Objectivity, Inc. Overview

• Established in 1988 and headquartered in Silicon Valley

• Industry pioneer and technology leader in the enterprise NOSQL market
  – Platform products enable real-time relationship analytics, network analysis, data fusion and metadata index management for any data type or format

• Unique distributed NOSQL data fabric delivering unparalleled performance and scalability for beyond-petabyte data volumes
  – Supports adaptive analytics for both data-at-rest and data-in-motion

• Proven platform with over a decade of enterprise deployments
  – Objectivity/DB™: Distributed big data and object management
  – InfiniteGraph™: Massively scalable graph database tool for big data analytics

• Loyal, blue-chip customer base across numerous verticals
  – Intelligence, defense, energy, telecommunications, process control, data intensive sciences, financial services, medical, ad platforms and Web 2.0

• Strong IP position supported by deep domain expertise in NOSQL
  – 6 patents granted and 6 pending
  – Hardened platform with ~5 million lines of code
The Problem

INFORMATION FUSION & INSIDER THREAT
Insider Threats and Analysis

• “Who is guarding the guards” problem
  – Accidental Insider
  – Malicious Insider
    • Current or former employee, contractor, or other business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information system (CERT)

• The average cost of a successful attack by insider is nearly 50 times greater than that of external attack (FBI, 2008)

• More than 50% of companies suffered an internally initiated cyber attack. Insider threat accounted for 23% of all cybercrime (CERT, 2012)

• In financial services industry, on average, over 5 years elapse between subject’s hiring and identified start of fraud
Changing Nature of Insider Threat

- It is a growing problem of increasing complexity
  - Beyond analyzing packet capture data, netflow data, access logs – structured data
  - Analyze unstructured data such email and blogs

- Help identify indicators and precursors of malicious acts
Insider Threat Drivers

• Overall growth of data availability and collection ("Big Data")
  – Availability of cost effective commodity servers

• Growing source of Big Data are machine generated
  – Sensors
    • Availability of powerful, cost-effective, increasingly small sensors
  – Machine logs

• Growing appetite and need for advanced analytics around “Big Data”
  – National security
  – Public safety
  – Competitive drive
  – Better decision making

• Increased access to information
  causing increasing leaks and insider threat concerns
Why are we using the phrase “Advanced Information Fusion” versus Data Fusion or Data Integration?

- The phrase data fusion and sensor fusion is used to described fusion of hard data (original JDL model) through multiple abstraction levels.

- Data integration usually refers to integration of data in various forms into a singular model to support specific analytic workloads at the same abstraction level.

- Fusion community established International Society of Information Fusion (ISIF) in part to address the notion of creating “information” from “data” that includes both hard data and soft data (human generated data).

- ISIF through Data Fusion Information Group (DFIG) updated the original JDL model to address the issues from new technology such as Big Data, advanced analytics, cloud computing and information management.
JDL Data Fusion Framework

Originally aimed at providing a process flow for sensor and data fusion.

Revised to address low and high level information fusion in the context of Big Data, IoT, and advanced analytics.
What we know, where we are now

INFORMATION FUSION & INSIDER THREAT
Robust networks allow increased collection and intelligence sharing leading to a combat advantage

However..

Exponential growth in volume, velocity and variety of data and relationships that must be organized effectively so that valuable intelligence can be quickly shared with the right decision makers.
Network Complexity

- Over 100 interconnects
- Over 20 node architectures
- 6 WAN architectures
- Protocols
- Distributed in numerous combinations
- Managed with over 20 tools
- Spectrum issues
- Services
- Hundreds of unique configurations

© Copyright 2015 Objectivity, Inc., All Rights Reserved
Commanders must take the information, analysis, and actionable intelligence generated by their organization and use it to generate actions and further information requirements for his unit.
Use cases

• Top government integrators all have some sort of fusion platform.

• Northrop Grumman, Lockheed Martin, General Dynamics, L3-Comcept, Raytheon, Boeing...

• Just about all use Objectivity/DB as the object repository.
Net-Centric Collaborative Targeting System (NCCT) is a Joint Coalition targeting system currently used in Afghanistan.

- Simultaneously focuses sensors on common targets to get very accurate information in real-time M2M interface between tactical and national ISR.
- Fuses multi-platform, multi-INT, multi-security level data to provide tracks with accuracy and pedigree in near real-time.
Analyst Support Architecture (ASA)

• Correlates multi-source data to provide a fused picture
• Compares the data against a knowledge model that provides the “expectation”
• Alerts an analyst when the incoming data does not match expectations
• Analyst can quickly drill down to all of the data relevant to an alert
• Highly configurable, even allowing the analyst to “do it the old fashioned way”
ASA – The Problem

- **Significant increase in data volume**
  - Rapid correlation of national and tactical multi-source data from defense and intelligence agencies to provide a fused picture.

- **Declining expertise with the data**
  - Compare the data against a knowledge model that provides the “expectation”.
  - Alert an analyst when data does not meet the “expectation”.
  - Allow the analyst to quickly “drill down” to all of the data relevant to the alert.
Multi-Intelligence Data Fusion Framework
Integrated Intelligence Fusion Architecture …

- User Interface Framework
- Middleware Framework: “Persisted Graph of Discovered Data Relationships” Fusion Layer/Objectivity/DB
- Data Retention Framework
- All Data Feeds
- Legacy Systems
- Distributed Storage

© Copyright 2015 Objectivity, Inc., All Rights Reserved
Common Big Data Architecture

Massively Parallel Data Streams

Un-structured, semi-structured, structured data

Visualization & Analytics Tools

The strategic competitors are all moving in this direction for Big Data

Observe — Orient — Decide — Act
Solution

INFORMATION FUSION & INSIDER THREAT
Information Fusion

- Information Fusion is the activity of combining multiple data sources (hard and soft data) to obtain improved information by enriching data at multiple abstraction levels with semantic context – Part of “Big Data Integration”

The fundamental characterization of information fusion involves a hierarchical transformation between observed parameters and a decision or inference produced by fusion process.

- High
  - Threat Analysis
  - Situation Assessment
  - Behavior of Entity
  - Identity of Entity
  - Position/Velocity
  - Existence of Entity

- Low
  - Making data available to users, processes, and applications
  - Integrating data with other sources

5. Making data available to users, processes, and applications
4. Integrating data with other sources

© Copyright 2015 Objectivity, Inc., All Rights Reserved
Why Objects?

- Data fusion dealt mostly with hard data – sensors.
- Objects are a good way to express this information.
- Information fusion brings a lot more soft (un-structured) data into the picture – social media such as e-mail, Twitter, Facebook, SMS, text, audio, video...
- Need better ways to understand soft data – meaning and context... ontologies...
- Objects AND relationships are needed to represent this information.
Why Objectivity?

- Proven track record and deployments of information fusion systems in both government (defense and intelligence), and commercial (oil & gas).
- Proven performance and scalability.
- Distributed architecture built in from the beginning.
- Highly reliable and scalable repository for a wide range of complex data types.
- Proven advantages in analyzing information in large and complex data volumes.
- Performance.
- Flexible development and deployment options.
Use cases

INFORMATION FUSION & INSIDER THREAT
General Use Case

Real-time Connection Platform
Search, Analyze and Store
Relationships and anomalies

Analysts

Internet

Server or Cloud

Networks

CDR Data
SMS Data
Structured Data
Unstructured Data
Transaction Data
Geo-Location Data

© Copyright 2015 Objectivity, Inc., All Rights Reserved
Cyber Security

Business Challenge
• Network threats are becoming more sophisticated
• Need to identify and respond to security threats in real-time
• Leverage IP, log, access as well as behavioral data

Solution
• Flexible graph analytical framework to identify anomalies, patterns and relationships
• Massively scaled, cloud-based analytics platform

Results
• Real-time response to threats
• Increased network safety and reliability
• Increase revenue and increase end-user satisfaction
Cyber Security

Real-time Relationship and Analytics Platform to detect emerging patterns

Network Devices

Analysts
Business Challenge

- Threats on Intellectual Property are becoming more sophisticated
- Need to identify and respond to threats in-time
- Monitor document access for unusual activity against norms, patterns...

Solution

- Flexible graph analytical framework to identify anomalies, patterns and relationships
- Massively scaled, cloud-based analytics platform

Results

- In-time response to threats against IP
- Increased IP protection
Intellectual Property Security

Real-time Relationship and Analytics Platform to detect unusual behavior

Analysts

Organization
Access Control Authorization
Documents
Mobile Social Network Analytics

Business Challenge
- Need new ways to capture and analyze customer usage patterns to drive revenue growth
  - Lack of visibility into distributed network data
  - Lack of real-time insight into end-user relationships and behaviors

Solution
- Real-time, distributed, connection platform provides:
  - Ingest and store all connection records
  - Consolidated view of subscriber relationships
  - Immediate access to reports

Results
- Improved subscriber service and satisfaction
- Improved visibility in transaction patterns
- Increased revenue
- Decreased liability from misuse of the network
Mobile Social Network Analytics

Real-time Connection Platform
Search, Analyze and Store Relationships

Analysts

Internet

Networks

CDR Data
SMS Data
E-mail Data
SN Data
Transaction Data
Geo-Location Data
Global Data Analytics

Business Challenge
• Integrate large scale and distributed data sets for public policy and social science on a global scale to detect patterns and identify outliers across time and space

Solution
• Real-time connection platform enabling:
  • Use of Big Data to understand impact of global events on society and human behavior
  • Improved public policy decision-making

Results
• Ability to create and analyze global models
• Insight into global models for solving world problems
Global Data Analytics

Green Layer – Visualization
Black Layer – Information Space / Analytics
Blue Layer – Security / Transformations
Red Layer – Data Sources