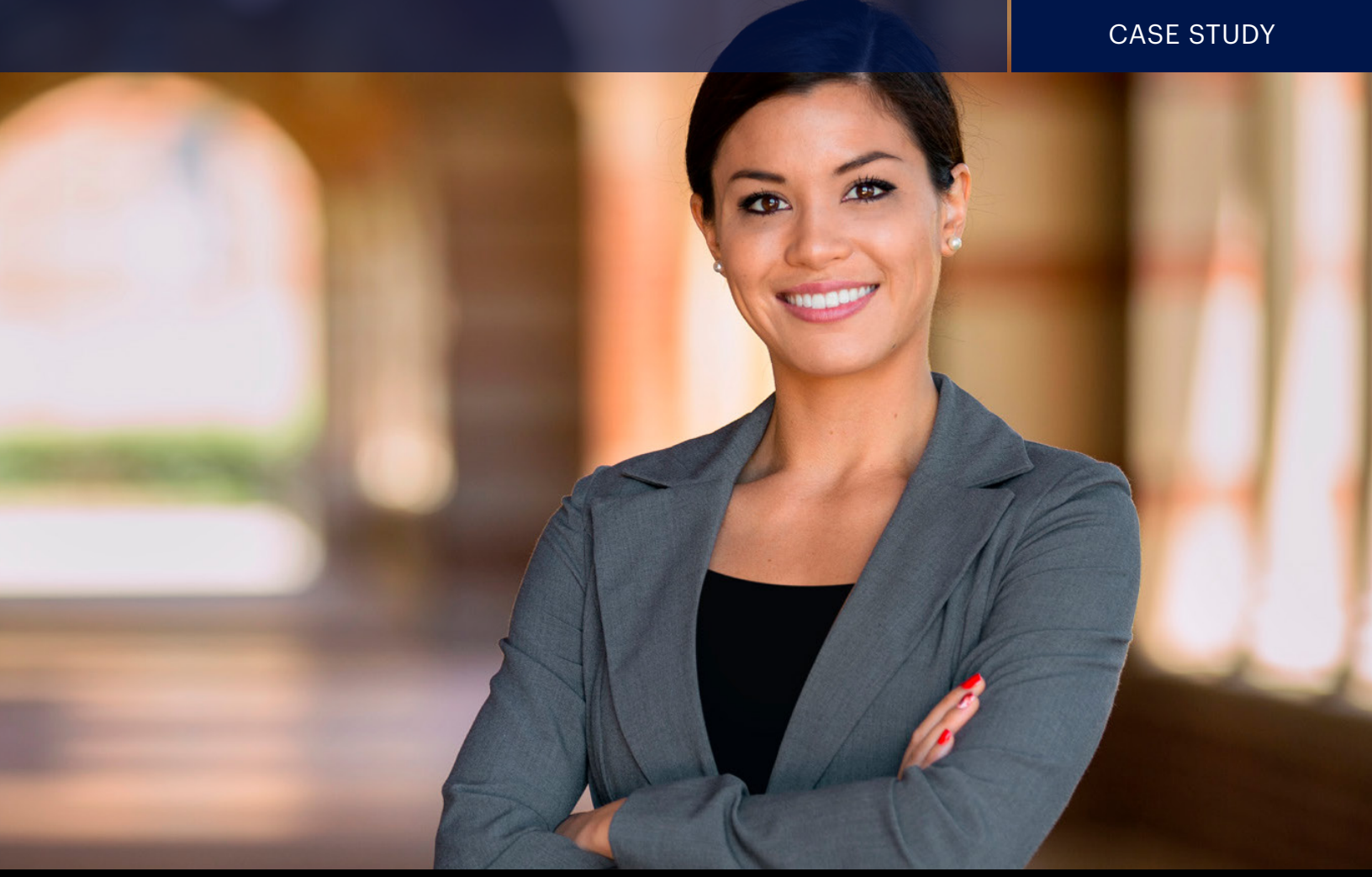
CASE STUDY



Keysight vTaps and Vision ONE

Addresses changing government infrastructure

KEYSIGHT

Organization

- Large U.S. government agency

Challenges

- Access to network packets in virtualized data center

Solutions

- One hundred virtual taps
- Two Vision ONE network packet brokers

Results

- Integrated visibility system for physical and virtual segments
- Ability to collect virtual traffic and pass to monitoring tools for trend analysis

Overview

Most government agency data centers in the United States are policy driven with procedures in place for monitoring everything occurring within each center. Many are now highly virtualized, and while the information technology (IT) teams recognize that visibility gaps exist, many are not aware of a solution. The Keysight account team introduced this large federal agency to Keysight's integrated virtualized visibility platform, which maximized monitoring effectiveness by ensuring proper access to the data the customer needed, when and where it needs it.

The customer IT team maintains a high level of visibility into physical networks by using numerous security, forensics, and application performance monitoring tools to perform extensive inspection. With most servers deployed as virtual machines (VMs) in a VMware stack, it recognized the visibility gap created by east–west traffic flowing between VMs. The customer recognized the need for a more reliable and holistic view of the network, traffic flows, and problem points. It decided to expand beyond basic virtual data access via native port mirroring and debugging by implementing an end-to-end visibility architecture that uses virtual taps (vTaps) for access, and network packet brokers (NPBs) to bolster security, simplify management/configuration, and improve the efficiency of its monitoring tools.

Moving to a fully virtualized data center, the customer had significant blind spots for east–west traffic between application and web service tiers running on the same host. Normal port mirroring offered by VMware ESXi did not work as the customer encountered multiple technical issues:

- In order to get access to packet data between VMs, the customer considered leveraging the natively available port-mirroring options on VMware's ESXi. However, this would create a number of security issues in a highly controlled environment.
- Not being able to filter at the source caused significant issues due to infrastructure change, cost requirements, and the amount of traffic to transfer from one data center to another.
- The customer needed to tap the virtual traffic in one data center and forward it to a different data center, where its analytics tools were located. The lack of tunneling options and difficulty in managing these (provided by VMware's native hypervisor environment) made it difficult to implement distributed end-to-end visibility.
- Enforcing security policies in a highly dynamic virtualized environment required continuous access to application data of interest, irrespective of VM mobility events.
- Enabling mirroring affected the performance of key workloads running on the same host.

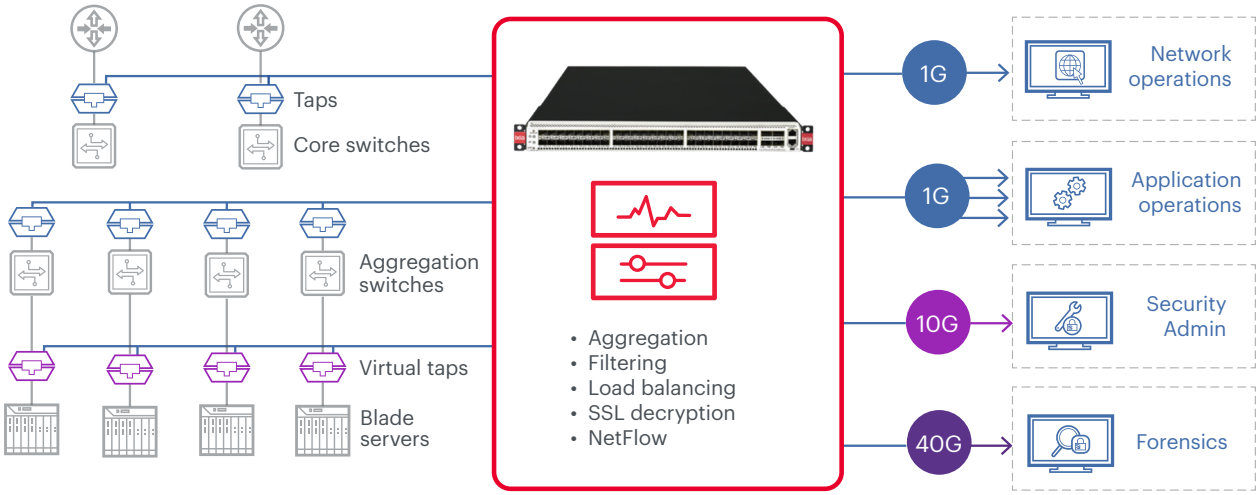
The Keysight Solution

What made Keysight's intelligent visibility platform especially powerful and best suited for this customer was the combination of vTaps and Vision ONE's intelligent packet processing capabilities. Together, these functions enabled packet and application data manipulation; NetFlow generation with advanced application identification and geographic location; secure sockets layer (SSL) decryption, load balancing; and many advanced packet processing capabilities, like deduplication, header stripping, and fragmentation. Examples include filtering at the application level, the generation of NetFlow data, SSL decryption, the generation of geo-location of users and devices, and the capture of browser information. The solution provides unprecedented insight into network traffic in both physical and virtualized multi-tenant environments.

Additionally, the customer recognized the following features of Keysight's vTaps as essential to implementing pervasive end-to-end visibility in its environment:

- 100% visibility of east–west, inter-VM traffic.
- Multiple tapping and tunneling options for data distribution, including Generic Routing Encapsulation (GRE), virtual local area network (VLAN), and encapsulated remote switch port analyzer (ERSPAN) allow maximum flexibility to provide data access and distribution across various remote sites and virtualized data centers.
- Non-proprietary and tool agnostic, able to send traffic to any existing security or performance monitoring tool.
- Easy and quick deployment to an entire virtual data center with VMware's vCenter.
- Hitless plug-in installations with no required VM maintenance mode.
- vMotion support, allowing the customer to migrate running VMs from one physical server to another without downtime and ensuring persistent access to virtual workloads being monitored.

After trying out 100 vTaps, the customer recognized Keysight's visibility solution benefits and is preparing to roll it out across all seven of its data centers. This will result in the deployment of several thousand vTaps and numerous NPBs throughout the network.



Key Takeaways

- Validation of the visibility architecture approach: This customer actively sought to improve network visibility in a systematic way. Keysight Visibility Architecture concepts let us present a holistic solution instead of a product-oriented approach.
- The east–west challenge is rapidly gaining awareness. Customers embarking on virtualization quickly realize that inter-VM traffic within servers constitutes a new blind spot that must be dealt with quickly and efficiently.
- Complex solutions are simple for Keysight; with the breadth and depth of Keysight's visibility portfolio and ecosystem of partners, no challenge is too large. From the network. Tap to the packet broker, we can mix and match products to deliver the right solution.