ThoughtData

DATA SHEET

NetSense Packet Sensor

Network and Application Monitoring Sensor Software using DPI Technology. Continuous observability into your business-critical applications using passive high speed packet capture, retrieval and analysis.

Organizations need continuous visibility into their enterprise IT applications to detect various issues related to health and performance of business-critical IT applications and services before any of those issues turn into a potential business loss. Swift visibility and investigation of application service impacting incidents to determine scope and impact, effectively reduces business loss, keeps your application services running, improves performance of your network, applications.

ThoughtData's NetSense packet sensor solution provides the best-in-class network data capture and retrieval solution with centralized analysis and visualization. It accelerates the unified observability into enterprise application services health & performance across on premises, hybrid IT, private cloud and public cloud environments while IT teams make technological transformations to support new business requirements.

ThoughtData's NetSense packet sensor solution provides seamless insight into network, application and infrastructure related health, 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. NetSense packet sensor provides various deployment choices as per your enterprise IT needs (see Figure 1 for typical Hybrid IT deployment)

NetSense Packet Sensor for on premises datacenters

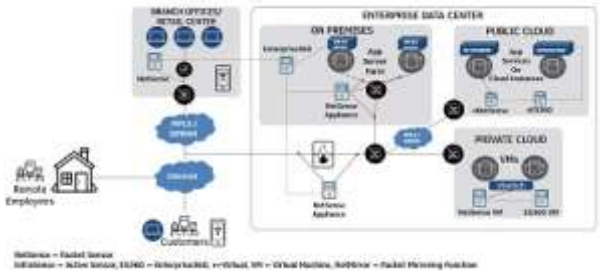
- Deploy as software on dedicated physical commercial off the shelf server with traffic feeds from critical network links for optimal observability
- Works on generic NIC cards for <10Gbps traffic requirements. High speed traffic capture NIC card is provided with software by ThoughtData for high traffic intensive workloads (10G, 40G, 100G Links)
- Install on standard Ubuntu based Linux OS.
- Choose packet recording as per your server storage capacity and data retention needs.
- Traffic feeds from port span/network taps/network packet brokers

NetSense Packet Sensor for Cloud(vNetSense)

- Built for passive enterprise traffic observability in private/public cloud environments
- East-west traffic observability between VM workloads and north-south traffic observability between VM and external applications
- For Private Cloud
    - Deploy vNetSense as a dedicated virtual machine on hypervisors in private cloud
    - Setup traffic feeds using virtual packet mirroring on distributed virtual switches on hypervisors
- For Public Cloud
    - Deploy vNetSense as a dedicated compute instance in any public cloud
    - Setup traffic feeds using cloud packet mirroring supported on public clouds (eg: aws, gcp)

For public clouds not supporting packet mirroring service (eg: azure) setup traffic feeds using vNetmirror directly on the application compute instances (requires an additional vNetSense compute instance)

***Figure 1**. ThoughtData NetSense packet sensor – How it works in a Hybrid IT deployment*



- **vNetMirror -** Passive observability is not directly possible in all public cloud environments (Except AWS, GCP) since cloud customers can't tap traffic directly from computing nodes. To solve this ThoughtData provides vNetMirror, a software solution which can be installed on any computing node in any public cloud. NetMirror captures all network traffic from one or more virtual interfaces on the cloud computing node on which it is installed and sends it to a dedicated vNetSense running in the same cloud VPC network. vNetMirror does not add any overhead on to the computing nodes. vNetmirror is support for both linux and windows-based compute instances.

NetSense Packet sensor Highlights

- **High-Performance**: Continuous high speed packet capture from critical network links.
- **High-Fidelity**: Real-time parsing & indexing of all captured packets, rich metadata extraction with data correlation. Continuous export of packet derived metadata in secured compressed binary format to ThoughtData's Enterprise360 application platform.
- **Fast Results:** Ultrafast search and retrieval of packets using session based indexing architecture.
- **Rich Context**: Layer 2 to 7 level traffic intelligence and key performance indicators extraction for troubleshooting.
- **Extensive Application Visibility:** Session level visibility into 40+ common enterprise protocols Eg: HTTP, SSL, DNS, SMTP, FTP, DHCP, RDP, SSH, SMB, SQL, Kerberos, SIP, SNMP, ICMP, NTLM, VPN (IPSEC, SSL) and many more.
- **Intelligent Capture**: Selective filtering of most important application to eliminate unwanted data capture.
- **Define Custom Applications:** Out of box capability to define custom applications.
- **Define Application Service Groups:** Out of box capability to define custom application service groups to get unified visibility into application services.

ThoughtData NetSense Packet Sensor software supports several configurations for different deployments in traditional on-premises to private or public cloud datacenters for optimized performance of packet metadata collection, visualization and analytics.

Table 1. NetSense Software Hardware Requirements – For on-premises deployment only

Traffic Monitoring Rates	Management Port	TrafficCapture Ports	Server Hardware Requirements	OS	Resource Requirements
< 1 Gbps	1 x 1Gbps	1 X 1Gbps NIC Card	Dedicated System (Any commercial desktop class system)	Linux Ubuntu/Redhat server OS	4CPU, 16 GB RAM. Storage: 1TB or more (Depending on packet data retention)
Up to 6 Gbps	1 x 1Gbps	1 X 10 Gbps NIC Card	Dedicated Server (Any commercial server- Eg: Dell/HP/Supermicro)	Linux Ubuntu/Redhat server OS	24CPU, 128GB RAM. Storage: 8TB or more – HDD - Minimum - SAS 10K RPM-12gbps, For OS- NVME/SSD – 2TB
6 to 20 Gbps	2 x 10GbE	4 X 10 Gbps NIC Card	Dedicated Server (Any commercial server- Eg: Dell/HP/Supermicro)	Linux Ubuntu/Redhat server OS	48CPU, 256GB RAM. Storage: 24TB or more – HDD - Minimum - SAS 10K RPM-12gbps, For OS- NVME/SSD – 2TB
Upto 40Gbps	2 x 10GbE	2 X 40 Gbps NIC Card	Dedicated Server (Any commercial server- Eg: Dell/HP/Supermicro)	Linux Ubuntu/Redhat server OS	96CPU, 512GB RAM. Storage: 96TB or more – HDD - Minimum - SAS 10K RPM-12gbps, For OS- NVME/SSD – 2TB

Note: NetSense packet sensor performance varies depending on the system compute resources and traffic data capture and storage requirements.

Enterprise360 Highlights

- **Out of box and customizable dashboards**: Out of box troubleshooting work flows for solving critical use cases and troubleshooting scenarios. Create and share custom dashboards
- **Fast Answers**: Quick and fast drill down to contextual information with powerful KPI meta data, discover problems and performance bottlenecks across network, applications, infrastructure, cloud. Investigate and find root causes, understand dependencies, drill down into packets and logs for evidence.
- **Powerful Search**: Accelerate search with powerful filter capabilities in each workflow or visualization to indexed metadata from various protocols such as Web, Email, VoIP, DNS, SMB, FTP etc.
- **Analytics:** Out of box and highly customizable alert configurations
- **Solution integrations**: Integrations to ITSM solution for alert to incident automations
- **Data Export:** Continuous export of packet meta to external solutions using open telemetry/OTLP

Table 2. Virtual NetSense for private or public cloud deployments

Virtual NetSense Specifications	Data Capture from 2 X Virtual Network Interfaces	Data Capture from 4 X Virtual Network Interfaces	Data Capture from 8 X Virtual Network Interfaces
Traffic Data Capture	< 1Gbps	1 to 2 Gbps	2 to 4 Gbps
CPU Cores	4 CPU Cores	8 CPU Cores	16 CPU Cores
Memory	16 GB RAM	32 GB RAM	64 GB RAM
Network Interface Controllers (NIC)	Separate virtual NIC for management & packet capture	Separate virtual NIC for management & packet capture	Separate virtual NIC for management & packet capture
Hard Drives	500 GB or more	2 TB or more	5 TB or more
OS	Linus based OS - (Ubuntu 22.04 Server) /Redhat		

To learn more about ThoughtData, visit: https://www.thoughtdata.com

ThoughtData, Inc.
9 Ledgerock way
Acton,
MA 01720, USA
413.404.0030
info@thoughtdata.com
ThoughtData Inc. All rights reserved.
ThoughtData is a registered trademark of ThoughtData Inc.

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 enterprise network threat technologies. 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