Why Most IT Professionals Don’t Want to Use Cloud-Native Monitoring Capabilities

A 2022 survey by Enterprise Management Associates (Network Visibility Architecture for the Hybrid, Multi-Cloud Enterprise) revealed that 99% of the enterprises surveyed were making at least some attempt to collect packet data in the cloud and supply it to their performance and security analysis tools. However, only 38% were relying on the native traffic mirror services of their cloud providers for this service. The other two-thirds of network infrastructure and operations, security, and data center operations teams were using 3rd party monitoring solutions, mainly consisting of cloud taps and packet brokers.

While there are lots of reasons that contribute to this decision, here are the four main macroscopic reasons that engineering teams don’t use cloud native monitoring capability:

1. Cloud services are not usually purpose-built for monitoring
2. If the cloud services are free or low cost, you get what you pay for
3. You can’t transfer native tools between multi-cloud environments
4. Cloud services are not suitable for a hybrid cloud environment

While advances continue in public cloud computing environments, most of the native cloud monitoring tools are not “enterprise grade” or purpose built. IT teams need full visibility into what is happening across their cloud network. This means they need full packet data, not simply log or flow data. While that information is useful, only full packet data that can be filtered provides the details to catch hidden security threats or performance problems. Healthcare providers and manufacturers were especially likely to favor full packets. North Americans favored this approach more than Europeans. IT executives also favor full packets more than middle managers and technical staff.

According to the EMA survey, here is the type and amount of the most popular monitoring data types:

- 46% use full packet data
- 38% packet meta data
- 16% packet header information

Costs play another role in the use of monitoring tools. Some vendors may give you free tools. But what is that worth, especially when you want packet data, and their tool gives you flow data? For instance, you need that packet-based data when you’re looking at end-to-end transactions. As an alternative, you could deploy a fleet of Linux servers in the cloud running TCPDUMP, instead of a packet broker, but then that option becomes extremely costly. You simply need the right tool — for the right job.

Another issue is that if you have a multi-cloud environment, you often can't transfer those cloud-provider tools to another cloud provider. So, now you have to get used to different tools that may not collect the same information in your separate public cloud instances. Third party solutions, however, often work with multiple vendors. This allows you to buy one type of packet broker and use it with different providers.

A hybrid of physical on-premises and a public cloud solution also benefits better from third-party solutions. In this type of solution, you may want to physically back-haul data from the cloud instance to your on-premises tools for deep security or performance analysis.

Benefits of Using Third-Party Visibility Software in the Cloud

The EMA survey uncovered the following specific benefits that IT teams experienced using third-party visibility solutions in the cloud:

- 54% saw improvement in reliability of data collection
- 36% had better administrative security (better control over traffic mirroring)
- 34% benefited from superior manageability / automation
- 32% were able to use the advanced packet filtering and modification features
- 30% found better integration with their visibility architecture in private infrastructure

The Weaknesses of Cloud Provider Traffic Mirroring Services

The EMA survey also uncovered the following issues that IT teams experienced using cloud-provider traffic mirroring services:

- 48% saw an increased security risk (due to malicious mirroring with compromised credentials)
- 33% suffered from tool management complexity (lack of automation)
- 30% experienced cloud provider lock-in (no multi-cloud visibility) for their services
- 28% saw higher than expected costs
- 27% said advanced features (masking, application identification) were unavailable

Reach out to Keysight Technologies and they can show you how to save money by optimizing your cloud and hybrid cloud security and monitoring 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:

KEYSIGHT

www.getnetworkvisibility.com/contact-us/