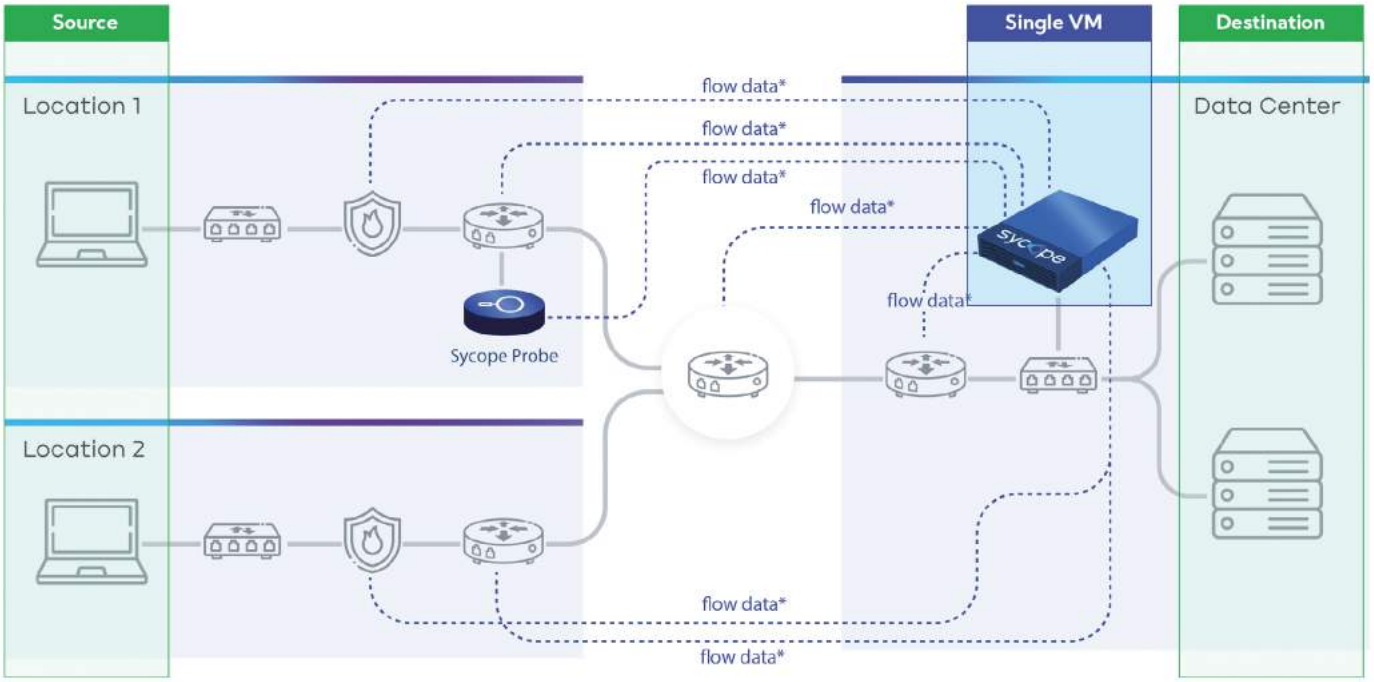
Sycope Datasheet

Sycope is a network traffic monitoring and security tool that uses real-time flow analysis with business context to improve performance and secure IT infrastructure. It records, processes, and analyzes all flow parameters, including SNMP, geolocation, and security feeds, to transform data into meaningful insights, detect network events and issues, measure delays, and identify security threats. Sycope's security feature is built using the MITRE ATT&CK framework. Sycope has security features including attack detection rules and incident detection mechanisms to keep the network safe from unwanted activities.



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

Example of Sycope's implementation in a multi-branch organization.

Key benefits

Compatible with any IT infrastructure

Adapt to new data source in your infrastructure (discovery mode).

Avoiding downtime, while it is still possible

Reduce risk and avoid costs caused cyber threats, app delays

Flexibility & customisation

Contextual search bar, Custom dashboards and widgets.

Analysing data having context

From generality to forensic details (drill-down data analysis).

Reduce time to respond

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

Monitor network traffic & performance (KPIs)

Track network traffic and key performance indicators (KPIs).

Key Features

Real-time flow analysis:

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

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.

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

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 Intelligence (CTI) platform.

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.

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 alert visualization on a time scale.
- Component tour - new features and updates tour.
- Rules creator -

Customisable dashboards

- Option to keep dashboards private or share with others.

Possibility to share a view with other users

- Option to save the time and expression for future use.

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.

Ready to use scenarios

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

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.

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.

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.
- Raporting system with exportable dashboards.

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 & KPIs, as well as Threat detection & Analysis, 30+ Network Threat Hunting Searchers, Security Use Cases

Alerting - more than 60 detection rules

The security module features over 60 rules covering MITRE tactics including i.e: Command and Control, Credential Access, Discovery, Exfiltration, Impact, Initial Access, and Lateral Movement. Example of security rules by technique

TECHNIQUE	ALERT NAME
Application Layer Protocol	Cleartext Application, OT Device Discovered,Suspicious IP – Malware Suspicious IP – Open DNS, Suspicious IP – Sycope Community
Non-Standard Port	Suspicious Port - Blocklist, Suspicious Port - Allowlist
Proxy	Suspicious IP – Proxy, Suspicious IP - TOR
Brute Force	Brute Force Attack
Adversary-in-the-Middle	Unauthorized LLMNR/NetBIOS Activity
Network Service Scanning	mDNS from Internet, Horizontal Scan, Suspicious IP – Scanner
System Network Configuration Discovery	Unauthorized DHCP Activity, Unauthorized DNS Activity, Abnormal flows ratios
Data Transfer Size Limits	Abnormal DNS Query Limit, Abnormal DNS Response Limit DNS Transfer Limit, High Data Transfer (Int) High Data Transfer (Int<->Ext), Large Size ICMP Packets Large Size TCP Packets, Large Size UDP Packets, SPAM
Endpoint Denial of Service	DDoS Attack, DDoS DNS Amplification Attack, DDoS Protocol Flood, DoS Attack
Phising	Suspicious IP – Phishing, Suspicious IP – Spam
Suspicious Port	Suspicious Port BL, Suspicious Port WL
Resource Hijacking	Suspicious IP – Cryptomining
Network Denial of Service	SYN Flood Attack
Drive-by Compromise	P2P Activity
Exploitation of Remote Services	Suspicious Host

TECHNIQUE	ALERT NAME
VISIBILITY dashboards	DNS Servers Discovery, Only SYN Client TCP Flag Initial connections from Public Ips, Only SYN Server TCP FlagInitial connections
PERFORMANCE dashboards	High Initial Server Response Time, High Server Network Latency High Client Network Latency

Key product dashboards groups

DASHBOARDS GROUPS	DESCRIPTION
VISIBILITY	
Traffic Summary	Overall view on network traffic including various statistics and KPIs.
TOPs	Dashboards focused on most noticeable elements from various network categories.
Protocols	A group of dashboards provides various information and statistics about discovered protocols.
MPLS	Provides various information and statistics about discovered MPLS labels.
IP Addresses	Dashboards provides various information and statistics about discovered IP Addresses.
Groups	A group of dashboards provides various information and statistics about IP mapped network groups.
Devices and Interfaces	A group of dashboards provides various information and statistics about discovered devices and interfaces.
Countries	Dashboards provides various information and statistics about discovered country-specific traffic.
Baselines	Dashboards focuses on traffic related metrics comparisons: current vs baseline.
Autonomous Systems	A group of dashboards provides various information and statistics about discovered autonomous systems.
Applications	A group of dashboards provides various information and statistics about discovered applications.
PERFORMANCE	
DNS	A group of dashboards provides various information and statistics about DNS traffic.
HTTP	A group of dashboards provides various information and statistics about HTTP traffic.
Network Anomalies	A group of dashboards focuses on Network Anomalies identification .
SECURITY	
SOC & KPIs	A group of dashboards including SOC dashboard (presenting security threats in the context of Tactics, Technics, groups, Countires, ASNs, Applications and other. The KPIs dashboards provides various business and audit related information about security risks and trends.
Threats Detection & Analysis	A group of dashboards The Threat Datection $ Analysisc Dashboards allows for multi-level analysisc of all security threates, regardless of whether they come from outside or inside the organization.

Collector hardware requirements

	BASIC	SMALL	MEDIUM	LARGE
Max number of flows	30k flow/s	60k flow/s	120k flow/s	250k flow/s
Max number of data sources	unlimited	unlimited	unlimited	unlimited
Supported VM Systems	VMWare 7 and higher recommended	VMWare 7 and higher recommended	VMWare 7 and higher recommended	VMWare 7 and higher recommended
BASE OS	BASIC	SMALL	MEDIUM	LARGE
CPU cores	22 pcs.	36 pcs.	48 pcs.	64 pcs.
RAM	22 GB	36 GB	48 GB	96 GB
STORAGE				
OS disk	128 GB (recommended SSD disks)	128 GB (recommended SSD disks)	128 GB (SSD disks required)	128 GB (SSD disks required)
Data disk	at the customer's discretion* (recommended SSD disks)	at the customer's discretion* (recommended SSD disks)	at the customer's discretion* (SSD disks required)	at the customer's discretion* (SSD disks required)

Licensing model - perpetual and subscription model (Visibility, Performance, Security)

Probe hardware requirements

Probe is available as a license for Virtual or Hardware Appliance. The performance of the Probe depends of the hardware resources. Please see below the requirements depends of the traffic throughput to monitor:

Traffic	< 100 Mbps	Between 100 Mbps and 1 Gbps	Between 1 and 10 Gbps	Above 10 Gbps
Flow Export Rate	< 100 FPS	< 1000 FPS	< 3000 FPS	3000+ FPS
Active Flow Cache	Thousands	Hundreds of Thousands	A few Millions	Tenth of Millions
CPU Type	2 cores	2 cores+	4 cores+	8 cores+
Memory	2 GB	2 GB+	4-8 GB+	16 GB+

Learn more about Sycope product by visiting our website https://www.sycope.com

2023/06/06/SYCOPE

www.sycope.com
contact@sycope.com

Warsaw, Poland
Goraszewska 19
02-910 Warsaw

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

Prague, Czech Republic
Freyova 12/1
190 00 Praha