Big Data for Fraud, Regulatory & Risk Management

Ensure your Big Data solution not only captures data, but also correlates, normalizes, and models it. Apply it to relevant use cases for a powerful solution for fraud protection, regulatory compliance and risk management. Here's how.

NG|Screener enterprise software platform is the strength behind NetGuardians' FraudGuardian and RiskGuardian solutions. Based on a unique, state-of-the-art Big Data model patented by NetGuardians, it integrates into your core banking software without impacting performance. It correlates data and analyzes user behavior across all banking channels, transactions and IT layers. This information is matched to critical use cases that regroup and implement best practices for fraud and risk prevention. This empowers you to organize and analyze Big Data to automate compliance, audit and reporting, as well as to detect atypical behavior immediately to intervene in human error or fraud.

Unique patented Big Data model built for banks:
Real-time data correlation, normalization and modeling

Banks rely on a complex IT structure of hundreds of systems from the network to core banking applications. These systems typically function as "silos", isolated by different use groups and different technology, making it extremely complex to extract and normalize data.

NG|Screener solves this with a **Data Collection Framework** that builds a consistent view of transactional and user behavior across functional silos and individual components of the information system. It integrates advanced technologies including **SIEM** (security and information and event management system), **SQL Tracking System** (database administrator tracking), and **Console Tracking System** (system administrator tracking). It makes it possible to integrate and exploit any kind of data from any kind of system regardless of the underlying technology. It supports a depth of analysis from days to years, depending on the size of the cluster you define.

Business controls and use cases

To make Big Data truly work for you, you need to keep the end-goal of fraud protection and regulatory compliance in sight. Once use cases that regroup and implement best practices are identified, it takes hundreds of controls and advanced algorithms to address them. **NG|**Screener does this using pattern-based intelligence, profiling capacity and predictive analytics.

Pattern-based intelligence: Identifies patterns within the masses of data in activity trails.

Profiling: Creates profiles around typical user activity at all levels and alerts to deviations.

Predictive analytics and machine learning: Built mainly on risk scoring and behavior change detection.

This intelligence is then brought together and applied to your specific control and operational risk challenges through unique Smart Controls Objectives (SCO's).

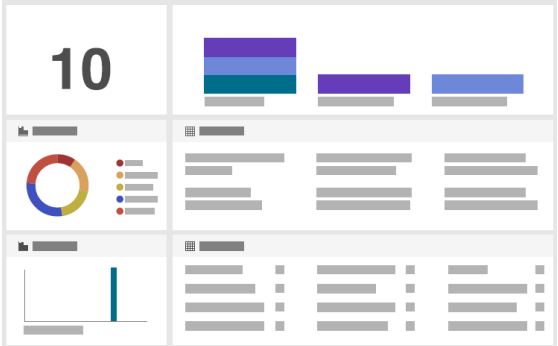
Smart Controls Objectives, pre-packaged in Intelligence Bundles, are available to address specific fraud and compliance objectives. For NetGuardians, the development of relevant SCO's is a priority that we

address through combined expertise of Risk Consultants and R&D. SCO's are continually updated so you stay on top of rapidly changing fraud and regulatory patterns.

SCO for key regulatory requirements:	**SCO for key fraud** challenges:
• FINMA 2008/21 • ISAE 3402 • ISO 27001 • SOX • Basel III • MAS • …and much more	• eBanking fraud • Cybercrime and identity theft • Bank card fraud • Payment fraud • Account takeover • …and much more

Once SCO's are implemented, any violation is demonstrated in automated reports. A user-friendly online dashboard interface offers high-level and detailed views so you can easily visualize the current state in terms of risk and compliance; design and implement controls; and perform forensics.

Printed report



On-screen dashboard view

Big Data vs. Business Intelligence (BI):
Make BI use cases enter the real-time world

Business Intelligence (BI) technology is useful for analysis and reporting, but some institutions attempt to "repurpose" BI to perform more complex investigation. This doesn't succeed because transactions and operations happen continuously while BI extracts metrics in a nightly batch, (when it impacts the transactional system less). BI reports are therefore always day-1 at best – a snapshot of the previous day's situation. This is particularly inadequate for fraud detection and prevention because the next day is simply too late.

NG|Screener, on the other hand, operates "live", transparently plugged into the operational system, without impacting performance. It uses Big Data to execute BI use cases in real-time, detecting fraudulent behavior and compliance violations at the precise time they happen.

Cooperation with existing systems

NG|Screener offers a particularly flexible and accessible means of leveraging Big Data because of its open architecture. You can adopt it as your Big Data platform for all your fraud detection and regulatory support needs, or your existing Hadoop or NoSQL platform can be integrated deeply and completely into **NG|**Screener to offer you the same functionality. **NG|**Screener is directly cooperative with most Hadoop systems and there are easy import-export connectors for NoSQL, NewSQL and ELK Stack systems. You can therefore take advantage of our expert-built Smart Controls Objectives and Updates Service, rather than having to devote internal resources to developing and continually updating controls for fraud and compliance objectives.