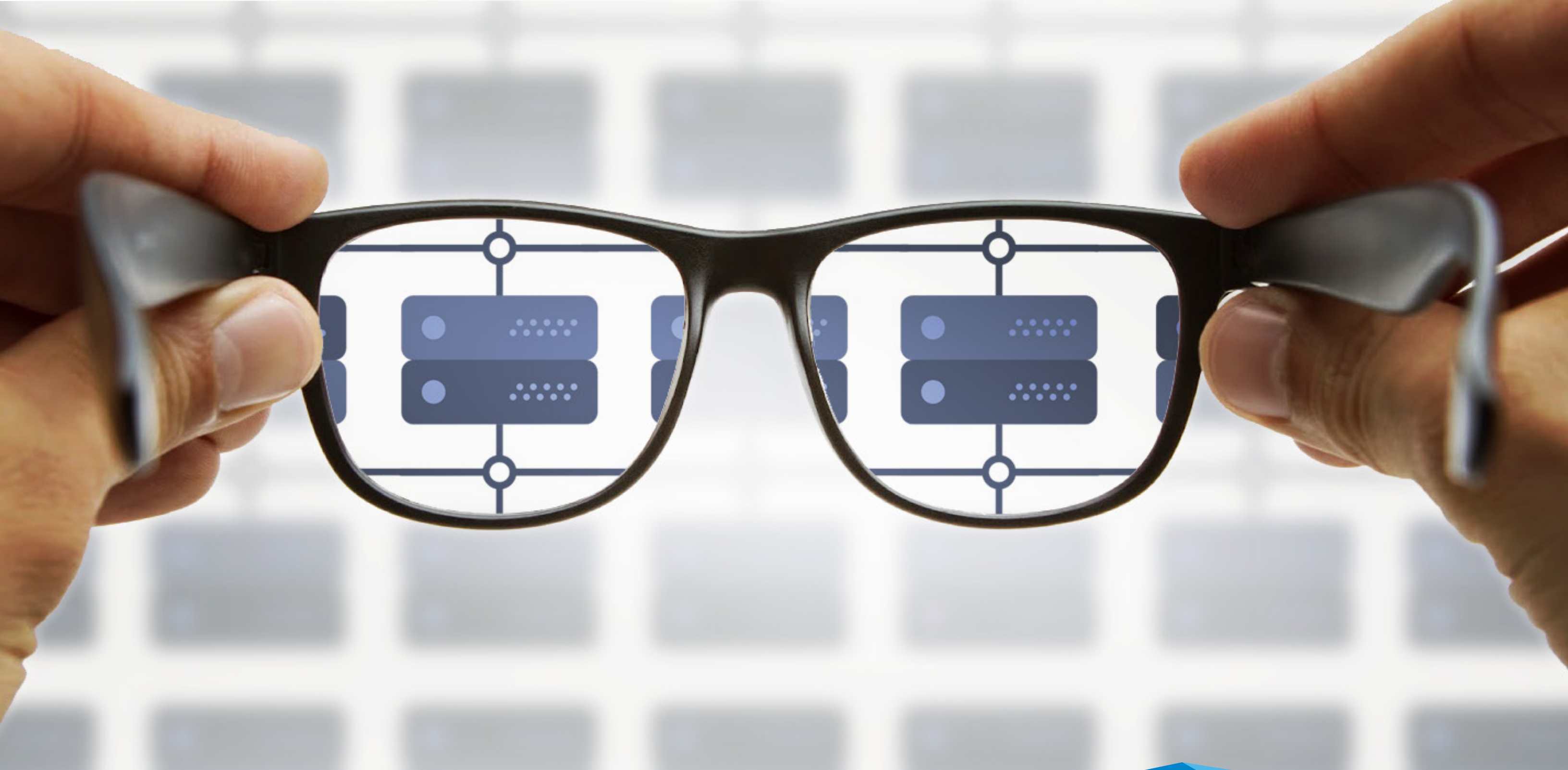
APCON
Solutions for Networks

Magnified Visibility for VMware Environments

Empowering Security & Overcoming Virtual Network Blind Spots



SOLUTION BRIEF

BRIDGING THE VISIBILITY GAP

between physical and virtual datacenters

Today, with most servers deployed as virtual machines (VMs) and many enterprises moving toward software-defined datacenters, the amount of virtual network traffic between VMs has increased exponentially. In an Accenture survey of 363 small, medium, and large enterprises, 95% of respondents believe all network services will be virtualized in the very near future. 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 datacenter can lead to significant blind spots and vulnerabilities throughout the network.

An example of not having visibility over East–West traffic is the traffic transmitted between the application and web service tiers running on the same host. 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 can become oversubscribed.
- Enforcing security policies in a highly dynamic environment requires continuous access to application data of interest.
- vMotion mobility can lead to a lack of network visibility as a result of the dynamic motion of virtual networks and machines changing locations.

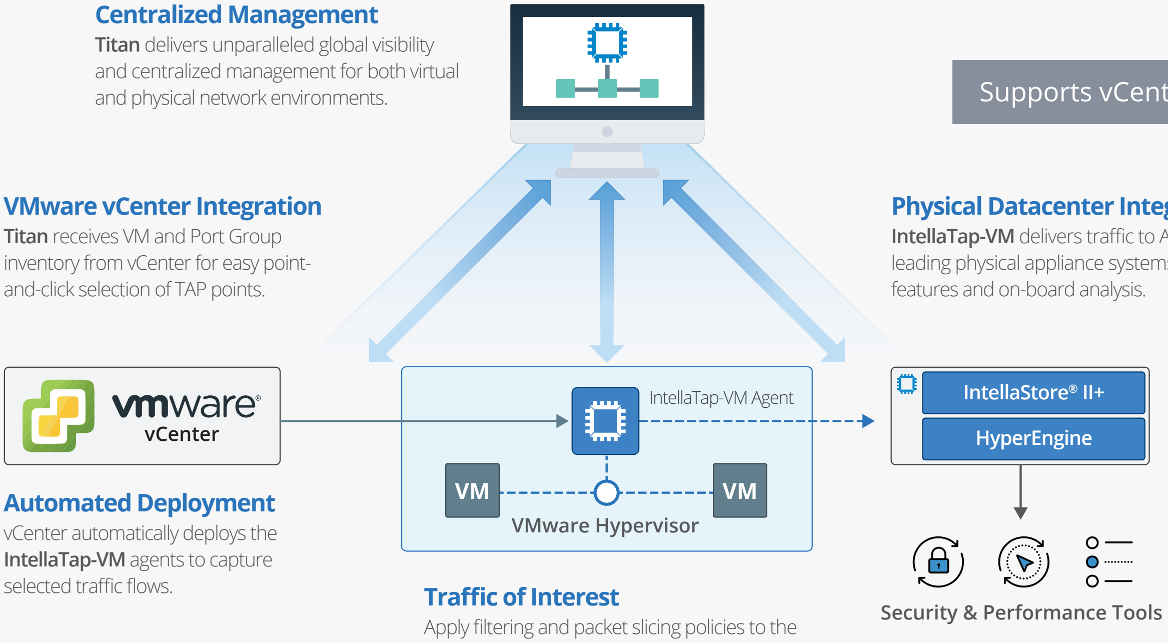
Often network professionals want to expand beyond basic native port mirroring by implementing an end-to-end visibility architecture that includes a network packet broker (NPB) to bolster security, simplify management/configuration, and improve the efficiency of monitoring tools.

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.

The APCON **SOLUTION**

IntellaTap-VM is an advanced feature within APCON's Titan software application that provides virtual network visibility and easy-to-use, point-and-click filtering of East-West virtual machine traffic flows.

Supports vCenter 5.5, 6.0, and 6.5



Centralized Management

Titan delivers unparalleled global visibility and centralized management for both virtual and physical network environments.

VMware vCenter Integration

Titan receives VM and Port Group inventory from vCenter for easy point-and-click selection of TAP points.

Physical Datacenter Integration

IntellaTap-VM delivers traffic to APCON's industry-leading physical appliance systems for advanced features and on-board analysis.

Optimize Existing Security Tools

Traffic flows can easily be directed to existing security and performance tools, improving functionality, efficiency, and preventing oversubscription.

Automated Deployment

vCenter automatically deploys the **IntellaTap-VM** agents to capture selected traffic flows.

Traffic of Interest

Apply filtering and packet slicing policies to the **IntellaTap-VM** agent, forwarding only traffic of interest.

The solution includes:

Centralized Management

Titan provides administration for the IntellaTap-VM virtual network visibility solution. Titan communicates with VMware vCenter to identify and activate capture points within the virtual network. It sets traffic filters, alerts you of migration events, and allows you to forward traffic through GRE tunnels.

Virtual Agent

IntellaTap-VM is a virtual monitoring solution that filters, encapsulates, and forwards virtual traffic. It takes the optimized packets and delivers them to your security monitoring tools.

Optional Physical Network Integration

The IntellaStore II+ Security Visibility Platform combines APCON's world-class packet aggregation and filtering technology with advanced features such as integrated traffic capture, storage, and on-board analysis tools. Network engineers can monitor networks in real time allowing for earlier security threat detection, investigation, and response.

APCON's HyperEngine high-performance network visibility solution aggregates traffic sources to execute advanced processing including deduplication, NetFlow generation, protocol header stripping, deep packet inspection, and tunnel termination for virtual network monitoring.

Benefits and Capabilities

- 100% visibility of VM traffic
- Automatic deployment of IntellaTAP-VM agents through vCenter
- Mirror traffic by port groups
- Apply traffic filtering and packet slicing policies
- Tunneling capabilities
- Optimize existing security tools
- Bandwidth reduction on production networks
- Little to no network impact during installation
- vMotion support, constant visibility of VM movements

The APCON Difference

APCON leverages its proprietary IP and deep expertise to provide flexible, focused solutions across:

- Government
- Financial Services
- Healthcare
- Manufacturing
- Higher Education
- Telecommunications

APCON solutions provide the flexibility and means to gain visibility to data more efficiently, resulting in savings across the board, including time, resources, and maintenance.

Service and Support

APCON's professional services team of certified engineers has years of experience optimizing network visibility strategies for businesses across the globe. In addition to providing installation assistance of existing analysis tools, this team proudly provides around-the-clock troubleshooting services and support.

About APCON

A privately held corporation, APCON is headquartered near Portland, Oregon, where it has operated since 1993. APCON's in-house staff manages product design and development, manufacturing, quality assurance and final testing, customer training and long-term servicing of its solutions — whether for a system with a single switch or a global installation that spans across multiple geographical or cloud locations.

APCON
Solutions for Networks

@APCON ▪ company/APCON