ThoughtData

DATA SHEET

NetMirror

Get passive observability in any public cloud with no overhead on to your application services or cloud infrastructure.

Passive observability is a major challenge in public cloud as there are no networking devices in public cloud environments which users can control. Access to network traffic is key to passive observability. Running sensors on computing nodes is not only challenging due to the distributed architectures but also a major concern for overhead on performance and cybersecurity. Recent cyber-attacks are good examples of how adversaries use 3rd party agent software's to compromise application services.

How it works

ThoughtData's NetMirror streams all the network traffic from the elastic compute instances running critical application services to virtual NetSense(vNetSense) running on dedicated compute resources in the same VPC network. (Refer Figure 1). The network traffic steaming is achieved through highly compressed and reliable TCP based tunnels established between NetMirror and vNetSense.

All network traffic processing happens on dedicated vNetSense computing nodes outside the application services infrastructure. NetMirror can be installed on any linux based computing node and can be orchestrated to come up as a service on computing nodes running in microservices architectures. One NetMirror an stream network traffic from multiple virtual interfaces from the same computing node. Each vNetSense can receive tunnelled packet streams from multiple NetMirrors and the solution can scale horizontally in the cloud network.

Packet slicing and high compression adds minimal overhead on to your VPC networks. Virtual monitoring interfaces are recommended to avoid all overhead into main VPC networks where end users connect to the application services. Multiple vNetSense in different public cloud environments can talk Enterprise360 providing a true passive and unified observability in multi cloud environments

ThoughtData's Enterprise360 solution provides seamless insight into network, application and infrastructure related failures and performance, helps you identify dependencies during incident triages, troubleshoot problems using various customizable work flows, find root cause, and gather evidence to fix issues with confidence.

ThoughtData's Enterprise360 Network Threat Intelligence allows you to identify and resolve security incidents faster by capturing, correlating and indexing metadata from packets and logs. With network forensics, you can detect a broad array of security incidents, improve the quality of your response and precisely quantify the impact of each incident.

Security Analysts can review specific network packets, logs and sessions before, during and after an attack. Being able to reconstruct and visualize the events triggering malware download or call-back enables your security team to respond effectively and swiftly to prevent recurrence. They can expand visibility into attacker activity by decoding protocols typically used to laterally spread attacks in a network.

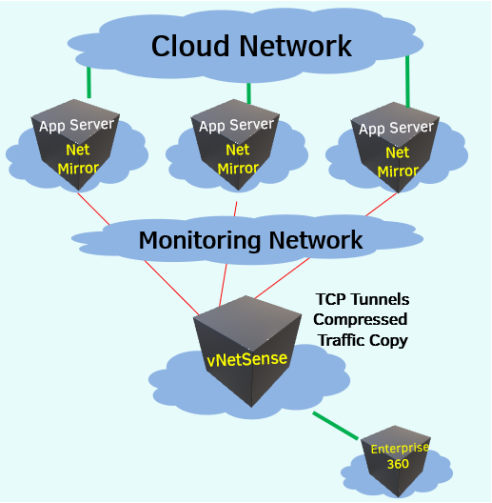

Figure 1. ThoughtData NetSense (packet sensor) appliances for packet capture and analysis

NetMirror Highlights

- **Passive Observability**: Continuous and passive network traffic streaming for observability in cloud.
- **High-Fidelity**: Real-time streaming of all network traffic to dedicated vNetSense outside. Dedicated TCP based compressed tunnel for data transfers for low traffic overhead in VPC networks.
- **Minimal to Zero Overhead:** Runs with very low and dedicated resources and adds no overhead to application services running on computing nodes
- **No Security Compromise:** NetMirror process does not interfere and has no connection with your application services leaving no room for cyber security compromise
- **Multi OS/Cloud Support**: Supported on any linux based server environments in any public cloud

Table 2. NetMirror Specifications

NetMirror Resource Requirements (per virtual interface)	Supported OS platforms	Public Cloud Environments	Scalability
20 MB Memory – Always runs in dedicated memory footprint. CPU Usage: <1%	Linux Fedora, Centos and Ubuntu based OS – All Versions	All cloud environments supported	Horizontal Scalability One NetMirror – Multiple Virtual Interfaces Traffic capture and streaming One NetSense – Multiple NetMirrors

ThoughtData, Inc.
9 Ledgerock way
Acton,
MA 01720
413.404.0030
info@thoughtdata.com

About ThoughtData Inc.

ThoughtData provides unified observability solutions to enterprise IT organizations.
Our solution offers a single unified platform that blends innovative network, application, infrastructure, cloud performance and cyberthreat monitoring. With this unique approach ThoughtData aims to reduce cost, mean time to respond (MTTR), tool clutter and increase end to end visibility into enterprise IT in one single solution.

ThoughtData