



**7SYSTEM**  
COMMITTED TO THE FUTURE



**DcDynamo**  
Network Management System

# DcDynamo

## NETWORK MANAGEMENT SYSTEM



**MSME**  
Government of India  
MSME Reg No. BR26D0053406





# DcDynamo – Network Monitoring Solution

By: 7System Technology Pvt. Ltd.



## Executive Summary

Modern enterprises depend on secure, high-performing, and well-monitored networks to run mission-critical operations. As IT environments grow in complexity, organizations need intelligent, unified solutions for visibility, incident response, configuration control, and predictive analytics.

**DcDynamo**, developed by **7System Technology Pvt. Ltd.**, is an end-to-end enterprise-grade **Network Monitoring Solution (NMS)** designed for performance monitoring, traffic flow analysis, configuration management, and centralized log intelligence across hybrid environments. It delivers unmatched visibility, deep analytics, and scalable monitoring across thousands of distributed devices—all with a modular and extensible architecture.

## Core Features



### Automatic Network Discovery

Auto-detect and map all devices using SNMP, LLDP, CDP, ARP, and ICMP. New assets are dynamically added to the inventory with accurate metadata.



### Real-Time Monitoring and Metrics

Monitor:

- Bandwidth usage
- Interface and port health
- CPU, RAM, disk usage
- Device uptime and errors
- Service and application availability

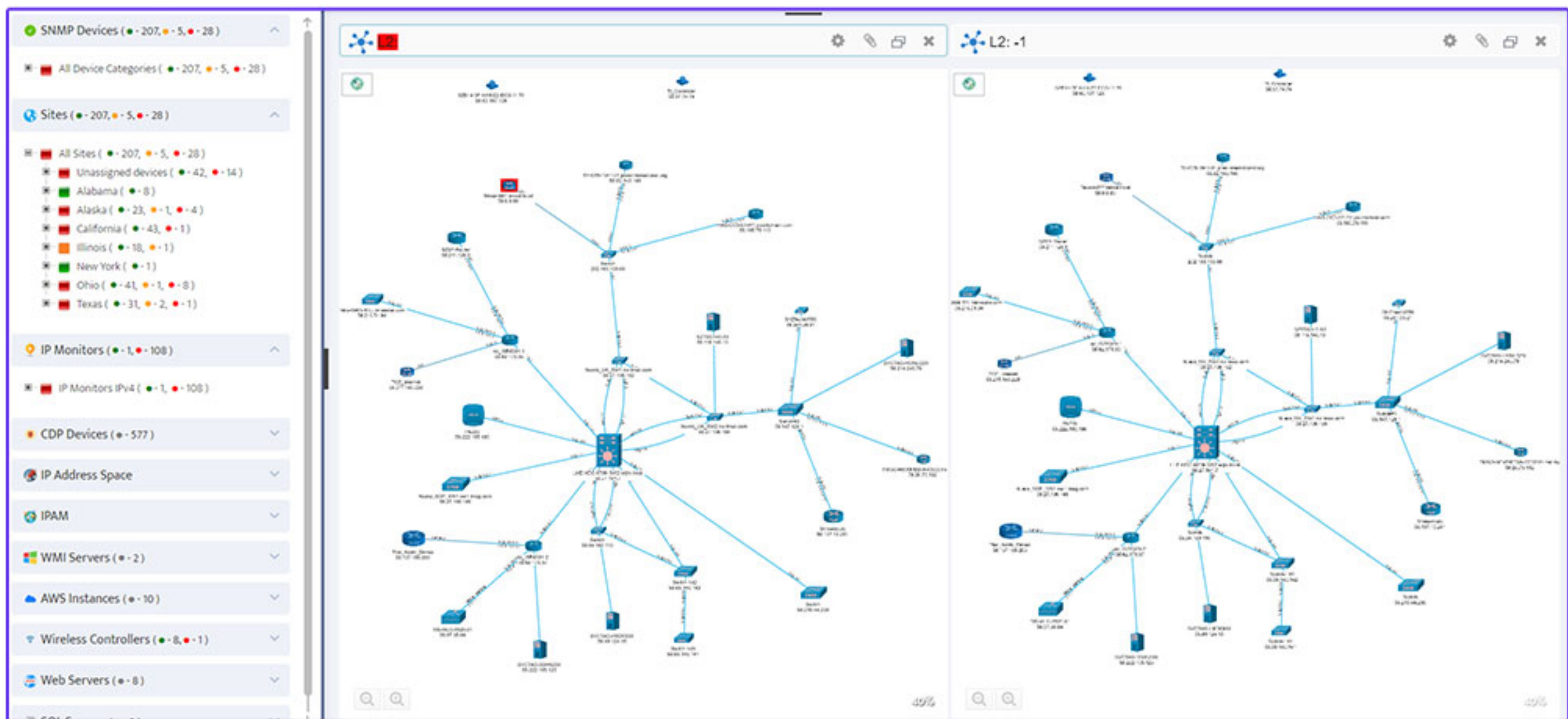
Retain historical data for capacity forecasting and SLA enforcement.





## Network Topology Mapping

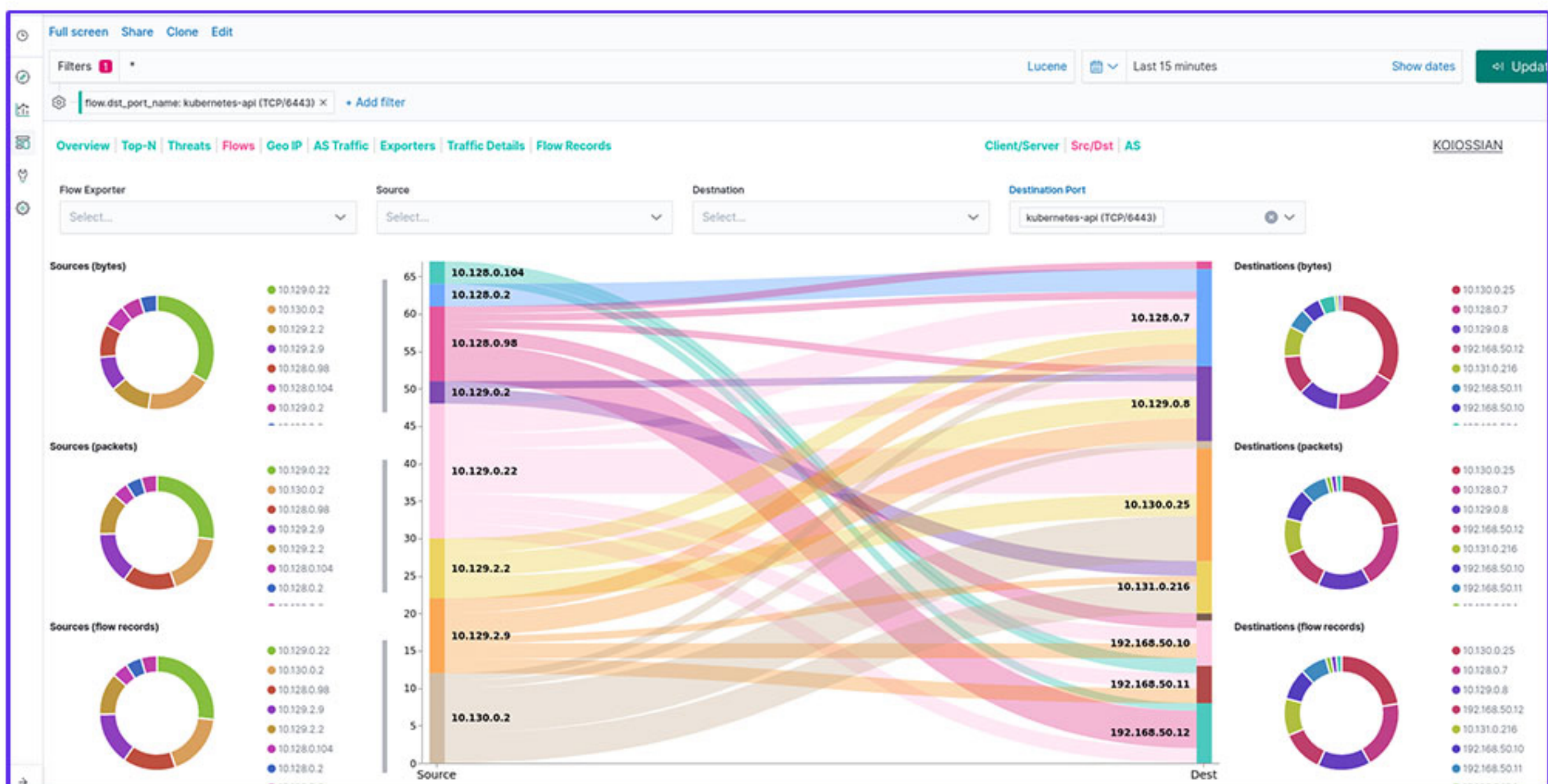
Generate visual Layer 2/3 network maps with auto-updating device positions, live link status, and drill-down device health. Optionally layer topologies by physical, logical, or geographic parameters.



## Traffic Flow Monitoring (NetFlow/sFlow)

Monitor real-time traffic patterns with:

- Top talkers and protocols
- Cross-segment communication flows
- Anomaly detection and congestion analysis
- Supports major flow protocols: NetFlow, sFlow, SNMP

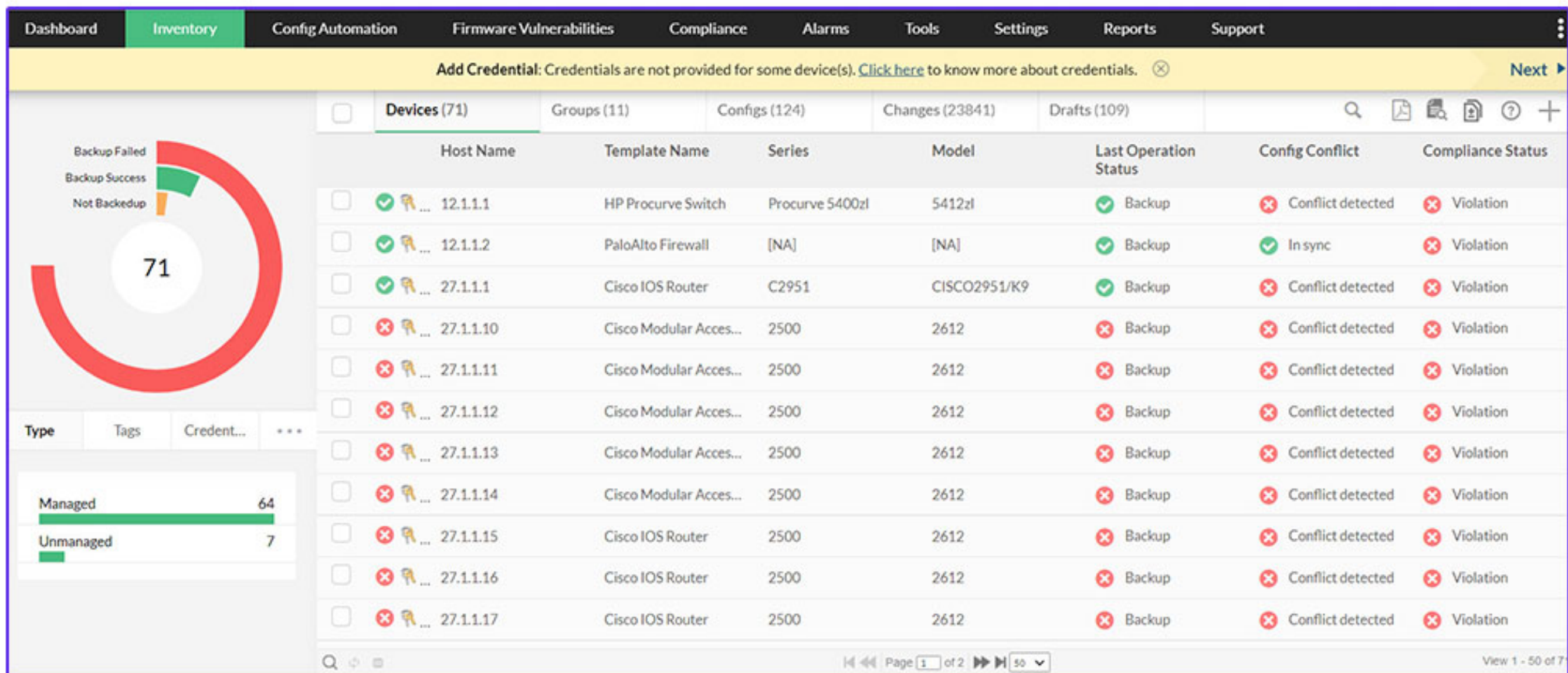






## Network Configuration Manager (NCM)

- **Automated configuration backup** for routers, firewalls, switches
- **Change tracking with diffs and rollback**
- **Policy enforcement** for compliance to internal/external standards
- **Configuration push** to supported vendors for bulk updates



## Log Management & Analysis (SIEM-lite Capabilities)

Ingest and analyze logs from:

- Network devices
- Servers (Linux/Windows)
- Firewalls and proxies
- Applications and APIs

Features:

- Centralized log collection (via syslog, GELF, or filebeat)
- Custom pipelines for parsing structured/unstructured logs
- Rule-based log enrichment (e.g., adding geo-IP, threat data, asset info)
- Indexing and high-speed querying of large log volumes
- Role-based log access with audit trails



## Index Set: Default index set

This is an overview of all indices (message stores) in this index set Graylog is currently taking in account for searches and analysis.

You can learn more about the index model in the [documentation](#)

Index prefix: graylog  
Shards: 4  
Replicas: 0

Index rotation strategy: PT12H (12h, 12 hours)  
Rotation period:

Index retention strategy: Delete  
Max number of indices: 15

11 indices with a total of 195,354,430 messages under management, current write-active index is graylog\_10.

Elasticsearch cluster is green. Shards: 44 active, 0 initializing, 0 relocating, 0 unassigned, [What does this mean?](#)

### graylog\_10 active write index

Contains messages up to a few seconds ago (279.9MB / 814,621 messages) [Hide Details / Actions](#)  
Range re-calculated an hour ago in 0ms, 33 segments, 0 open search contexts, 0 deleted messages

**Primary shard operations**

Index:	470 ops (took a few seconds)
Flush:	0 ops
Merge:	31 ops (took a few seconds)
Query:	1,512 ops (took a minute)
Fetch:	224 ops (took a few seconds)
Get:	0 ops
Refresh:	324 ops (took a few seconds)

**Total shard operations**

Index:	470 ops (took a few seconds)
Flush:	0 ops
Merge:	31 ops (took a few seconds)
Query:	1,512 ops (took a minute)
Fetch:	224 ops (took a few seconds)
Get:	0 ops
Refresh:	324 ops (took a few seconds)

**Shard routing**

S0 S1 S2 S3

Bold shards are primaries, others are replicas. Replicas are elected to primaries automatically when primaries leave the cluster. Size and document counts only reflect primary shards and no possible replica duplication.

Active write index cannot be closed Active write index cannot be deleted

### graylog\_9

Contains messages from 3 days ago up to an hour ago (15.2GB / 50,882,127 messages) [Hide Details / Actions](#)  
Range re-calculated an hour ago in 23504ms, 87 segments, 0 open search contexts, 0 deleted messages

**Primary shard operations**

Index:	0 ops
Flush:	4 ops (took a few seconds)
Merge:	0 ops

**Total shard operations**

Index:	0 ops
Flush:	4 ops (took a few seconds)
Merge:	0 ops



## Alerting & Correlation Engine

- Event-based and condition-based alerts
- Combine log data and metric thresholds for richer context
- Alert deduplication, correlation, and suppression
- Notifications via Email, SMS, Slack, Teams, or custom Webhooks
- Escalation and acknowledgment workflows built in
- Integration with ticketing or SIEM workflows

## Alerts

Incident

Export as [CSV](#) [Add Alert Profile](#) [Manage Alert Profiles](#) [Settings](#)

View: Active alerts [Today](#)

Critical Alerts 34 Trouble Alerts 0 Attention Alerts 0 All Alerts 34

	Time Generated	Alert Message Format	Alert Status	Workflow Status	Source
<input type="checkbox"/>	2024-07-10 14:42:00	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	Open	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:42:00	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	Open	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:41:47	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	Open	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:41:47	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	Open	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:41:33	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	In Progress	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:41:33	Trend Micro OfficeScan : Report proxy status, target url = [https://os...	Open	Run Workflow	Trend Micro OfficeScan
<input type="checkbox"/>	2024-07-10 14:41:30	Microsoft-Windows-Security-Auditing : The handle to an object was ...	In Progress	Run Workflow	Microsoft-Windows-Security-Audi...
<input type="checkbox"/>	2024-07-10 14:41:30	Microsoft-Windows-Security-Auditing : The handle to an object was ...	In Progress	Run Workflow	Microsoft-Windows-Security-Audi...
<input type="checkbox"/>	2024-07-10 14:41:30	Microsoft-Windows-Security-Auditing : The handle to an object was ...	In Progress	Run Workflow	Microsoft-Windows-Security-Audi...
<input type="checkbox"/>	2024-07-10 14:41:30	Microsoft-Windows-Security-Auditing : The handle to an object was ...	In Progress	Run Workflow	Microsoft-Windows-Security-Audi...



## Advanced Search and Forensic Tools

- Full-text and field-based log search
- Filter logs by source, severity, message content, time range, etc.
- Structured query support for forensic investigations
- Saved searches and dashboards for repetitive use
- Export logs or filtered data as JSON, CSV, or Syslog





### Dashboards and Visualizations

- Drag-and-drop customizable widgets
- Real-time charts, metrics, logs, topology, and alerts
- Custom views per team or user role
- Correlation widgets to show logs + metrics + alerts in one view



### Security Event Monitoring & Threat Indicators

- Detect brute force attempts, port scans, and traffic anomalies
- Map log activity to IP reputation or threat intelligence feeds
- Alert on known bad actors or patterns
- Watchlists and threat detection rule engine
- Geo-IP mapping of log sources for visibility into global events



### Role-Based Access Control and Audit Logging

- RBAC with granular permission controls
- Read/write/limited-view log access
- User-level audit trails and session tracking
- Support for LDAP, SSO, and 2FA



### REST API and Integration Support

- Integrate with existing tools (ticketing, CMDB, orchestration)
- Use Webhooks for triggering external actions
- Feed logs or metrics into external dashboards or automation tools
- Plugin support for log shippers, input collectors, or custom scripts

## Deployment Models

### On-Premises Deployment

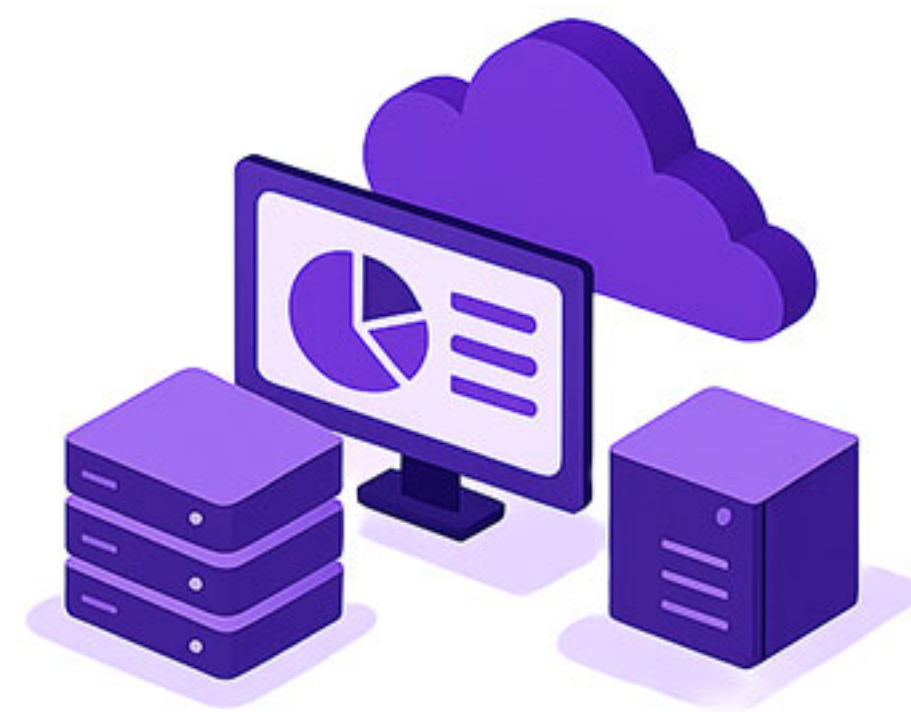
- Hosted entirely on your infrastructure
- Ideal for privacy-sensitive or air-gapped environments





## Hybrid Cloud Architecture

- Cloud-based dashboard
- On-site log collectors and pollers
- Suited for organizations with distributed or multi-site operations



## Always-On IT, Always in Control

Stay ahead with real-time diagnostics and proactive monitoring that resolves issues before they escalate.



### Keeping IT Operations Smooth, One Node at a Time

Behind every resilient IT network is a team that doesn't sleep on alerts.

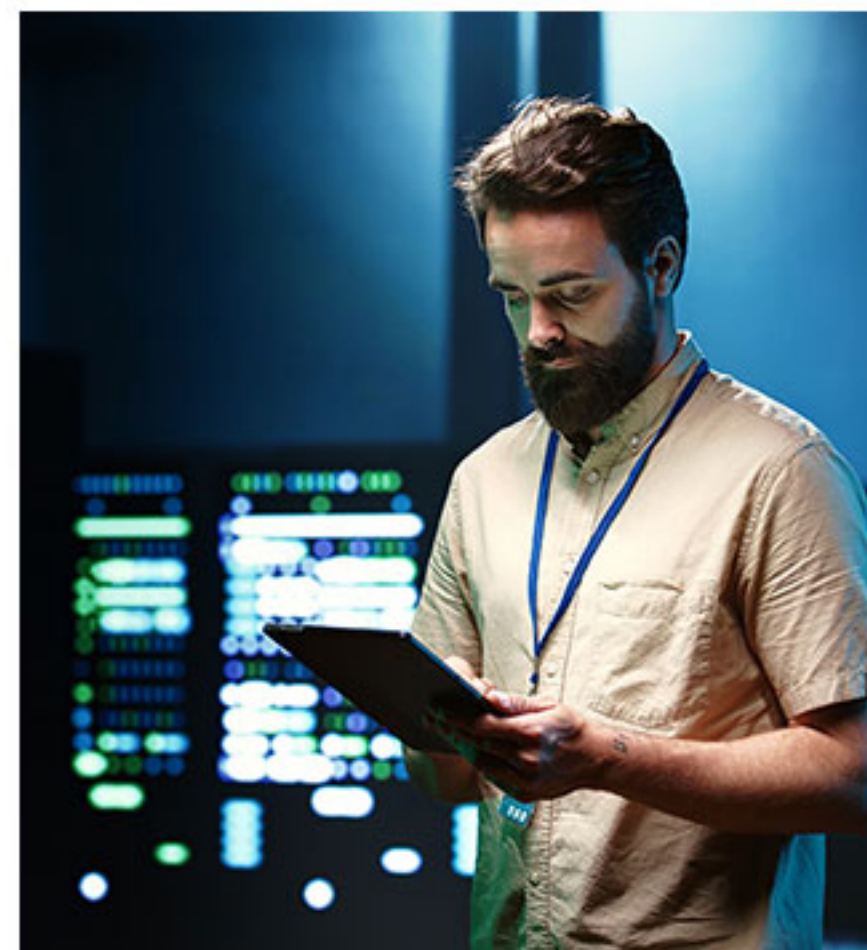
DcDynamo empowers your engineers with live network visibility and instant diagnostics—so issues get resolved before they're noticed.



### Real Stories. Real Results. Real Uptime.

A leading ISP reduced downtime by 70% with DcDynamo's real-time alerts and automated remediation tools.

Your IT team deserves tools that do more than just monitor—they need tools that act.



### Built with Trust. Backed by Experts.

DcDynamo is designed by network engineers, for network engineers.

From enterprise data centers to distributed setups—our platform scales with your infrastructure and grows with your ambition.



# Certifications & Partnerships

Your Trusted Tech Partner for Government & Enterprise Solutions



**GeM Registered Vendor**



**MSME & Startup India Certified**



**Cloud/Tech Partnerships**



**ISO 14001 Certified Company**



# Contact Us

Your Trusted Tech Partner for Government & Enterprise Solutions

## 7SYSTEM TECHNOLOGY PVT. LTD.


○ CIN: U74999UP2021PTC140513

○ GSTIN: 07AABCZ6799B1ZY

---

### OFFICE ADDRESS

C-32, II Floor Kaushambi, Ghaziabad 201012

 +91-999-060-1505

 info@7system

 www.7system.in

