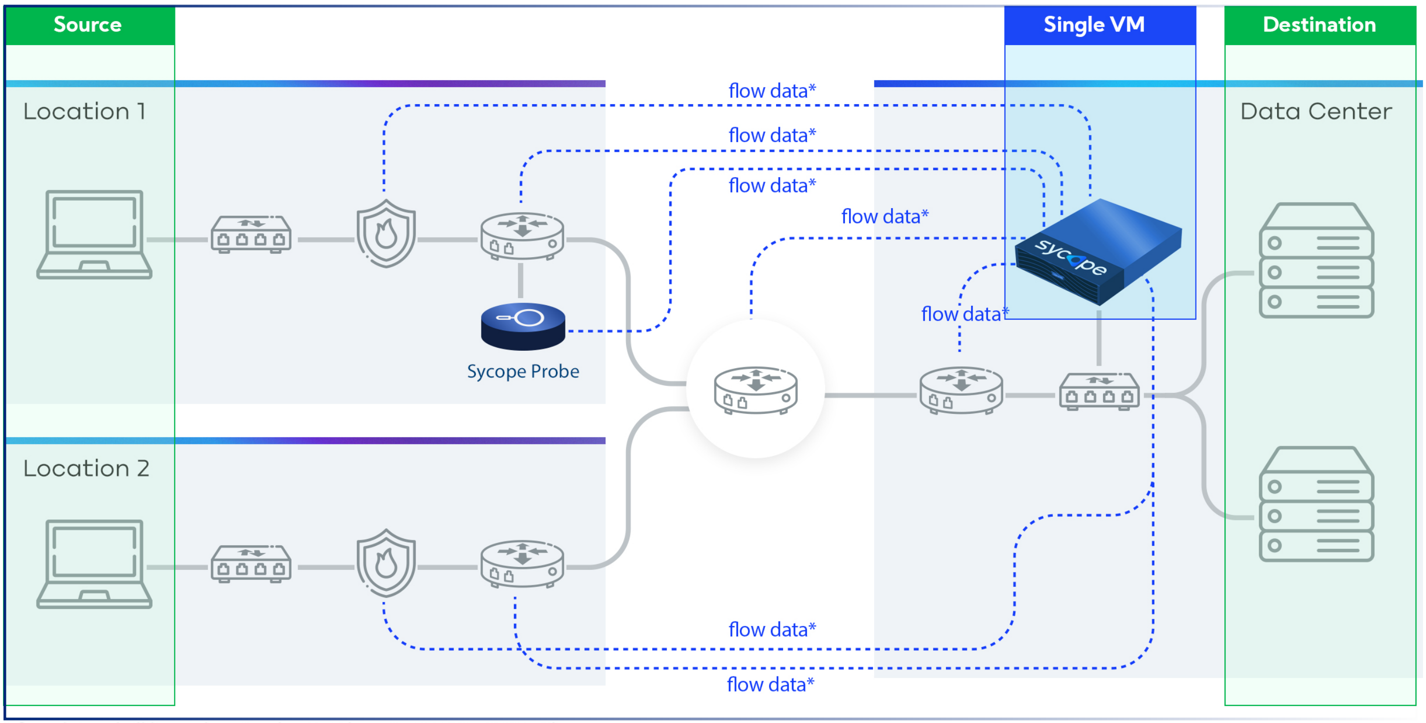
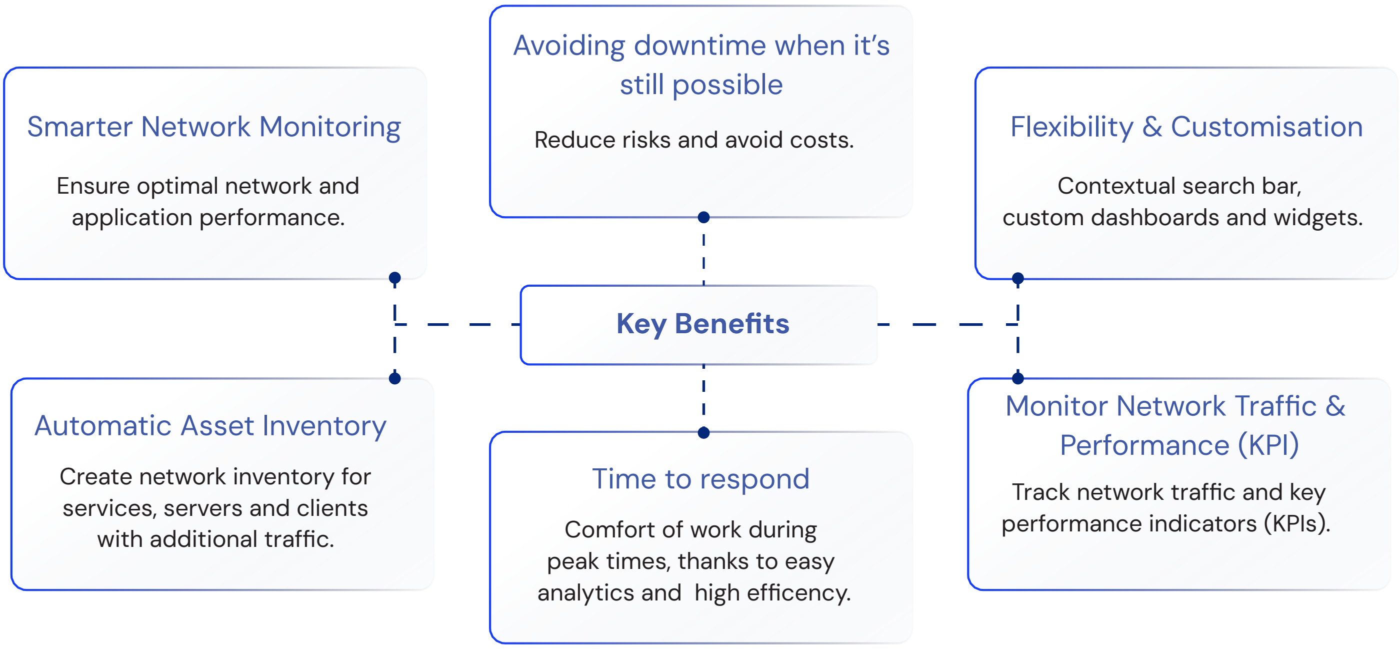
sycope

Sycope is a network traffic monitoring and security tool that leverages real-time flow analysis with business context to enhance performance and secure IT infrastructure. It records, processes, and analyzes all flow parameters, including SNMP, geolocation, and security feeds, transforming data into meaningful insights to detect network events and issues, measure delays, and identify security threats. Additionally, Sycope utilizes the NetFlow protocol for IT asset discovery. The system is equipped with multitenancy, enabling the management of multiple entities and/or independent IT networks from a single, central console.



* flow data - shall be underestood as NetFlow v5 v9, NSEL, IPFIX, sFlow.

Example of Sycope implementation in a multi-site organization.



Key Benefits

Avoiding downtime when it's still possible

Reduce risks and avoid costs.

Smarter Network Monitoring

Ensure optimal network and application performance.

Flexibility & Customisation

Contextual search bar, custom dashboards and widgets.

Automatic Asset Inventory

Create network inventory for services, servers and clients with additional traffic.

Time to respond

Comfort of work during peak times, thanks to easy analytics and high efficency.

Monitor Network Traffic & Performance (KPI)

Track network traffic and key performance indicators (KPIs).

Real-time flow analysis

- NetFlow v5/9/10, IPFIX, NSEL, sFlow, sampling supports.
- Enhanced by SNMP, geolocation, security feeds.
- Data deduplication.
- NQL authorial query language.
- Support for IPv4 and, IPv6.
- Non-standard fields analysis including NAT, MPLS, DNS analysis.

Asset discovery

Independent module created to facilitate inventory management, focusing on devices, their usage, the connections between them and to/from the external hosts.

Ability to define **Traffic Rule Profiles** for matching Server-to-Server and Client-to-Server connections, according to such values as IPs, Subnets, Ports or Protocols.

Custom Asset Metrics: enabling the storage of historical data and integration with CMDBs systems.

Asset Device View (new drilldown action): in-depth analysis of a specific endpoint or server.

Multitenancy

- Functionality allows for monitoring of multiple sites and/ or restricted IT networks from a single, central console.
- Master admins can grant access for local clients' admins via RBAC functionality if necessary.
- Enhanced jumpstart allows to license tenant's with minimal effort, utilizing the same configurator as standalone instances.
- Secure communication and access for Master Console initiated always from the tenant's instances, allowing both remote data collection and remote access without any external connection requirements.
- Service Provider can manage up to 100 instances on a single Master Console allowing flexibility in service agreement signing/renewal/disposal.

Analyse Data with a focus on network observability

Analyse data using diverse fields:

- Fields type indlude: AS, IP, Application, Protocol and more.

Analyse non-standard flow fields:

- Example of non-standard flow fields: Forwarding Status, Retransmitted In Bytes, Retransmitted Out Bytes, Retransmitted In Packets, Retransmitted Out Packets, Client Max TTL, Client Network Time, Server Network Time and more.

Choose from multiple calculated metrics (calculated based on flow fields):

- More than 40 calculated metrices including: Sum Flows/s; Unique Client Ips, Sum Avg Packets/s, Sum Client Bits/s, Unique ASNs, Avg Out Packets/s, Out Retransmitted Packets, % In Retransmitted Packets.

Select date/time range over standard values:

- Choose from predefined or custom timeframes.

Advanced Custom Aggregations

- Enable to set a dynamic key field value and any metric for them. The Aggregations can be freely edited, duplicated, exported and deleted.

Playground

- Enable to test NQL queries, examine the functionality of the search bar query, and evaluate the generated results.

Fast access to essential information

Interactive diagrams, tables, and maps equipped with relevant data, statistics, and indicators are part of the system, enabling network behavior pattern analysis and facilitating incident management for detected issues.

Extensive filtering:

- Maintain the time context and filters between views.
- Save complex search filters and time context (bookmarks).
- Drill-down widget, filtering widget, fly-out statistic.

Automatic mapping of values in the system:

- User configurable sets of names, terms, values.
- Out-of-the-box: application names, countries, AS, MITRE techniques.

Easy top-down access:

- Drilldown mechanisms enable viewing of data for a specific port, interface or IP address.

Access to external services

- The system enables access to external services, such as VirusTotal, directly from the view under analysis (using right click button) and further analysis of data.
- **Feeds server** – dynamic identification of the global threats based on integration with the Sycope Cyber Threat Intel ligence (CTI) platform.
- **Deep Search in Lookups:** the search results display all relevant Lookup names, along with direct access to their defined parameters, the matched value, and its type. All enhancing configuration management and provides greater visibility.

Powerful GUI

Unique searchbar:

- Hinting, colouring, syntax validation, query builder and bookmarks, selected elements in convenient editable tiles.
- Search history – quick access to previously used values for efficient reuse.

Quick Setup:

- Deploy and configure Sycope with just few steps using the Quick Setup wizard. Define such objects as Hosts, Subnets, Application, Rules and Data Retention, with additional suggestions.

Built-in Dashboards:

- Over 100 built-in dashboards organized using three concepts – Trends, Overview and Details. Dedicated main view with colourful tiles and grouping.

Informative visualizations:

- Graph types: time series (line, bar, scatter), gauge, pie chart, graph, kpi, map, sankey diagram, sunburst, tree, tree map, table, radar.
- Trajectory - especially useful for lert visualization on a time scale.
- Component tour - new features and updates tour.
- Rules creator.
- Widget personalization. Objects grouping.

Dynamic Baseline:

- Compare metrics in different time ranges, visualize/filter both baseline and metric together on a single plot (both rules and widgets), display trend and utilize recurrence.

Quick Analysis

An easy-to-use view allowing for quick analysis of ad hoc data without the necessity to create widgets or dashboards.

Discovery Mode
Possibility to add custom NetFlow field to the system for dedicated analysis and presentation of data (e.g. fields specific to a certain type of brand of equipment.)

Ready to use scenarios

The security module features pre-configured analytical scenarios to simplify the analysis and conclusion-making process for critical security issues.

Advanced system administration tool

- Data role-based access control (data RBAC) scan effectively limit access from the UI point of view and data access perspective: selected streams and individual exporters.
- Active Directory integration, REST API, retention time counter, system notification.
- Update Portal containing system updates for all modules available 24/7.
- Simple reporting system with exportable dashboards.

User Scripts

- Allows for automatic communication by POST json message with external systems using the REST Client.
- Alerts can be send to external systems and applications.

Rest API

- **Custom Streams:** capturing historical data, flexibility and multisource approach – to conduct in-depth root cause analysis.
- **Seamless Integration in Sycope:** lookups editing possibilities, alerting for any custom integration
- Integration with **Zabbix** and **Suricata** with dedicated dashboards.

Empowering flexibility

- Flexible presentation of network traffic paths for monitored devices with views, bookmarks.
- Customizable dashboards and widgets available.
- Alert policies easily defined with flexible UI.
- Data retention management made flexible.

Key Modules Features

VISIBILITY	L3 and L4 data analysis, network data mining, lists of connections per IP address, protocol, port, country, ASN or QoS., Network traffic analysis at the level of a single TCP/ UDP port UDP port, out of the box anomaly detection, dedicated dashboards, DNS analysis.
PERFORMANCE	L7 analysis, dedicated probe (including measurements of fields: % Client Retransmitted Packets, % Server Retransmitted Packets). Response time measurement, Real-life app performance measurement, Retransmissions detection, Combine network applications and metrics, additional data sources (DPI for L7), dedicated performance dashboards.
SECURITY	More than 45 security detection rules, Detection rules customization. Active mitigation using NAC system, MITRE ATT&CK Framework mapping, Sycope CTI (Actively monitors number of sources, analyses, and generates a unified list of current Indicator of Compromises (IoCs), Ability to create custom rules, dedicated security dashboards including SOC.
ASSET DISCOVERY	Resource inventory based on Network Traffic Analysis. 100% passive – no network scans. Host/services/application dependencies. Key services which work on and are use by the host.

Key product dashboards groups available out of the box

VISIBILITY	Traffic Summary, TOPs, Protocols, MPLS, IP Addresses, Groups, Devices and Interfaces, Countries, Baselines, Autonomous Systems Applications
PERFORMANCE	DNS, HTTP, Network Anomalies
SECURITY	SOC & KPIs, Threats Detection & Analysis, Alert Management
ASSET DISCOVERY	Asset discovery dashboard, Asset Device View, Asset Device Traffic

Alerting - more than 60 detection rulest

The security module features over 60 rules covering MITRE tactics including i.e: Command and Control, Credential Access, Discovery, New Security Alert Manager: event classification, status tracking, assign users per alert option. Exfiltration, Impact, Initial Access, and Lateral Movement.
Example of security rules by technique.

TECHNIQUES	Application Layer Protocol, Non-Standard Port, Proxy, Brute Force, Adversary-in-the-Middle, Network Service Scanning, System Network Configuration Discovery, Data Transfer Size Limits, Endpoint Denial of Service, Phishing, Resource Hijacking, Drive-by Compromise, Exploitation of Remote Services.
ALERT NAME	Cleartext Application, OT Device Discovered,Suspicious IP – Malware, Suspi- cious IP – Open DNS, Suspicious IP – Sycope Community, Suspicious Port BL, Suspicious Port WL, Suspicious IP – Proxy, Suspicious IP – TOR, Brute Force Attack, Unauthorized LLMNR/NetBIOS Activity, mDNS from Internet, Horizontal Scan, Suspicious IP – Scanner, Unauthorized DHCP Activity, Unauthorized DNS Activity, Abnormal flows ratios, Abnormal DNS Query Limit, Abnormal DNS Response Limit, DNS Transfer limit, High Data Transfer (in), High Data Transfer (in+), High Data Transfer (in++), Large Size TCP Packets, Large Size UDP Packets, Possible SPAM activity, DDoS Attack, DDoS DNS Amplification Attack, DDoS Protocol Flood, PoDs Attack, Phishing, Suspicious IP – Spam, Suspicious Port BL, Suspicious Port WL, SYN Flood Attack, P2P Activity, DNS Servers Discovery, Only SYN Client TCP Flag Initial connections from Public IPs, Only SYN Server TCP Flag Initial connections, High Initial Server Response Time, High Server Network Latency, High Client Network Latency, SMB Traffic to External Networks, Suspicious SSH protocol change, Suspicious Protocol Mixing, TFTP Amplification Attack, SNMP Amplification Attack, CLDAP Amplification Attack, SSDP Amplification Attack, NTP amplification attack, mDNS amplification attack, Excessive ICMP Requests, Frequent Short-Lived Connections, Lateral Movement Detection, Sudden Ingress from High-Risk Countries, Possible DNS Amplification Attack, Botnet Attack via DNS, Potential Virus Outbreak

Collector hardware requirements

	BASIC	SMALL	MEDIUM	LARGE
Max number of data flows	30k	60k	120k flow/s	250k flow/s
Max number of data sources	unlimited	unlimited	unlimited	unlimited
Max number of subnets	unlimited	unlimited	unlimited	unlimited
Max number of network sessions	400	800	1.5 M	3 M
Max number of unique IP address daily	700	1.5 M	3 M	6 M
Supported VM	VMWare 7 and higher recommended	VMWare 7 and higher recommended	VMWare 7 and higher recommended	VMWare 7 and higher recommended
BASE OS				
vCPU Cores	22	36	48	64
RAM	22 GB	36 GB	48 GB	96 GB
STORAGE				
OS disk	128 GB (recommended SSD disks)	128 GB (recommended SSD disks)	128 GB (recommended SSD disks)	128 GB (recommended SSD disks)
Data disk	at the customer's discretion (recommended SSD disks)	at the customer's discretion (recommended SSD disks)	at the customer's discretion (recommended SSD disks)	at the customer's discretion (recommended SSD disks)

sycope

www.sycope.com
contact@sycope.com

Sycope specializes in advanced IT solutions for monitoring and enhancing network performance and security. Developed by experienced engineers with backgrounds in global APM, NPM, and SIEM systems, our platform is built on insights gained from over 400 successfully completed projects focused on network efficiency, application performance, and cybersecurity.

Warsaw, Poland
Goraszewska 19
02-910 Warsaw

Bucharest, Romania
66, Petru Maior Str.,
011 264 Bucharest

4