second approach is to purchase purpose-built security tools for the cloud. This includes encrypting data at rest and also active threat detection tools like a SIEM or IDS. These tools provide out-of-band anomaly analysis. However, this is still not the same as deploying an inline IPS solution, which would have the ability to invetigate and stop threats in real-time. So, trade-offs to your security risk plan will need to be made.

Public cloud vendors do not allow customers access to their network and system layers to deploy any inline security (e.g., intrusion prevention system (IPS), data loss prevention (DLP), or web application firewall (WAF)) tools, as this can create a security risk to their network. So, if you plan to deploy inline security protection, you should understand that it probably won't be a "bump in the wire configuration" that you are used to for on-premises devices, like a typical IPS.

A third option to mitigate the threat would be to use a hybrid architecture that allows you to keep your existing security tools within the physical premises to inspect high risk data (or even general data if you want). Based upon your risk plan, this may provide the protection you need and minimize business risk to an acceptable level. Note, most cloud computing vendors charge you to export data. However, the data bandwidth costs can be limited by simply transferring only the relevant data to the on-premises tools.

Cloud performance measurement is vendor dependent

Another important question to answer is how you plan to accurately gauge the impact of poor network performance on your cloud-based application workloads? 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.

During the migration process, proactive monitoring of both your on-premises and cloud environments will be useful. Many organizations that just blindly port services and applications to the cloud find cloud network issues quickly, particularly performance issues.

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 delivering.

Business intelligence applications are one example of a problem area. After porting the service, you may find that it runs slower (after you receive multiple customer complaints). The result is often an increase in more CPU, RAM, and interconnect bandwidth. This creates an unplanned and perpetual cost increase.

During the migration process, proactive monitoring of both your on-premises and cloud environments will be useful. Many organizations that just blindly port services and applications to the cloud find cloud network issues quickly, particularly performance issues.

Proactive monitoring allows you to accurately understand what is happening and determine where problems are located within your cloud network. As mentioned earlier, once you migrate to the cloud, application performance monitoring will become difficult if you do not properly plan for it. You will not have the data you need natively from the cloud service provider. This loss of data needs to be planned for so that it can be remedied or mitigated.

Cloud Native Vs. A Hybrid Approach To Maximize Network Visibilty

The easiest way to achieve network visibility is to implement a visibility architecture—which is an end-to-end infrastructure that enables physical and virtual network, application, and security visibility. Once the architecture is in place, you can implement various different solutions, i.e. use cases, that you need and optimize those for on-premises, cloud, or hybrid networks. The first step is to install sensors into the cloud network. This allows you access to the data you need, when you need it.

Once sensors are integrated into the system, that technology can expand as necessary (assuming the right vendor was chosen) to accommodate the volume of workloads required. New workload instances will automatically start new sensors which will then report to the management system, creating an automatic scaling solution. Data that is needed for the on-premises equipment can also be exported as necessary through a tunnel so that the requisite data can be analyzed by appropriate security and monitoring devices.

For a cloud native approach, replicated data packets can then be forwarded on to your security and monitoring solutions for deep packet inspection. To address performance in the cloud, you'll need to install your own proactive monitoring solution that allows you to place software sensors across your network so that you can actively poll the different segments to understand how your network and your applications are performing.

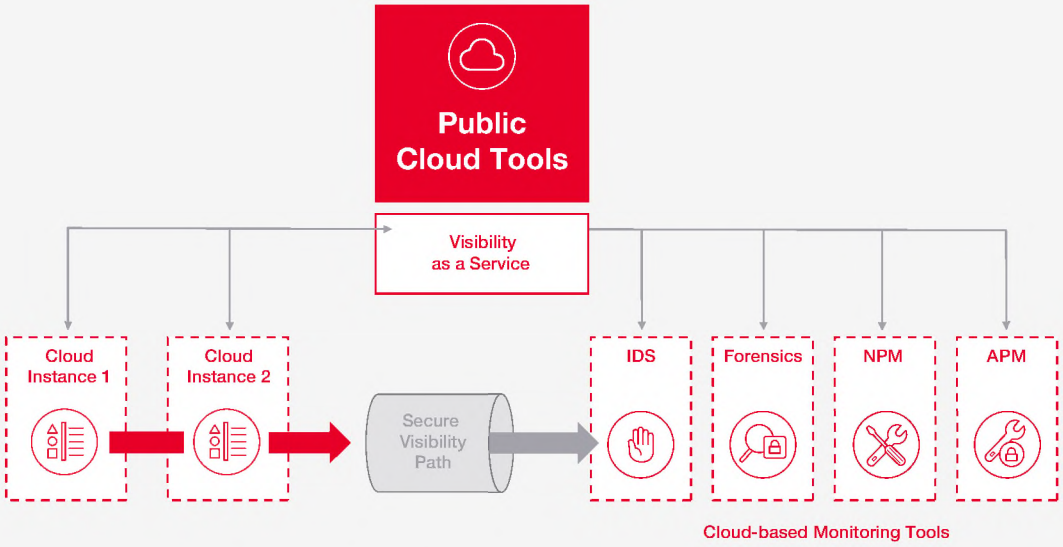

Figure 2. Cloud-Native Data Monitoring

In a hybrid scenario, critical packet data can be exported at will to your existing physical (on-premises) environment. This includes the ability to pass data on to out-of-band security tools like an intrusion detection system (IDS) or DLP, if you don't have those tools deployed yet in your cloud environment. Utilizing existing on-premises tools allows you to increase the return on investment (ROI) that you have already made into those tools.

In a hybrid scenario, critical packet data can be exported at will to your existing physical (on-premises) environment

Here are a few options to consider for a hybrid environment:

- Deploy a sensor(s) for the cloud network to get visibility and access to packet data
- Port data from the cloud to on-premises tools as needed to control cloud data monitoring costs and extend your current investment in those on-premises tools
- Deploy proactive performance monitoring across cloud and physical networks
- Maintain application performance capabilities by using captured packet data

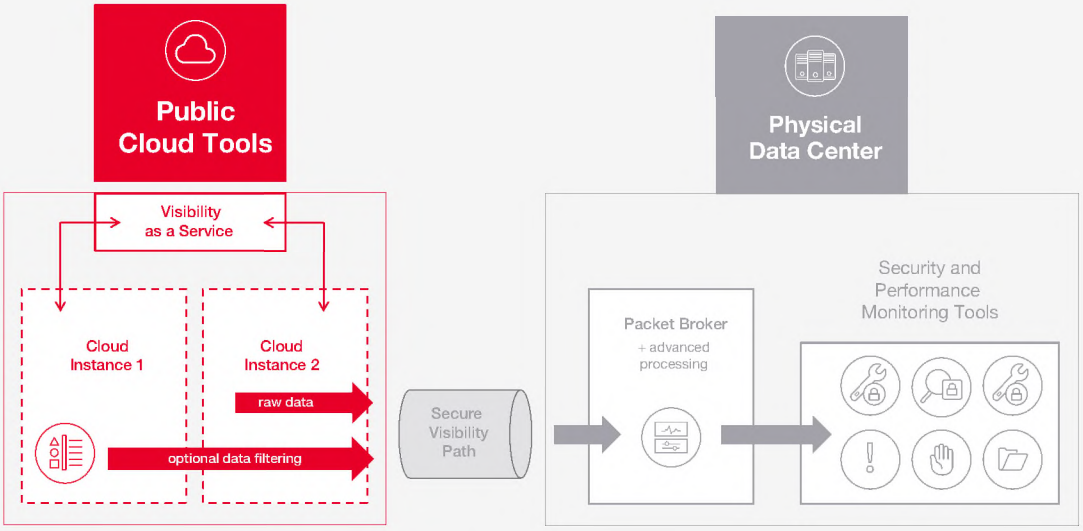

Figure 3. Hybrid cloud and on-premises example

Conclusion

Understanding the implications of a cloud network before deployment of that network is extremely important from a network security, application performance, and network cost perspective. There are three areas that can have an important impact to the network:

- Transferring services and applications from an on-premises to a cloud network can result in unplanned cost increases due to network visibility and performance issues
- Inline tools cannot be deployed in the cloud which weakens network security
- A sensor is required to capture the appropriate packet data for forensic security and application performance management
- Performance monitoring is critical to avoiding surprises when the network goes live

Implementing a visibility architecture enables the fundamental capture and sharing of the valuable data needed for security and performance troubleshooting. Once a monitoring data sensor is installed into the cloud network, you will have the access to the packet data you need. This data can be delivered to either cloud-based tools or on-premises tools for data analysis including network troubleshooting, application performance monitoring, deep packet inspection, regulatory compliance validation, application intelligence monitoring, or other specialized monitoring function.

Implementing a visibility architecture enables the fundamental capture and sharing of the valuable data needed for security and performance troubleshooting. Once a monitoring data sensor is installed into the cloud network, you will have the access to the packet data you need.

A proactive monitoring solution can help you anticipate and mitigate performance issues for both your on-premises and cloud applications. With proactive monitoring, you can gather baseline performance data from both environments before migrating any functions to the cloud, and then observe your cloud performance as services and applications are migrated. Once particular services are migrated to the cloud, proactive testing can be used to determine how the service or application will behave in the new cloud environment. This gives you advance warning of any problems and also gives you an opportunity to perform a rollback, if needed, before too many users are affected.

Proactive monitoring also allows you to characterize your cloud network to validate the SLA that the cloud provider was contracted to deliver. Should the provider be under-performing, you have objective data that can be used to start a conversation on service cost refunds or discounts.

Ixia network visibility solutions are a powerful way to optimize your network monitoring architecture and strengthen your network security. For more information on network monitoring solutions, visit www.keysight.com.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES