Datasheet

FlowStash

Unify, Enrich, Normalise and Broker Flow Data

Maximise visibility and availability of carrier scale flow data for enhanced forensics and analysis capabilities

The FlowStash from Telesoft is a scalable high performance platform that transforms, enriches and brokers flow data from numerous physical and logical network assets. The FlowStash consolidates streaming, analysis and classification of network flow meta-data, efficiently preprocessing data for delivery to third party traffic collection and analysis tools.

The FlowStash eliminates network visibility blind spots by unifying data across a single entry point, ingesting multiple flow data inputs and formats such as NetFlow, IPFIX, sFlow, jFlow and cFlow. The FlowStash normalises all flow data to the data formats required by multiple concurrent downstream traffic collection and analysis tools.

Processed flow records are enriched with meta-data based on user defined classification and third party threat intelligence, enabling multi-layered threat detection and mitigation. Flow enrichment includes entity tagging, IP Reputation, Geo IP and ASN. Entity tagging allows the user to define managed objects such as logical subnets and to map meta-data to matching flow records. The FlowStash uses the most up-to-date Threat Intelligence (IP Reputation) to identify and tag flow records associated with known adversary infrastructure.

The FlowStash allows you to pinpoint geographical locations, regions, or other useful location information such as organisation or ISP based on IP addresses, which is provided by Geo IP and ASN tagging.

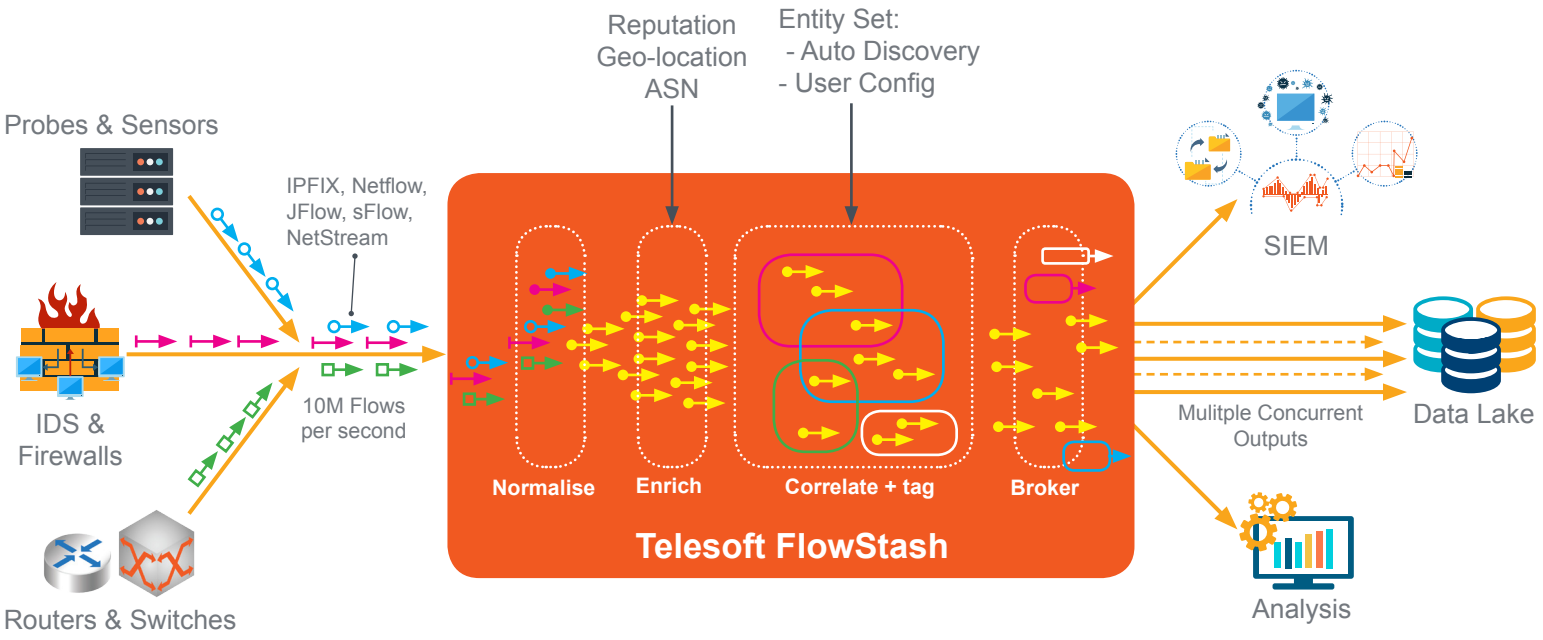
Enriched flow records can be exported to a wide range of collection and analysis tools including ElasticSearch, Apache Kafka, SiLK, syslog, etc. and generic collectors using Netflow and REST/JSON.

Key Features

Highly scalable architecture provides unmatched performance, processing over 10M records per second.	Total visibility of up to carrier scale networks such as ISP, NSP, CSP and Large Enterprise.
Support for multiple data generators/sensors and formats (IPFIX, NetFlow v1, v5 to v9, sFlow, jFlow and NetStream).	Can be deployed in any environment, compatible with all industry standard flow exporting devices i.e. probes, switches and routers.
Hardware offload of downstream analysis using flow enrichment and entity tagging.	Create entity sets for categorisation and monitoring of physical and logical network assets and services, CNI (government infrastructure, telco, cloud services, etc), OT (power, utilities, transport, etc), high value target IPs and hosts.
Traffic classification and categorisation - IP Reputation, Geo-IP and ASN/ Organisation enrichment.	Accurate reflection of the threat landscape at the point of ingess, enabling multi-layered threat detection and improved analysis and forensics.
Support threat intelligence from multiple sources such as STIX and TAXII.	Identify potential threats e.g. Botnet CnC, Malware, etc. allowing rapid incident response.
Data brokering to multiple concurrent downstream consumers supported – ElasticSearch, Apache Kafka, SiLK, Netflow, Hadoop (HDFS), syslog, etc.	Real-time normalisation and brokering optimises flow data sent to collection and analysis tools, without losing accuracy.

© copyright 2019 by Telesoft Technologies. All rights reserved. Commercial in Confidence.

FlowStash Example Configuration



Technical Specifications

Supported Input Formats	IPFIX, Netflow (v1, v5 to v9), JFlow, sFlow, NetStream
Supported NetFlow Transport Protocols	UDP, TCP, SCTP
Supported Export Formats	JSON (identifiers using IANA IPFIX Assignments), IPFIX, Netflow (v1, v5-v9), CSV, syslog
Supported Collectors	Telesoft TDAC, ElasticSearch, Apache Kafka, Apache Hadoop, SiLK, REST/HTTPS
Export Rate Control (per collector)	Full Flow Rate or 1 in N or limited rate
Bidirectional Flow Support	RFC 5103
Flow Enrichment	User Defined Entity Sets IANA service names IANA protocol names Geo-Location (ISO 3166) AS Numbers
Supported OS	Redhat Enterprise Linux v7 or later Docker Supported

Order Options

Part Number	Description
500003095	FlowStash Capacity Licence (100k flows/second)

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

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

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

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.

© copyright 2019 by Telesoft Technologies. All rights reserved. Commercial in Confidence.