

Financial Crime: Fraud Detection, Anti-Money Laundering, Employee Surveillance and Cybersecurity

Why a New Approach is Needed

With the rapid increase in the volume and sophistication of financial crime, financial services firms can no longer afford to rely on yesterday's technology. What's needed is a shift from pattern-monitoring to **operational real-time threat detection**, enabling same-day remediation with fewer false positives. At the same time, compliance officers, struggling to stay on top of increasing regulatory burdens, need a **single, agile platform** for fast data ingestion, analysis and discovery — plus the peace of mind that comes from partnering with **proven industry experts**.

Cray Analytics: Benefits for Financial Crime Prevention

- Find threats faster
- Reduce false positives
- Investigate exceptions faster
- Reduce the cost of security and compliance
- Improve productivity with an integrated Hadoop®/Spark™ and graph platform
- Gain peace of mind and confidence in your security posture

“Cray's Urika-GX platform allows the Smart Data based analytics of NextAngles to scale to handle the workloads of the world's largest financial organizations. The kind of insights that currently require hundreds of man hours of work can be generated at a fraction of the effort and cost; and within minutes of the events.”

—Suresh Nair, Chief Architect & CTO, NextAngles

Criminal Threats in Financial Services

Financial crime takes many forms — insurance fraud, insider trading, money laundering, cyberattacks, etc. While these threats are diverse, fighting them depends on common tactics. You need to look at anomalous interrelationships in high volumes of very complex, real-time structured and unstructured data. Complex pattern matching is used to detect new threats and establish new rules that minimize false positives. Rules are used to scan transactions in real time. Investigators then need productive tools to look into each exception.

Identifying the anomalous small events that indicate malicious activity is a highly compute-intensive problem. Firms are looking to exploit new AI-type technologies that look at many more data sources and help them create more effective crime-spotting models. They are using a combination of machine learning and graph analytics to spot anomalies that form complex relationships between many factors in many data sources. This places exceptional demands on a compute infrastructure. Machine learning is highly compute intensive, and to be effective, complex graph analytics needs huge memories that are bigger than the largest compute node.



What Effective Threat Detection Looks Like

Successful threat detection systems share the following qualities:

- Best-in-class predictive analytics with the agility to respond quickly, often in real time, to changes in behavioral patterns
- Continual, aggressive monitoring of interactions to ensure compliance
- Ability to digest and process structured and unstructured data continuously
- Extreme speed so that alerts can be generated in time to avoid losses
- Support for a comprehensive workflow to define, communicate, monitor, test and audit policies and controls, and to present risk and controls evidence to management and regulators

The Cray Analytics Solution

The Cray® Urika®-GX platform is the first agile analytics platform fusing supercomputing with an open, enterprise framework. The Urika-GX platform lets analysts run Hadoop, Spark and graph concurrently.

Cray Inc.
901 Fifth Avenue, Suite 1000
Seattle, WA 98164
Tel: 206.701.2000
Fax: 206.701.2500
www.cray.com

SOLUTION BRIEF: FINANCIAL CYBERSECURITY

Key Capabilities

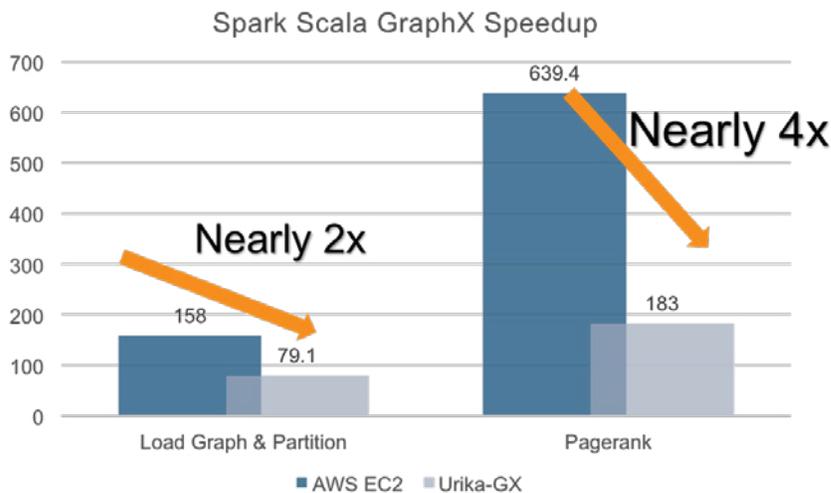
- Single system tuned for data-intensive and highly iterative workflows across all areas of business, from fraud and security issues to quant model creation and backtesting
- Integrated platform enables all forms of analytics, including large-scale nonpartitioned graph, on a single system
- Cray Aries™ interconnect for the fastest available in-memory analytics, plus Cray Graph Engine for fast complex pattern matching
- In-memory semantic graph database based on W3C standards such as RDF and SPARQL
- Integrated parallel filesystem enables faster data load times
- Open framework for integration, extension and customization

Analytics Benefits for Financial Services Firms

With Cray's Urika-GX platform, banks and financial firms can drastically improve anomaly detection to improve the quality of response to fraud while enabling steep gains in compliance department productivity. The Urika-GX is tuned for serious speed on noisy data with complex relationships; the same system can also be used for other analytics areas within financial services, significantly improving quantitative model creation and backtesting to ultimately heighten confidence in trading strategy returns.

As a result, financial-services firms can identify and resolve threats faster, gaining peace of mind and confidence in their security posture. Clients can also reduce compliance costs and improve system and analyst productivity. In addition, massive speed and reduced latency delivers faster time to value than would be possible with other commercial systems or home-grown solutions.

In one test, the Urika-GX system **doubled the speed of Amazon EC2 for a graph load/partition benchmark and provided page rank four times faster.**



Highlights low-latency/high-bandwidth Aries interconnect on Urika-GX system



For More Information

- [Get Urika-GX system details](#)
- [Learn more about Cray's cybersecurity solutions](#)
- [Learn more about Cray solutions for financial services](#)