Ixia CloudLens: Managing the Elastic Cloud Visibility Surface

The attack surface of a software environment is the sum of the different points where an unauthorized user (the attacker) can try to gain access to, or otherwise impact, that environment. With the strong growth of public, hybrid, and virtual private clouds, on top of the traditional enterprise private cloud, the size of the attack surface increases dramatically. Effective monitoring in these multi-tenant environments, where usage is elastic and access is limited, requires its own type of visibility.

A common set of visibility tools must span these different deployments while also supporting existing physical networks. These tools need to look beyond simple data access, integrating a sophisticated security fabric to sift through vast quantities of data. Any solution must address the needs of enterprises and cloud-native software as a service (SaaS) companies, many of which are also leveraging new software-defined wide area network (SD-WAN) deployments, as well as the service providers themselves.

In the cloud, the attack surface has become a multi-faceted, constantly in motion visibility surface that needs its own monitoring and management.

KEYSIGHT TECHNOLOGIES

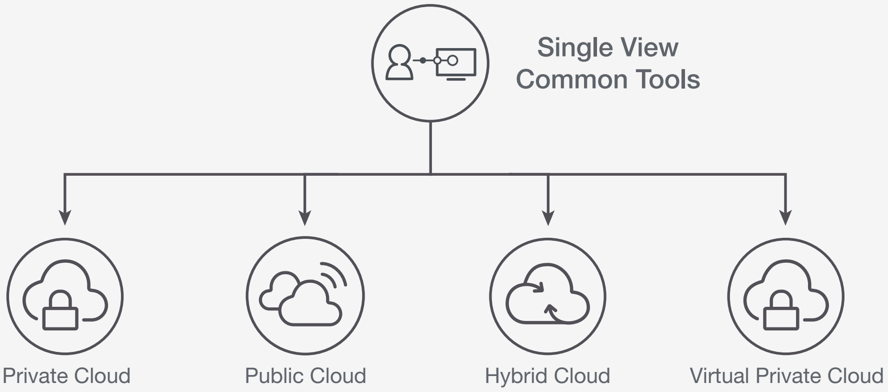


Diagram 1. Four cloud types.

There are four types of clouds where visibility is needed, each with different characteristics.

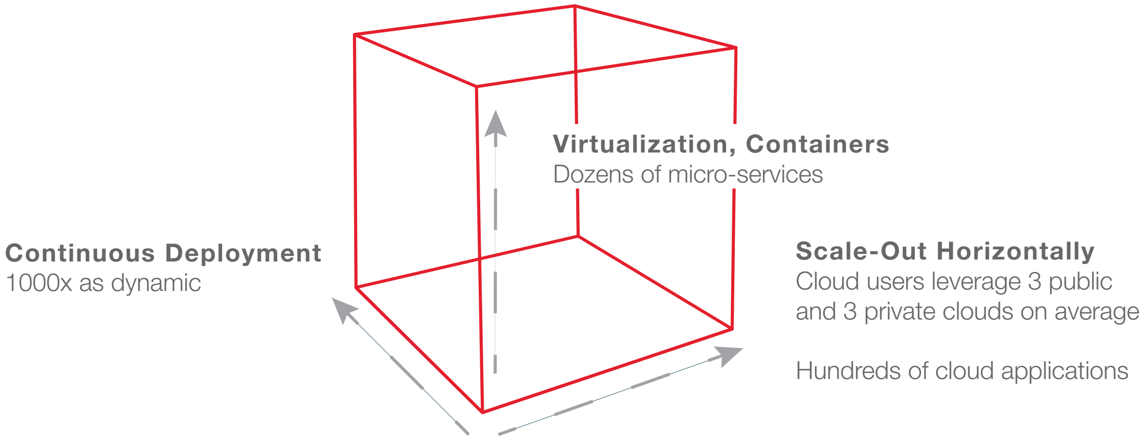
- **Private Cloud:** Deployed and managed by the enterprise, private clouds rely on dedicated resources that are easily accessible and controlled.
- **Public Cloud:** Services like Amazon Web Services (AWS), Google Cloud, Microsoft Azure, and others offer much less expensive multi-tenant services on shared infrastructure with elastic compute and storage capabilities. Public cloud adoption continues to expand rapidly with AWS S3 growing over by over 650% between 2006 and 2013.[1] Predictions for public cloud workloads show it growing at least 400% from 2015 to 2020.[2]
- **Hybrid Cloud:** A combination of the first two with orchestration tying them together. Over 82% of enterprises are moving in this direction as more make tradeoffs between network control and affordability.[3]
- **Virtual Private Cloud (VPC):** A set of partitioned public cloud resources that look much like a private cloud. They use public cloud infrastructure but are not multi-tenant. This is useful for hosting more sensitive data and applications.

[1] https://aws.amazon.com/blogs/aws/amazon-s3-two-trillion-objects-11-million-requests-second/
[2] https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html
[3] https://www.rightscale.com/lp/state-of-the-cloud

How Visibility Is Adapting to the Cloud

In parallel to the diversity of cloud growth, the nature of the visibility surface is evolving. This growth has occurred in three separate dimensions.

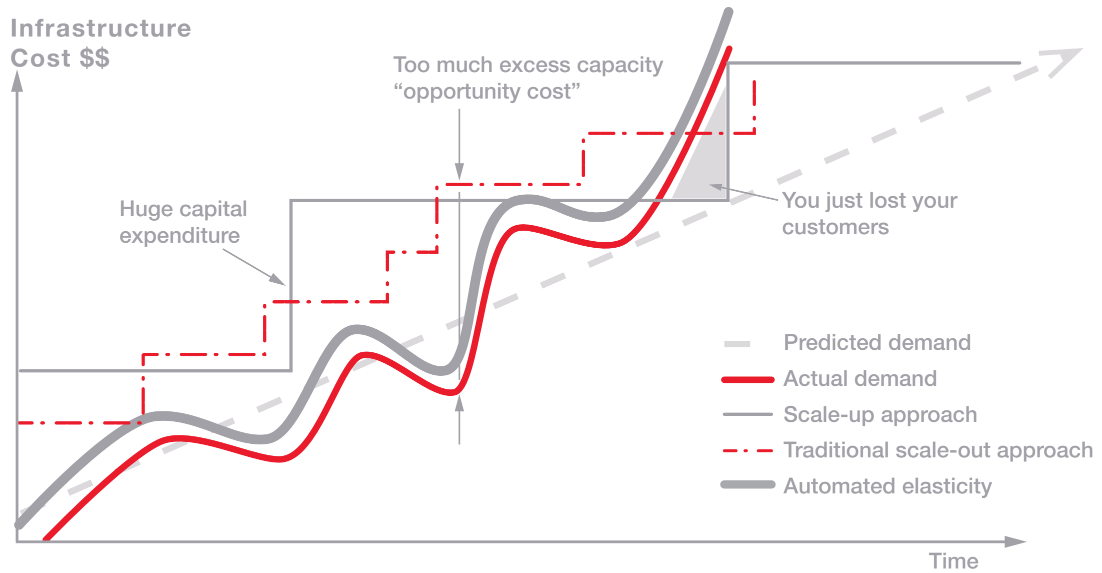
- **Horizontal scale**: Within the cloud, loads scale out horizontally. More users and greater workloads are accommodated automatically. The number of cloud services a typical company uses is growing, as well. Statistics show that 1 in 10 cloud services used by the average enterprise have been vetted by information technology (IT) professionals.[4] Consider that the typical enterprise uses three public and three private clouds. Scaling starts by identifying the number of attack surfaces and having elastic monitoring capable of scaling.
- **More containers**: The number of virtual machines (VMs) deployed within an enterprise is growing. Containers multiply this density 10-fold or more,[5] as each application may employ multiple containers. Security rules proliferate, and IT faces decreasing visibility for business-critical applications. Scaling is managed using role-centric monitoring solutions.


Virtualization, Containers
Dozens of micro-services
Continuous Deployment
1000x as dynamic
Scale-Out Horizontally
Cloud users leverage 3 public and 3 private clouds on average
Hundreds of cloud applications

- **Elasticity**: Individual VMs, containers, and therefore, their hosted applications have shorter lifespans, requiring continual awareness of the actual state of the environment. As an example, consider how to archive and retrieve monitored traffic from a container that no longer exists. Enterprises increasingly deploy DevOps tools like Chef and Puppet to assist, but there is only so much expertise to go around, and inefficient lifecycle load management impacts profitability. In fact, 26% identify cloud cost management as a significant challenge but don’t have the resources or expertise to address it.

[4] http://info.skyhighnetworks.com/rs/274-AUP-214/images/WP_Skyhigh_Cloud_Adoption_Risk_Report_Q4_2015.pdf

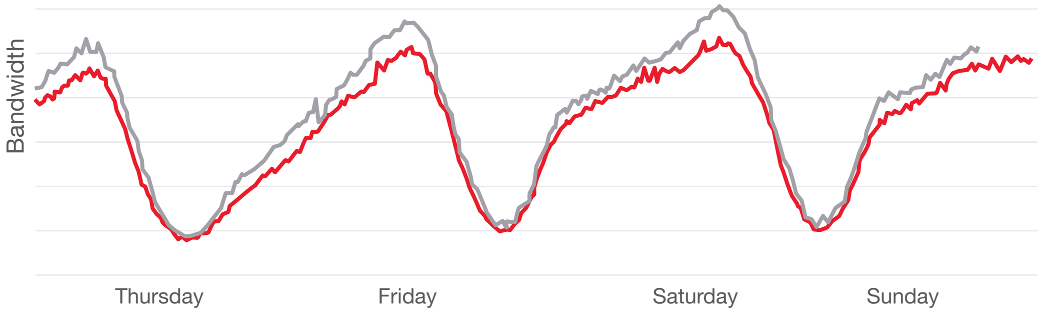
[5] https://www.datadoghq.com/blog/the-docker-monitoring-problem/



Automated Elasticity + Scalability

Elastic Visibility

The advantage of public cloud resources are their elasticity—or the ability to scale up or down based on instantaneous need. Visibility must also be elastic in the same way that compute, storage, and networking loads within the cloud scale automatically and on-demand. Provision too quickly, or with insufficient granularity or insight as to actual requirements, and you are left with stranded resources. Rely on existing manual tools that cannot keep up, and the network is unprotected. The figure below depicts this issue, with resources peaking at certain times of the day, and dropping in others.



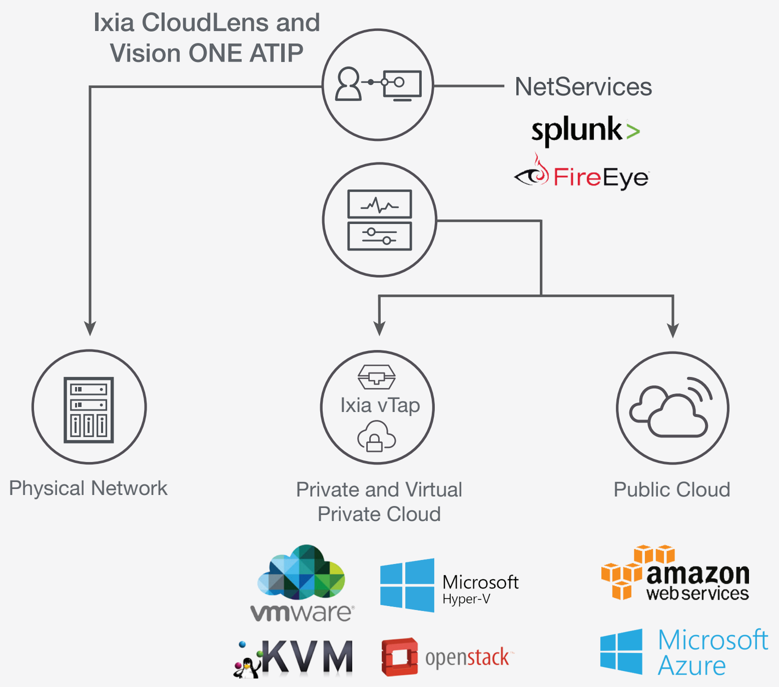
Network #2 - Netflix Traffic Comparison

We see this in everyday life. Stock trading is highest during times when the market is open but drops dramatically when it is closed. Similarly, video streaming services, like Netflix, peak on evenings and weekends but drop during the day and times when the majority of people are sleeping. And even within a cloud deployment that is not growing daily, traffic volume may vary widely over a 24-hour period. Consider what that implies in compute and storage requirements—and now associate that to visibility.

An automated solution for accessing, consolidating, and monitoring virtual traffic within and across cloud-based environments is critical. This is what we mean by a cloud security fabric: virtual visibility that translates into better security, as well as centralized security processes that can be executed and implemented across cloud boundaries. This results in security that can better and automatically scale as your workloads grow and you dive further into the cloud.

Ixia CloudLens™

Ixia CloudLens meets the scale and elasticity requirements of the new world of visibility, spanning the different cloud environments and offering insight, monitoring, performance, and security. It uses a security fabric that combines context awareness and intelligence and offers deeper visibility and actionable insight across virtualized environments.



- For the private cloud, Ixia's Phantom™ vTaps monitor VMWare, Microsoft Hyper-V, KVM, and where deployed, OpenStack.
- Public cloud support via Ixia's CloudTap™ includes both AWS and Azure, with more to come. This includes self-service capabilities.
- Vision ONE™ with its Application and Threat Intelligence Processor (ATIP) ties this all together with advanced network packet broker (NPB) capabilities that extend to external platforms such as firewalls, helping to maintain security and identify and resolve performance problems across both physical and virtual infrastructures.
- CloudLens NetServices is the repository for detection, mitigation, active validation, and forensics solutions, some offered by Ixia, and others by third parties, such as Splunk and FireEye. A NetServices advantage is that the tools are guaranteed to automatically scale with the needs of the deployment.
- Centralized monitoring spans an enterprise's private and public clouds, as well as traditional data centers, where deployed.

Enterprise Use Case

But what does this mean to the enterprise? Consider the following...Newco is in the midst of a transition to the public cloud and has critical applications deployed in a traditional data center, while others are deployed within its private cloud. Given a recent security breach, the head of IT, Marsha, has been tasked with implementing malware detection across all three environments.

Marsha deploys CloudTap within the public cloud, deploys Phantom vTap in the private cloud, and has a pre-existing VisionONE network packet broker in the data center. The first step is to identify a malware detection tool. Here, she goes to the NetService marketplace and selects one that will do the job. She also has future plans to deploy a third-party next generation firewall, also available via the marketplace. In both cases, the tools and applications are validated by Ixia and offer a consistent experience across the different environments, while scaling automatically, as required.

Her next step is to determine which hosts require the tool. Using CloudLens, Marsha literally turns back the clock, identifying those servers that were compromised. Although they reside in the data center, Ixia's Vision ONE offers her the same flexibility that she would have with cloud monitoring. Next, she leverages Ixia ATIP application monitoring to identify other services, such as email, that require protection.

The final step is to set automation. For the cloud, a server can be quickly brought down and replaced, if compromised. A snapshot of the system will help with future forensics. For the data center, if a server cannot be brought down, a high-priority ticket will be created for immediate action.

Conclusion

In this evolving world of the cloud, you require a solution that is agile, secure, and automated, and that spans the growing visibility surface. The growing attack surface has created a multi-faceted, constantly-in-motion, next-generation “visibility surface” that needs to monitored and managed. And, you need to manage this with a common set of tools that spans your different cloud environments while supporting existing physical networks—a solution based on a sophisticated security fabric that effectively handles the vast quantity of data available. Ixia CloudLens delivers this solution for enterprises, cloud-native SaaS companies, and service providers, while also supporting evolving SD-WAN deployments.

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