SOLUTION BRIEF

Data Center: Big Data and Analytics
Lowering Business Risk

Stop Fraud in its Tracks with Real-Time Predictive Detection

Reduce fraud with Intel® architecture-optimized real-time analytics, cognitive computing, data streaming, and machine learning. Transform big data into actionable fraud prevention and detection insight.

This solution brief describes how to solve business challenges through investment in innovative technologies.

If you are responsible for...

- **Business strategy:** You will better understand how a predictive fraud detection solution will enable you to successfully meet your business outcomes.
- **Technology decisions:** You will learn how a predictive fraud detection solution works to deliver IT and business value.

Executive Summary

Undetected fraud events are real. All businesses know it, but they cannot see where they are being attacked. Fraud costs the global economy tens of billions of dollars every year. The first step to understanding fraud is knowing where it exists. Then a path to remediation and continued prevention is possible. Perpetrators of fraud count on flying beneath the investigative radar, masking illicit activities with seemingly benign business processes. Fraudulent transactions can be repetitive but small, or stealthy theft rings can employ insiders or break sanctioned trade workflows undetected. Legacy rule-based, fraud-detection tools do not use modern techniques to address the context of new attack vectors. But things are about to change.

Data scientists, fraud analysts, and forensic investigators can now add a new tool to their tool chest—real-time fraud-detection solutions that use non-deterministic artificial intelligence. It is now possible to create predictive anti-fraud context with traditionally unconnected silos of disparate data sources. These solutions are powered by and optimized for Intel® technology, expediting results that can substantially reduce the cost of finding fraud while simultaneously preventing millions of dollars in damages.

Adding real-time fraud detection to a business' fraud control system makes detecting theft and eliminating fraud rings faster, easier, and more effective than using legacy solutions alone. Companies using advanced fraud-detection solutions gain peace of mind—their fraud controls can slash the huge cost of fraud immediately and keep pace with new technology developments and new attack vectors in the future.

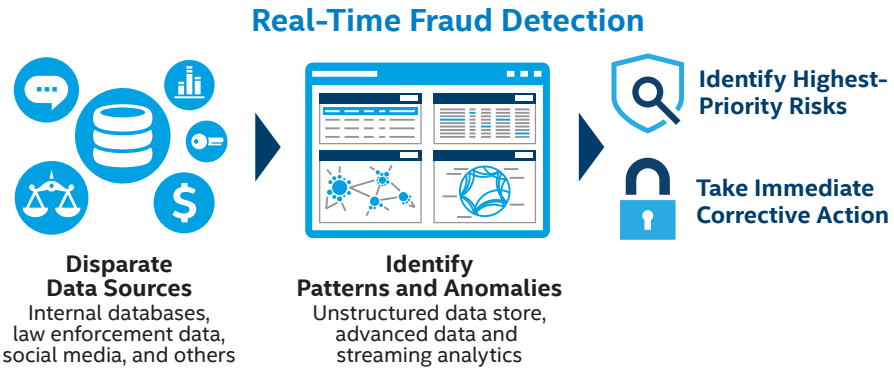

Figure 1. Fraud detection just got easier—fraud intelligence software optimized for Intel® architecture finds problems in near real time.

Author

Jeff Towle
Security Solutions Architect Manager
Industry Sales Group, Intel

Solution Benefits

- Faster time-to-detection using optimized hardware- and software-based high-performance analytics
- Application of business context for optimizing models and detecting emerging risk exposures
- Lower cost through fewer false-positives and a future-ready fraud-detection paradigm
- Easier modifications and faster response to changing fraud schemes

Business Challenge: Inability to Connect the Dots

Fraud is like the common cold: it affects everyone and is difficult to cure. Stock traders, banks and credit unions, credit card companies, insurance payers, and firms with valuable intellectual property are targets of fraud—every day. According to a report from CaseWare Analytics, the industries most plagued by internal fraud are financial services, communications, technology, and entertainment.[1]

It is not that these companies are oblivious to the problem. In fact, eCommerce merchants and financial institutions are expected to spend USD 9.2 billion on preventing fraud by 2020—a 30-percent rise over current levels.[2] Despite their best efforts, however, fraud continues to rise:

- Three percent, or USD 60 billion, of all healthcare spending is lost to fraud.[3]
- In 2015, 11 out of the 15 small credit union closures were caused by fraud.[1]
- According to the 2015 Identity Fraud Study, USD 16 billion was stolen from 12.7 million consumers in the US in 2014, resulting in a new identity fraud victim every two seconds.[4]
- Fraud costs the property and casualty insurance industry USD 30 billion each year in the United States alone.[5]

Every company has instituted some level of fraud control. But legacy systems fail to provide adequate insight. These systems were designed for single sources of data. They fail to take into account modern levels of connectivity, cloud-based services, and mobile applications. There are many new points of vulnerability that need to be monitored, and legacy fraud-detection systems simply cannot keep up. Also, attacks are growing more sophisticated and powerful. They can happen quickly and be extremely invasive. This trend narrows the window during which response can mitigate damage.

The result of relying on legacy anti-fraud systems is that companies know fraud exists but they lack solid metrics to gauge where the losses are occurring. Many times, fraudulent transactions are small (but numerous). Quite often, fraud-detection and investigation units operate in silos and a large enterprise may have dozens of isolated databases, applications, and watch lists. This creates a lack of risk context from an enterprise perspective, and does not give investigators clues to drill down to deep-dive forensics. The patterns of risk are just too faint to make actionable. To understand these fraud risk patterns, enterprises need to quickly correlate data silos for context and create baselines of normal behavior that can be monitored automatically.

The Threat Is Real

Most fraud is camouflaged, hiding amongst valid business processes and business records. An advanced, holistic approach to fraud detection can help bring fraud to light, as in the following examples:

- 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 risk analysis.[6]
- Within the insurance industry, fraud can span from opportunistic individual claims to organized multi-million dollar rings that involve staged auto accidents and participating medical equipment providers and clinics. Advanced fraud analytics can help identify the connections that lead to fraud identification.[7]
- Credit card companies process tens of thousands of credit card transactions each second. Advanced streaming analytics can compare typical spending amounts, types of purchases, and spending locations with real-time data to flag anomalies in spending habits.
- In today's global economy, high-tech companies increasingly rely on collaboration, including video conferencing. However, the same tools that enable collaboration can pose exfiltration risks. Powerful, real-time analytics of streaming data can help pinpoint possible instances of intellectual property leakage before irreparable damage is done.

Solution Value: Better Visibility, Faster Resolution

Deploying a fraud-detection solution that can integrate many sources of data and handle real-world volumes and velocities of data can result in more visibility into fraudulent activity. Considering that the Association of Certified Fraud Examiners reports that the typical organization loses five percent of its annual revenue to fraud,[8] shutting down even one fraud ring can save thousands or even millions of dollars.

The key to a modern, advanced fraud-detection system is a departure from rule-based, non-predictive detection to a non-deterministic approach that can find problems that a company does not even know exist (Figure 2). This approach relies on several areas of artificial intelligence, including machine learning, deep learning, and cognitive computing. Using these techniques to quickly analyze huge amounts of data, analysts can create benchmarks of normal activity and behavior patterns. These benchmarks then help classify and enumerate instances of fraud and isolate business processes that can be stopped or investigated.

Companies deploying a real-time fraud-detection solution can expect the following benefits:

- **Easily scale** the analysis of big data to efficiently detect known, unknown, and emerging risks.
- **Streamline remediation efforts** through automated discovery and alert monitoring.
- **Quickly drill down** into related information and determine if a given anomaly is truly a risk.
- **Reduce fraud-prevention costs** by freeing expensive resources to investigate legitimate attacks rather than pursuing false-positive dead ends.
- **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.
- **Mitigate risk exposure surfaces** now and in the future.

The solution's power lies in the ability to process vast amounts of heterogeneous data, correlate the data to identify anomalies, and deliver actionable business intelligence. Instead of relying on knowledge of known fraud patterns, the solution can process years of data to uncover hidden indicators of fraud, helping to enrich existing methodologies and speed investigations. Machine learning and visual analytics find hidden, deep-level patterns of fraudulent or outlier behavior that can be used on previous fraud data findings. Fraud investigators can benefit from automated alerts and easy integration with the existing security information and event management systems or forensic tools reduce the cost of fraud investigations.

Coalesce Data Silos into the Fraud Big Picture

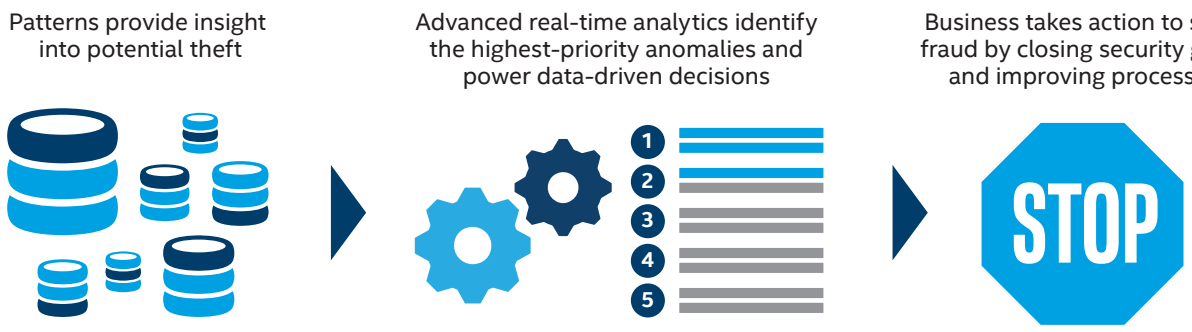

Figure 2. High-performance non-deterministic analytics and multiple detection methods monitor more risks—in very large data volumes—in less time.

Solution Architecture: Predictive Fraud Intelligence at the Speed of Business

Real-time fraud detection is not a proof of concept or a science experiment. Many forward-thinking companies around the world are already adding the solution to their existing fraud controls to significantly cut fraud losses. The solution can be deployed on premises, or as a cloud-based service—the choice should align with other business processes and requirements.

The solution architecture (Figure 3) is founded on a massively scalable and high-performance infrastructure that provides reliability and the necessary compute speed to handle vast quantities of data in seconds (not weeks, like legacy systems). The exact makeup of the infrastructure depends on the workloads and applications; it is important to right-size infrastructure components to the business need. Layered on top of the hardware are additional scalable and optimized platforms that ingest, process, analyze, and visualize disparate data sources.

- **Scalable, fast, reliable, and secure hardware.** Businesses can deploy servers using the Intel® Xeon Phi™ processor, the Intel® Xeon® processor E5 family, or the Intel Xeon processor E7 family according to workload requirements. These processors include Intel® Advanced Encryption Standard–New Instructions (Intel® AES-NI) for accelerated encryption and Intel® Virtualization Technology (Intel® VT) for hardware-enhanced protections and efficiencies for virtualized systems. Intel® Ethernet Converged Network Adapters and Intel® Solid State Drives (Intel® SSDs) that feature Non-volatile Memory Express (NVMe) for complex and real-time analytics operation round out the underlying hardware infrastructure.
- **Optimized data ingestion and storage.** Parallel data ingestion from a wide variety of data sources (both structured and unstructured) combined with an unstructured data store support high-speed data aggregation and data monitoring. These layers of the solution architecture are optimized for Intel® hardware to create efficient, scalable platforms.
- **Powerful real-time analytics.** Software that utilizes machine learning libraries, cognitive computing techniques, Spark* streaming reference architectures, and other analytic tools train over the data looking for

Technology Innovation for Fast, Scalable Cyber Security

- Intel® architecture provides an affordable, massively scalable foundation for real-time fraud detection.
- Advanced unstructured data lakes can cost-effectively collect and store huge quantities of data and provide actionable insight to a diverse range of users.
- Open source tools such as Apache Spark* and Kudu* enhance big data processing capabilities.
- Intel® Math Kernel Library and Intel® MPI Library speed results through direct processor access.
- Intel's network of system and solution integrators extends industry expertise to help with implementation details as well as the analysis, interpretation, and response to cyber security alerts.

Real-Time Predictive Detection Solution Architecture

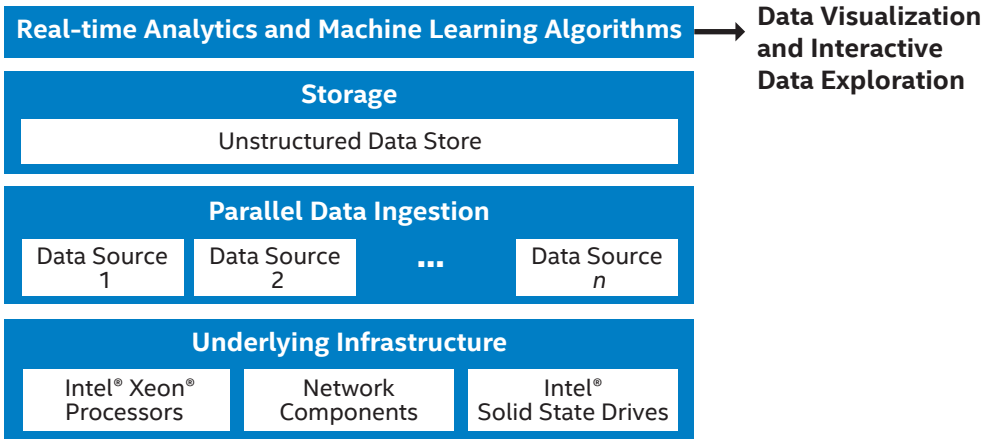

Figure 3. Intel® technology supports world-class innovation in fraud intelligence to inspect anomalous transactions and data traffic.

anomalies that can alert the business to fraudulent activity patterns. Intel works closely with third-party solution providers to fine-tune leading analytics packages to take advantage of the latest Intel hardware capabilities.

- **Data exploration and visualization.** Advanced tools that facilitate creative, interactive exploration and insights complete the solution stack. These tools go far beyond spreadsheets full of numbers to tell the full story behind the data. Drill-down and interactive capabilities help identify patterns and relationships in data that were not initially evident—powering self-service business intelligence.

Conclusion

Data scientists can now have real-time access to a wide variety of structured and unstructured data and the ability to perform complex analytics quickly, without overspending on large-scale systems and specialized programmers. Powerful software from industry-leading solution providers that is optimized for scalable Intel architecture can help businesses use non-deterministic techniques to find new fraud patterns and gain actionable insight to fraud sources and methodologies. The resulting reduction in fraud can contribute to the company's bottom line immediately and reduce future risk exposure.

Find the solution that is right for your organization. Contact your Intel representative or visit **intel.com/analytics.**

Solutions Proven By Your Peers

Intel Solutions Architects are technology experts who work with the world's largest and most successful companies to design business solutions that solve pressing business challenges. These solutions are based on real-world experience gathered from customers who have successfully tested, piloted, and/or deployed these solutions in specific business use cases. Solutions architects and technology experts for this solution brief are listed on the front cover.

Learn More

You may also find the following resources useful:

- Nervana Next Generation Platform for Machine Learning
- Saffron Streamline*
- Accenture Cyber Intelligence Platform
- Cloudera Press Release: Open Source Community Continues to Fight Against Cybercrime with Apache Spot
- MIT: Training a Big Data Machine to Defend
- Intel® Xeon® Processor E7 v4 Family

[1] "Fraud a Growing Risk for Credit Unions," Anu Sood, casewareanalytics.com/blog/fraud-growing-risk-credit-unions

[2] "Spending on online fraud prevention to soar by 30% by 2020," Liz Morrell, marketingtechnews.net/news/2016/jun/14/spending-online-fraud-prevention-soar-30-2020

[3] "Three percent, or $60 billion, of all health care spending is lost to fraud," lexisnexis.com/risk/downloads/idm/bending-the-cost-curve-analytic-driven-enterprise-fraud-control.pdf

[4] "5 Top Fraud Risks for Financial Institutions in 2016," Hagai Schaffer, securitytoday.com/articles/2016/01/27/5-top-fraud-risks-for-financial-institutions-in-2016

[5] "Deloitte: Workers' Compensation, Auto Lead in P&C Fraud Claims," wci360.com/news/article/deloitte-workers-compensation-auto-lead-in-pc-fraud-claims

[6] "Five reasons fraud rings are hard to spot," Chris Swecker, sas.com/en_us/insights/articles/risk-fraud/fraud-rings-are-hard-to-spot

[7] "Detecting and Reducing Cost of Fraud Rings," saffrontech.com/wp-content/Fraud-Case-Study-final2.pdf

[8] "How to Find and Stop Fraud Within Your Organization," Craig Hirsch, forbes.com/sites/forbesleadershipforum/2012/04/18/how-to-find-and-stop-fraud-within-your-organization

0117/JGAL/KC/PDF ♻ Please Recycle 335184-001US