ThoughtData

DATA SHEET

NetSense (Packet Sensor)

Continuous observability into your enterprise IT network using passive high speed packet capture, retrieval and analysis.

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

ThoughtData's NetSense sensors provides the best-in-class network data capture and retrieval solution with centralized analysis and visualization. It accelerates the unified observability into enterprise network, application, infrastructure & cloud performance 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 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 Enterprise 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.

NetSense 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 dedicated server on any commercial server class machines (Eg: Dell/IBM/HP/Supermicro Etc) with traffic feeds from critical network links for optimal observability
- Works on generic NIC cards. High speed NIC card provided by ThoughtData for traffic intensive workloads (1G, 10G, 100G Links)
- Install on any linux(Fedora, Centos, Ubuntu) based servers.
- Choose optional packet recording as per your server storage capacity and use case needs.

NetSense Packet Sensor for Cloud(vNetSense)

- Built for passive enterprise traffic observability in private or public clouds
- Deploy vNetSense as a dedicated virtual machine on hypervisors in private cloud or as a computing node in any public cloud

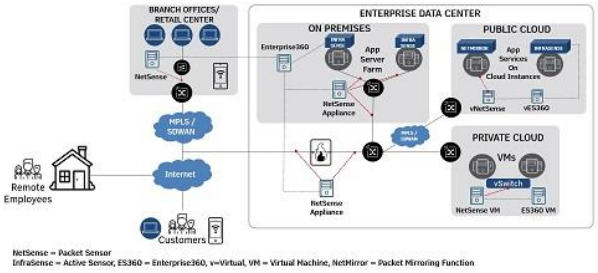

Figure 1. ThoughtData NetSense (packet sensor) – How it works – Hybrid IT deployment

NetSense (Packet sensor) Highlights

- **High-Performance**: Continuous, packet capture from enterprise network critical links.
- **High-Fidelity**: Real-time parsing & indexing of all captured packets, rich metadata extraction with correlation to connection attributes from InfraSense sensor. Continuous export of packet derived metadata in secured compressed binary format to ThoughtData's Enterprise360.
- **Fast Results:** Ultrafast search and retrieval of packets using indexing architecture
- **Rich Context**: Layer 2 to 7 level intelligence and key performance indicators extraction for troubleshooting
- **Extensive 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 and many more
- **Intelligent Capture**: Selective filtering of most important application to eliminate unwanted data capture.
- **Network Threat Visibility:** Out of box capability to detect Network based threats and anomalous network behaviours

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

Table 1. NetSense Software Requirements – Suggested on premises deployment

Network Traffic Links	Management Port	Typical traffic rates	Server	OS	Resource Requirements
4 X 1Gbps	2 x 1GbE	500 Mbps per port	Dedicated Server (Any commercial server-Dell/HP/IBM/Supermicro)	Linux based OS (Fedora 31(recommended) and above, Centos 9 and above, Ubuntu 20.04 and above)	2CPU/8GB RAM per 1G Link Total 8 CPU/32 GB RAM for 4X1Gbps. Storage: 2TB or more (Depending on packet data retention)
4 X 10 Gbps	2 x 10GbE	5 Gbps per port	Dedicated Server (Any commercial server-Dell/HP/IBM/Supermicro)	Linux based OS (Fedora 31(recommended) and above, Centos 9 and above, Ubuntu 20.04 and above)	8CPU/32GB RAM per 10G Link Total 32 CPU/128 GB RAM for 4X10Gbps. Storage: 8TB or more (Depending on packet data retention)
1 X 100 Gbps	2 x 10GbE	50 Gbps per port	Dedicated Server (Any commercial server-Dell/HP/IBM/Supermicro)	(Fedora 31(recommended) and above, Centos 9 and above, Ubuntu 20.04 and above)	48 CPU/256GB RAM per 100G Link Storage: 32TB or more (Depending on packet data retention)

Note: All performance values vary depending on the system configuration and traffic profile being processed.

Enterprise360 Highlights

- **Visualization**: Customize IT troubleshooting work flows including out of box work flow templates, Control the metrics, visualization methods and data queries and work flow drill through links. Create and share custom dashboards
- **Fast Answers**: Quick and fast drill down to contextual information With our powerful meta data, discover problems and performance bottlenecks across network, applications, infrastructure, cloud and cyber security. 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:** Build easy to use and customizable alerts on the visualizations, Deliver alerts to central repository via syslog, email etc.
- **Solution integrations**: Integrations to Microsoft ITSM, ServiceNow, Ansible, dockers for orchestrated deployment. Cloud data integration with Azure Monitor, Amazon Cloud Watch. Cyber security integrations - Threat Intelligence, STIX/TaxII, IDS/IPS(Suricata/Snort)
- **Data Export:** Continuous and secured export of correlated and enriched metadata to data lakes, Build your own applications and services.

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
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	300 GB or more	500 GB or more	1 TB or more
OS	Linus based OS - (Ubuntu 20.04 and above (Preferred) OR Fedora 31 and above OR Centos 9 and above)		

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

ThoughtData, Inc.
9 Ledgerock way
Acton,
MA 01720
413.404.0030
info@thoughtdata.com
©2021 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