ThoughtData

DATA SHEET

Enterprise360

Get unified and actionable visibility into your enterprise IT network. Pro-actively detect and triage network, application, infrastructure, and network threat issues in one single solution.

Organizations need continuous visibility into their enterprise IT network to detect various issues related to performance and network threats 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 early in their life cycle and re-secures your network.

Enterprise360 solution pairs the best in class network data capture and retrieval solution with centralized analysis and visualization. It accelerates the unified visibility into enterprise network, application, infrastructure & cloud performance while IT teams make technological transformations to support new business requirements.

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 workflows, find root cause, and gather evidence to fix issues with confidence.

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

Security Analysts can review specific network packets, logs and sessions before, during and after a network threat. 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 their strategies and exploitation methods used to laterally spread threats inside the network.

This unique combination of high-performance log and packet capture and in-depth correlated analytics driven from packets and logs helps quickly recognize and monitor every element of a network threat.

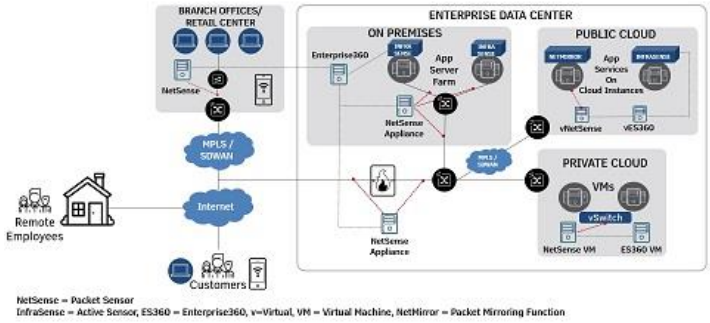

Figure 1. ThoughtData Enterprise360 Deployment in typical hybrid enterprise IT

Enterprise360 Feature Highlights

- **Out of box troubleshooting workflows** – Accelerate your IT incidence response with out-of-box investigation workflows for most common applications/protocols like HTTP, SSL, SMTP, DNS, DHCP, SMB, SIP, NTLM, Certificates, FTP, RPC, DCE, RDP, Certificate, Remote Users, Server Infrastructure, Process Log Monitor, Network Threat Monitor etc.
- **Fast Answers**: Quick and fast drill down to contextual information. With our powerful correlated analytics discover problems and performance bottlenecks across network, applications, infrastructure, cloud and network threats. Investigate and find root causes, overall impact, understand dependencies, drill down into packets and logs for evidence
- **Analytics**: Build easy to use and customizable alerts on the visualizations. Deliver alerts to central repository via syslog, email etc.
- **Flexible Visualizations**: Customize your IT troubleshooting workflows including out of box workflow templates. Control the metrics, visualization methods and data queries and work flow drill through links. Create and share custom dashboards.
- **Solution integration roadmap**: Integrations to Microsoft ITSM, ServiceNow, Ansible dockers for orchestrated deployment. Cloud data integration with Azure monitor, Amazon CloudWatch. Network threat 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.

Enterprise360 appliances support several configurations for different deployments in traditional physical/virtual data-centers and public cloud for optimized performance of metadata collection, visualization and analytics.

Table 1. Enterprise360 Software Requirements – Suggested on premises deployment

#Sensors Supported	Management Port	Server	OS	Resource Requirements
Upto 4 NetSense Sensors each with 4X1Gbps & Upto 10 InfraSensors	2 x 1GbE	Dedicated Server (Any commercial server-Dell/HP/IBM/Supermicro)	Linux based Server OS Ubuntu 20.04 and above	8CPU/32GB RAM Storage: 1TB or more (Depending on historical data retention)
Upto 8 NetSense Sensors 16 Links X 1Gbps each + 16 Links X 10Gbps each Upto 25 InfraSensors	1 x 10GbE	Dedicated Server (Any commercial server-Dell/HP/IBM/Supermicro)	Linux based Server OS Ubuntu 20.04 and above	24CPU/96GB RAM Storage: 8TB or more (Depending on historical data retention)

Note: Performance/Scalability varies depending on the system configuration and traffic profile being processed.

Enterprise360 Deployment and Scalability

- **Highly Scalable Architecture:** Enterprise360 distributed architecture allows you to seamlessly scale your visibility into every part of your network with distributed computing, database and UI nodes, spin off computing nodes and database nodes to distribute the meta data workloads, plan your storage needs for historical meta data retention and get the best value and performance of your solution deployment.
- **Deploy Anywhere**: Enterprise360 solution architecture allows you to deploy our solution in various formats, you can choose to deploy as software only or software + hardware appliance or virtual appliance in traditional on premises/virtual data-centers & public cloud-based deployments.
- **Seamless Workflows**: Pre-correlated data sets allow seamless transition across various work flows with metadata derived from packets to logs to flow getting the best value out of data sets in your incident triage.
- **Built in redundancy**: Allows to choose data replication factor during deployment and there is no need to deploy separate standby servers for data redundancy.
- **Restful Configuration API**: Allows to orchestrate and automate configuration for various deployments and also choose your own UI visualization application and connect to Enterprise360 database using RestAPIs

Table 2. Requirements for Virtual Enterprise360. For Private Cloud - Supports ESX, KVM, and HyperV. For Public Cloud – Install software directly on computing instance.

#Sensors Supported	CPU Cores	Memory	Storage	OS
Upto 4 NetSense Sensors + Upto 10 InfraSensors	4 CPU Cores	16 GB RAM	500GB or more	Linux based Server OS Ubuntu 20.04 and above
Upto 8 NetSense Sensors + Upto 25 InfraSensors	8 CPU Cores	32 GB RAM	1TB or more	Linux based Server OS Ubuntu 20.04 and above

Schedule a Entperise360 Demo Session, visit: https://app.acuityscheduling.com/schedule.php?owner=19948963

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

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

About ThoughtData Inc.

ThoughtData provides unified visibility 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