BUSINESS BRIEF

Big Data & Analytics

Stay Ahead of Fraud with Big Data Analytics

Powerful computing and software technologies enable real-time fraud detection to cut losses and reduce risks

5% ANNUAL REVENUE

AMOUNT TYPICAL ORGANIZATION LOSES TO FRAUD PER YEAR[1]

A Rising Tide Across All Industries

- **Healthcare:** 3% (USD 60 billion) of all spending lost to fraud[4]
- **Banking:** 11 out of the 15 small credit union closures in 2015 caused by fraud[5]
- **Consumer:** A new identity fraud victim every two seconds[6]
- **Insurance:** USD 30 billion in U.S. property and casualty fraud losses annually[7]

Industry Strategic Challenges

Fraud is on the rise–and no industry is immune. From healthcare to insurance to firms with highly valuable intellectual property, targeted companies are losing billions. In fact, it is estimated that the typical organization loses five percent of its annual revenue to fraud.[1] Hit particularly hard are financial services, communications, technology, and entertainment.[2]

In an effort to stem the losses, eCommerce merchants and financial institutions alone are expected to spend USD 9.2 billion on preventing fraud by 2020–a 30 percent rise over current levels.[3] But they are hampered by increasingly sophisticated fraud schemes and legacy detection systems that can't keep up. A key challenge is that fraud perpetrators bury repetitive but small fraudulent transactions in seemingly benign business processes, making them hard to detect.

Companies need smart, reliable ways to monitor patterns of suspicious behavior that come with the transformation of online business, connectivity, cloud-based services, and mobile applications. Most legacy fraud detection tools are rule-based and are limited to finding known issues. The challenge is to find emerging, unknown fraud patterns that a company doesn't know exist. By tapping metadata from numerous sources and data types, crucial contextual relationship patterns can predict and prevent illegal, fraudulent activity. Though most organizations have huge volumes of data at their disposal, few of them have effective methods to extract, transform, and load it to create actionable information to act quickly enough to mitigate risk. Until now.

By using machine learning and artificial intelligence, powered by high-performance computing, disparate data sources can be correlated into powerful real-time fraud detection insight. These advanced platforms can wrap around and complement existing fraud control systems to enhance theft detection and eliminate fraud rings faster and more effectively than legacy solutions alone.

Business Drivers and Desired Outcomes

- Reduce fraud prevention costs by freeing expensive resources to investigate legitimate attacks rather than false positive dead ends.
- Mitigate risk exposure surfaces now and in the future by deploying a real-time fraud detection solution that will:
- Provide actionable metrics to gauge where losses are occurring
- Easily scale the analysis of big data to efficiently detect known, unknown, and emerging risks
- Eliminate false positives by drilling down into event information to quickly determine if a given anomaly is truly a risk
- Employ automation with discovery and alert monitoring to streamline remediation efforts

- Generate prioritized reports of new and emerging risks quickly and efficiently, even as requirements change
- Perform ad hoc analyses in real time to address new questions and issues
- Integrate real-time fraud findings into any incident management system or SIEM platform for advanced forensic automation capabilities

Digital Transformation and Business Innovation

New real-time fraud detection tools go beyond ineffective legacy systems and rule-based, predictive detection. Instead, they use a non-deterministic approach that monitors suspicious behaviors a company doesn't even know exist. Using advanced artificial intelligence technologies, they quickly analyze massive amounts of heterogeneous data. Baselines of normal activity are created to identify anomalies and isolate, audit, and/or stop vulnerable business processes.

Enabling Transformation

With powerful software from industry-leading solution providers optimized for scalable, efficient hardware from Intel, businesses can use advanced techniques to find suspicious patterns and gain actionable insight into fraud sources and sophisticated attack methodologies. Companies can now perform complex analytics quickly, without overspending on large-scale systems and specialized programmers.

Solution Summary

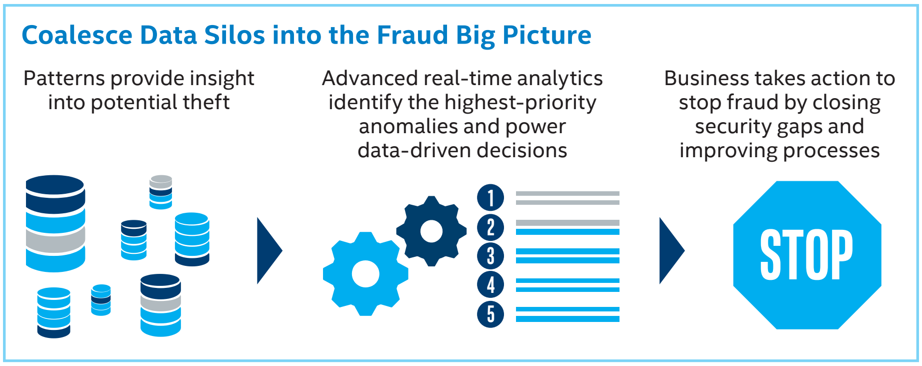
Using big data with analytics software powered by Intel® technology, data from heterogeneous sources is processed, correlated, and transformed into actionable fraud prevention intelligence. Instead of relying on knowledge of known threats, the solution can process years of stored data to uncover hidden indicators of fraud, enhance existing processes, and speed investigations.

Solution Ingredients:

- Intel® architecture: Affordable, scalable foundation for real-time fraud detection
- Advanced unstructured data lakes: Cost-effective collection and storage for large data volumes
- Open source tools such as Apache Spark* and Kudu*: Enhanced big data processing capabilities
- Intel® Math Kernel Library and Intel® MPI Library: Direct processor access that speeds results
- Intel's Solution Integrator network: Industry expertise to help with solution implementation and cyber security alerts

Strategic Solution Partners

- Accenture
- Nervana Systems
- Cloudera Enterprise
- Saffron Technology



Coalesce Data Silos into the Fraud Big Picture

Patterns provide insight into potential theft

Advanced real-time analytics identify the highest-priority anomalies and power data-driven decisions

Business takes action to stop fraud by closing security gaps and improving processes

40 PREVIOUSLY UNKNOWN FRAUD RINGS

In one pilot project for a large bank, 40 previously unknown fraud rings were detected by pooling data from dozens of databases, then performing a broad analysis.[8]

Where to Get More Information

Please visit intel.com/analytics

[1] http://www.forbes.com/sites/forbesleadershipforum/2012/04/18/how-to-find-and-stop-fraud-within-your-organization/#76a28743b30d
[2] https://www.casewareanalytics.com/blog/fraud-growing-risk-credit-unions
[3] http://www.marketingtechnews.net/news/2016/jun/14/spending-online-fraud-prevention-soar-30-2020/
[4] http://lexisnexis.com/risk/downloads/idm/bending-the-cost-curve-analytic-driven-enterprise-fraud-control.pdf
[5] https://www.casewareanalytics.com/blog/fraud-growing-risk-credit-unions
[6] "5 Top Fraud Risks for Financial Institutions in 2016," Hagai Schaffer, https://securitytoday.com/articles/2016/01/27/5-top-fraud-risks-for-financial-institutions-in-2016.aspx
[7] https://www.wci360.com/news/article/deloitte-workers-compensation-auto-lead-in-pc-fraud-claims
[8] http://www.sas.com/en_us/insights/articles/risk-fraud/fraud-rings-are-hard-to-spot.html

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration.

No computer system can be absolutely secure. Check with your system manufacturer or retailer.