Cloud Visibility Overcomes Security Limitation of Turnkey Private Cloud

For government entities, network security is mission-critical and subject to strict regulations. That is why this customer, who was deploying a turnkey private cloud platform, was concerned when they realized their provider could not supply the data needed by their threat detection and security analysis solutions. Without the ability to examine packets for potential threats, their new private cloud would present a considerable risk to their network.

In search of a solution to provide access to packet data, this government customer turned to Keysight, who worked alongside their security solutions provider to deploy a total cloud visibility solution and eliminate this serious security issue.

Some Organizations Are Prohibited from Using Public Clouds

While cloud computing offers significant benefits, some organizations do not want to, or cannot legally, connect their computing infrastructure to the internet. This is often the case for government agencies and companies with major federal contracts, that are required to adhere to strict security guidelines. A secure private cloud, with no connection to the internet, offers the best of both worlds: the flexibility and cost efficiency of cloud, with the isolation and separation

Company:
National government with secure, centralized technology environment

Key Issues:
- Azure Stack private cloud platform unable to provide access to traffic packets
- Need ability to monitor all virtual traffic so security solutions can detect threats and ensure compliance

Solutions:
A comprehensive private cloud visibility solution, consisting of:
- Hundreds of Keysight CloudLens classic vTaps and new vTap Sensors
- Twenty Keysight Vision Edge and dual Vision ONE network packet brokers

Results:
- Private cloud platform is no longer a critical security vulnerability with Keysight's packet access solution
- Faster identification and resolution of threats across hybrid IT environment
- Future ability to use Vision ONE NPBs to deliver optimized traffic to network and application performance monitoring solutions

KEYSIGHT TECHNOLOGIES

required for compliance.

Turnkey Private Clouds Are a Compelling Option

Major public cloud providers are stepping up to meet the needs of organizations that cannot use public clouds and have no desire to build and maintain their own private cloud. Several providers now offer a turnkey private cloud platform, with features similar to their public cloud offering, that is completely isolated from the internet, easy to deploy, and flexible to scale. Users are responsible for keeping their cloud deployment updated, but they have no need to hire cloud architects or developers to maintain the platform or its features, which is where many do-it-yourself clouds turn costly and unwieldy. In this use case, the customer chose Azure Stack, a turnkey private cloud platform from Microsoft.

Unfortunately, the convenience of using a pre-built platform came with a trade-off. Azure Stack does not give administrators access to the underlying infrastructure components, such as the hypervisor layer. This limitation meant the security team would not have access to the virtual traffic in their private cloud, which had serious

"As a government entity, we are not allowed to use public clouds or any solutions that require us to be connected to the internet."

– Chief Information and Security Officer, National Government

implications for security.

Packet Data Is a Must for Effective Security Monitoring

Governments set up private clouds to host applications in a centralized environment because they can be more easily secured and protected. In this case, the plan was to send traffic from several government agencies—including immigration, security, and law enforcement—to a private cloud for monitoring by best-of-breed solutions.

The government's security and risk management team chose a leading security vendor to provide products for network and endpoint threat detection and security forensics. These solutions use deep packet inspection to understand the context of communications moving through the network and to identify "indicators of compromise" that provide evidence of a network attack or data exfiltration. Packet detail would be critical to timely, accurate detection and resolution of security issues. Without access to packet data, the customer would not be able to adequately protect their private cloud.

> "We plan to expand the Keysight | Keysight visibility platform, to provide relevant packet data to our network and application performance monitoring solutions, as well."
>
> – Lead Solution Architect, National Defense Agency

You Need Packet Access for Every Cloud You Deploy

The customer considered using the existing Gigamon network visibility platform in their data center, but it did not have a solution for accessing packets in the Azure Stack cloud. Keysight is the only vendor that deploys sensors right inside the private cloud platform to see every virtual packet and send them on for monitoring, when necessary.

Keysight engineers deployed CloudLens vTap Sensors to access packets in the Azure Stack platform, along with classic CloudLens vTaps to access virtual traffic from other on-premises infrastructure. Together, these products allow the customer to monitor all the traffic that passes through their network, even when IT does not have access to the physical infrastructure.

CloudLens vTap - Cloud Sensors Architecture

No hypervisor access required

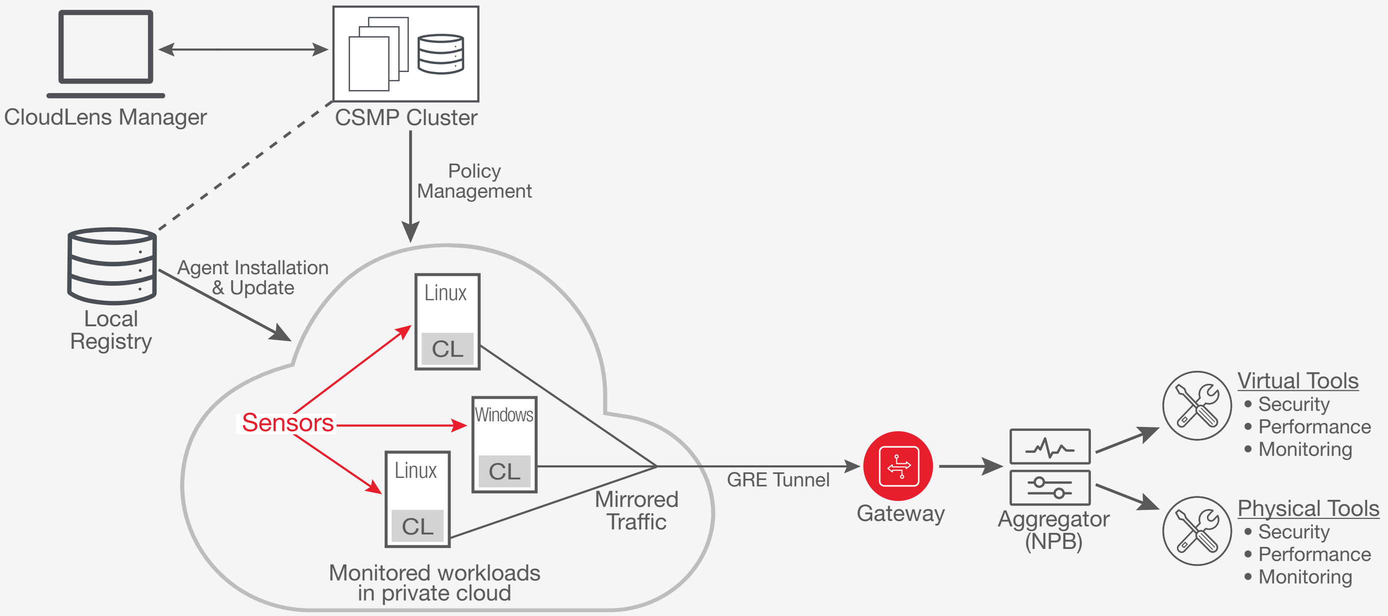

Figure 1. Basic operation of Keysight CloudLens vTap Sensors

Security Monitoring Is More Efficient with Packet Filtering

In addition to packet access, the Keysight visibility platform uses a powerful processing inside its NPBs to strip away unnecessary data and isolate the packets that require security inspection. Pre-processing significantly reduces the load on monitoring tools and can reduce the need to add capacity. Keysight's NPBs can also decrypt secure packets for faster processing, eliminating the need for a separate decryption device.

In this case, the customer also chose to aggregate packets at the network edge to improve performance using Keysight Vision Edge NPBs. In the data center, a pair of powerful Vision ONE NPBs ensure that optimized, pre-processed traffic is delivered to security solutions without disruption. With Vision ONE's drag-and-drop interface, administrators can easily direct traffic to multiple monitoring solutions, simultaneously, to further accelerate threat identification and resolution.

Summary

This government customer chose an Keysight cloud visibility solution to ensure that the traffic moving through their Azure Stack secure private cloud is adequately monitored for threats and anomalies. With security enhanced, their secure private cloud platform will provide the flexibility and cost efficiencies needed to drive a strong return on their investment.

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