

400G FLOWPROBE

TRAFFIC MONITORING IN 400GBPS BLOCKS

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 at 400Gbps. 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 and IP-in-IP) providing visibility of encapsulated traffic to further enhance visibility and protection over your network, reducing the opportunity for cyber threats to hide and further increasing threat detection.



KEY FEATURES

Instruments up to 280 Million concurrent flows at a churn rate of 5M sustained, 7M peak flows/s	Monitor large scale network traffic for cyber security analysis, NPMD and compliance
Passively monitors 4 x 100GbE	Connect to large scale monitoring infrastructure, peering links, national xSP and large data-centres
De-tunnels GTP, GRE, MPLS and IP-in-IP 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 BGP, SSL, DNS, HTTP host and HTTP URI	Layer 7 visibility and control for granular user management
Exports flow records to Telesoft TDAC or other compatible IPFIX collector or JSON consumer	Quickly deploy accurate, large scale network visibility and analysis
Application and content classification in encrypted TLS1.0 - 1.3	Actionable intelligence in current & emerging encryption standards

HEADQUARTERS

Telesoft Technologies Ltd
Observatory House, Stour Park
Blandford DT11 9LQ UK
+44 (0)1258 480880
+44 (0)1258 486598
sales@telesoft-technologies.com

LONDON

Telesoft Technologies Ltd
The Shard
Floor 25
32 London Bridge Street
London SE1 9SG
sales@telesoft-technologies.com

ASIA

Telesoft Technologies Ltd
Tapasya Corp Heights
Ground Floor, Sector 126
Noida, 201301
+91 120 612 7725
salesindia@telesoft-technologies.com

AMERICAS

Telesoft Technologies Inc
430 National Business Parkway
Suite 480, Annapolis Junction
MD 20701
USA
salesusa@telesoft-technologies.com

TECHNICAL SPECIFICATIONS

Physical	<ul style="list-style-type: none"> • 1RU 19-inch rack mount • 1.7x17.2x30.6 in (4.3x43.7x77.7 cm)
Monitoring Interface	4 x 100GBASE-LR4 QSFP28
Tunnelling Support	Configurable to automatically detect and de-tunnel: MPLS, IPinIP, GRE, GTP
Flow Export Interface	<ul style="list-style-type: none"> • 10GbE Fibre Interface with swappable transceivers • Up to 32 IPFIX collectors
Throughput	<ul style="list-style-type: none"> • 7M simplex flows per second • 280M active flows
Flow Record Format	<ul style="list-style-type: none"> • IETF RFC7011/RFC7012 IPFIX • Export formats: IPFIX, JSON (Netflow/IPFIX/ JSON) • Supported Collectors: Telesoft TDAC, Kafka, Elastic or other IPFIX/Netflow compatible collectors
Enhanced flow data	<ul style="list-style-type: none"> • 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 • TCP session timing (SYN / SYN-ACK): Detect anomalies and classify traffic • JA3 SSL fingerprinting enables MD5 checksum identification against a JA3 database
Power Stats	330W typical, and 380W peak

ORDER OPTIONS

Part Number	Description
500003074	400G FlowProbe, 1U, QSFP28, 4x100GbE
500003082	100G QSFP28 LR4 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.



Telesoft Technologies, the Telesoft Technologies logo design, ThinkEngine, Triton, HINTON, OKEFORD, TDAPI, MPAC, MILBORNE, C-CURE and ARNE are trademarks or registered trademarks of Telesoft Technologies Ltd or its subsidiaries. All other brand or product names may be trademarks of their respective companies. All rights reserved.