TELESOFT

DATASHEET

TDAC

TDAC provides network visibility, indicators of compromise and actionable intelligence across national scale networks, helping you to protect your infrastructure, your data, your network users, CNI and ultimately your reputation

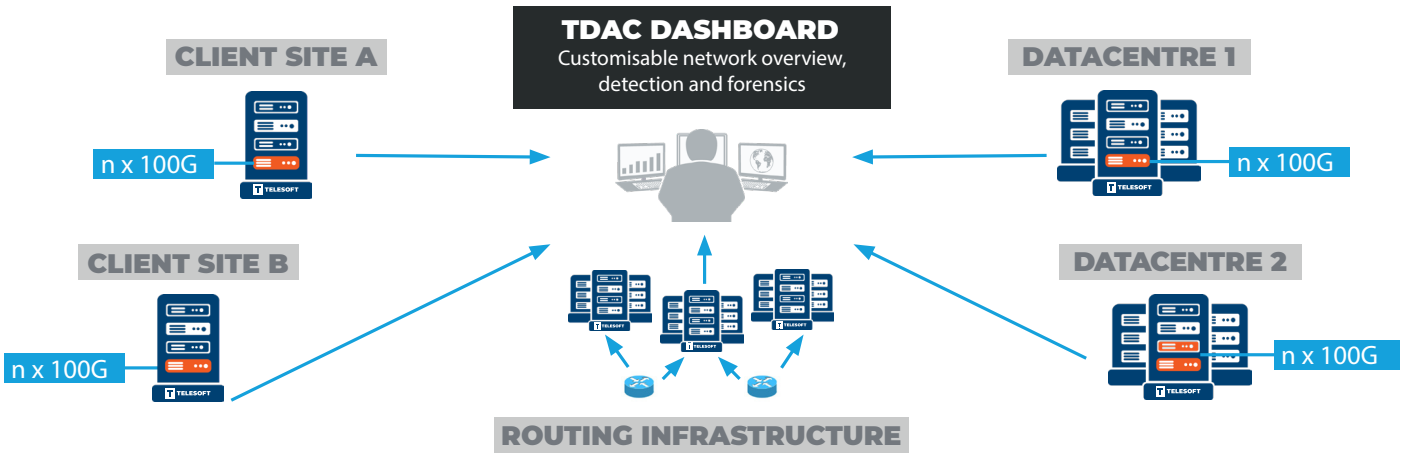
TDAC (Telesoft Data Analytics Capability) is a cost effective, field proven, ultra-high-rate monitoring, analytics and forensics platform. TDAC ingests and analyses millions of events per second, including network flow data, IDS alerts and system logs, enhancing data with known threat intelligence (including IP reputation, threat classification, geo-location), partitioning and pre-analysing data for rapid sub-second query by Incident response and Forensics teams.

Typically deployed on networks running at multiple 100Gbps, TDAC provides dashboards and query widgets for a visual picture of network performance and health, alerts to indicate anomalous behaviour, a RestAPI interface for integration with other automated tools and a Kafka interface for third party streaming analytics tools.

TDAC scales horizontally according to the resources allocated to it and can retain data for months across Peta-Byte storage. The TDAC UI and RestAPI incorporates features to accelerate turning this huge volume of raw data into actionable intelligence, including navigation by preset groupings (such as Application, Service, BotNet, CNI, business area etc.), enrichment with threat classification data, query path tracking (as 'forensic pathways') and continuous query analysis, giving sub-second query time.

DATA MONITORING, ANALYTICS AND FORENSICS PLATFORM TDAC

TDAC EXAMPLE CONFIGURATION



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

KEY FEATURES	
National network scale	Total network visibility of threats and performance where previously not possible
Low latency query (typically > 1 minute)	Works with Incident response work flow, allowing rapid response
Enhances data with IP reputation and Geo location	Reduces analysis time – enables faster response
User configurable and auto discovered data grouping “entity-sets”	Reduce background noise and prioritise Infrastructure group, Application, Service, Subnet, BotNet, CNI, business area... reduce alert fatigue
Accelerated cached queries for prioritised data groups	Sub-second detection and analysis for rapid incident response
Works with Telesoft 2x100G FlowProbe	Immediate access to enhanced analysis above L4 including DNS, SSL and HTTP information, not usually available from standard flow export
Works with Telesoft CERNE IDS	Access enhanced analysis with IDS alerts and rapid retrieval of session pcap
Configurable user roles, access and dashboards	Have a single tool usable by multiple groups, including incident response, analysis, forensics

TECHNICAL SPECIFICATIONS	
Input Formats	• Network data reporting from JSON, IPFIX, syslog, IoT/sensor logs, web server/application logs • Natively works with existing network infrastructure export and reporting. • Reputation intelligence from any STIX compatible source. • Natively works with Telesoft FlowProbe for L4-L7 analysis • Natively works with Telesoft CERNE storing IDS alerts and enabling rapid session pcap retrieval
Output Formats	GUI dashboard reports, JSON REST API and automated alerting to SOC systems
Hardware and Software	• Runs on X86 infrastructure • Available pre-installed on HP DL380 or supermicro 2U • Linux CentOS 7.1 • 10G fibre network required • Mesh or Centralised • Full high availability • Management interfaces on 1GbE
Performance	• Ingestion: Millions of network events per second • Curation: Up to Petabyte scale • Delivery: Reports and forensics in seconds

ORDER OPTIONS	
Part Number	Description
500003049	TDAC Software License
500003030	TDAC Warm Data Node
500003031	TDAC Hot Data Node
500003028	TDAC No Data Node
500003024	Onsite engineering service

TELESOFT