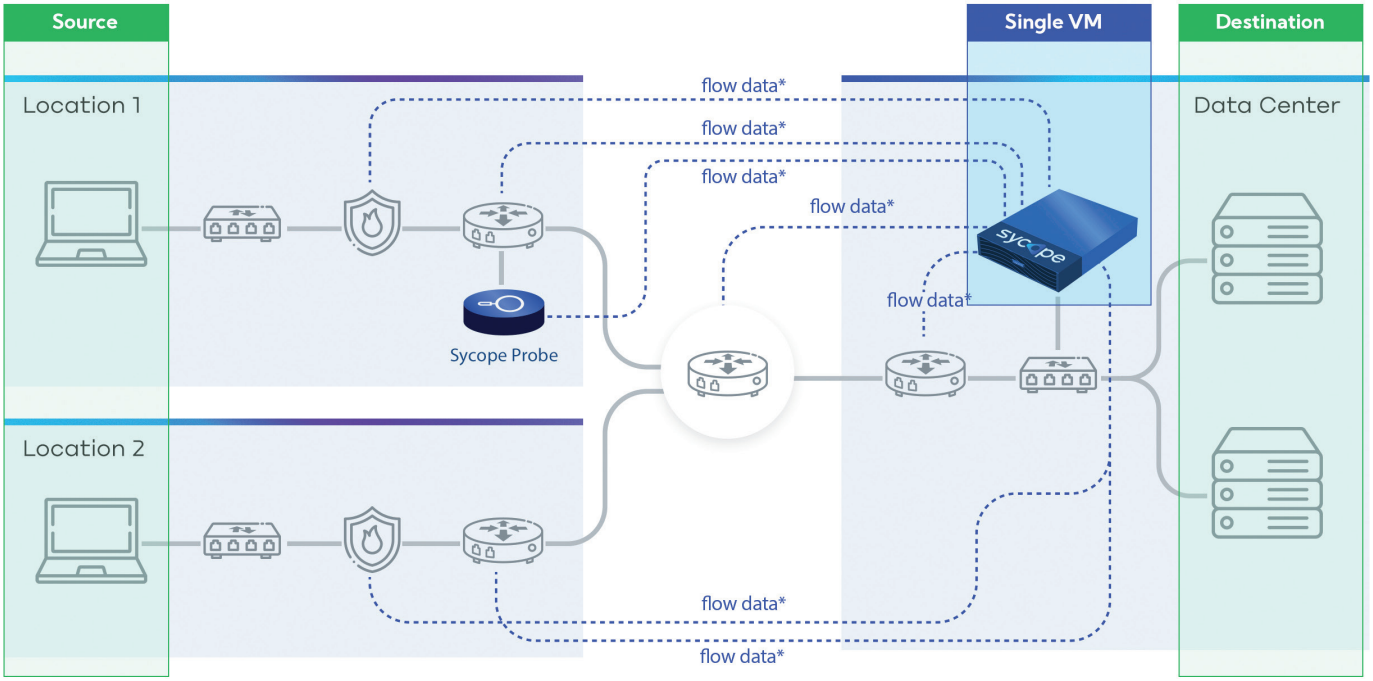
Sycope Datasheet

Sycope is a network traffic monitoring and security solution using real-time flow analysis, enriched with business context, to help businesses assess performance and protect IT infrastructure. It records, processes, and analyses all parameters contained in flows, enhanced by SNMP, geolocation, and security feeds. Sycope is designed to discover network events and issues, measure delays and identify security threats. The security feature of Sycope is created based on the MITRE ATT&CK methodology. Rules and security incident detection mechanisms make it possible to detect attacks and undesirable activities on the network.



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

Implementation of the Sycope system in a network on the example of a two-branch company.

Key benefits

Smarter network monitoring

Ensure optimal network and application performance

Avoiding downtime, while it is still possible

Reduce risk and avoid costs

Flexibility & Customisation

Contextual search bar, Custom dashboards and widgets

Analysing data having context

From generality to forensic detail

Time to respond

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

System coherency

3 modules, one informative GUI

Key Features

Real-time flow analysis:

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

Big Data dedicated for network observability:

Analyse data choosing from many fields:

- AS Name by IP, IP Address Name, AS Names, Application Name, Protocol Name, Server IP, Name, Client IP Name, AS Name, ToS Names, Interface Name, Exporter IP (Name), Exporter Location, Exporter Description, ToS Name, Direction, Application ID, Server TCP Flags, Client TCP Flags, Bytes, Packets.

Analyse non-standard flow fields:

- PostNatSrcIp, postNatSrcPort, applicationId, firewallEvent, fwExtEvent, minPacketLength, maxPacketLength, flowLabel, clientMaxTtl, srcVlan, dstVlan, ipv6OptionHeaders, mplsLabel1-5, retransmittedInPackets, retransmittedOutPackets, retransmittedInBytes, retransmittedOutBytes, clientNetworkTime, serverNetworkTime, initialServerResponseTime.

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

- Sum Flows/s; Sum Out Bits/s, Sum In Bits/s, Sum Bits/s, Sum Server Bits/pkt, Sum Client Bits/pkt, Sum Bytes/packet, Sum Packets/flow, Sum Packets/second, Sum Client Bits/flow, Sum Server Bits/flow, Sum Bytes, Sum Server Packets/flow, Sum Client Packets/flow, Unique Client Ips, Sum Avg Packets/s, Sum Client Bits/s, Sum Server Bits/s, Sum Server Packets/s, Sum Client Packets/s, Sum Packets, Unique Server Ports, Unique Server Ips, Unique ASNs, Avg Out Packets/s, Avg In Packets/s, Avg Packets/s, Packets/s, Avg Flows/s, % Out Retransmitted Packets, Avg Server Packets/flow, Avg Server Bits/flow, % In Retransmitted Packets, Avg Client Packets/flow, Avg Client Bits/flow, Avg Server Bits/pkt, Avg Client Bits/pkt, Bits/s, Bits.

Select date/time range over standard values:

- Choose from predefined or custom timeframes.

Fast access to critical information

The system has been provided with interactive diagrams, tables and maps containing critical data, statistics and indicators, enabling the analysis of network behavior patterns and supporting the incident handling of discovered issues.

Extensive filtering:

- Maintain the time context and filters between views.
- Easily move filters between the 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.

Informative visualizations:

- Graph types: time series (stacked, line, bar), comparison bar, pie chart, sankey diagram, table.
- Component tour - new features and updates tour.

Customisable dashboards

- Make dashboards private or share across with others.

Possibility to share a view with other users

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

Ready to use scenarios

- Analytical scenarios implemented in the module facilitate analysing and drawing conclusions concerning the most important security-related aspects.

Empowering flexibility

- Paths of network traffic for monitored devices presented in flexible views.
- Possibility to create your own dashboards and widgets.
- Define alert policies with flexible UI.
- Flexible managing of data retention.

Advanced system administration tool

- **RBAC, Active Directory integration, REST API.**
- Update Portal containing system updates for all modules available 24/7.
- Raporting system with exportable dashboards.

Easy licensing model

- Modules: Visibility, Performance, Security.
- Perpetual and subscription model.

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.

More than 45 security detection rules

The security module contains more than 45 rules regarding seven MITRE tactics: Command and Control, Credential Access, Discovery, Exfiltration, Impact, Initial Access and Lateral movement. Examples of threats detected by Security module.

TECHNIQUE	THREATS DETECION
Application Layer Protocol	Cleartext Application, OT Device Discovered,Suspicious IP – Malware Suspicious IP – Open DNS, Suspicious IP – Sycope Community
Non-Standard Port	Suspicious Port BL, Suspicious Port WL
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

Key product dashboards

DASHBOARD	DESCRIPTION
VISIBILITY	
Total traffic Overview	Overall view of Network Traffic.
IP Addresses Details	Detailed view of Network traffic splits by IP Address.
Groups Overview	Overall view of Network Traffic splits by Group.
Interfaces Overview	Overall view of Network Traffic splits by Interface.
Top 10 Server IPs in last 15 minutes Timeline	Top 10 Server IPs in last 15 minutes Timeline.
Top 10 Client IPs in last 15 minutes Timeline	Dashboard shows TOP 10 Client IPs in last 15 minutes time window.
Finding Anomalies	Dashboard helps to find anomalies on network like miss configuration of SPAN or Netflow, potentially forgotten services, potentially network scans and recondenses.
Protocols Overview	Overall view of Network Traffic splits by Protocol.
Tos Overview	Overall view of Network Traffic splits by ToS.
Applications Overview	Overall view of Network Traffic splits by Application.
Applications Details	Detailed view of Network Traffic splits by Application.
ASNs Overview	Overall view of Network Traffic splits by ASN.
IP Addresses Overview	Overall view of Network Traffic splits by IP Address.
Countries Overview	Overall view of Network Traffic splits by Country.
IP Addresses Details	Detailed view of Network Traffic splits by IP Address.
PERFORMANCE	
IP Addresses Performance	Advanced view shows performance metrics for IP Addresses provided by nBox probe.
Application Performance	Advanced view shows performance metrics for Applications provided by nBox probe.
SECURITY	
SOC	The SOC Dashboard is a set of widgets presenting security threats in the context of Tactics, Technics, groups, Countires, ASNs, Applications and other attributes for last 1 hour refreshed every minute. Dedicated to department like SOC who deal with 244/7 security monitoring.
KPIs	The KPIs Dashboard helps security managers and investigetors in monitoring security risks and threats.
Threats Corelations	Threats Correlations dashboard allows for multi-level analysisc in context of Ips, Groups and Countries.
Threats Analysis	The Threat Analysisc Dashboards allows for multi-level analysisc of all security threates outside or inside the organization.

Alerting

MODULE	ALERT NAME
VISIBILITY	DNS Servers Discovery, Only SYN Client TCP Flag Initial connections from Public Ips, Only SYN Server TCP Flag
PERFORMANCE	High Initial Server Response Time, High Server Network Latency High Client Network Latency
SECURITY	Large Size ICMP Packets, Large Size TCP Packets, Suspicious IP - Scanner Suspicious IP – TOR, Suspicious IP – Malware, Suspicious IP – Proxy, DDoS Attack, Suspicious IP – Phishing, DDoS DNS Amplification Attack, Abnormal flows ratios, Brute Force Attack, Cleartext Application, Abnormal DNS Response Limit, Abnormal DNS Query Limit, DoS Attack, DDoS Protocol Flood, Rogue RDP Access, Large Size UDP Packets, Horizontal Scan, Unauthorized NFS Export Data, Suspicious Host, Suspicious IP - Sycope Community, Suspicious IP - Open DNS, Suspicious Port WL, Suspicious IP – Cryptomining, Suspicious IP – Spam, SYN Flood Attack, P2P Activity Unauthorized LLMNR/NetBIOS Activity, Unprotected Docker Daemon, OT Device Discovered, Multicast DNS from Internet, DNS Transfer Limit Unauthorized Internet Access, Unauthorized RDP from Internet High Data Transfer (Int), High Data Transfer (Int<-> Ext) Vertical Scan Detected, Unauthorized DHCP Activity, Unauthorized DNS Activity, Virus Outbreak, SPAM, Suspicious Port BL, APIPA address assinment, Unauthorized LDAP Activity, Email Worm, Large Google Drive Upload Traffic, Botnet

Collector hardware requirements

	BASIC	SMALL
Max numer of flows	30k flow/s	60k flow/s
Max number of data sources	unlimited	unlimited
Supported VM Systems	VMWare 6.5 and higher	VMWare 6.5 and higher
VISIBILITY		
CPU	16 vCPU	32 vCPU
RAM	18 GB	36 GB
LAN Interfaces	2x1 Gbit/s	2x1 Gbit/s
Storage	500 GB for OS and >0,75 TB for Storage	500 GB for OS and >1,5 TB for Storage
SECURITY		
CPU	+2 vCPU	+4 vCPU
RAM	+2 GB	+4 GB
PERFORMANCE		
CPU	+2 vCPU	+4 vCPU
RAM	+2 GB	+4 GB

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+

2022/09/26/SYCOPE

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

Sycope is focused on designing and developing highly specialised IT solutions for monitoring and improving network performance. Our solutions were created and developed by engineers, who have been working on the issues of network performance, application efficiency and IT security for over 20 years. Using the solutions from global APM/ NPM and SIEM providers, they have completed more than 400 projects. As Sycope we transform data into actionable insights, giving you answers not only data.

www.sycope.com
contact@sycope.com

Warsaw, Poland
Goraszewska 19
02–910 Warsaw

Prague, Czech Republic
Freyova 12/1
190 00 Praha