WHITE PAPER

Security and Performance Monitoring in the Public Cloud

Introduction

Even as workloads move to the cloud, information technology (IT) must continue to maintain data and application security, optimize performance, and resolve issues as quickly as possible. But getting access to traffic data in the public cloud can be a challenge. Once you have the data, you then need a way to sort and filter it, so security and performance monitoring solutions can process it with maximum efficiency. This paper explores the pros and cons of different approaches to monitoring in the public cloud.

Data Collection

Security and performance management require access to packet data, which is inspected and analyzed by monitoring tools for anomalies and patterns. Data is easily intercepted as it moves between physical devices in the data center, but in the cloud, data moving between virtual resources like Web browsers, applications, and databases—referred to as east-west traffic—is more difficult to intercept. When an organization uses a public cloud provider, the underlying infrastructure is completely transparent, and seeing data is even more challenging. Public cloud visibility solutions overcome this challenge by embedding a sensor inside each cloud instance that is spun up. The sensor can access all the data generated in that instance and deliver it to security and performance monitoring solutions.

KEYSIGHT TECHNOLOGIES

Two Models for Data Processing and Monitoring

Once data traffic is obtained from the public cloud, it must be securely delivered to monitoring tools. Today, organizations have access to cloud-based monitoring, as well as traditional tools that run in the data center. Deciding whether to monitor in the cloud or transfer data back to the data center depends on several different factors. In both cases, a visibility solution can make monitoring more efficient and cost-effective by sorting and filtering raw traffic, stripping away unnecessary data, masking sensitive information, and seeing deep inside packets to identify relevant information, such as user Internet Protocol (IP) address, device, operating system, application, or location.

Now let us examine the pros and cons of monitoring public cloud data in each location and when each approach makes sense for an organization.

Approach #1: Monitoring in the data center

With this approach shown in Figure 1, an organization transfers public cloud traffic back to the data center for monitoring using a secure transport mechanism. This is frequently done when organizations are in the initial stages of cloud migration and not yet ready to rebuild their security and performance monitoring architecture. Another use case would be when regulatory compliance cannot be achieved using cloud-based tools.

Once public cloud traffic arrives in the data center, a visibility processing engine can be used to filter out irrelevant data and apply advanced functions, such as de-duplication, secure sockets layer (SSL) decryption, packet trimming, etc., prior to sending data to monitoring tools. Processing reduces the volume of data that must be inspected or analyzed by monitoring tools to stretch tool capacity and extend useful life.

A variation on this approach is when an organization processes the traffic in the public cloud, closer to the source, and sends only filtered traffic back to the data center for monitoring. Cloud-based filtering reduces the volume of traffic that needs to be transferred and the related cost of the backhaul.

Advantages of data center packet processing:

- Minimal capital expenditures – no need to purchase new tools
- Minimal change to operations – no retraining of staff, no change management required
- Low risk – mature tools offer advanced features and proven support
- Compliance – on-premises processing may be required for certain security regulations

Challenges of Security Monitoring

Even when organizations move workloads to the cloud, they are still responsible for the security of user data and transactions. Key challenges include:

Security Policies:
Organizations need a system where security policies can be applied consistently and automatically, whether a workload is running in the data center, private cloud, or public cloud.

Access to Packets:
As workloads move to the cloud, packet-level data is not available, making it difficult to block known-bad IP addresses.

Tool Availability:
Traditionally, enterprises have used a variety of deep packet inspection and loss prevention tools, but many of these tools are not available in the cloud.

Multi-Tenancy:
Although the provider's intent is to maintain strict separation between tenants, there is always the risk that access might be inadvertently extended.

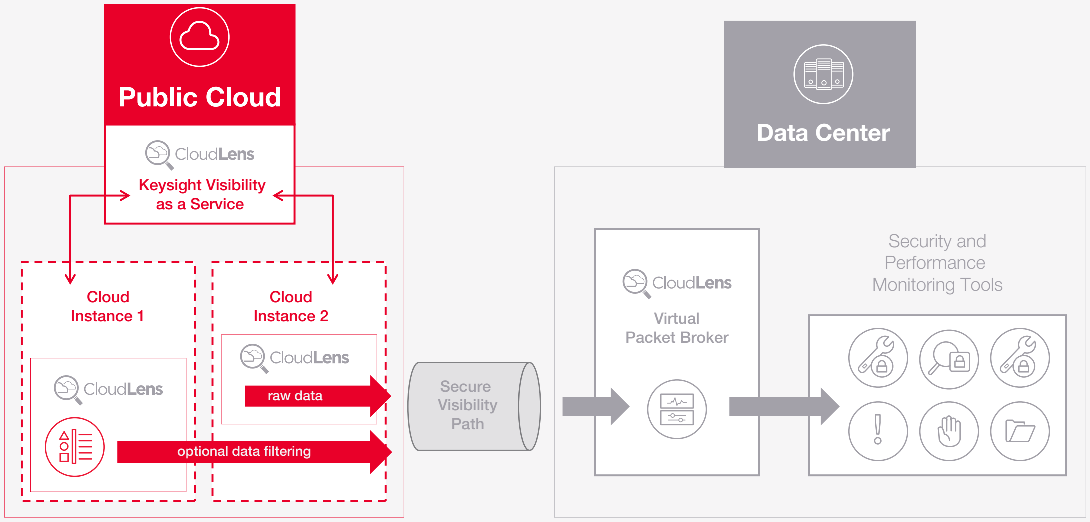

Figure 1. Data Monitoring in the Data Center

Disadvantages of data center packet processing:

- **Inability to dynamically scale along with cloud instances**
- **High cost of data transfer** – cloud providers charge to transfer data, which can be significant for unfiltered data
- **Latency** – backhauling data from the cloud provider can have a significant impact on latency

Approach #2: Data monitoring in the cloud

An alternative to backhauling traffic to the data center is to monitor data in the cloud to more fully realize the flexibility, speed, and infrastructure savings of cloud computing.

Visibility solutions to filter and optimize public cloud traffic can be based on two very different architectures. The first uses a centralized, cloud-based node to aggregate and filter traffic from multiple cloud instances. The problem with this design is that the aggregation node is a single point of failure in the architecture and can become a bottleneck as traffic volume increases. Adding a second node requires additional management and coordination. The result is that a centralized architecture can be less reliable and more expensive to operate, adds latency, and limits dynamic scalability.

Another architectural option—referred to cloud-native—is based on a distributed peer-to-peer model that establishes direct traffic paths from cloud instances generating data to cloud instances monitoring data. This architecture is scalable on demand and functions more like the cloud itself. This design, shown in Figure 2, eliminates the centralized node and single point of failure and increases overall efficiency. The direct connections are made via a secure, encrypted path to ensure data integrity.

The cloud-native model uses a centralized management layer running in the public cloud to create and manage policies for different data groups. Policies are then automatically applied to each new instance in that group to simplify management and eliminate configuration errors.

Advantages of cloud-based packet processing:

- Flexibility and on-demand scalability – data collection and filtering can be automatically initiated each time a new instance is launched
- No dedicated visibility infrastructure – data collection and filtering can be provided as a service with no capital investment required
- Reduced time to resolution – threat identification and issue resolution may be accelerated if data does not need to be transferred to the data center for monitoring
- Easy operation – a Web-based, drag-and-drop interface simplifies configuration and policy management and pushes data to Docker-based tools automatically

Disadvantages of cloud-based packet processing:

- Tool costs – you need monitoring tools or services capable of receiving secure traffic (e.g., containerized using the latest version of Docker)
- Tool functionality – cloud-based tools may not yet provide the same advanced features and reliability as data center tools
- Increased cloud expense – cloud capacity must also support traffic collection and filtering

Challenges of Performance Monitoring

In the cloud, you have far less control over application performance and more potential factors to evaluate. Key challenges include:

Interdependency:
Most cloud infrastructure involves multiple interdependent tiers, complicating root cause analysis.

Visibility:
Cloud environments involve multiple domains of control, which are incompatible with strong centralized monitoring.

Lack of Packet Data:
Without access to packets, it can be difficult and time-consuming to isolate and resolve performance issues.

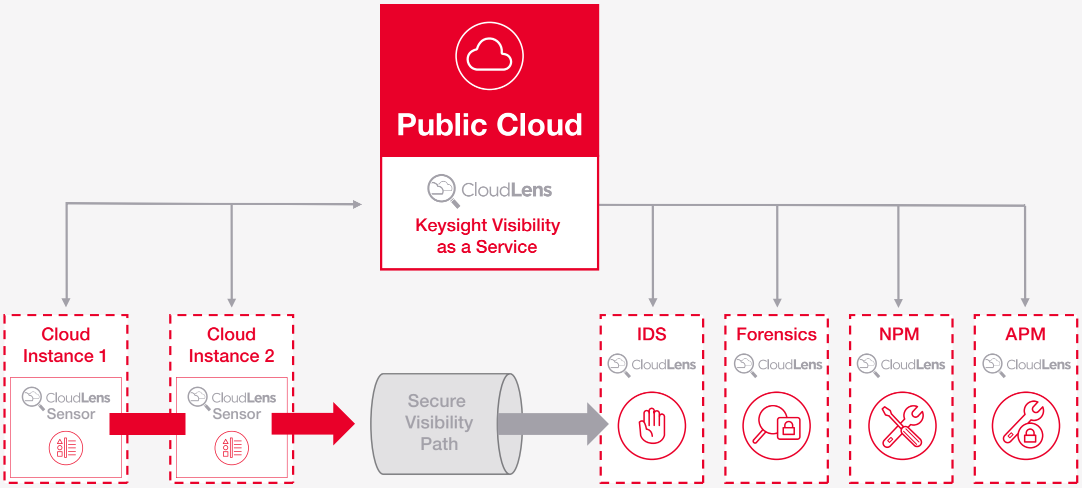

Figure 2: Cloud-Native Data Monitoring

A Hybrid Approach

Considering the limitations of the first two approaches, an organization may want to combine the best of both models in a hybrid approach. Consider a situation where, for compliance purposes, you need to continue using a particular deep packet inspection tool on-premises, even though you are now generating traffic in the cloud for certain applications (e.g., customer relationship management or payroll management). With a hybrid approach, you can deploy cloud-native traffic capture and filtering to collect the data, eliminate duplicate packets, and trim the data down to the only the most relevant information. You can then transmit the condensed data via a secure virtual path to a physical packet broker with the ability to monitor and load balance between your on-premises tools.

Of course, a successful hybrid model is dependent on complete access to the traffic data generated in the cloud. With a cloud visibility solution, you can sort and filter cloud traffic and delivery to your tried-and-true on-premises monitoring tools at the same time you are delivering relevant traffic to any new cloud-native tools. Even better, if you use a single visibility architecture to serve both kinds of tools, it can help minimize complexity, find breaches faster, help control operating costs, and accelerate problem resolution. Having one interface to build and manage packet filtering policies that are applied automatically to traffic, no matter where it is collected, will save manpower and reduce the number of errors.

Keysight's Cloudlens™ Visibility Solution

Keysight knows that a paradigm shift, like the migration to cloud, takes time. Traditional approaches may need to coexist with new approaches for many organizations. Keysight solutions not only support monitoring in either location, but simplify management across the two—which can be the biggest benefit.

Keysight CloudLens is available for both private/on-premises and public cloud environments and uses the same Web-based management interface for both. With CloudLens, you can create and manage policies and data filters once and have those rules applied across both environments. CloudLens uses a packet broker to sort and filter virtual traffic for delivery to tools located on premises. CloudLens is hosted in the public cloud by Keysight and offered as a visibility service to sort and filter traffic in the cloud, with no need for additional supporting infrastructure at all.

What makes Keysight's public cloud visibility solution unique is its peer-to-peer architecture. This approach is completely distributed and preserves the benefits of cloud computing. Competitive solutions, on the other hand, rely on a centralized node to receive and process cloud traffic, which introduces the well-known limitations of monolithic infrastructure: upper limits on size, difficulty scaling, cost, and inflexibility.

In contrast, the peer-to-peer approach of Keysight CloudLens offers many advantages for effective monitoring:

- **Performance:** Keysight's cloud visibility architecture was purpose-built for managing virtual cloud traffic, rather than being a cloud-enabled version of its data center solution. Keysight uses container technology to fully embed its technology in each cloud instance, so you do not have to backhaul all your cloud traffic to the data center for filtering and tool processing.
- **Flexibility:** Keysight's cloud agnostic design, leveraging container technology, can operate within any cloud service provider and offers maximum flexibility as your cloud strategy changes and evolves.
- **Reliability:** Keysight's peer-to-peer model, where virtual cloud traffic is delivered directly to your tools, increases reliability across the system. In contrast, solutions that rely on a centralized processing engine have a single point of failure, where failure of the central node causes the entire data delivery system to fail.
- **Scaling:** Keysight's approach activates virtual traffic tapping and filtering at the time a new cloud instance is initiated, for complete cloud scaling. A solution with a centralized processing engine has an upper limit on how much traffic it can handle before it needs to be upgraded and, therefore, does not support the same easy, cost-effective scalability.

Summary

As workloads move to the cloud, organizations must adjust their strategies for accessing and monitoring traffic data. They first need to access or tap traffic that is moving between cloud instances and then decide on a strategy for packet filtering and grooming—to help their monitoring tools work efficiently and cost-effectively. Keysight's unique CloudLens solution enables packet processing to be done in the cloud and then delivered either directly to cloud-based tools or transferred back to the data center for monitoring on-premises. The best overall monitoring strategy for many organizations will be a hybrid approach that supports continued use of powerful on-premises tools, combined with newer cloud-native tools, where available. With Keysight's hybrid approach, security is maintained at full strength, while the organization transitions to the flexibility, speed, and cost savings of cloud computing.

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