TELESOFT

DATASHEET

FLOWPROBE

UNSAMPLED TRAFFIC MONITORING

Full network visibility with the world's highest density enriched flow metadata generator

UNSAMPLED
FlowProbe provides enriched, unsampled, real-time flow records across all network sessions for use in cyber, NPMD and compliance monitoring.

L4 - L7 VISIBILITY
Seamlessly fuse L7 protocols including HTTP, SSL, SIP, DNS and TCP session timing information before delivery to SecOps and digital forensics teams providing accurate, real-time intelligence for comprehensive cyber threat investigations. Up/down link flows are stitched together into one record for effective downstream analysis and data volume reduction.

DEPLOYMENT
Rapidly deployable and easy integration enables visibility for deep cyber threat analysis on high volume networks, monitoring up to 400Gbps per appliance. The 1U appliance is easily incorporated in all server rooms for comprehensive coverage of large network deployments, peering links or data centre backbones.

DE-TUNNELLING
Automatically detect tunnelled traffic (GRE, GTP, MPLS, IP-in-IP, PPTP, and Tunnelled Ethernet over GRE) providing visibility of encapsulated traffic to further enhance visibility and protection over your network, reducing the opportunity for cyber threats.

KEY FEATURES	
Instrument 240 Million concurrent flows at a rate of 7M flows/s	Monitor large scale network traffic for cyber security analysis, NPMD and compliance
Passively monitors up to 4 x 100GbE in a single 1U appliance	Connect to large scale monitoring infrastructure, peering links, national xSP and large data-centres
De-tunnels GTP, GRE, MPLS, PPTP, IP-in-IP, and Tunnelled Ethernet over GRE traffic	Monitor large scale/national xSP and telco networks
Duplicate packet detection and removal	De-duplication improves monitoring tools efficiency, accuracy and storage requirements
Enhances records with SSL, DNS, SIP, ASN Numbering, HTTP host and HTTP URI	Layer 7 visibility and control for granular user management
Exports flow records to Telesoft TDAC Platform or other compatible IPFIX collector or JSON consumer	Quickly deploy accurate, large scale network visibility and analysis

COMPETITIVE ADVANTAGE
Telesoft FlowProbe is highly cost effective in terms of TCO compared with industry peers, delivering a higher density platform with lower power consumption and cooling requirements.

Telesoft FlowProbe can be configured in multiples of 100 GbE interfaces which do not require addition of servers/chassis but license to add interfaces, requiring minimal operational and maintenance costs.

TELESOFT HEADQUARTERS
Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
sales@telesoft-technologies.com

ATCO-TELESOFT
TEDJA8069, 8069, 4th Street,
5249, Prince Muhammad Ibn
Saud Dist., 32241,Dammam,
Kingdom of Saudi Arabia
+966 (0) 13 833-5588, Ext.220
Rohit Singh - rohit.singh@atco.com.sa

ATCO COMMERCIAL
EDJA8069, 8069, 4th Street,
5249, Prince Muhammad Ibn
Saud Dist., 32241,Dammam,
Kingdom of Saudi Arabia
+966 (0) 13 833-5588, Ext.233
atcocommercial@atco.com.sa

TECHNICAL SPECIFICATIONS		
	200GBPS FLOWPROBE	400GBPS FLOWPROBE
Physical	1RU 19-inch rack mount- 1.7x17.2x30.6 in (4.3x43.7x77.7 cm)	
Monitoring Interface	2 x 100GBASE-LR4 QSFP28	4 x 100GBASE-LR4 QSFP28
Tunnelling Support	Configurable to automatically detect and de-tunnel: MPLS, IPinIP, GRE, GTP, PPTP (PPP over GRE), and Tunnelled Ethernet over GRE.	
Flow Export Interface	• 10GbE Fibre Interface with swappable transceivers • Up to 16 IPFIX collectors	• 10GbE Fibre Interface with swappable transceivers • Up to 32 IPFIX collectors
Throughput	• 4M simplex flows per second • 120M active flows	• 7M simplex flows per second • 240M active flows
Flow Record Format	• IETF RFC7011/RFC7012 IPFIX • Export formats: IPFIX, JSON (Netflow/IPFIX/ JSON) • Supported Collectors: Telesoft TDAC Platform, Kafka, Elastic or other IPFIX/Netflow compatible collectors	
Enhanced Flow Data	• HTTP Host and URI: Rapidly know which IP addresses have visited which websites without any additional lookup, check for abnormal behaviour and look for connections to rogue URIs • HTTP Return Code: Check for abnormalities, such as machine initiated attacks indicated by a high level of 404 • Supports SIP method, request URI and response code • Server Name from SSL certificate exchange: Check for abnormal behaviour or investigate specific servers of interest • DNS query name, response name, address: Detect suspicious and rogue DNS servers • Correlation of IP address to autonomous systems (AS), to map network infrastructure utilising BGP information • TCP session timing (SYN / SYN-ACK): Detect anomalies and classify traffic • JA3 and JA3S SSL fingerprinting enables MD5 based checksum identification against a JA3 database • Identify specific Client and Server SSH implementations with HASSH (SSH Fingerprinting) • Payload Hash: The payload of the first packets in a flow are hashed. Hashes are stored within the flow record, which enables identification of security risks such as port scanning • Sequence of Packet Length & Time (SPLT): If enabled, the payload length and inter-packet duration, in milliseconds, are collected for the first set of TCP and UDP packets in the flow. TCP SEQ and TCP ACK are also collected for each TCP packet • JA4 and JA4S (with licensing) fingerprinting of encrypted TCP and QUIC network traffic	
Power Stats	330W typical, and 400W peak	400W typical, and 550W peak

Note - Additional features within the 400G FlowProbe do not adversely impact the overall performance.

ORDER OPTIONS		
	200GBPS FLOWPROBE	400GBPS FLOWPROBE
Part Number	Description	
500003047	200G FlowProbe, 1U, QSFP28, 2x100GbE	N/A
500003074	N/A	400G FlowProbe, 1U, QSFP28, 4x100GbE
500003082	100G QSFP28 LR4 Transceiver	
500003167	100G-DR Single Lambda PAM4 QSFP28 Transceiver	
500002853 (Note 1)	10GBase-SR optical SFP+ transceiver 850nm, single-mode LC	
500003012 (Note 1)	10GBase-ER optical SFP+ transceiver 1550nm, single-mode LC	
500002852 (Note 1)	10GBase-LR optical SFP+ transceiver 1310nm, single-mode LC	

Note 1 - Optional collector interface transceivers.
Other transceivers may be used but must be on approved list. Contact Telesoft for more information.