NetGuardians

NG|Screener Products and Architecture

Ljupce Nikolov
August 2018

swiss made software

Summary

- Solution Architecture
- NG|Appliance
- Data Collection Framework
- NG|Screener Connectors
- NG|Screener Solution components

Our approach

Collect

Connect to all sources and acquire data in real-time

Correlate

Find relations between data points in different sources

Analyze

Separate signal from noise to identify real fraud

Alert

Apply controls to detect suspicious events

Prevent

Give users tools and workflows to resolve cases

NoSQL Storage / Big Data Processing

Application components

Collect

Correlate

Analyze

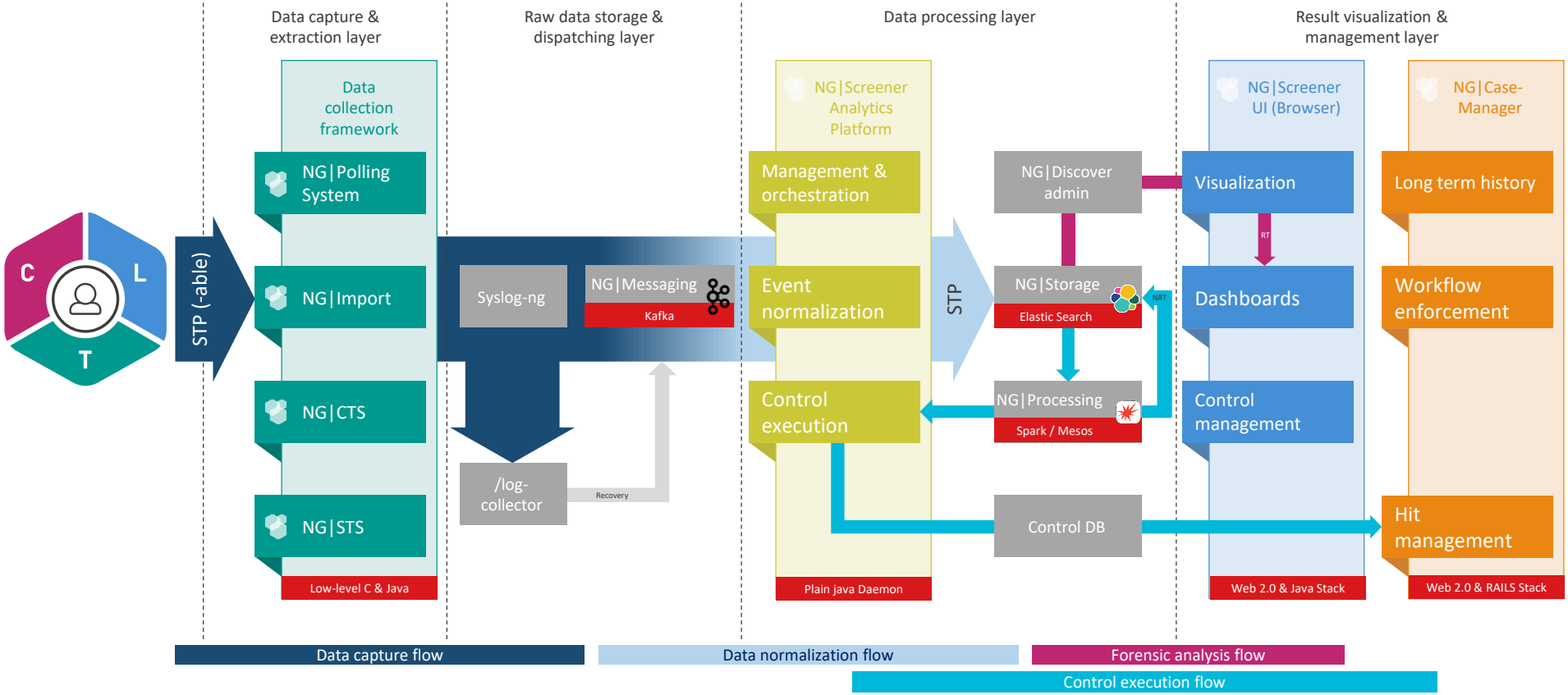
Alert

Prevent

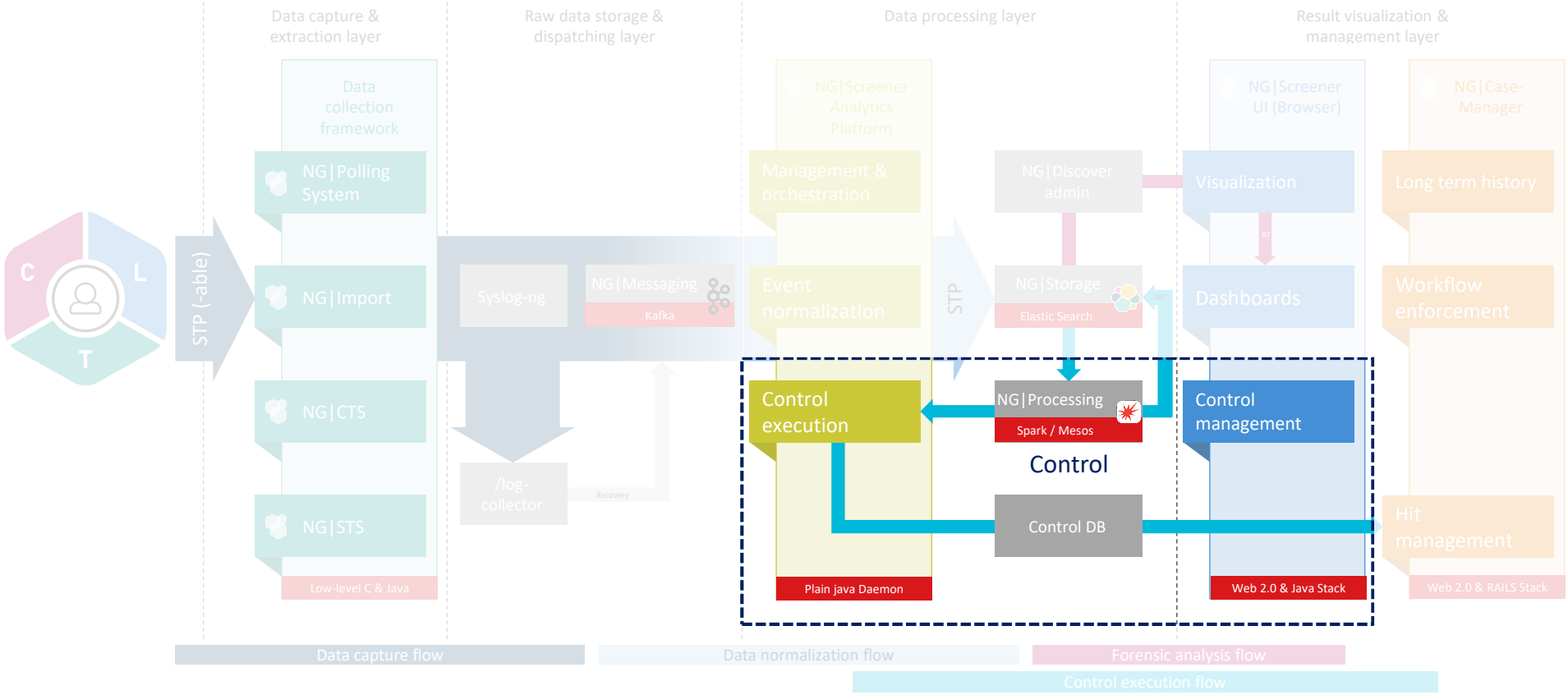
- Data Capture
  - NG|Polling System
  - NG|Import
- Data Interception
  - NG|STS
  - NG|CTS
- Log File data model
- business mapping
- NG|Storage Forensic model
  - Transactions
  - Channels
  - IT Layers
- NG|Screener Analytics Platform
  - Processing
  - Messaging
- Controls
  - Pattern-based intelligence (Rules)
  - Profiling
  - Machine Learning
- NG|Scoring API
- NG|Screener UI
  - Visualizations
  - Dashboards
- NG|Case Manager
  - Long term history
  - Workflow

NoSQL Storage / Big Data Processing

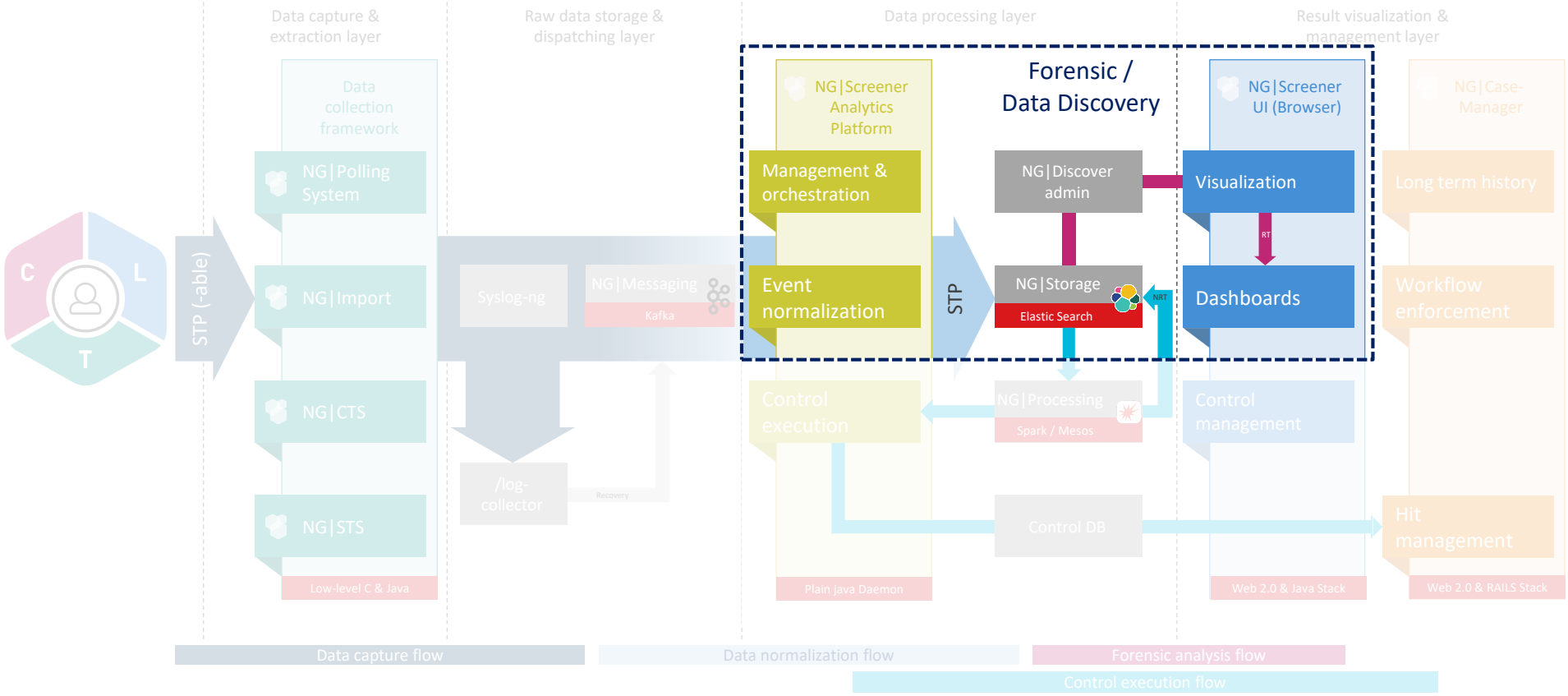
Application architecture



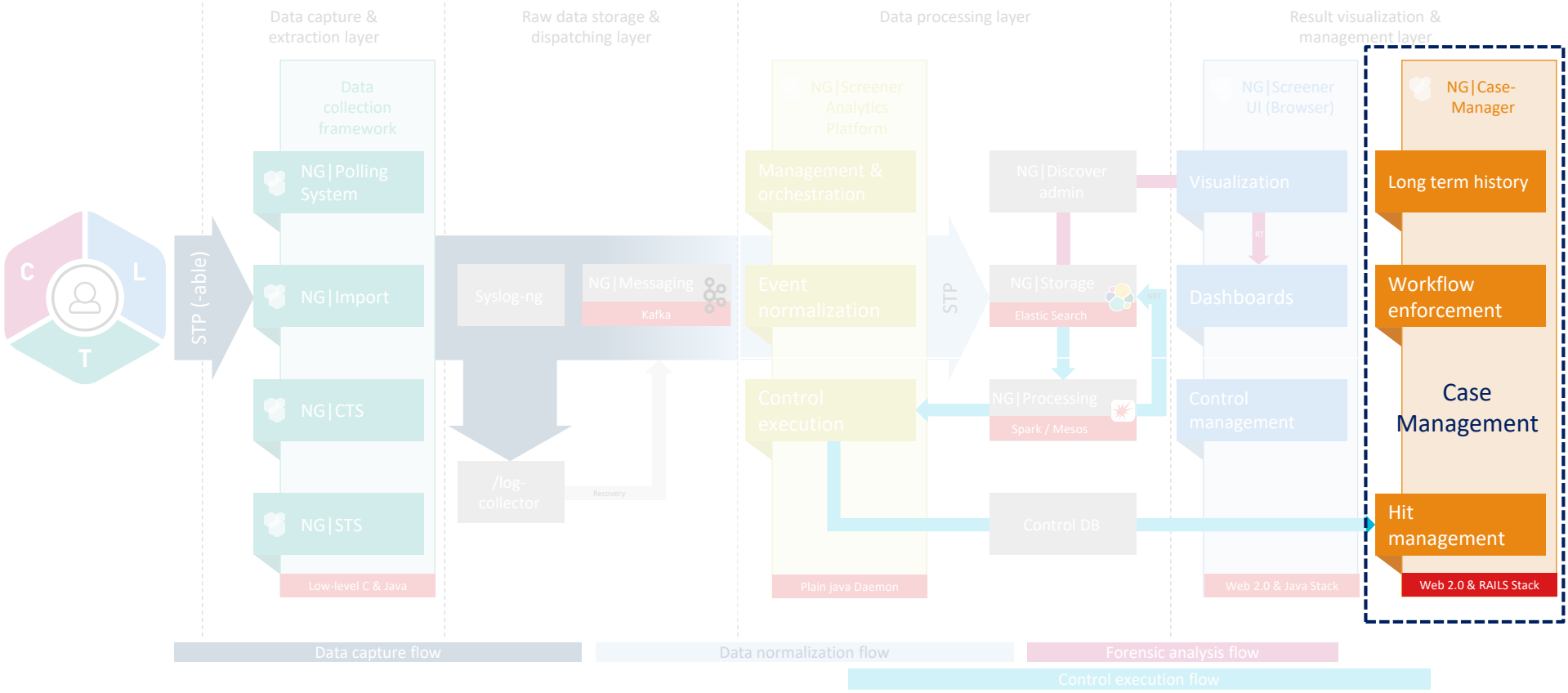
Control Application



Forensic Application



Case Management Application

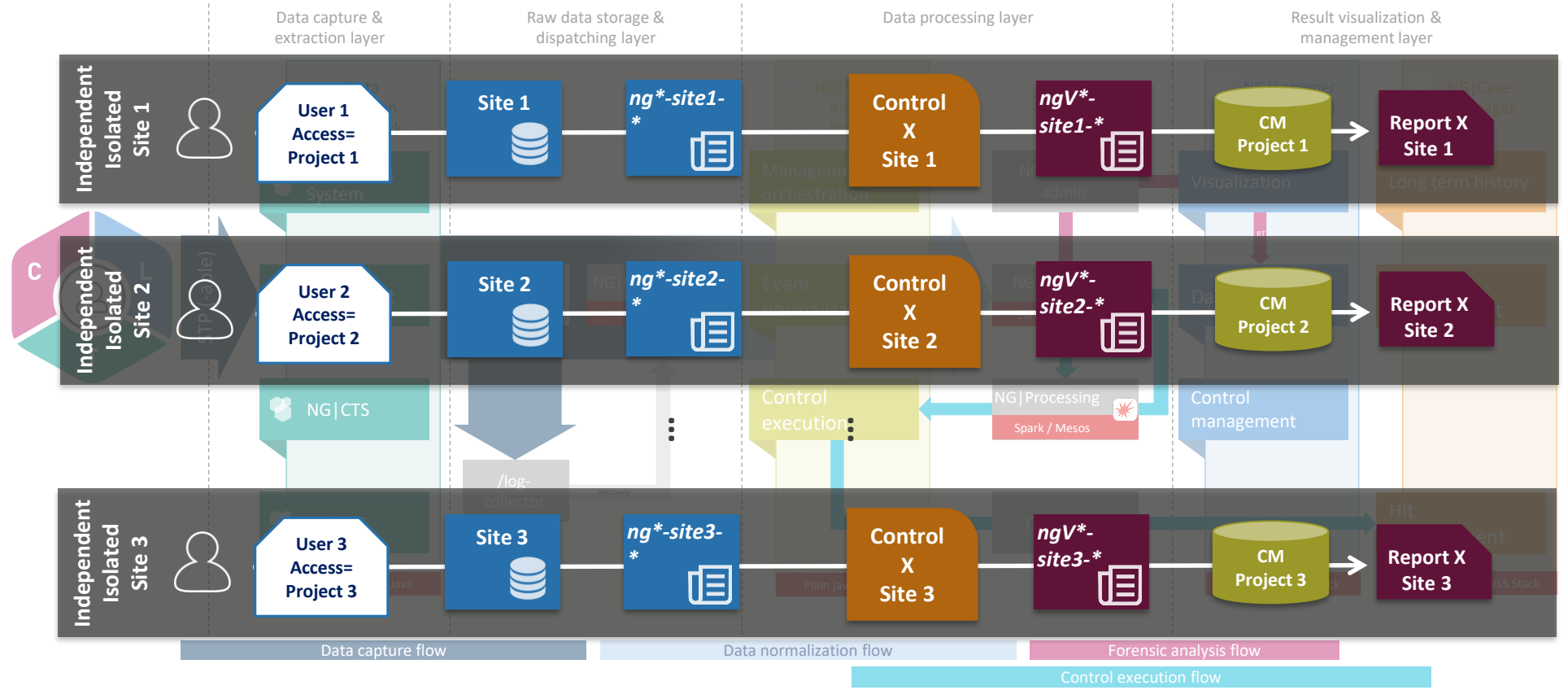


Multi-tenancy

- Multi-tenancy in NG|Screener
  - Enables single NG|Screener platform to host several sites, entirely isolated from each others

- Principles
  - Notion of tenant linked to notion of hosts
    - One tenant is associated to one or several hosts.
    - One host cannot correspond to several tenants
    - Hosts are prefixed by tenants
  - Security is based on hosts
  - Different URLs for different tenants

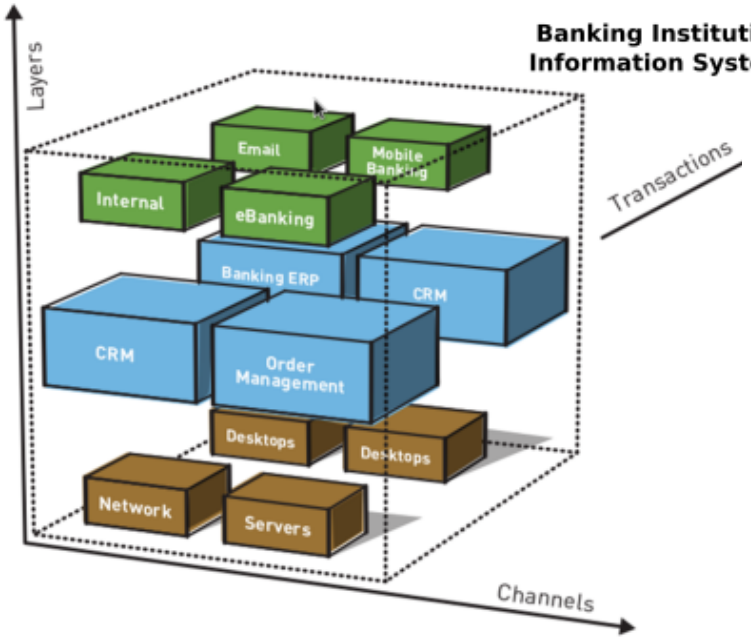
Multi-tenancy – Principle



NG|Appliance

- Virtual or Hardware appliance
- Custom OS based on CentOS 7
  - Hardened Appliance
  - Added needed dependencies
  - Preconfigured appliance ready for software install
- Also install on RHEL 7 provided by customer
- Administration via Web Interface (Management Center) of Linux command line

Data Collection Framework



Data capture & extraction layer

Data Polling
- JDBC
- LDAP
- WMI
- etc.

File Transfers

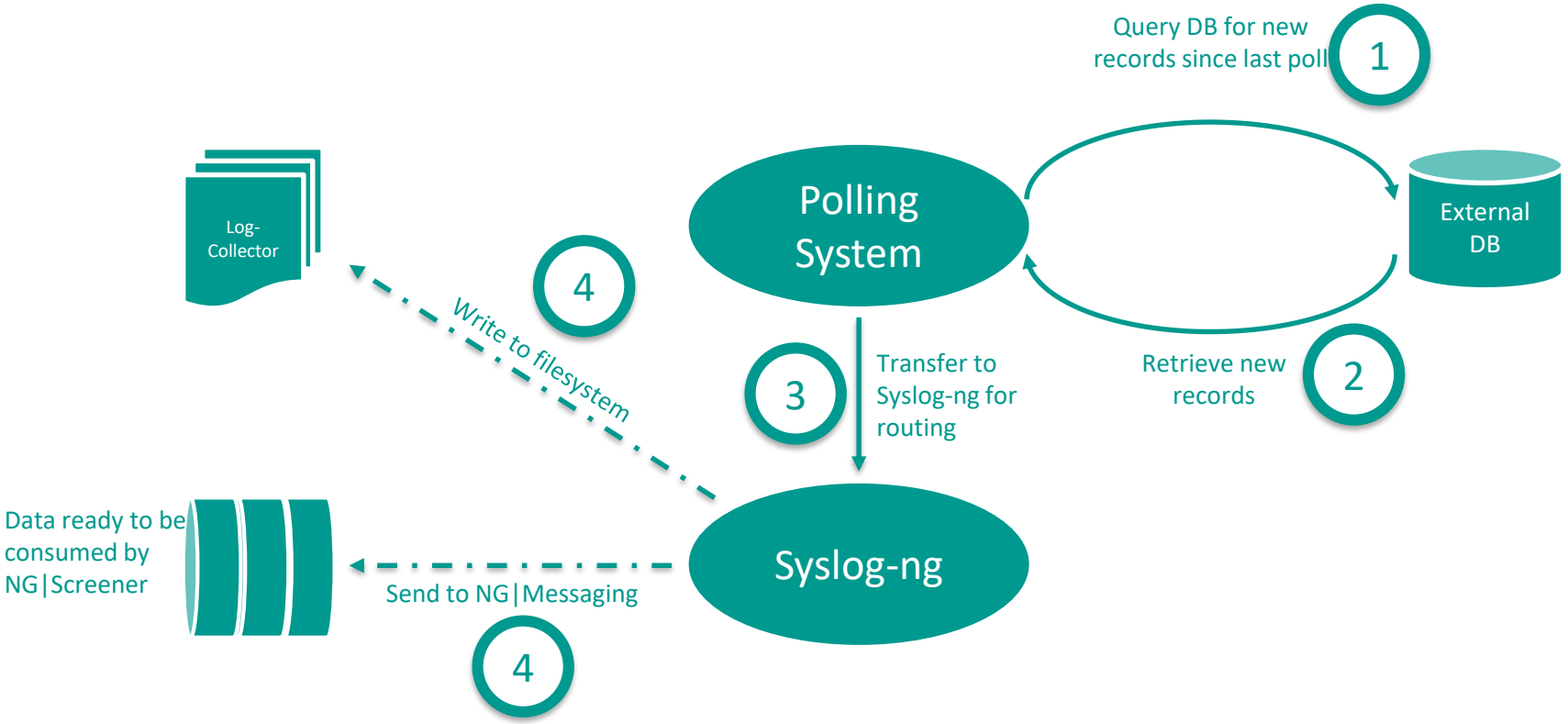
Messaging (Push)
- JMS, MQ, etc.
- Syslog
- Proprietary proto.
- Etc.

Channel Intercept.

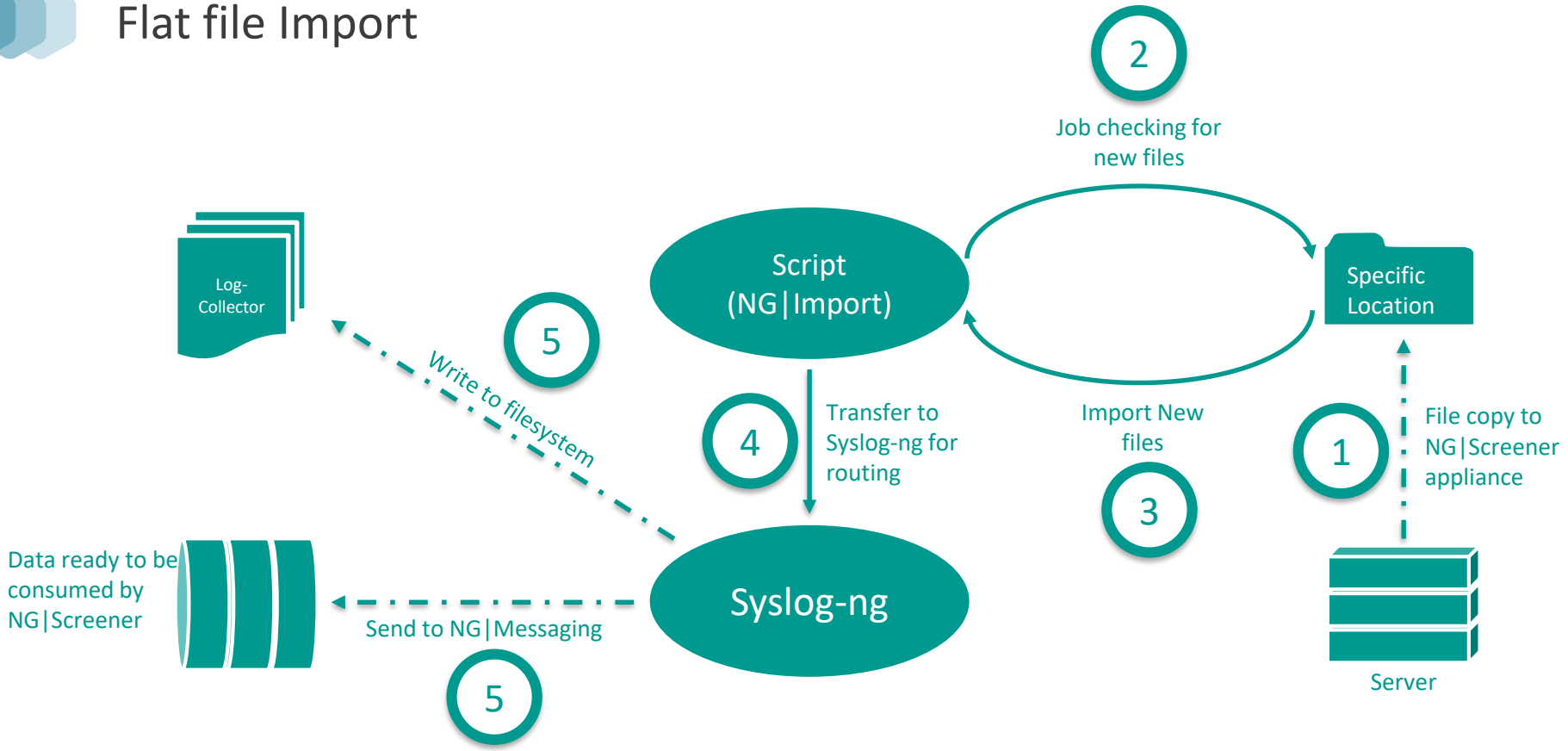
Data collection framework

- NG|Polling System
- NG|Import
- NG|CTS
- NG|STS

Database Polling



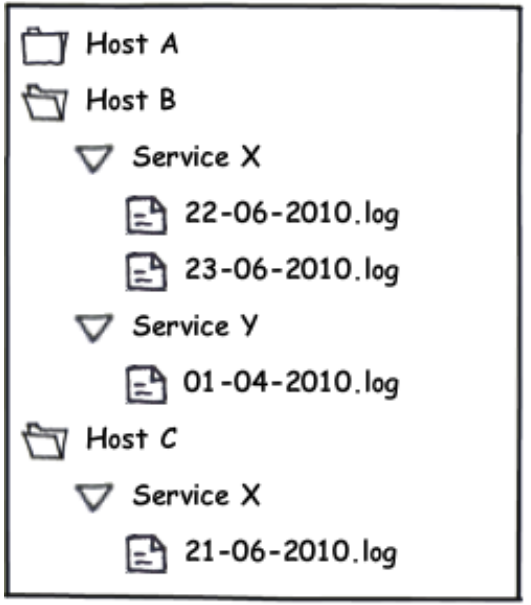
Flat file Import



Data Collection Framework

Data Storage

- Audit trails are centralized under /log-collector directory
- This folder is structured by Year / Host / Service
- Filenames are formatted dd-mm-yyyy.log
- Files get compressed after 2 days to gain space
- Audit trails are compliant with Syslog log format



Raw Audit trails Storage

NG|Screener Connector

- Passive component (or collection of configurations) that allows NG|Screener to collect and analyze data for a specific data source.

- It includes
  - Data capture routing rules and configuration samples
  - Interpretation dictionary to translate captured data to NG Business data model
  - Start packaging of connectors to have dashboards, exporting targets, CM configurations, etc..

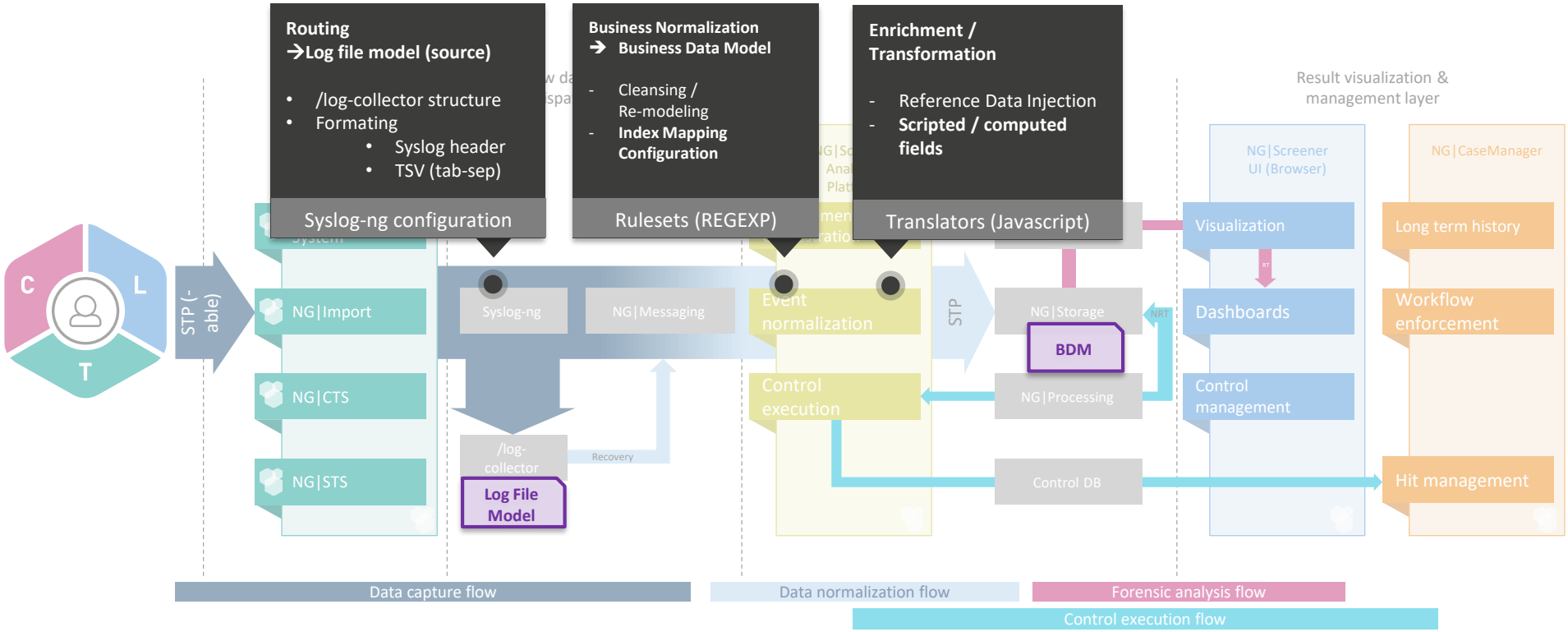
- A connector is needed for each type of data source that is collected on NG|Screener

NetGuardians

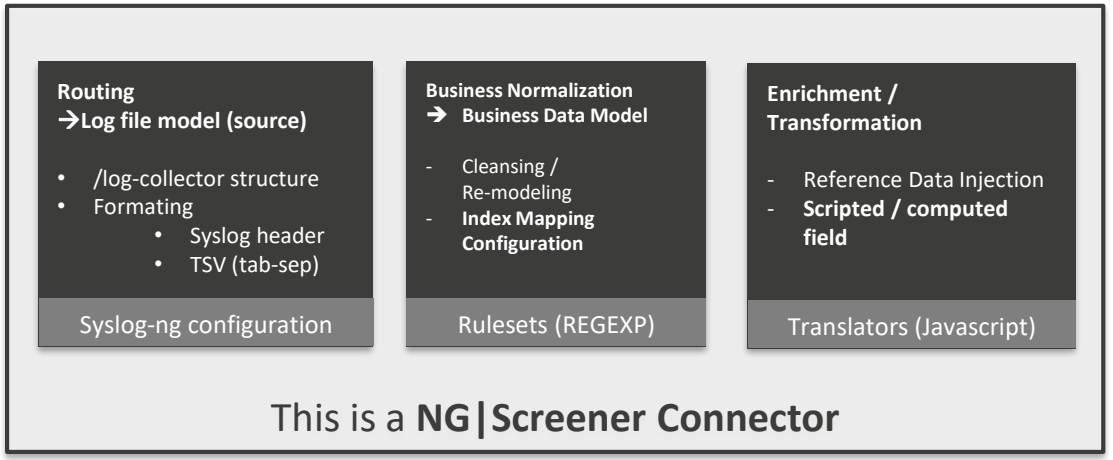
What is technically a connector?

swiss made software

NG|Screener Connector



NG|Screener Connector

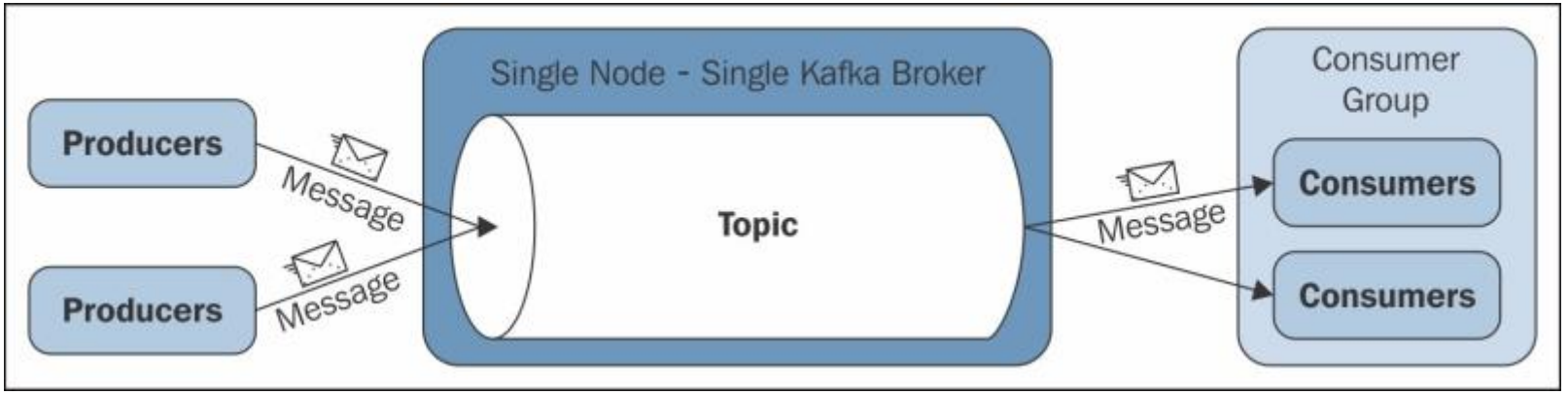


- Connectors are **RPM packages of configuration**
- We have define **hundreds of connectors** at NetGuardians / only a dozen are mainstream (heavily maintained)
- Customer can request their own connectors (for specific data sources)

NG|Messaging

- Big data ingestion technology
- Could scale ingestion line out on several nodes
- Producer-Consumer paradigm
- Based on Apache Kafka product

NG|Messaging



- Producers will be all data collected by DCF (Data Collection Framework)
  - Syslog-ng will be the actual Producer
- There is one topic that will be the flow of events coming from syslog-ng
- Consumer is the ng-screener daemon. It will get the data and normalize them into Business data model

NG|Screener Daemon

- Core Analytics Orchestrator
- Scheduling and managing all platform operations and computations
- Operates
  - Data ingestion
  - Control Execution
  - Aggregation process management

NG|Storage

- Big data / NoSQL Data storage engine
  - Full text search
  - Document database
  - Can be distributed
- Enable to scale out infrastructure
  - New nodes can be added
- Key component of the data discovery feature of NG|Screener platform
- Based on ElasticSearch

ElasticSearch

NG|Auth

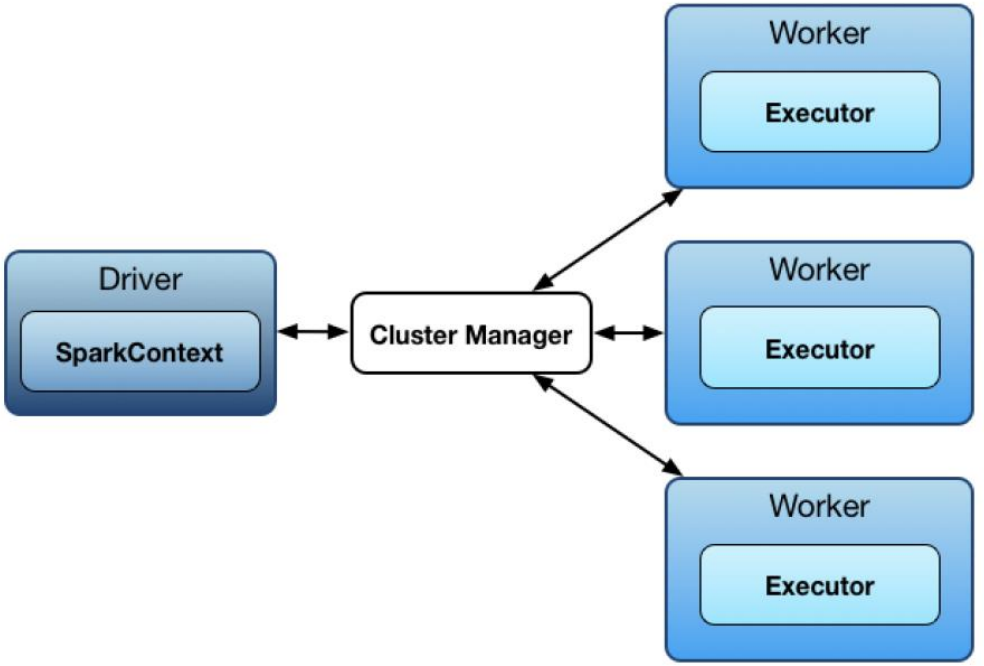
- Component to provide Single-Sign On feature on NG|Screener platform
- For NG|Screener UI and Case Manager
- Will handle authentication (either local or LDAP)
  - But not authorizations (application specific)
- Based on Keycloak

NG|Processing

- Big data processing engine
- Scale out data processing layer
- Controls to perform efficient computations
- Based on Apache Spark / Apache Mesos

NG|Processing

- Driver receive job to be executed (execute python code)
  - Screener Daemon will talk with the driver
- It talk to a single coordinator called master
- Master will manage workers on which executors will be running

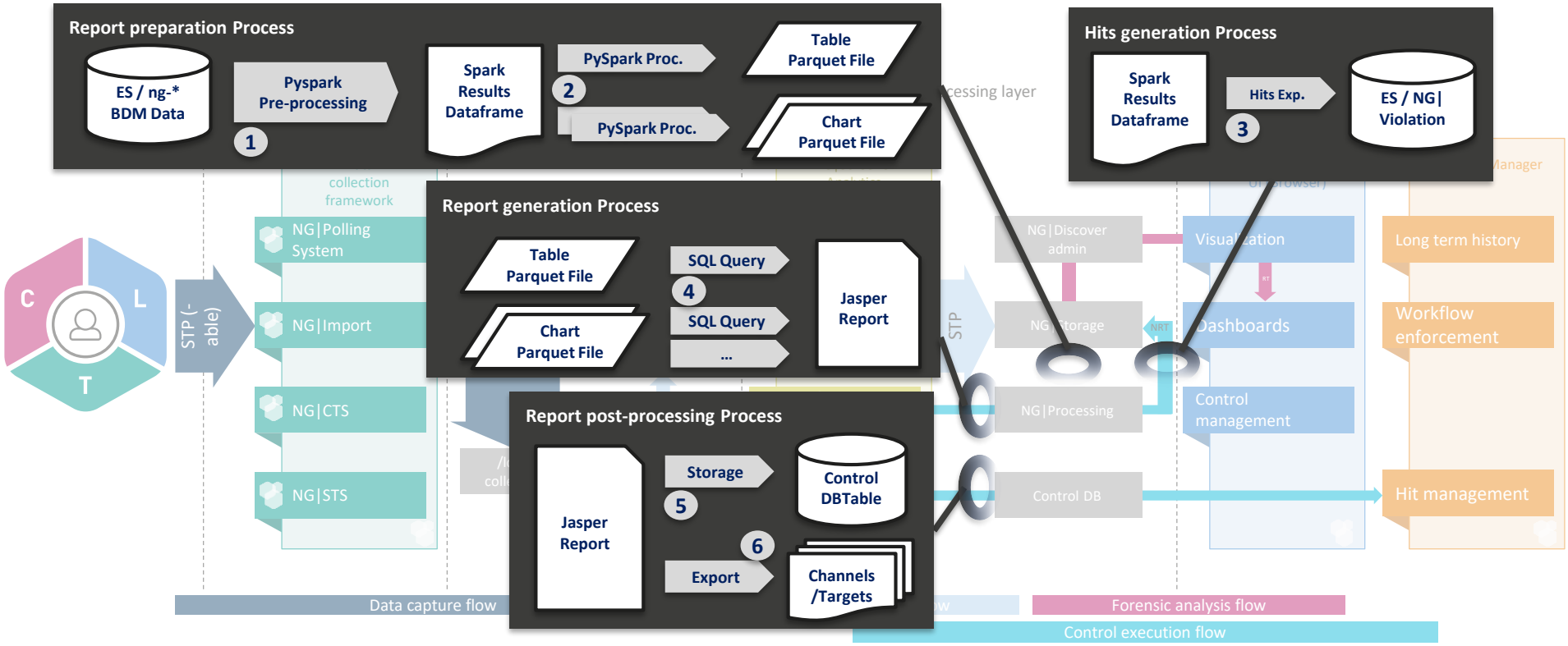


NetGuardians

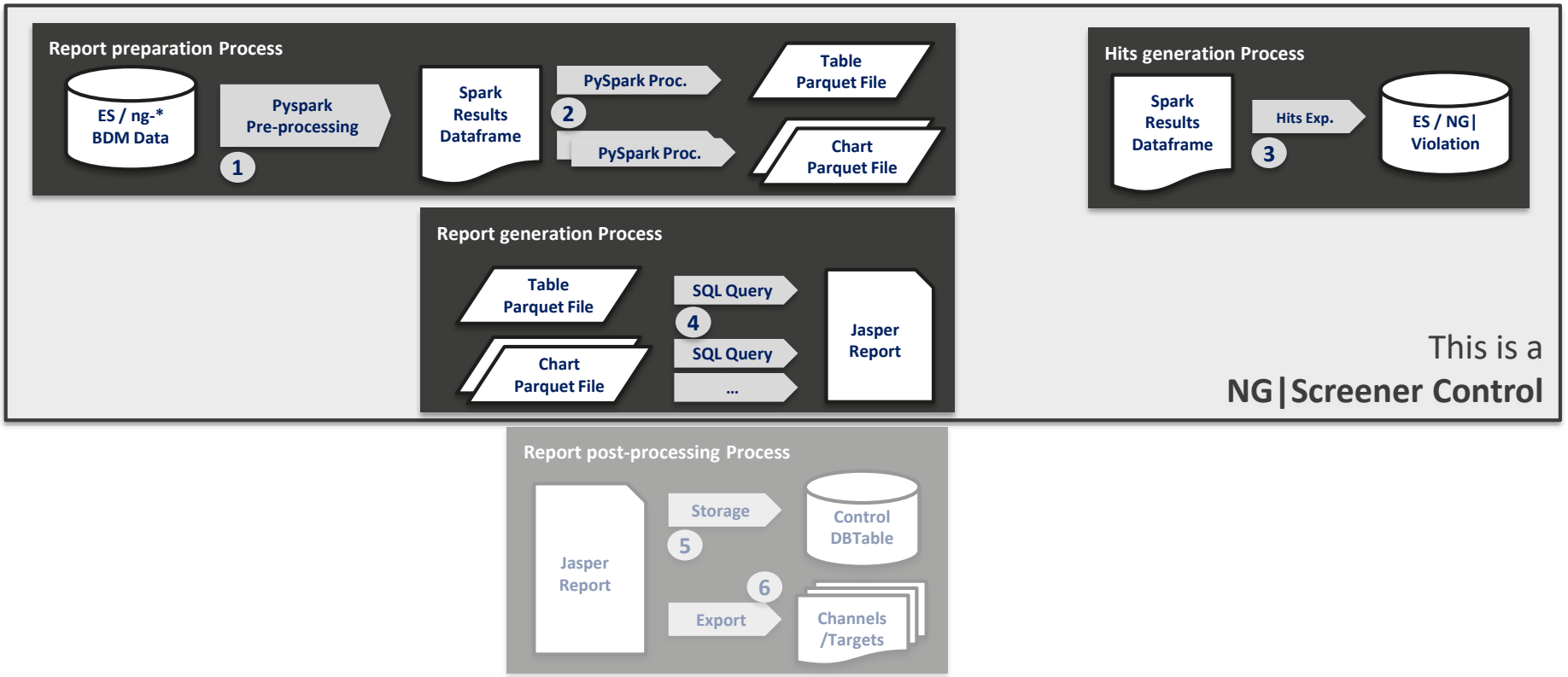
What is technically a control?

swiss made software

NG|Screener Control



NG|Screener Control



NG|Screener UI

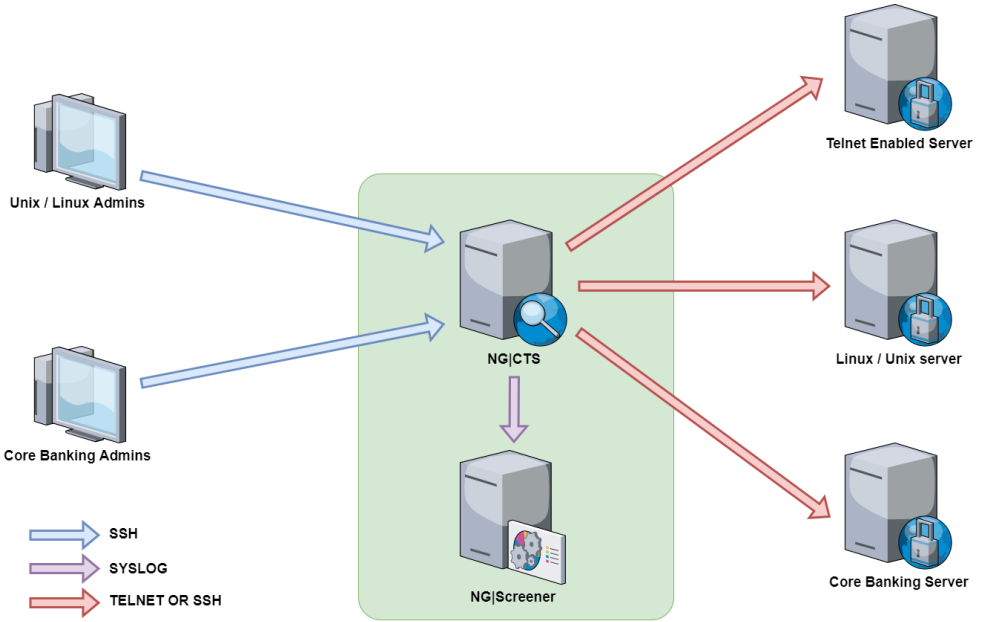
- Comprehensive Web user interface
- Get the most of the data delivered by NG|Screener
- Will let
  - Navigate through data using dashboards and forensic views
  - Manage Controls
  - Administrate the application
    - Users
    - Channels for export
    - Aggregations for profiling
    - …

NG|Case Manager

- Allows users to manage Fraud, audit, security incidents generated by NG|Screener.
- Configure workflows for incident escalation, documentation and validation.
- Keeps a long term history of incidents (and actions done on them)

NG|CTS

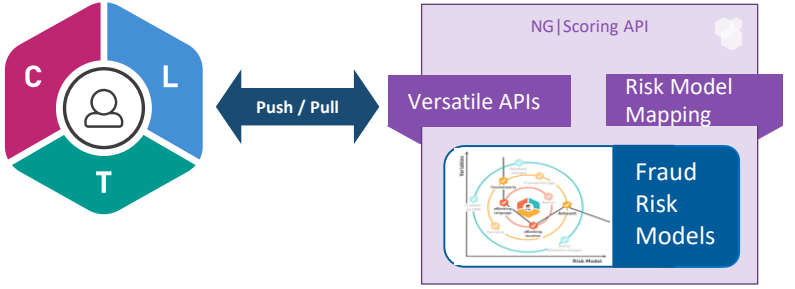
- SSH/Telnet proxy that will record activities done by System admins
- Provides access control for critical servers
- Accountability for admin actions



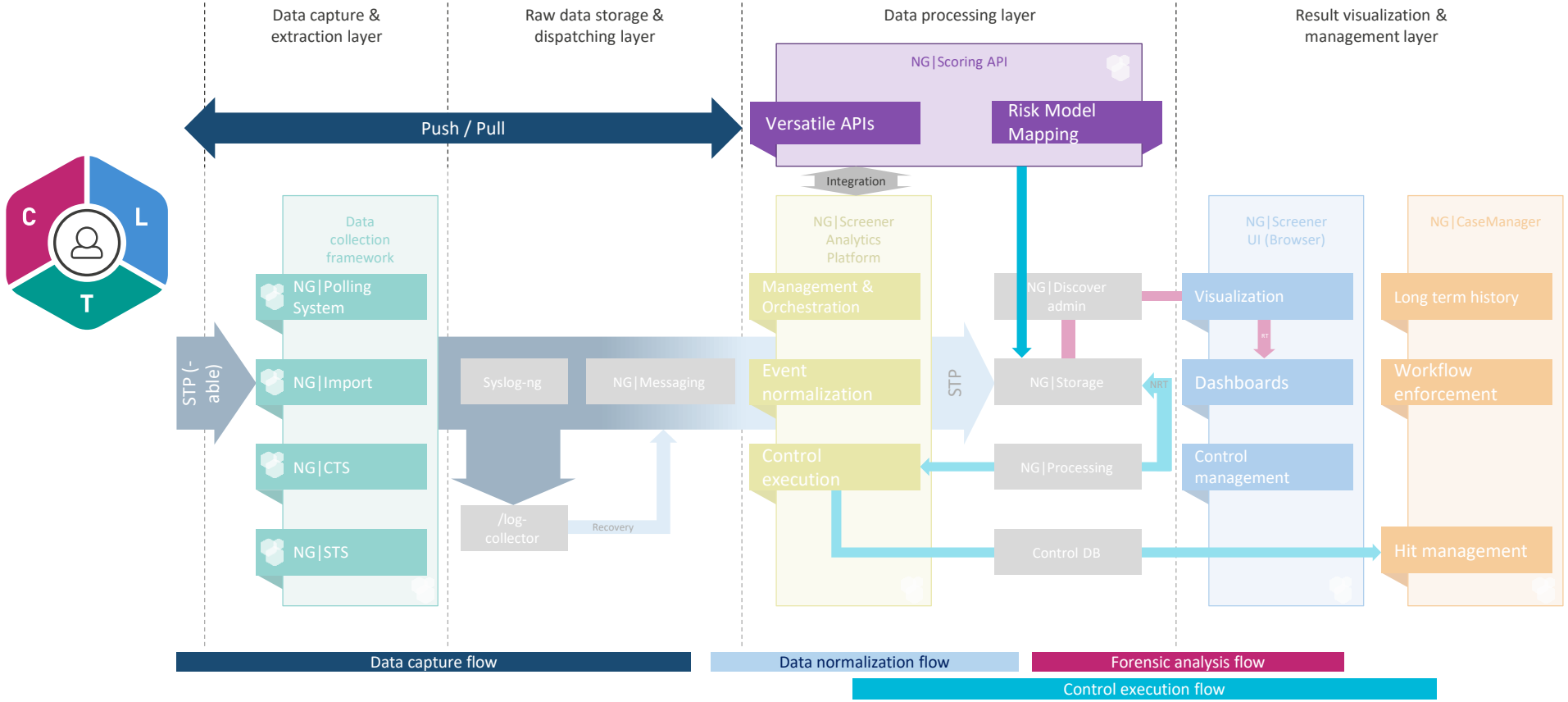
Real-time Scoring API

The NG **Real-time Scoring API Module**

- is an NG|Screener **Platform plugin**
- exposing **Profiling** and other advanced **models**
- to **real-time access** through **various protocols**
- for tighter integration within the bank IS
  - Optional Module / custom deployment
  - Supported protocols : JSON/REST, JMS (MQ), XML/WS-*
  - Versatile interface : API can be adapted to **suite the bank specifications** regardless of the internal scoring models design
  - Multiple models can be exposed to multiple endpoints / queues / etc.
  - Real-time ➔ under a second response
  - Throughput dependent on hardware



Scoring API - Application architecture



THANK YOU!

Contact us

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60
F +41 24 425 97 65

NetGuardians Africa

KMA Centre , 7th floor,
Mara Road Upper Hill,
Nairobi, Kenya

T +254 204 93 11 96

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987

NetGuardians
Eastern Europe

Koszykowa 61, 00-667
Warsaw, Poland

NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003