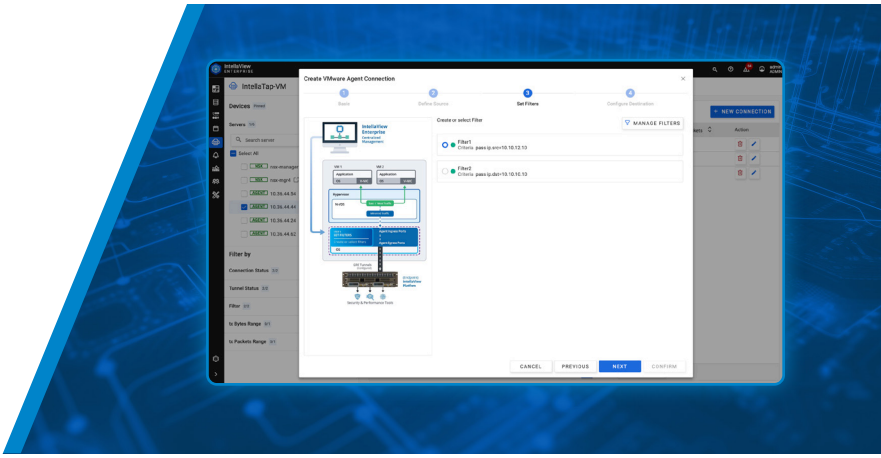
BROCHURE

Magnified Visibility for VMware Environments

EMPOWERING SECURITY & OVERCOMING VIRTUAL NETWORK BLIND SPOTS



KEY FEATURES

Simple and Efficient UI
With a few clicks, IntellaTap-VM gives you visibility into your VMware network traffic.

Unified Virtual & Physical Network Visibility
IntellaTap-VM and IntellaView Enterprise deliver a global view of your network environment.

Scalable to Meet Your Needs
Whether you have 10 VMs or hundreds, we have you covered.

Automated Deployment
IntellaTap-VM integrates with VMware and NSX-T Manager for automated agent deployment.

BENEFITS AND CAPABILITIES

- 100% visibility of VM traffic
- Apply traffic filtering and packet slicing policies
- Tunneling capabilities
- Optimize security tools
- Bandwidth reduction on production networks
- Little to no network impact during installation

BRIDGING THE VISIBILITY GAP BETWEEN PHYSICAL AND VIRTUAL NETWORK ENVIRONMENTS

Today, with most servers deployed as virtual machines (VMs) and many enterprises moving toward software-defined data centers, the amount of virtual network traffic between VMs has increased exponentially. As more networks become virtualized, a visibility gap occurs. Much of the East-West traffic (or traffic between VMs) never actually leaves the virtual environment, and more importantly, never traverses the physical network where traditional monitoring technologies are deployed.

Now more than ever, businesses need a reliable and holistic view of the network, traffic flows, and problem points. If not managed correctly, moving to a virtualized data center can lead to significant blind spots and vulnerabilities throughout the network.

An example of not having visibility of East–West traffic is the traffic transmitted between the application and web service tiers running on the same host. Many IT professionals deploying basic port mirroring offered by VMware ESXi often encounter multiple technical issues.

NETWORK AND SECURITY TEAM HEADACHES

- Not having visibility of intra-VM traffic can create many security issues such as malware or code injections traveling undetected between VMs.
- Leveraging natively available port-mirroring options within VMware ESXi can cause unnecessary strain on your production network due to the sheer amount of unfiltered traffic.
- Security and network tools become oversubscribed, leading to dropped packets.
- Enforcing security policies in a highly dynamic environment requires continuous access to application data of interest.

Often network professionals want to expand beyond basic native port mirroring by implementing an end-to-end visibility architecture that includes a network observability solution to bolster security, simplify management/configuration, and improve the efficiency of monitoring tools. However, deploying these tools can pose several challenges. Automation, scalability, and configuration are all considerations; in addition, deploying and configuring vTaps manually can result in downtime and prolonged deployments/setups within a virtual network.

CENTRALIZED MANAGEMENT

Integrated physical and virtual network visibility requires centralized management that's easy to use.

FILTERING TRAFFIC OF INTEREST

IntellaTap-VM TAPs and filters user-selectable virtual machine traffic, then sends only traffic of interest across the physical network.

USE EXISTING TOOLS

Enterprises have significant investment in security and diagnostic tools that safeguard networks and keep them running well. APCON's integrated virtual and physical network visibility solution can direct all traffic of interest to one or more tools giving security experts complete visibility across the entire network while, at the same time, increasing tool efficiency.

WHY CHOOSE APCON'S PRODUCTS?

APCON blades boast intuitive graphical user interfaces (GUIs) seamlessly integrated into world-leading physical switches, providing scalability to effectively monitor the continuously expanding landscape of enterprise data centers.

Scalable Solutions

Reliability & Redundancy

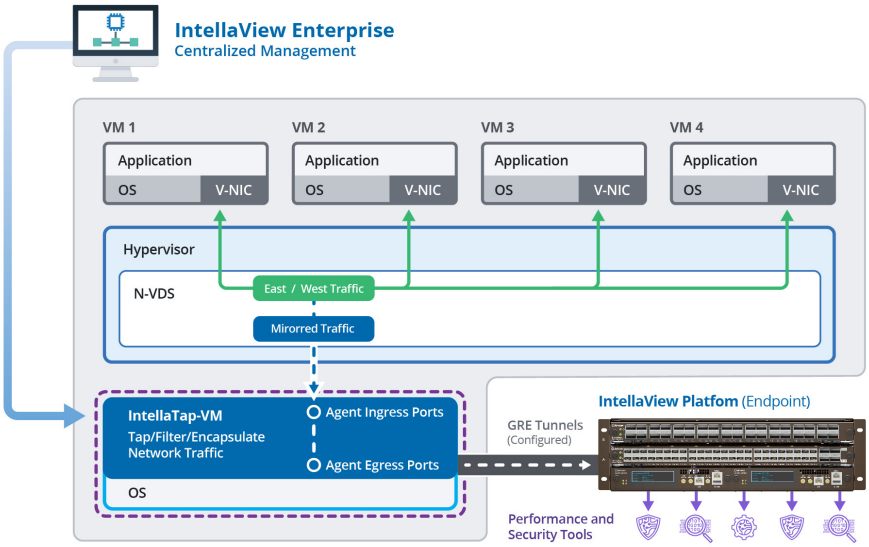
Density & Throughput

Innovative Design

APCON'S INTELLATAP-VM SOLUTIONS

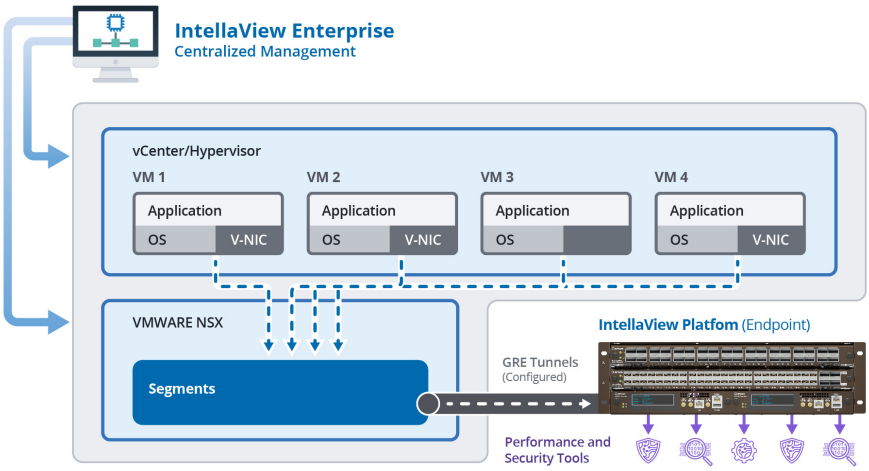
VM Monitoring Solution Overview

The VM Monitoring solution relies on customers deploying a compatible Virtual Machine with one or more interfaces in the virtual network of interest, as well as one or more interfaces with access to the physical network. In this solution, IntellaView Enterprise does not deploy a virtual machine, nor create or manage interfaces on the target agent. Customers mirror traffic of interest to a port on the VM agent using their own virtual network tools. IntellaTap-VM Monitoring provides the ability to specify packets to be forwarded with user-defined packet filters and multiple tunnel endpoint addresses.



NSX Manager Solution Overview

VMWare's NSX is a network hypervisor that provides a platform to manage virtualized network deployments. NSX supports both vSphere environments as well as non-vSphere environments. APCON's IntellaTap-VM NSX-T basic solution utilizes REST API to give our partners the ability to create logical port mirroring that replicates and redirects the traffic, fully encapsulated within a Generic Routing Encapsulation (GRE) tunnel(s), and filtered to network-analyzing tools.



APCON Solutions for Networks

APCON, Inc. ▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070
+1 503–682–4050 ▪ 1–800–624–6808 ▪ **apcon.com**

24008-0724