

Joint Solution Brief

Extend data visibility to dynamic, multitenant public cloud environments

The Challenge

Provide data visibility into a dynamic public cloud environment with the same transparency as for a physical data centre – even if, in the public cloud, responsibility for IT infrastructure is split between the tenant and cloud provider, and the underlying infrastructure is neither visible nor accessible to the tenant.

Integrated Solution

Gigamon's GigaSECURE® Security Delivery Platform decouples data collection, aggregation and customisation from operational tools, and guarantees data visibility across all infrastructure types, independent of the underlying technology.

Key Benefits

- **Gigamon virtual TAP technology** handles the agility of a public cloud environment to ensure accurate data collection of network communication
- **Data visibility** is a prerequisite to validate data privacy, e.g. for trading members sharing a common exchange connection, and the only way to monitor and analyse complex network setups using multicast in a public cloud environment
- **Same level of transparency** for data visibility in the public cloud as for an on-premises data centre
- **Investment protection** for the existing operational tool landscape to commonly manage the cloud and on-premises installations
- **Easy and cost-effective solution** for testing new tools or introducing new cloud-based technologies with minimum effort

Introduction

To increase flexibility of their IT infrastructure, more and more enterprises are considering a cloud solution as part of their IT strategy. And, due to agility and cost-effectiveness, many are turning to a public cloud as an on-demand resource, to which they can partially or completely migrate their applications.

However, the challenges of security, application and network performance management still remain, because visibility of data streams is THE essential requirement for security, application and network performance management.

In traditional data centres these challenges are addressed using physical TAPs, SPAN ports and packet broker tools to collect, aggregate and provide data in the formats required by operational tools for security, performance management, threat prevention etc. And because IT teams have full control over all the layers within their data centre's infrastructure, they can use whichever technologies best fit their needs.

But in a public cloud environment, the underlying infrastructure is controlled and operated by the cloud provider, with the IT organisation focusing on configuring the infrastructure according to their needs and those of their applications. It is this shared responsibility for the different layers of the IT installation that results in limited data visibility.

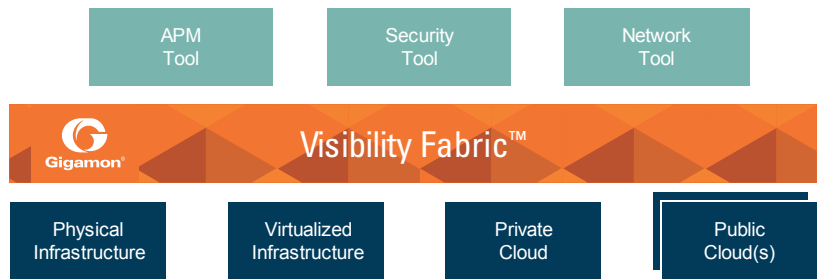
Also, because the architectural approach has changed from one based on the required numbers of servers to one focusing on applications and services, a major consequence is that a relatively static environment is replaced by a dynamic IT infrastructure that permanently and automatically adjusts itself according to the loads demanded by users and applications. So whereas from a cost point of view this looks an optimal solution, as resources are only paid for as required; from a visibility standpoint the constantly changing cloud environment is a major problem for data visibility.

Migration to the cloud therefore raises the question not only of migration of the application itself, but also how to migrate and configure the associated management tools (which are usually focused on a static IT environment), protect existing investments in these tools (e.g. licenses, skills etc.) and evolve their associated operational processes.

The Gigamon and operational services Joint Solution

Gigamon offers a solution to these issues through the use of virtualised TAP technology for public and private clouds. As in a traditional data centre, the basis of this technology is to decouple the collection, aggregation and customisation of the data stream from the tools analysing the data – with the Gigamon Visibility Fabric™ linking the two layers.

This decoupling results in a situation where only the data collection layer is technology-dependent. As in a traditional data centre where a physical TAP is used to link to a cable or SPAN port, a virtual TAP is used to gather the data from the virtual cable connecting the servers to the VPC.



The agility of the cloud environment is handled by the Gigamon Fabric Manager, which is linked to the API of the public cloud provider and controls all TAPs across the installation. Fabric Manager also controls and configures virtualised GigaVUE® V Series visibility nodes that aggregate, select, optimise and distribute traffic. These nodes only provide data to the various operational tools as needed, thereby optimising the use of these tools; while traffic optimisation also reduces the costs associated with external public cloud traffic.

Due to the availability of physical and virtual TAPs for all steps of technology evolution (physical data centre, virtual data centre, private and public cloud), common operational tools for security, application and network performance management etc. can be used for all parts of the IT installation, independent of the underlying infrastructure.

Due to the availability of physical and virtual TAPs for all steps of technology evolution (physical data centre, virtual data centre, private and public cloud), common operational tools for security, application and network performance management etc. can be used for all parts of the IT installation, independent of the underlying infrastructure.

Use Case by operational services – Amazon AWS

operational services, one of the leading ICT service providers in the German market, has implemented a reference installation using Gigamon virtual TAP technology in an Amazon AWS public cloud, based on a business scenario from the finance industries, the aim of which is to provide a geographically independent solution to connect to the simulation environment of a major German trading venue’s trading system.

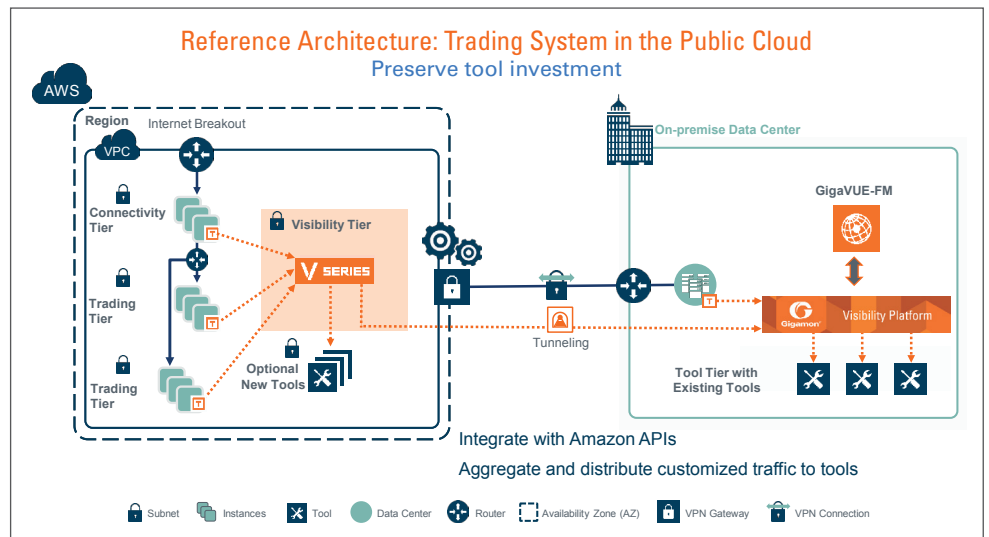
To accomplish this, an AWS VPC was configured with a connectivity tier, responsible for handling the connection to the central trading backend; and several trading tiers, configured within the VPC, to ensure customer privacy and data protection within the architecture.

The major challenge in this kind of situation is the distribution of market data. Because the exchange trading system relies on the use of multicast to forward market data to the trading servers, and AWS does not natively support this protocol, some additional network setup was required. (Transaction routing to the exchange can be provided natively within the AWS infrastructure.)

Gigamon virtual TAP technology was used to guarantee data visibility across all tiers, ensuring data privacy for each member is not only

theoretically available, but is kept and controlled for every single transaction and confirmation. In addition, the enhanced network setup is closely monitored to ensure any abnormalities within the market data streams are detected and followed up.

Due to decoupling the underlying technology from the operational tools, all existing monitoring, analysis and reporting tools at an organisation’s own data centre can be used without any additional licenses or setup, by simply linking the output path of the AWS visibility tier back to the data centre. New tools can also easily be tested, simply by linking the output path of the visibility tier to another target, e.g. a cloud-based tool for anomaly inspection of network communication, or any other use case.



Learn More

For more information on the operational services and Gigamon solution, contact:



kai.behning@o-s.de
www.operational-services.de



www.gigamon.com