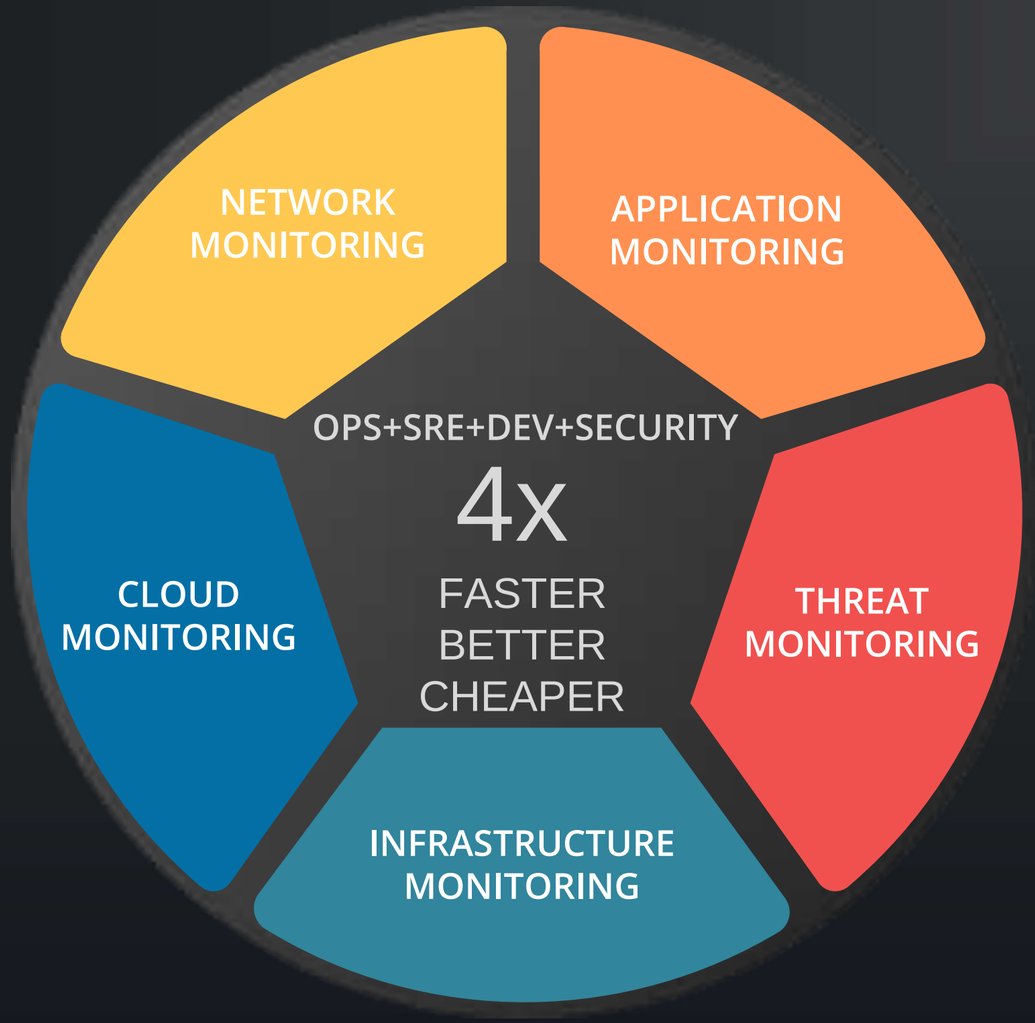
ThoughtData

Enterprise360

Unified IT Observability Software Solution



ThoughtData Advantage

Agentless Monitoring | Deploy Anywhere | Integrations to ITSM/SIEM

Deployment

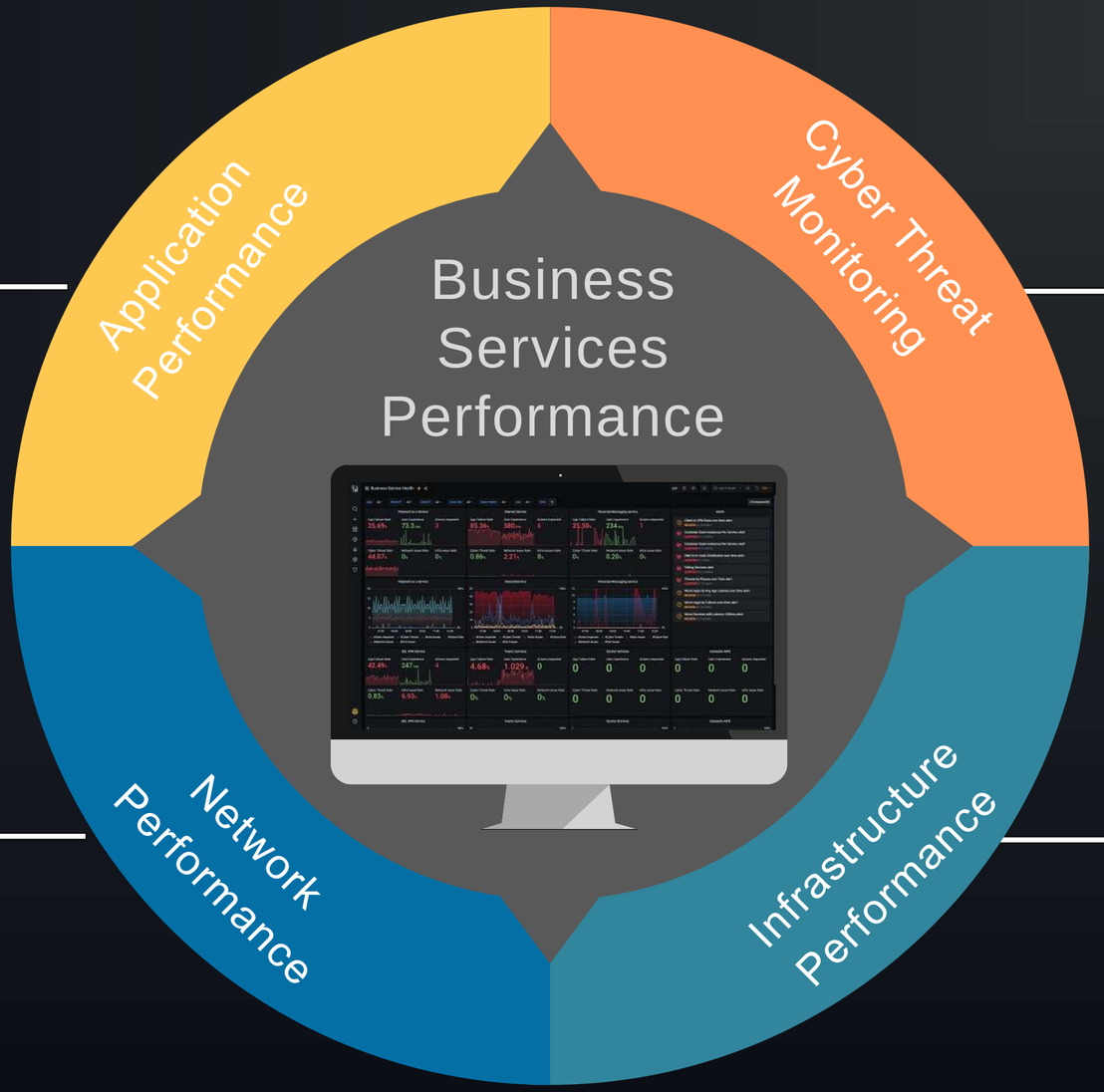
Customer Hosted | ThoughtData Hosted

Managed Service

Consulting | Implementation | Services

ENTERPRISE360

Unified Observability Platform – Use Cases Coverage



- User Experience
- App Failures
- Transaction Tracing
- External API Performance

- Threat Detection
- Threat Investigation
- Threat Evidence
- SIEM Integration

- Link Performance
- Bandwidth Issues
- Capacity Planning
- Network Issues

- Server Performance
- Devices Performance
- Synthetic Tests
- Cloud Infra Performance

ThoughtData

ENTERPRISE360

Unified IT Observability Coverage

Network Monitoring	Application Monitoring	Infrastructure Monitoring	Threat Monitoring	Cloud Monitoring	Integrations
Packet based Layer 2-7 Traffic Monitoring	APM agent based monitoring for Java, NodeJS, Golang, Python etc Apps	Server Monitoring using remote SSH/WMI/SNMP or Agent	MITRE ATT&CK framework threat detection & investigation	Public cloud infra monitoring (AWS, Azure, GCP etc)	ITSM Integration (Servicenow, Jira etc)
SNMP based device monitoring (Any device/MIB)	Database Monitoring (ES, MySQL, Mongo, Maria DB etc)	Disk/Storage Monitoring	DDoS threat detection & investigation	Cloud DB Services Monitoring(ES, MySQL, MongoDB etc)	SIEM Integrations
App-specific monitors (HTTP/s, DNS etc)	Real User Monitoring(RUM) Rest API Monitoring	Virtual Infra Monitoring (Vmware ESXI)	Reputation threats using Stix/Taxii	Serverless Function Monitoring(Beta)	BI Tools Integrations(Power BI, Grafana etc)
Device specialized NPM monitors (Cisco, Vmware etc)	Docker Monitoring SAP Monitoring Thread Dump Analysis	Synthetic Test Monitoring (Any HTTP/s URL)	Network Anomalies	AWS Cloud Watch, Azure Monitor GCP Monitor	Automation Integrations
VPN Monitoring Network Maps	Custom app specific log monitoring JVM/JMX Monitoring	Network Devices Monitoring Routers/Switches etc	Certificate Threats & Network Risks	Cloud API Monitoring	Alert/Report Integrations(Email, Teams, Slack etc)

ENTERPRISE360

Business Service Health & Performance Monitoring Dashboard

ENTERPRISE360 – Business Service Health Dashboard

<u>Use Cases</u>

Real time and historical health and performance of your business critical service in one single dashboard

Get visibility into App, Database, Network, Infra Issues in one dashboard

Customize your dashboard according to your team needs – Sample illustration example for SAP business service

ENTERPRISE360

Application Performance Monitoring(APM) Workflows

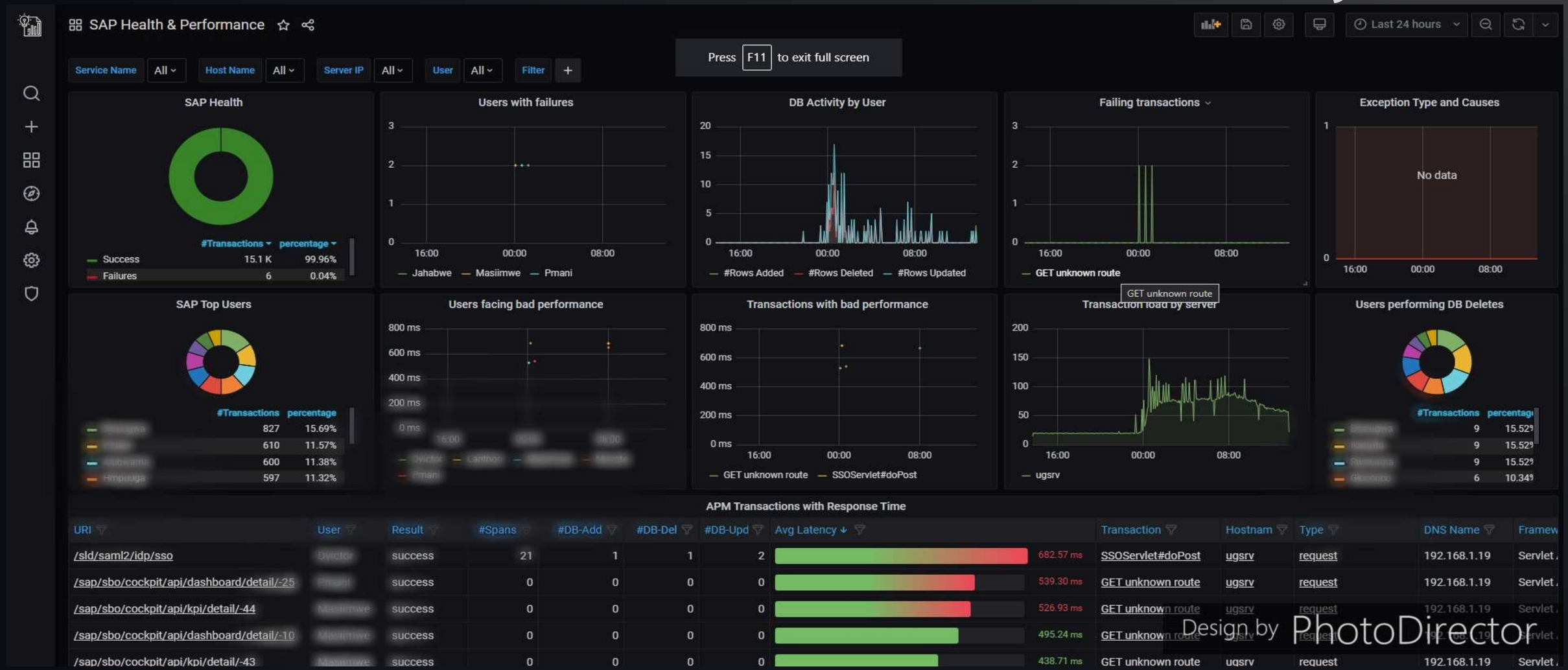
ThoughtData

ENTERPRISE360

APM Coverage

Sl No	Category	Requirement/Use Case
1	APM	Capability to have a custom dashboard to monitor health and performance of a entire business service with real time visibility into health and performance of each application, dependent application, database and infrastructure associated with the application
2	APM	Capability to visualize, track and investigate each application transaction per web URL with key performance indicators like errors, latency
3	APM	Capability to visualize, track and investigate each application sub transactions per web URL - all the way upto middleware to database layers with key performance indicators like errors and latency
4	APM	Capability to monitor health and performance of applications built on Java, Node JS, Golang, Python etc based application frameworks
5	APM	Capability to monitor health and performance web applications like tomcat, apache, nginx etc
6	APM	Capability to monitor non standard applications running in the network
7	APM	Capability to monitor application specific logs derived from application servers
8	APM	Capability to monitor all external API and dependent application calls and track their performance end to end
9	APM	Capability to monitor JVM/JMX metrics to ascertain the performance, resource constraints and issues
10	RUM	Capability to monitor user experience of web based application using real user monitoring technology(RUM)
11	API Monitoring	Capability to monitor any rest API using http/https URL
12	DB Monitoring	Capability to monitor databases like SQL, MYSQL, MariaDB, MongoDB, Elasticsearch, HANA DB etc with detailed KPIs
13	Thread Dump Monitoring	Capability to monitor thread dump on application server with visibility into deadlock and other conditions per process
14	Stack Trace Monitoring	Capability to remotely extract stack trace for application processes
15	SAP Monitoring	Capability to monitor SAP business application end to end with customized monitoring
16	Synthetic Tests	Capability to monitor Synthetic tests for any web based application with customizable HTTP/HTTPs URLs
13	DB Monitoring	Capability to monitor each database query and query performance
16	Alerts and Reports	Alert on any metric on any dimension on any chart, Get Alerts on email, slack, teams etc, auto generate tickets using service now etc Setup and generate adhoc and scheduled reports on any dashboard. Get CSV report with data to play around in excel format

ENTERPRISE360 – APM Transactions Summary



Use Cases

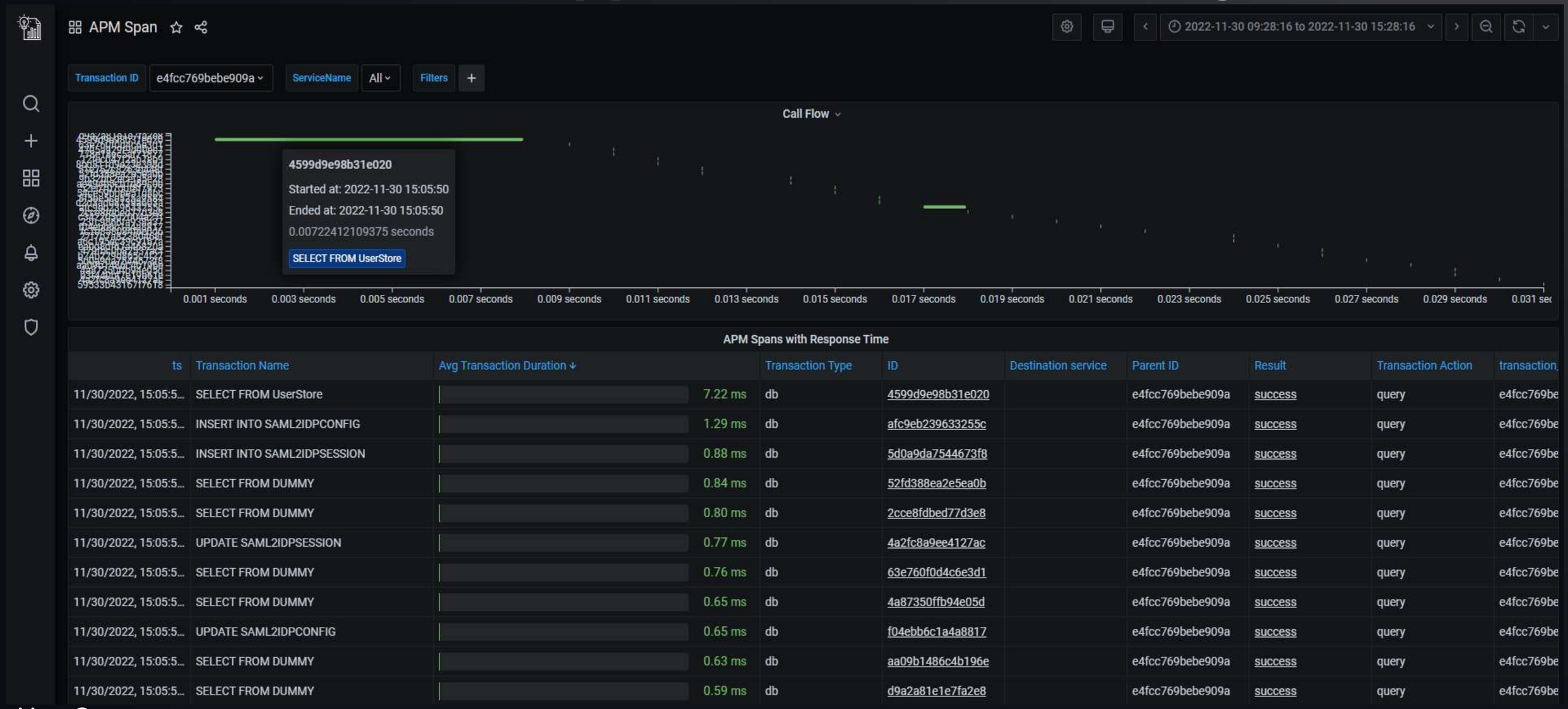
Per URL transaction tracing

Drilldown to see sub transactions and their individual performance

Drilldown to see all database queries and their performance

Drilldown to see all external API transactions and their performance

ENTERPRISE360 – App Transaction Tracing



APM Spans with Response Time

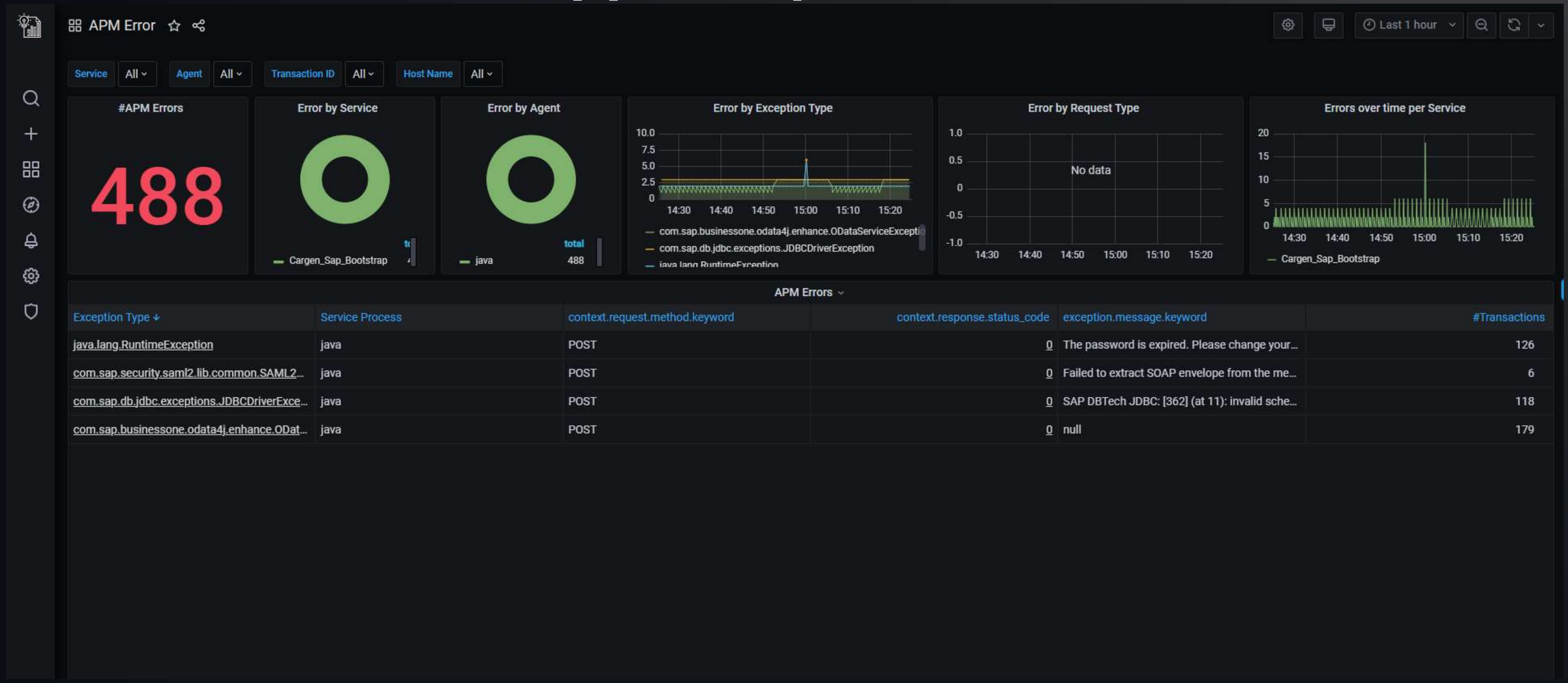
ts	Transaction Name	Avg Transaction Duration	Transaction Type	ID	Destination service	Parent ID	Result	Transaction Action	transaction
11/30/2022, 15:05:5...	SELECT FROM UserStore	7.22 ms	db	4599d9e98b31e020		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	INSERT INTO SAML2IDPCONFIG	1.29 ms	db	afc9eb239633255c		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	INSERT INTO SAML2IDPSESSION	0.88 ms	db	5d0a9da7544673f8		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.84 ms	db	52fd388ea2e5ea0b		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.80 ms	db	2cce8fdbed77d3e8		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	UPDATE SAML2IDPSESSION	0.77 ms	db	4a2fc8a9ee4127ac		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.76 ms	db	63e760f0d4c6e3d1		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.65 ms	db	4a87350ffb94e05d		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	UPDATE SAML2IDPCONFIG	0.65 ms	db	f04ebb6c1a4a8817		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.63 ms	db	aa09b1486c4b196e		e4fcc769bebe909a	success	query	e4fcc769be
11/30/2022, 15:05:5...	SELECT FROM DUMMY	0.59 ms	db	d9a2a81e1e7fa2e8		e4fcc769bebe909a	success	query	e4fcc769be

Use Cases

Trace and investigate each app transaction, get visibility into sub transactions and call flow diagram

Get visibility into all database queries, middleware transactions and also external API calls

ENTERPRISE360 – App Exceptions Monitor

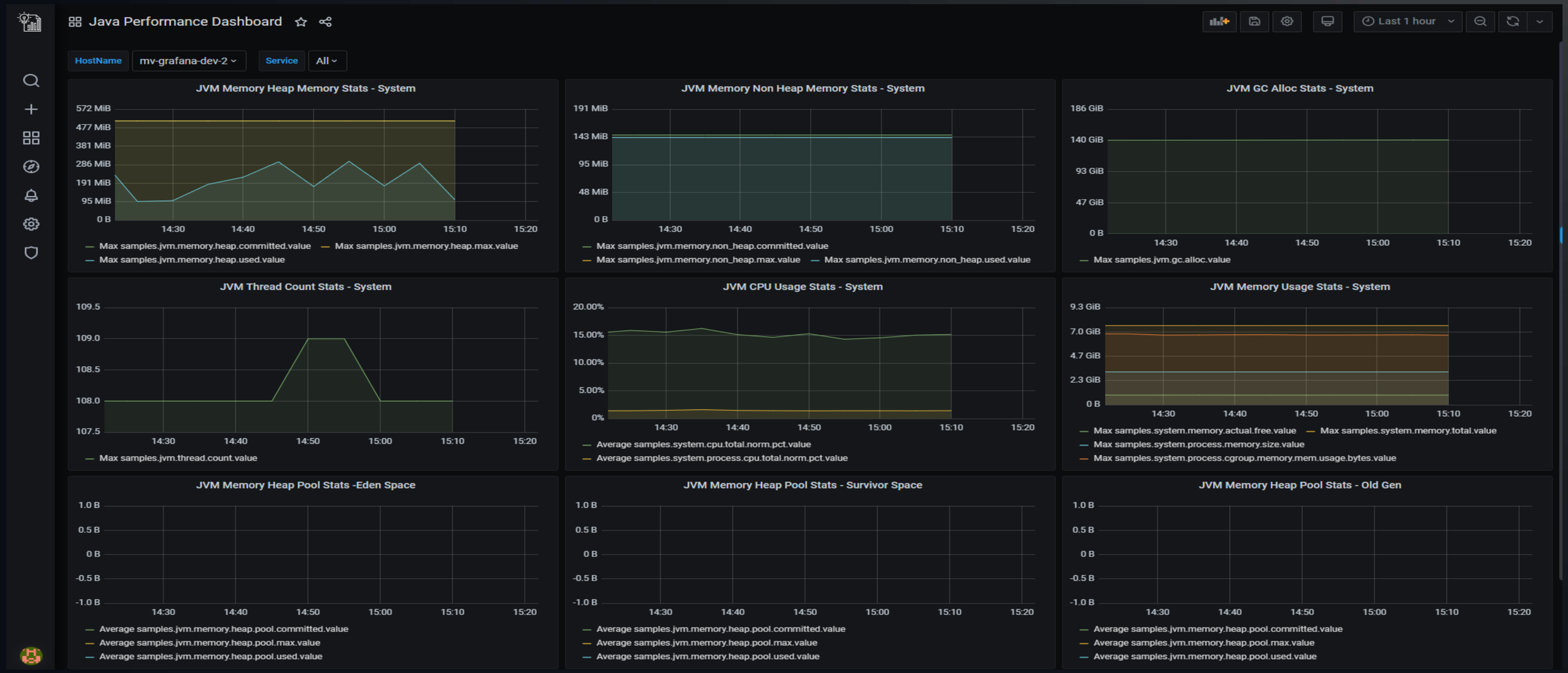


Use Cases

Detect and investigate each exception on your application

Get visibility to stack trace and also threat dump analysis

ENTERPRISE360 – Java Performance Dashboard



Use Cases

Get visibility performance of JVM/JMX on your Java processes

Investigate performance bottlenecks in JVM which can impact your app performance

ENTERPRISE360

Infrastructure Performance Monitoring(IPM) Workflows

ThoughtData

ENTERPRISE360

IPM Coverage

Sl No	Category	Requirement/Use Case
1	Infrastructure Monitoring	Holistic view of entire IT infrastructure in one single dashboard with status of devices and devices running into infrastructure problems along with alerts
2	Infrastructure Monitoring	Monitor all critical servers/devices in the network remotely without needing to install any software agents on the servers or devices
3	Infrastructure Monitoring	Monitor all critical servers and devices using agents where remote monitoring is not feasible or available
4	Infrastructure Monitoring	All credentials used for monitoring infrastructure are TLS encrypted and stored in the solution – no risk of breach
5	Infrastructure Monitoring	Choose between SSH/WMI/SNMP for remote infrastructure monitoring depending on type of server
6	Server Health Monitor	Auto detect server configurations like server name, OS, vendor, #CPU, total memory and disk space configured on the server
7	Server Health Monitor	Visualize resources usage on each server like CPU utilization per cpu, memory usage, free memory, swap memory, network I/O, disk I/O, network latency per interface
8	Server Health Monitor	Visualize per process resources usage on each server like CPU utilization per cpu, memory usage, free memory, swap memory, network I/O, disk I/O, network latency per process
9	Server Health Monitor	Monitor disk usage by file system, partition and also per mount points
10	Vmware ESXI Monitor	Monitor overall resources of Vmware EXSI host like cpu, memory, disk I/O, network I/O
11	Vmware ESXI Monitor	Monitor resources of Vmware EXSI host like cpu, memory, disk I/O, network I/O per process on the EXSI host
12	Vmware ESXI Monitor	Monitor data stores configured and used in the Vmware EXSI host
13	Device specific infra monitoring	Monitor device specific common resources like power supply, fan, voltage etc
14	Device specific infra monitoring	Monitor device specific infrastructure resources usage using vendors specific MIBS over SNMP
15	Cisco Monitor	Monitor health of all Cisco devices like router, switches, firewalls, access points etc. Get visibility into cpu, memory, disk I/O, network I/O on each device and also device specific hardware health
16	Alerts and Reports	Alert on any metric on any dimension on any chart, Get Alerts on email, slack, teams etc, auto generate tickets using service now Setup and generate adhoc and scheduled reports on any dashboard. Get CSV report with data to play around in excel format
17	Customizable Monitors	For any device which supports SNMP

ENTERPRISE360 – Infrastructure Health Summary

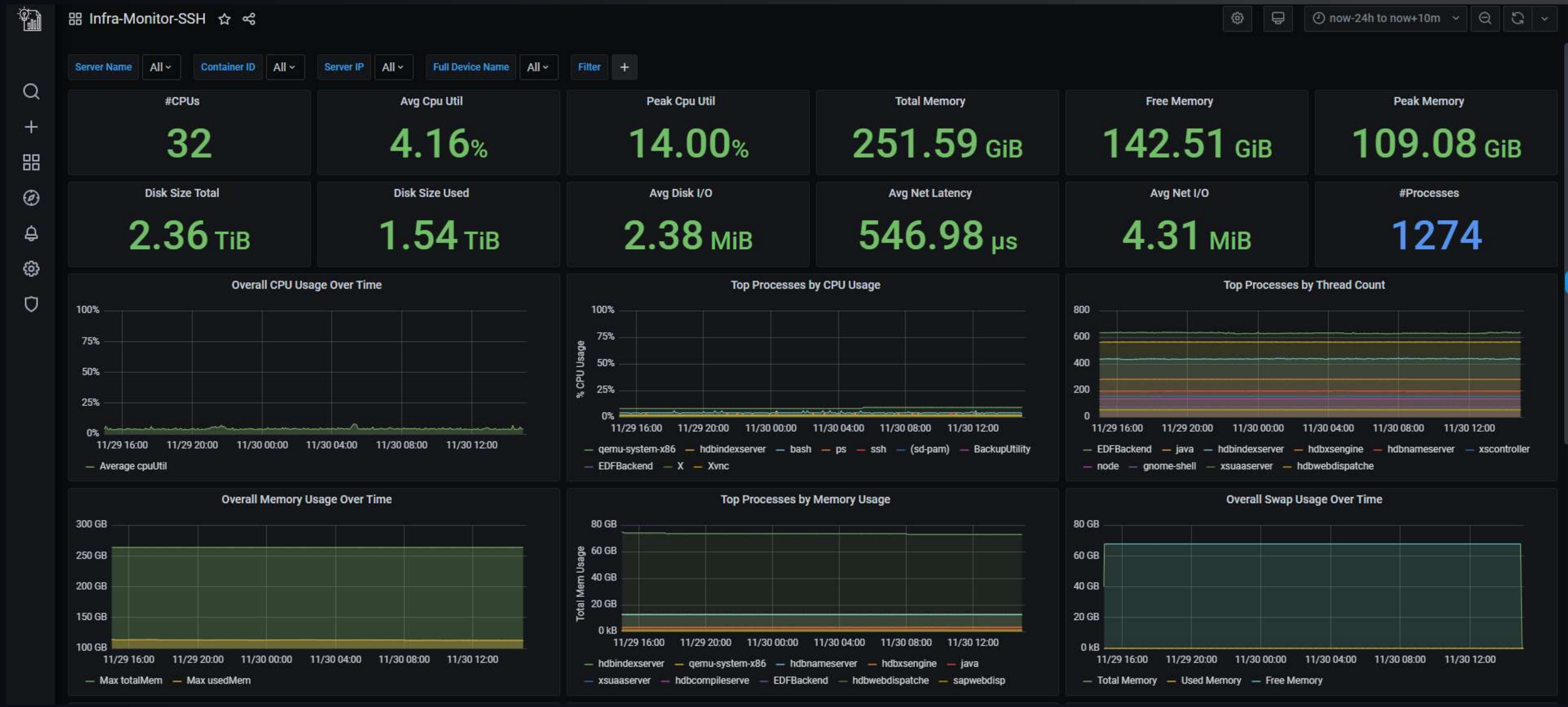
Use Cases

Overall view of device health summary in IT network

Devices UP/Down Status. Devices running into CPU, Mem, Storage, Disk I/O, Network I/O issues

Device based resource usage alerts

ENTERPRISE360 – Server Health Monitor



Use Cases

Monitor each server health in detail

Resource usage: CPU, memory, storage, disk I/O, network I/O, process level performance & storage monitor

ENTERPRISE360 – Storage Monitoring

<u>Use Cases</u>

Monitor storage on each server

Get visibility into storage usage on mount points, file systems, partitions

ENTERPRISE360 – Synthetic Monitor

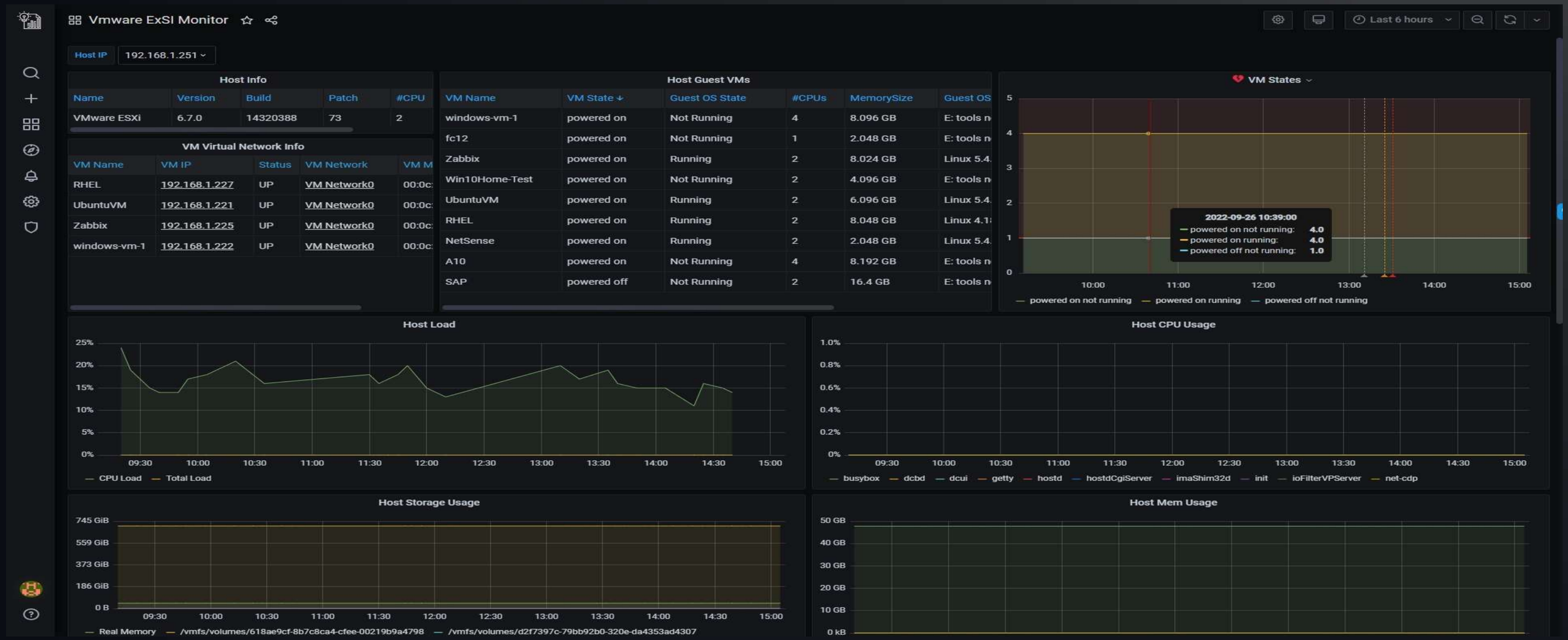
Use Cases

Setup a synthetic test to any web based HTTP/HTTPs url or a rest API

Get performance statistics on your applications generated from real simulated tests from different geo locations

Get status of the service, connection failures and latency metrics and setup alerts for services

ENTERPRISE360 – Vmware Exsi Monitor



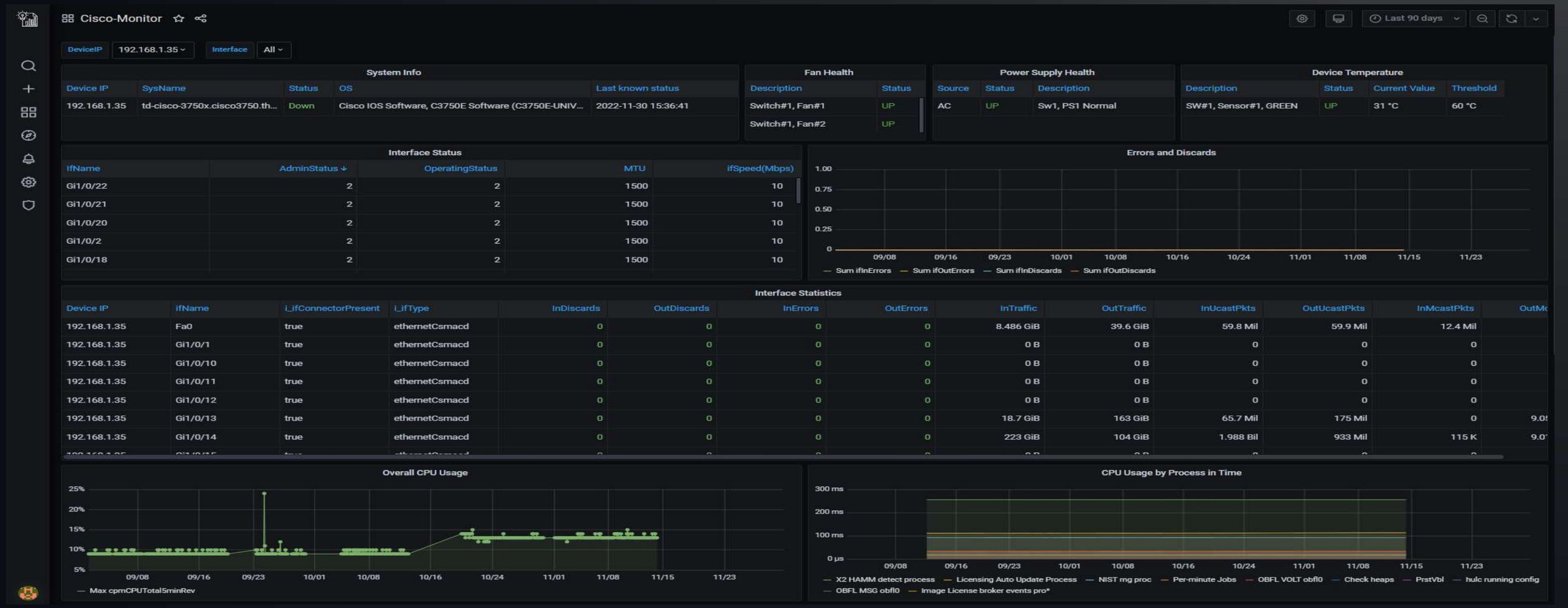
Use Cases

Get real time health and performance of each Esxi host in your IT environment

Get visibility into VMs, allotted resources for each VMs on every Esxi host, Get visibility into usage of VMs on each Esxi host

Get visibility into resource performance of each VM on the Esxi host

ENTERPRISE360 – Cisco Monitor



Use Cases

Get real time health and performance of each Cisco Device in your IT environment

Get visibility into resource and network performance on each switch, router, firewall, access points etc

Get visibility into hardware issues on each cisco device

ENTERPRISE360

Network Performance Monitoring(NPM) Workflows

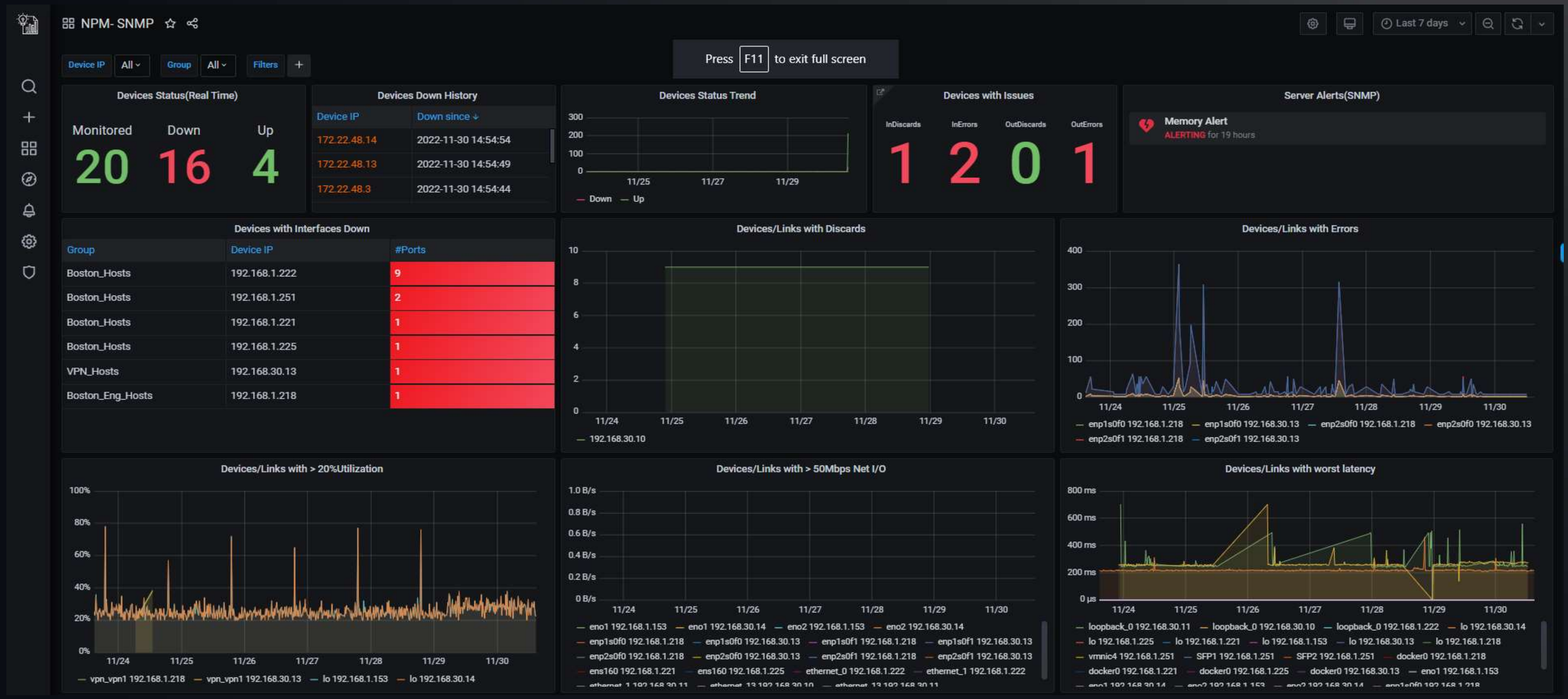
ThoughtData

ENTERPRISE360

NPM Coverage

Sl No	Category	Requirement/Use Case
1	Traffic Monitoring	Get holistic view of entire network in a single network map visualization
2	Traffic Monitoring	Visualize network traffic per each Router/Switch link - Traffic throughput rate, utilization, pps
3	Traffic Monitoring	Detect and investigate network errors like In/Out retransmissions, In/Out errors, In/Out drops per each Router/Switch link
4	Traffic Monitoring	Detect and investigate TCP related problems like resets, timeouts, zero window etc
5	Traffic Monitoring	Host specific traffic monitoring providing information about all application transactions performed by the host and traffic monitoring specific to the host
6	Traffic Monitoring	Detect and monitor non standard applications running in the network
7	Traffic Monitoring	Define sites and visualize all traffic and application monitoring per site
8	Traffic Monitoring	Trace each network connection at IP flow and application session level and investigate problems, Get packet level evidence
9	Traffic Monitoring	Monitor all VPN and MPLS traffic, detect and troubleshoot problems in VPN/MPLS connections
10	Application Monitoring	Visualize network traffic per each application - app specific Traffic throughput rate, utilization, pps per server/site
11	Application Monitoring	Detect and investigate application specific problems like HTTP, DNS, SMB, SMTP, SSL Errors etc on all common applications
12	Application Monitoring	Investigate application specific problems like HTTP URLs, DNS Queries, SSL transactions etc
13	Application Monitoring	Investigate application specific using monitors workflows designed specially for HTTP, DNS, SSL etc
14	Application Monitoring	Define a application service comprising of various servers and applications running on them for a collective visualization of the service
15	Application Monitoring	Application service level dashboard which can be customized for names of panels and metrics
16	Alerts and Reports	Alert on any metric on any dimension on any chart, Get Alerts on email, slack, teams etc, auto generate tickets using service now etc Setup and generate adhoc and scheduled reports on any dashboard. Get CSV report with data to play around in excel format

ENTERPRISE360 – NPM Summary

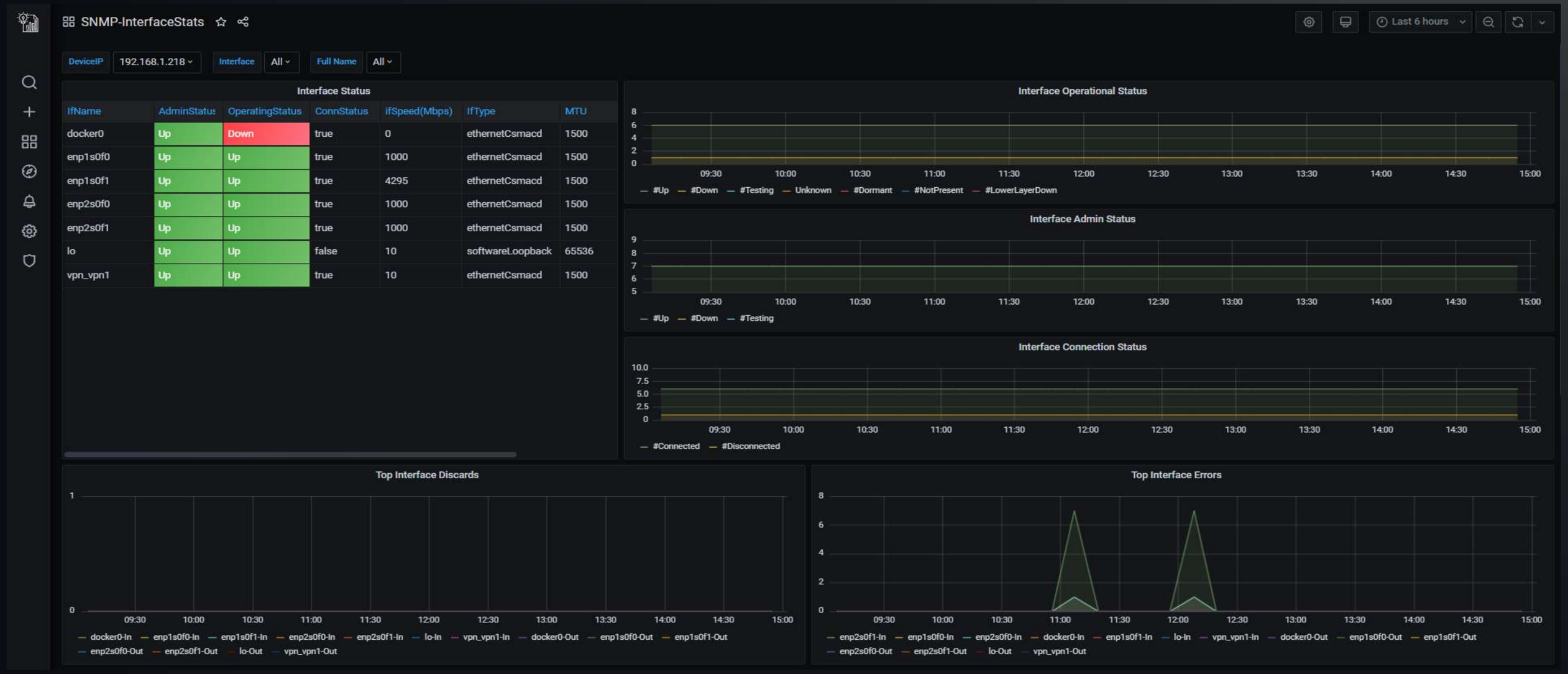


Use Cases

Overall view of network health across all links across all devices in IT network

Identify links with bandwidth issues, errors and discards, drilldown to investigate each link

ENTERPRISE360 – Device Network Monitor

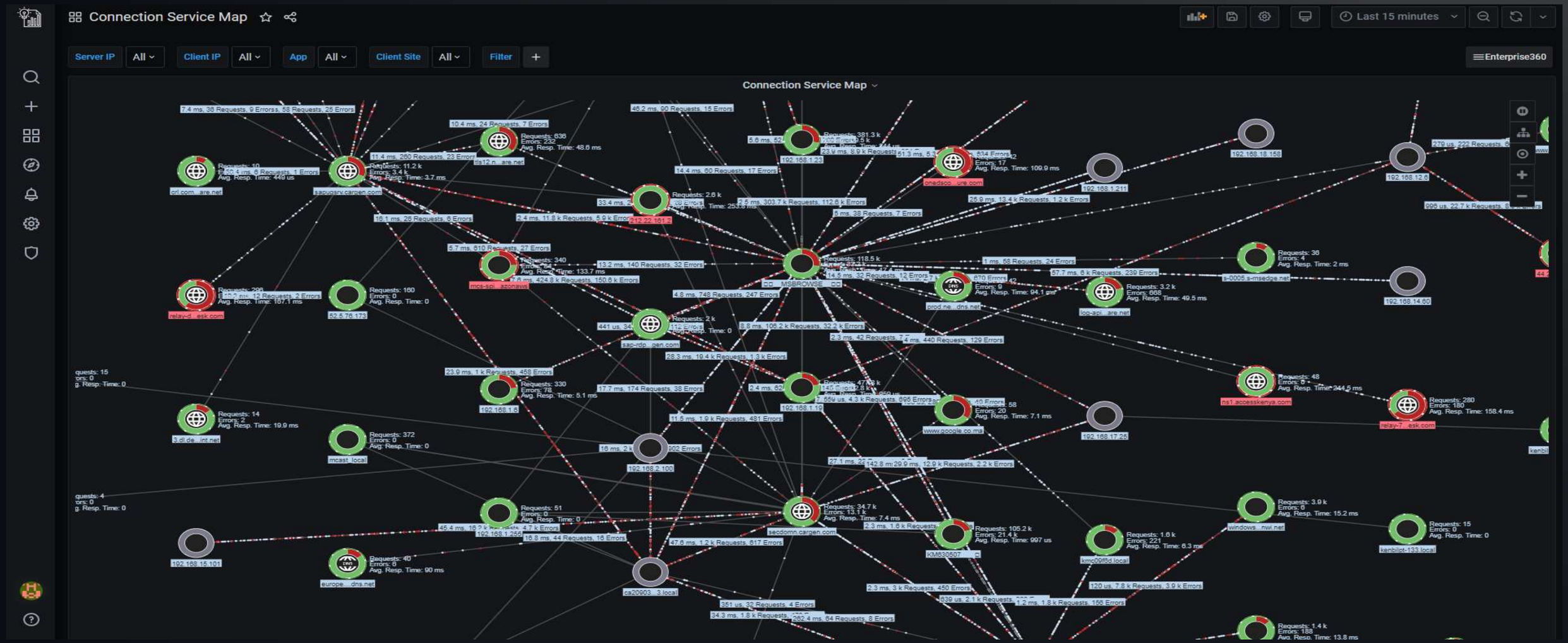


Use Cases

Monitor network performance of each router/switch etc per each port/interface

Interfaces UP/Down Status, traffic statistics, errors, discards

ENTERPRISE360 – Network Maps



Use Cases

Overall view of device health summary in IT network

Devices UP/Down Status. Devices running into CPU, Mem, Storage, Disk I/O, Network I/O issues

Device based resource usage alerts

ENTERPRISE360 – Unknown Apps Monitor

Use Cases

Get visibility into all unknown or non standard apps running in your IT network

Investigate non standard ports open, traffic volumes and servers running non standard apps

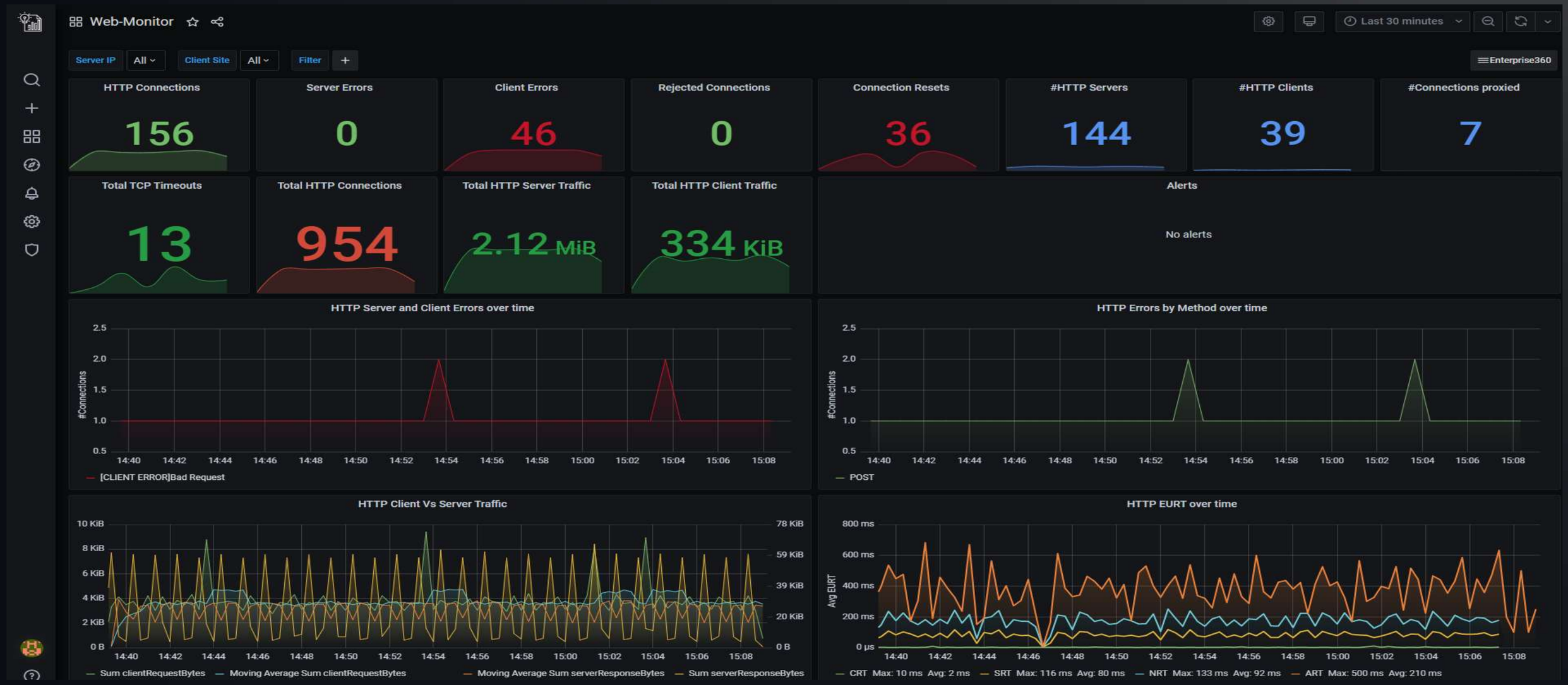
ENTERPRISE360 – DNS Monitor

<u>Use Cases</u>

Detect and investigate all DNS related issues like errors, latency, query load etc

Get visibility to performance of each DNS server or relay, track each DNS transaction performance

ENTERPRISE360 – Web/HTTP Monitor



Use Cases

Detect and investigate all HTTP related issues like errors, latency, URL based performance load etc

Get visibility to performance of each web server or proxy. track each HTTP transaction performance

ENTERPRISE360 – SSL Monitor

<u>Use Cases</u>

Detect and investigate all SSL related issues like errors, latency, auth, key, encryption algorithms performance

Get visibility to performance of each SSL server or proxy. track each SSL transaction performance

ENTERPRISE360

Cyber Threat Monitoring(CTM) Workflows

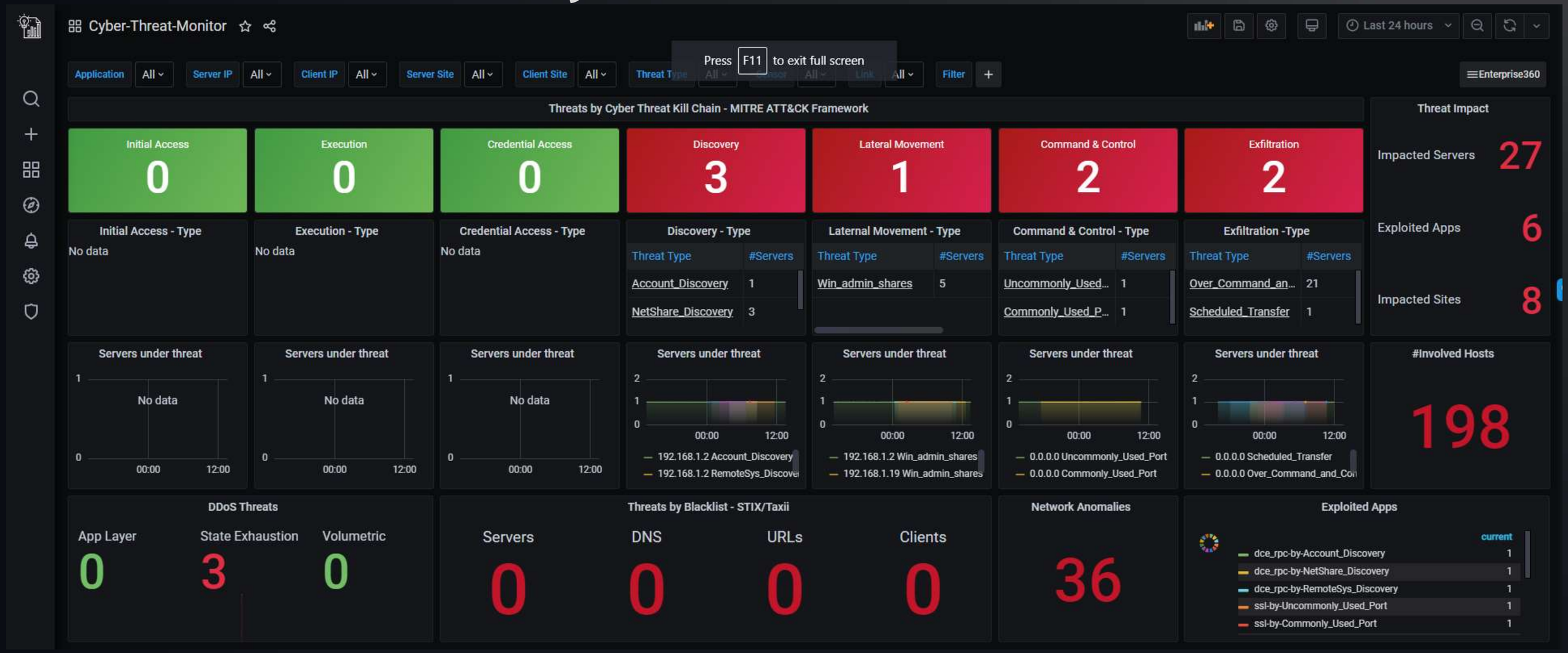
ThoughtData

ENTERPRISE360

CTM Coverage

Sl No	Category	Requirement/Use Case
1	Threat Detection	Detect and investigate cyber threats in real time in the IT network
2	Threat Detection by stage	Detect and investigate each stage of the threat like initial compromise, discovery, lateral movement, command and control, exfiltration
3	Initial Access Threats	Detect and investigate threats in this category Eg: spearfishing , spam emails etc
4	Credential Access Threats	Detect and investigate threats in this category Eg: hijacking passwords, brute force etc
5	Discovery Threats	Detect and investigate threats in this category Eg: network, app, port discovery etc
6	Lateral Movement Threats	Detect and investigate threats in this category Eg: windows shares, network shares etc
7	Command and Control Threats	Detect and investigate threats in this category Eg: uncommon SSL connections, external to internal SSL connections etc
8	Exfiltration Threats	Detect and investigate threats in this category Eg: internal to external unusual data movements, periodic data movements, scheduled data movements etc
9	Threat Knowledge Base	Know more details about the threat by a threat knowledgebase linked to each detected threat
10	Threat Investigation	Investigate threats in detail to understand the impact of threats, servers, hosts and apps on which threat is running and also source of origination of the threat
11	Threat Evidence	Get evidence of the threats like sample network traffic trace or server logs to confidently take actions on the threats
12	DDOS threats	Detect and investigate DDoS threats like amplification, state exhaustion and application layer attacks and perform full investigation to understand source and impact of the attack on applications and users
13	Reputation threats	Track every network connection inbound our outbound which is going to or coming from a known malicious source like bad reputation DNS hosts, website URLS or Public server IPs and immediately flag the threat and also get details of associated threats with the source
14	Threat Intelligence Integration	Integration with popular threat intelligence feeds and use the feed for threat detection in the IT network
15	Certificate Threats	Detect and investigate SSL certificates related threats like untrusted, self signed and expired certificates on web servers in the IT network

ENTERPRISE360 – Cyber Threat Monitor



Use Cases

Real time visibility into cyber threats and attacks

MITRE ATT&CK Threats, DDoS Threats, Reputation Threats, Network anomalies

Drilldown into deep threat investigation to assess impact with evidence

ENTERPRISE360 – Cyber Threat Investigation

Use Cases

Investigate all cyber threats, threat impact, apps, nodes, servers involved

Drilldown further to get visibility into each threat investigate further to get evidence using network traffic

ENTERPRISE360

Single solution for all your IT monitoring needs

See it in action ! Sign up for demo today !

Demo Signup