IBM Content 2014
Information. Insights. Results.

Jonathan Muise | U.S. Counter Fraud Solutions | IBM Software
jmuise@us.ibm.com
May 8th, 2014

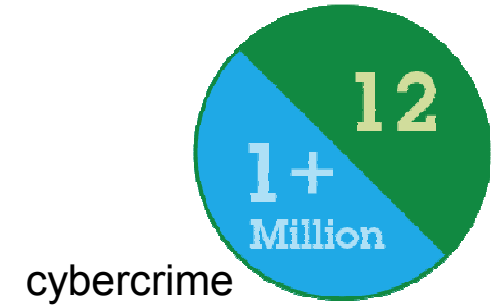
Smarter Counter Fraud From IBM

New Threats. New Thinking. A Smarter Approach To Counter Fraud

© 2014 IBM Corporation

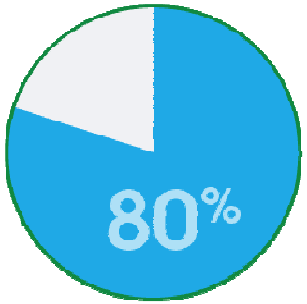
Cyber
Fraud
Intelligence
Expertise
Integration
Unaffordable
Security
Prevent
AML
Smarter
Improper payments
Fraud and
Avoidable
Risk
Governance
Unacceptable
Costly
Financial
P&C claims
Brand
Counter
Crimes
Technology
Value
Complexity
Tax
fraud
Crime
Customer retention
Big Data and
Malicious
Analytics
Vision

The facts are alarming

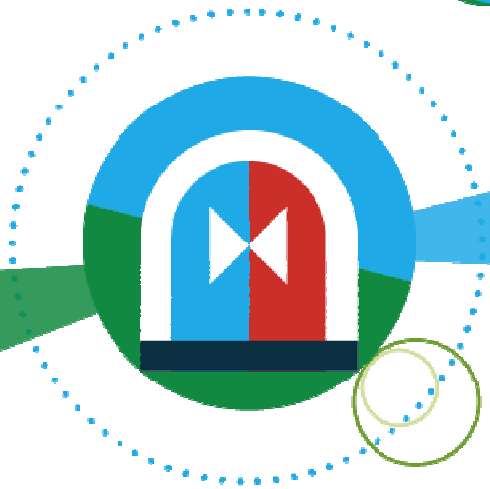


cybercrimes per second (1)

cybercrime victims daily (1)

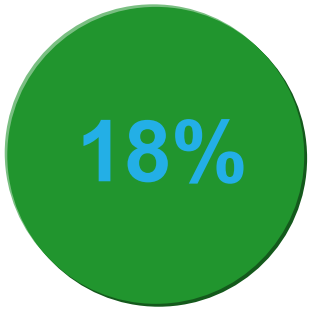


of schemes are perpetrated by organized criminal groups (2)



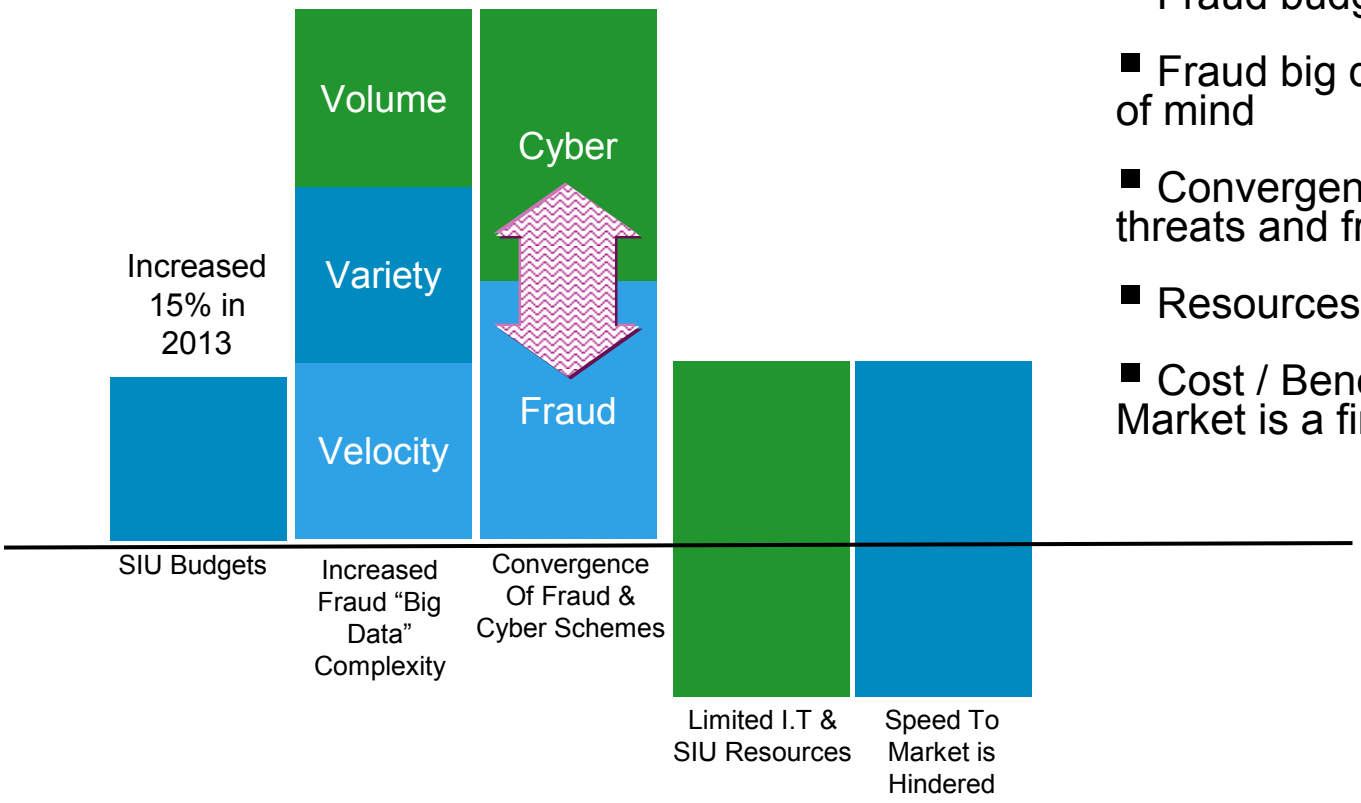
new criminal health care fraud investigations opened by US Justice Department in 2012 (5)

Estimate of cost of fraud globally



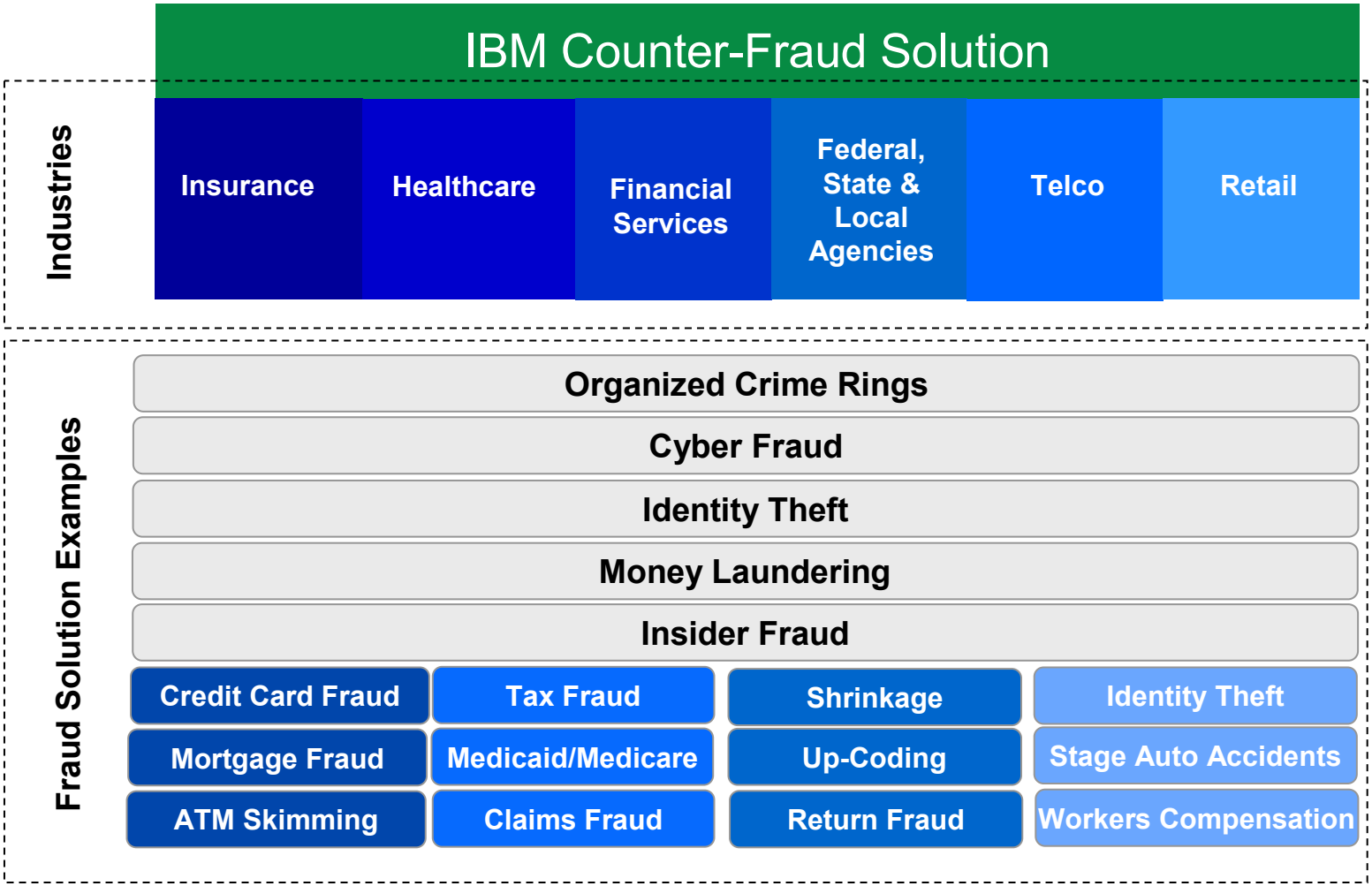
SIU Investigations initiated increased

What is the business problem we are solving for organizations?

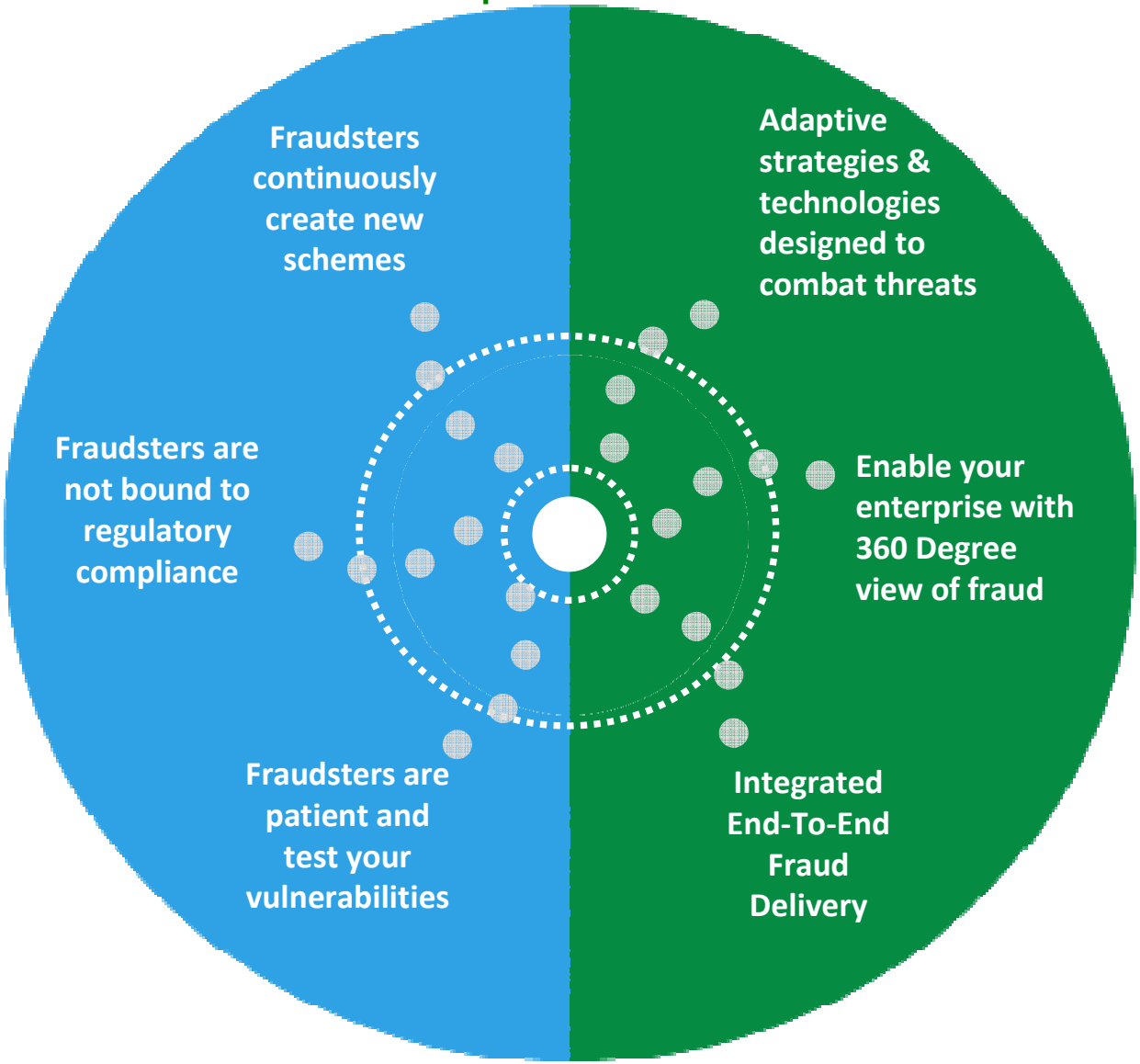


- Executives are taking notice
- Fraud budgets have increased
- Fraud big data priorities are top of mind
- Convergence between cyber threats and fraudsters is on the rise
- Resources continue to lag
- Cost / Benefit vs. Speed to Market is a fine balance

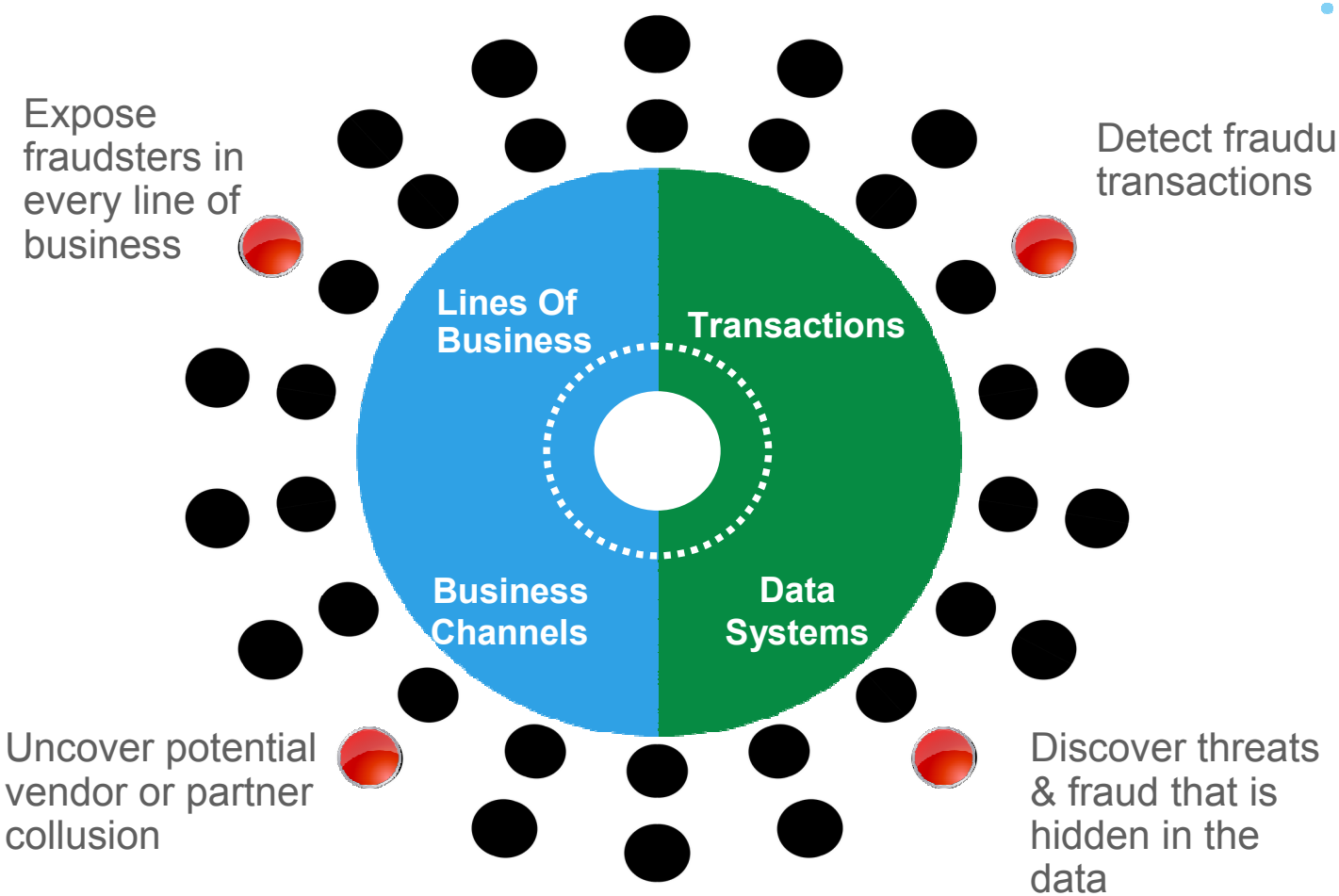
Fraudsters continuously adapt with new schemes to defraud your business



Fraudsters continuously adapt. New technology enables your business to adapt faster.

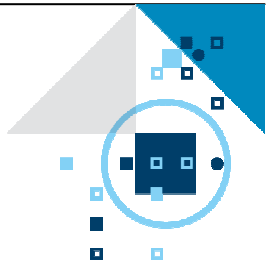


Organizations need to take an enterprise view to combat fraud and gain insights into the potential exposure.



Counter-Fraud management from IBM addresses each phase of an enterprise fraud approach

Counter-Fraud management from IBM offers distinctive and robust capabilities



Advanced industry libraries
Data models | Predictive models | Rules | Reports | Process | External fraud data and more

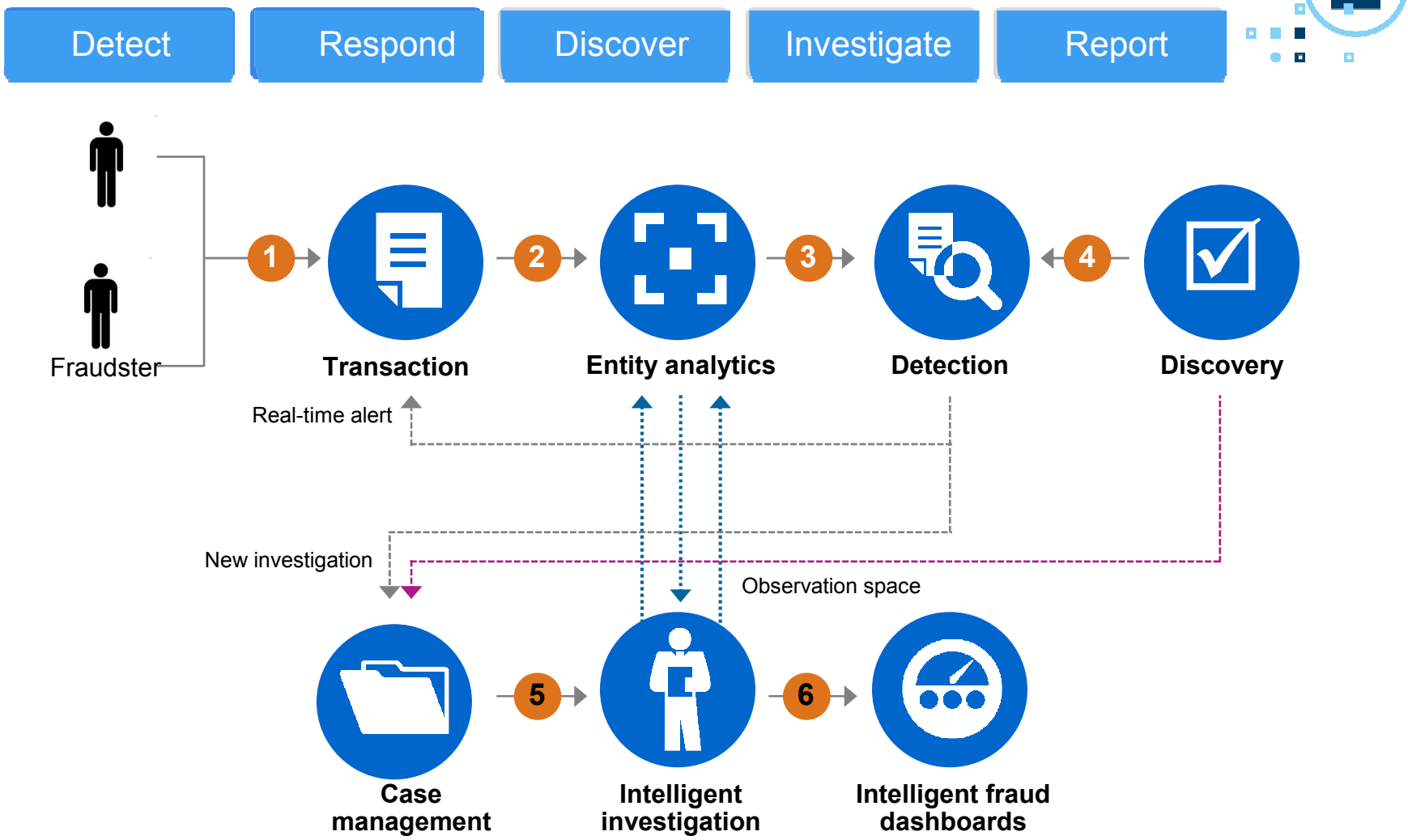
Real time | In time — Back-office analytics

Detect	Respond	Discover	Investigate	Report
Fraud Predictive analytics Fraud Decisions, Models & Rules	Action Guidance Rules	Big Data Fraud Evaluation Identification	Case management Content analytics Link-Visual analysis Forensic analysis	Fraud Dashboards Operational reporting Case briefings Feedback

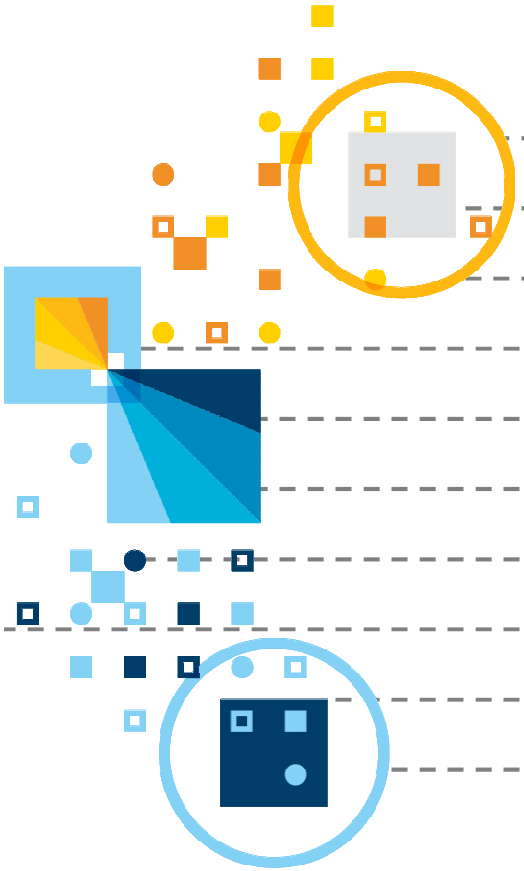
Observation space

Information domains | Internal sources | External sources | Evolving unstructured sources | Fraud use case libraries

Counter-Fraud scenario walk-through

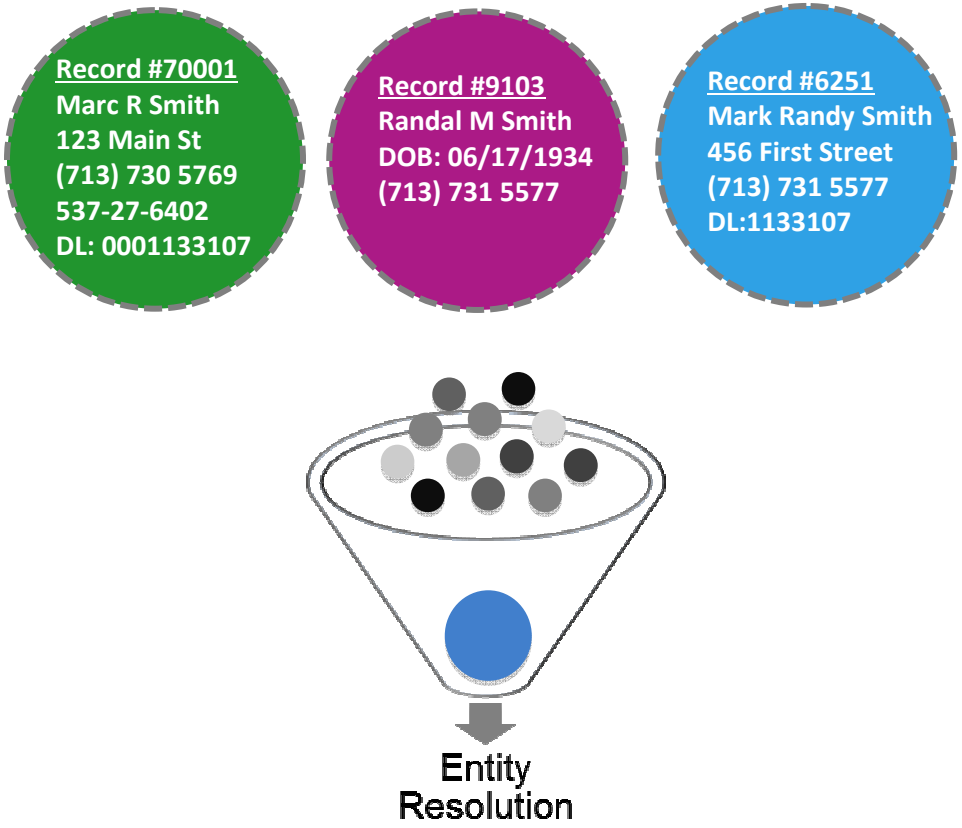


Counter-Fraud management from IBM employs multilayered analytical techniques



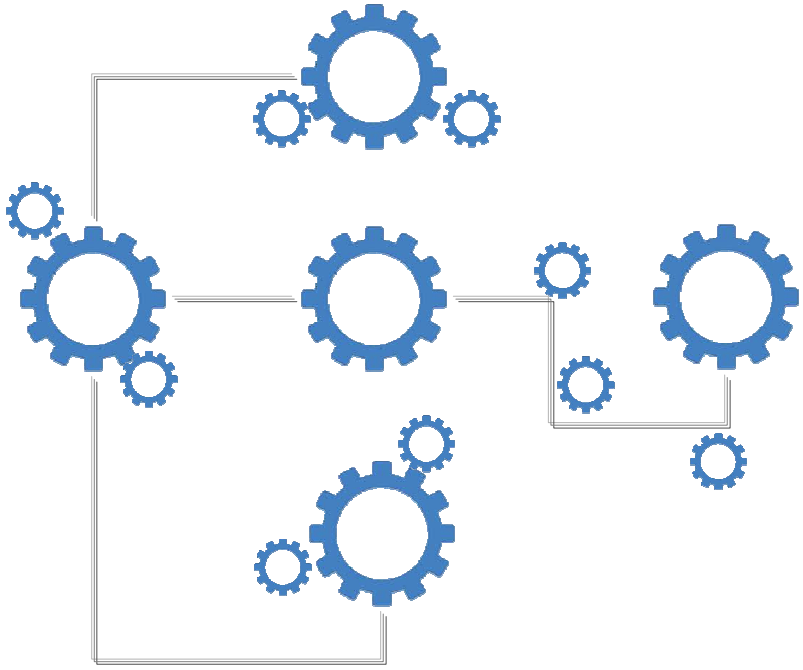
- Entity analytics
- Predictive analytics
- Behavioral analytics
- Big data
- Context analytics
- Content analytics
- Decision management
- Geospatial analytics
- Forensic analysis
- Social network analysis

Entity Analytics – "Who is who?" & "Who Knows Whom"



- **Real-time entity resolution and association discovery**
- **Increases detection accuracy**
- **Identifies fraudsters with multiple identities and exposes the truth**
- **Global Name recognition**
- **Proprietary matching engine - rules based, fuzzy logic**
- **Analyst configurable**

IBM Counter-Fraud Analytics:

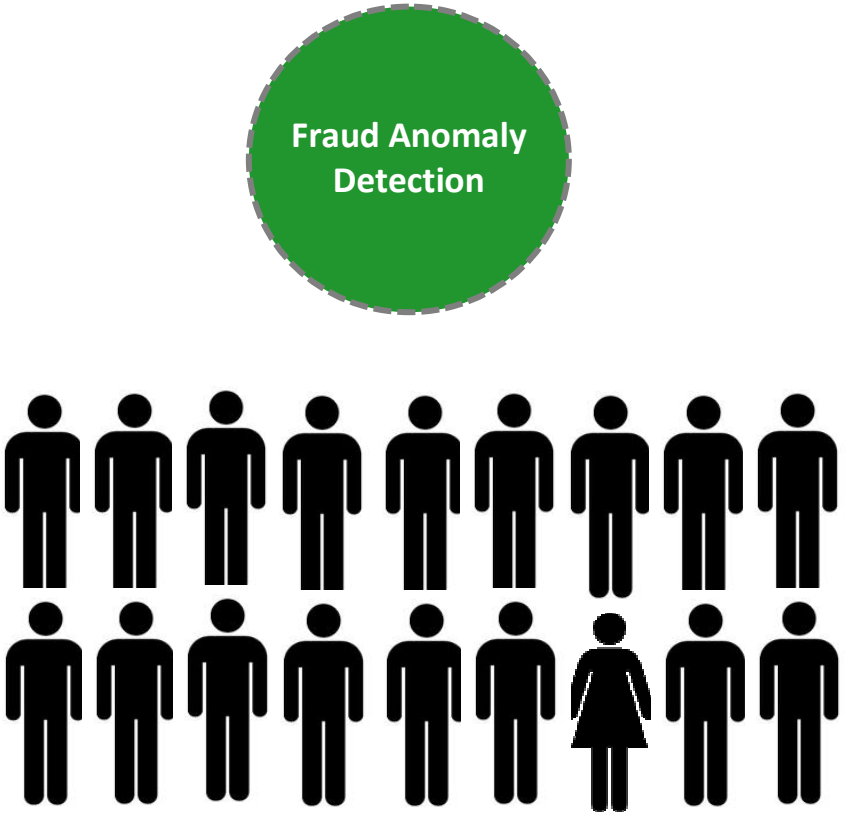


- Flexibility to blend fraud Rules & Models
- Easily deploy predictive fraud analytics
- Identify fraud patterns and trends
- Leverage text mining to extract critical information from structured or unstructured data
- Real-time entity monitoring
- Business led application

Discover Provider Fraud within Insurance

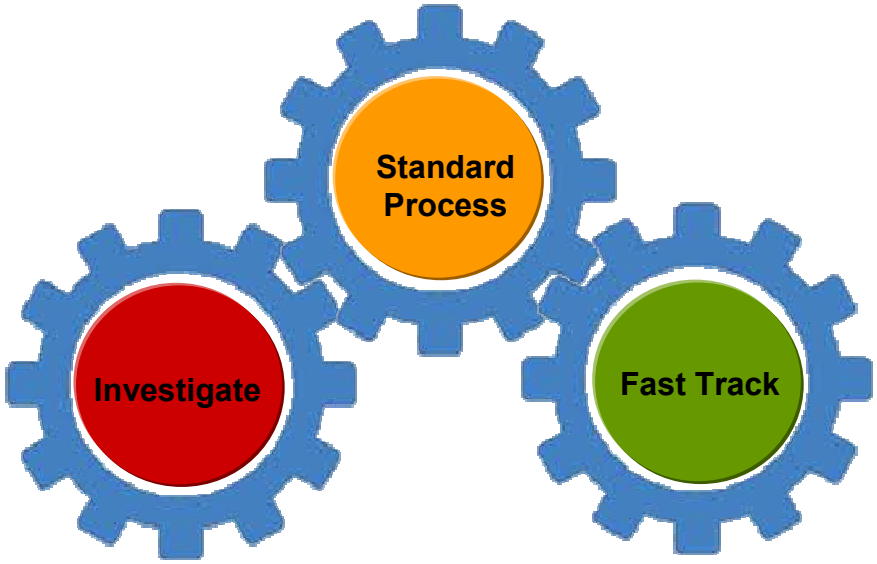
- Discover fraudulent claims related to providers
- Contains over 9,500 pre-built behavior models & risk indicators
- Apply proven models to gain deeper insights into providers associated with claims
- Dramatically drives discovery lift rates
- Use of provider and member watch lists
  - Detect suspicious providers and members retrospectively
- Use of “smart” business rules
  - Generate smart business rules that are based on statistical scoring and outlier detection
  - Easily understood by investigators and can drive substantial revenue recoveries

IBM Counter-Fraud: Anomaly Detection



- Leverages structured fraud data such as claims, transactions, social media, collusion, etc.
- Applies text mining to extract critical information from incident notes
- Identify entities that have different behavior from similar entity types
- Alerting specialists to potential loss or fraudulent activity in real time
- specialists can quickly implement the next-best action and route suspicious claims to investigators.
- detects questionable behavior, communications or relationships.

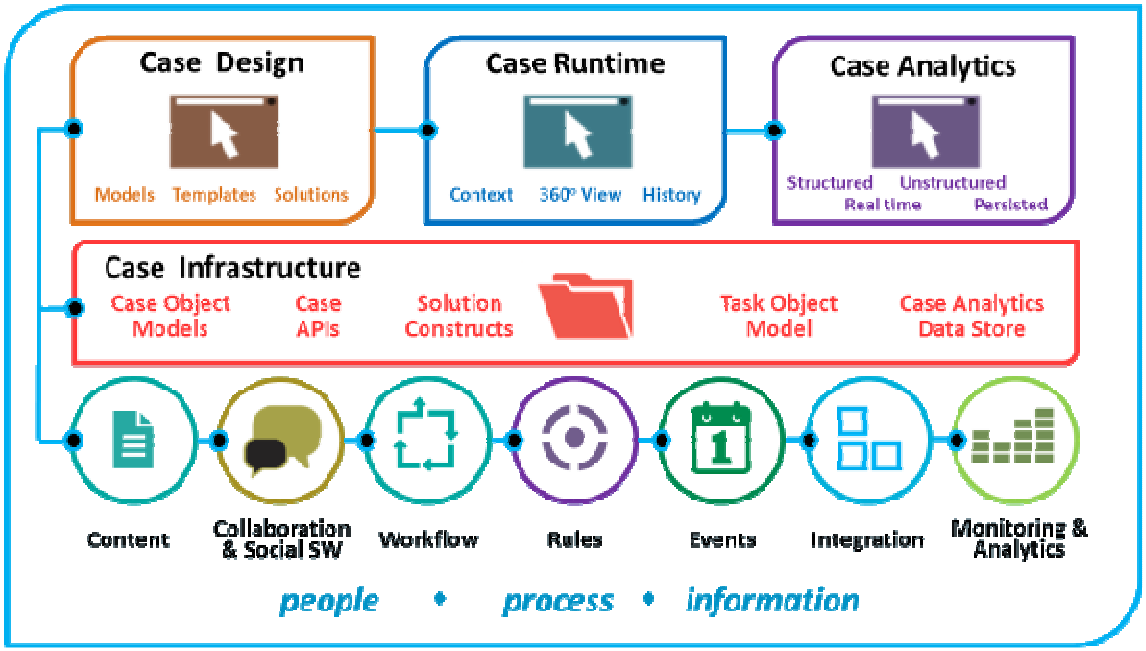
IBM Counter-Fraud: Decision Manager allows business analysts to configure rules and combine models to optimize results



1. **Flexible and adaptive environment for fraud identification**
2. **Combines Rules, Predictive Analytics, and Entity/Link Analysis**
3. **Real-time entity monitoring**
4. **Business led application**
   - Easily modify rules and decision outcomes
   - Simulation and What/If Analysis

IBM Counter-Fraud: Case Management

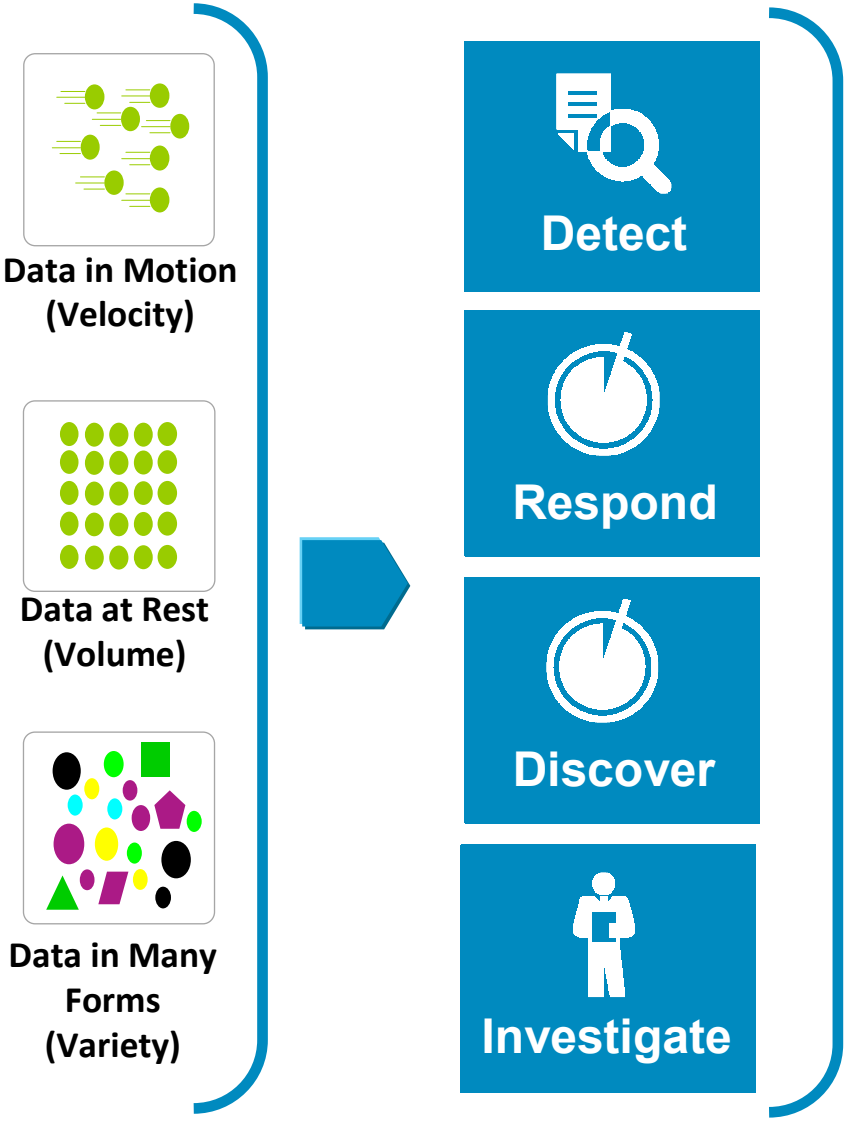
Designed with fraud units in mind to manage, assign and report against fraud throughout a transaction or process



- **Rapid time-to-value; better, faster, more cost effective Fraud investigations**
- **Organizations will not lose sight of fraud cases**
- **Cases are always visible and can be escalated with timers and rules**
- **All information is integrated within the context of a fraud case**

IBM Counter Fraud "Big Data"

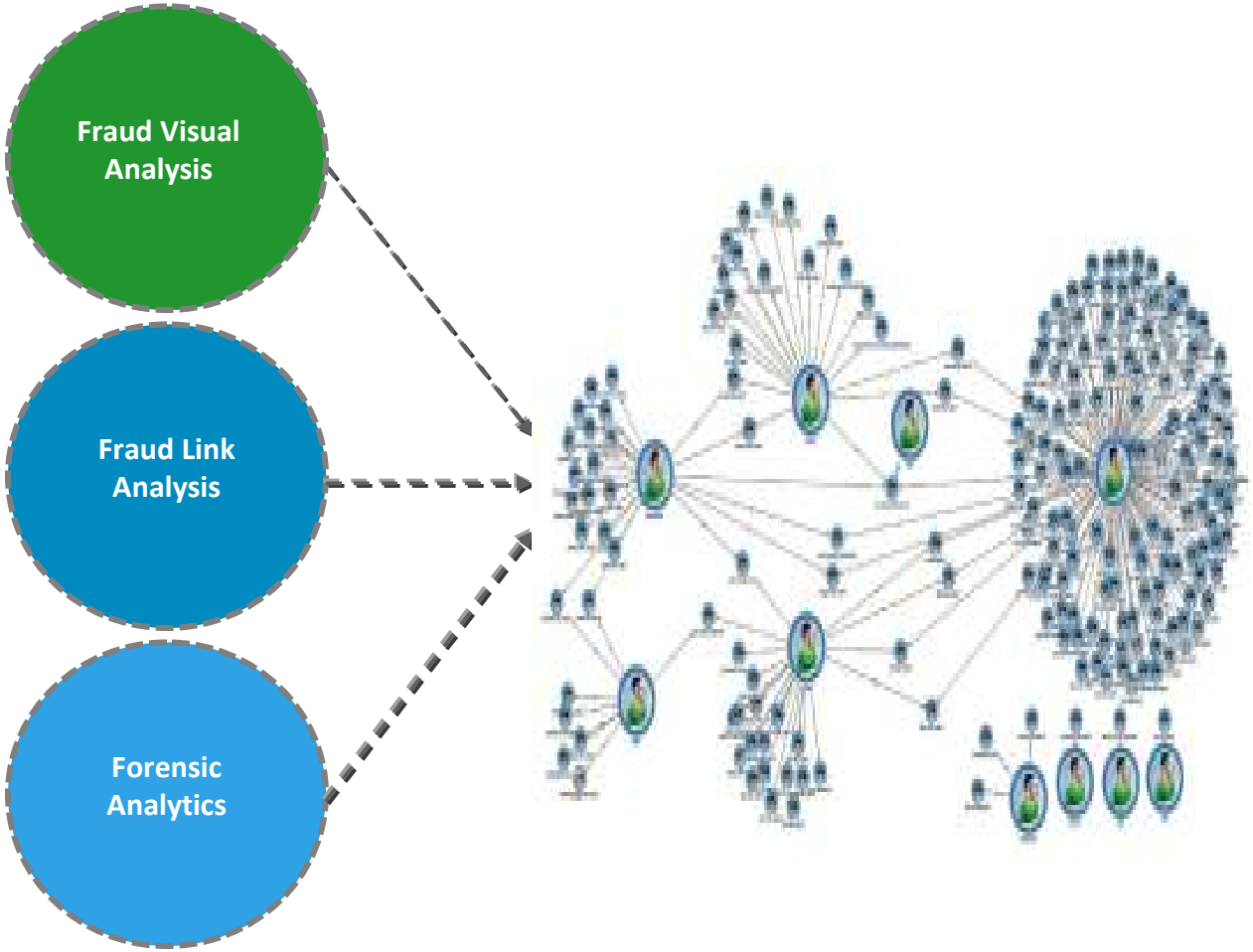
Uncover and discover fraud hidden in the data across the enterprise



1. Uncover fraud hidden in big data
2. Discover fraud across data types. structured / unstructured
3. Quickly turn data into action within the SIU and claims
4. Leverage the extensibility and scalability to harness the velocity, volume and variety of data in the enterprise

IBM Counter-Fraud Investigations

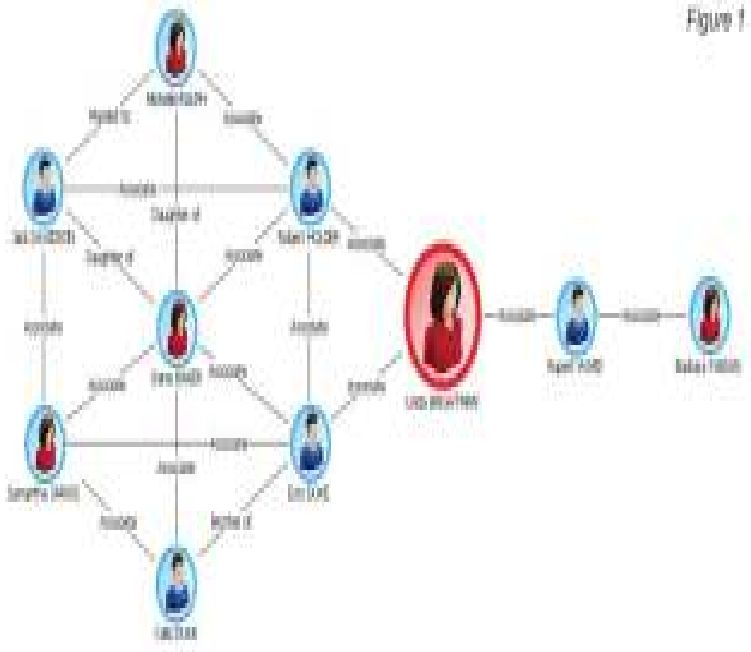
IBM's Counter Fraud Investigations bring together seemingly unrelated information for high-value awareness and provides sophisticated solutions



- **Share & Collaborative on fraud intelligence**
- **Powerful forensic discovery**
- **Geo Spatial Analysis**
- **Structured & Unstructured Analysis**
- **Embedded Media Analysis**
- **Powerful Analysis Filters**
- **Combines data extraction, manipulation, analysis and visualization**

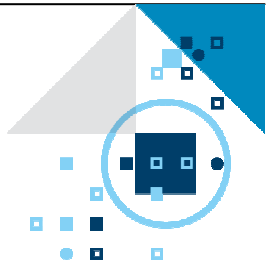
IBM Counter-Fraud: Social Network Analysis

IBM's Counter Fraud Investigations bring together seemingly unrelated information for high-value awareness and provides sophisticated solutions



- Visual and mathematical analyses of complex human and computer networks
- Discover sources and distribution of power: Who knows whom; who does business with whom; and who wields greatest power
- See how communications flow in networks and sub-networks
- Monitor patterns between communications nodes, performance and key goals
- Combines data extraction, manipulation, analysis and visualization
- Centrality, Betweeness, Closeness, Degree, Eigenvector, Link Direction and Weight

Counter-Fraud next steps for customers



Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

Thank You!

감사합니다
Natick
Grazie
Danke
Ευχαριστίες
Dalu
Obrigado
Thank You
Köszönöm
Tack
Спасибо
Dank
Gracias
谢谢
Merci
Seé
ありがとう