IEEE SmartGridComm™
IEEE INTERNATIONAL CONFERENCE ON SMART GRID COMMUNICATIONS

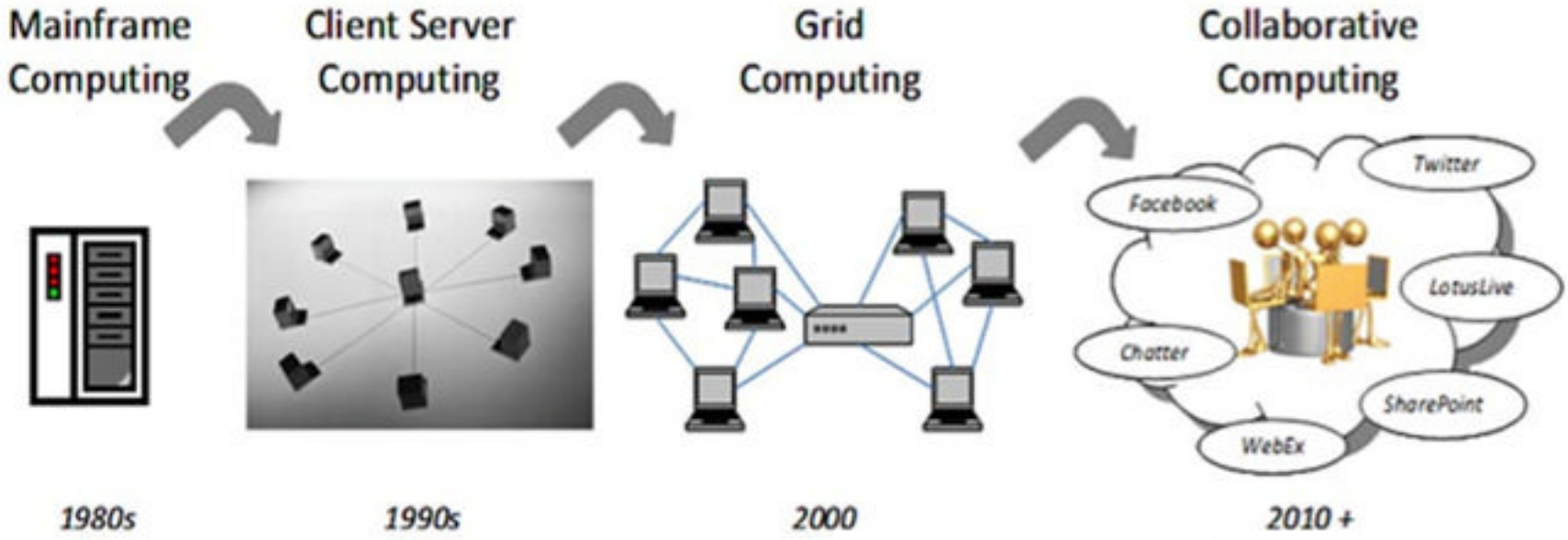
ViaSat

Big Data Analytics for Smart Grid Security Intelligence

November 4, 2015

Stefan Jucken
Global SatCom & Critical Infrastructure Protection
Secure Network Systems
ViaSat Inc.

Technological Paradigm Shifts



Source: BofA Merrill Lynch Global Research; Salesforce.com

DATA SCIENCE

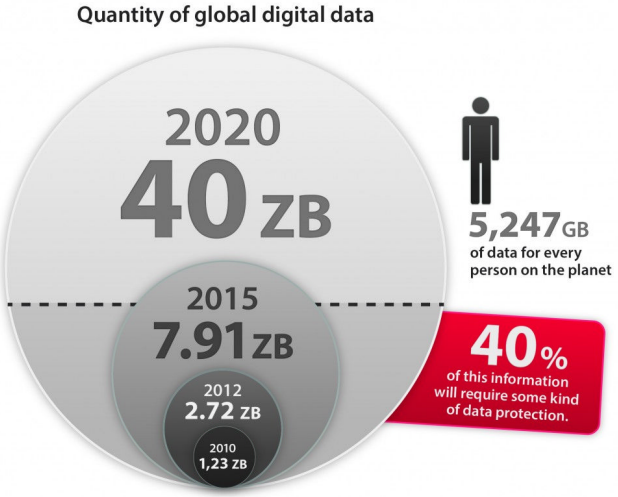
Machine Learning

DISTRIBUTED PROCESSING

In Memory Computing

REDUCED COST

Sensors and Devices Connectivity



IT Paradigm Shift

Traditional Computing

- HW Centric & Intense
- Data Consistency and Integrity
- Find & Analyze stored information
- Batch paradigm - pull
- Query Driven

Big Data Computing

- Application & Data Centric
- Speed and Flexibility
- Analyze Data in Motion
- Low latency paradigm – push
- Data Driven

Business

- Determines what questions to ask

IT

- Structures data to answer that question

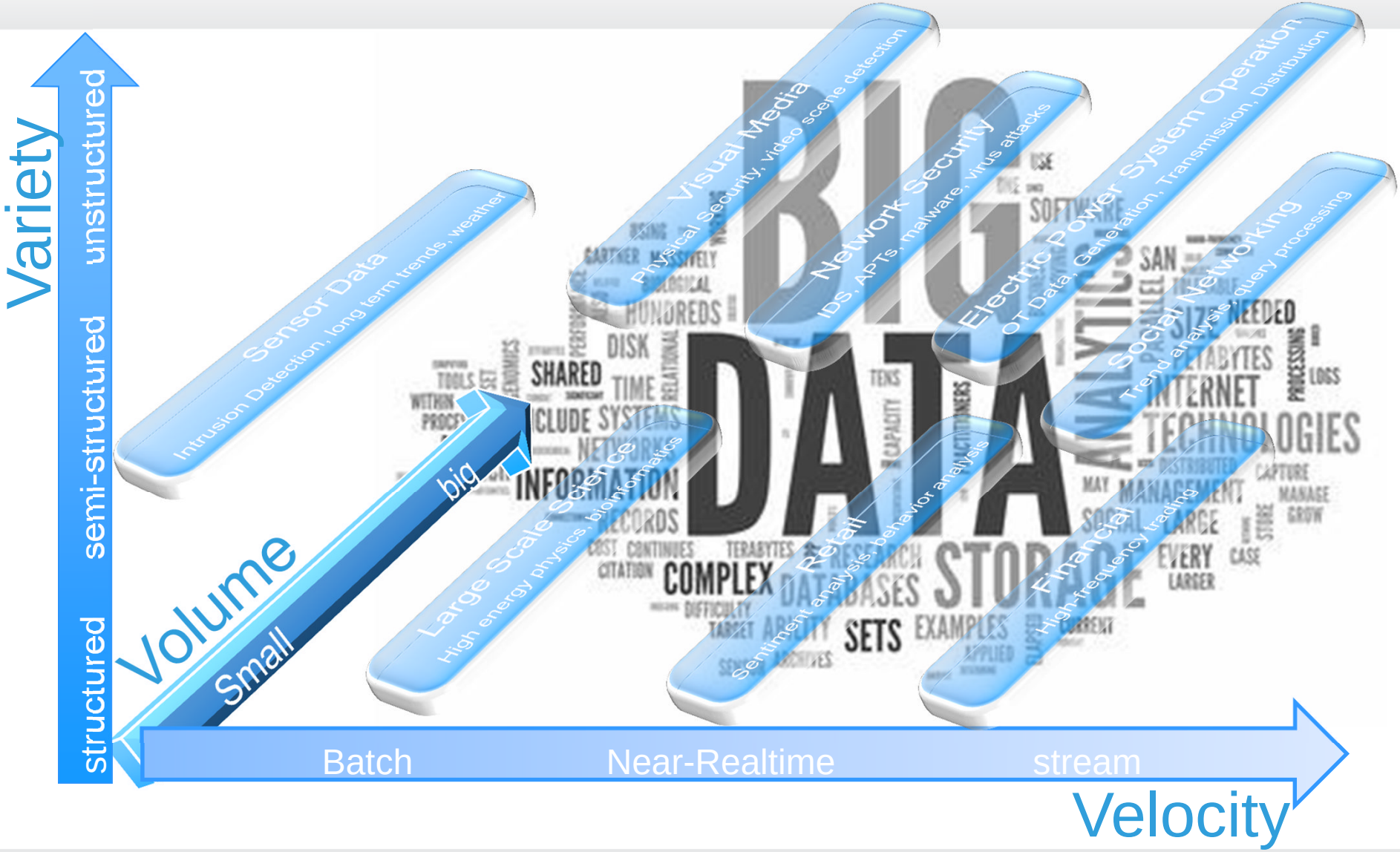
IT

- Delivers platform to enable creative discovery

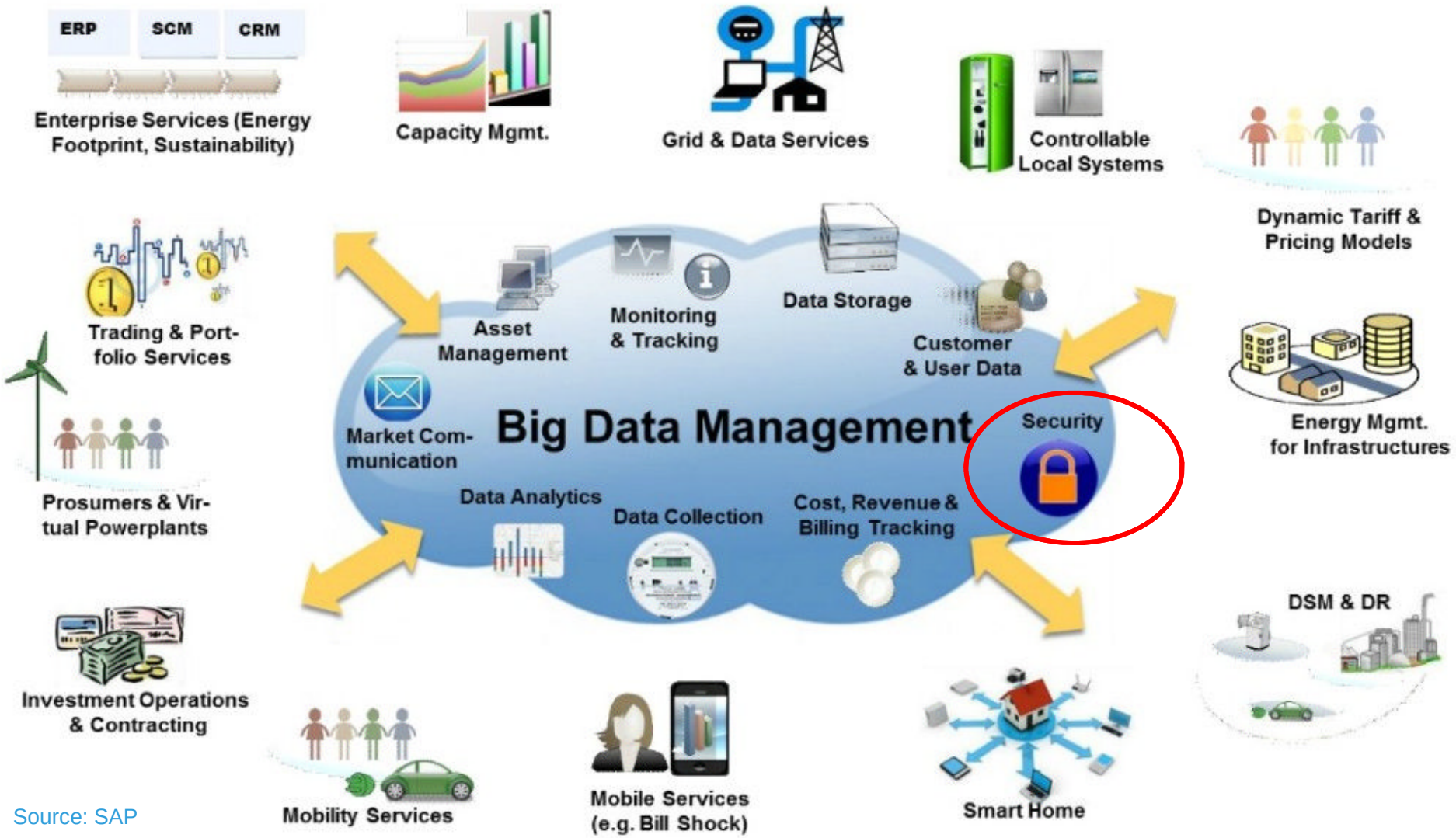
Business

- Explores what questions could be asked to create new bus. models

Big Data Taxonomy: V³



Big Data in the Smart Grid



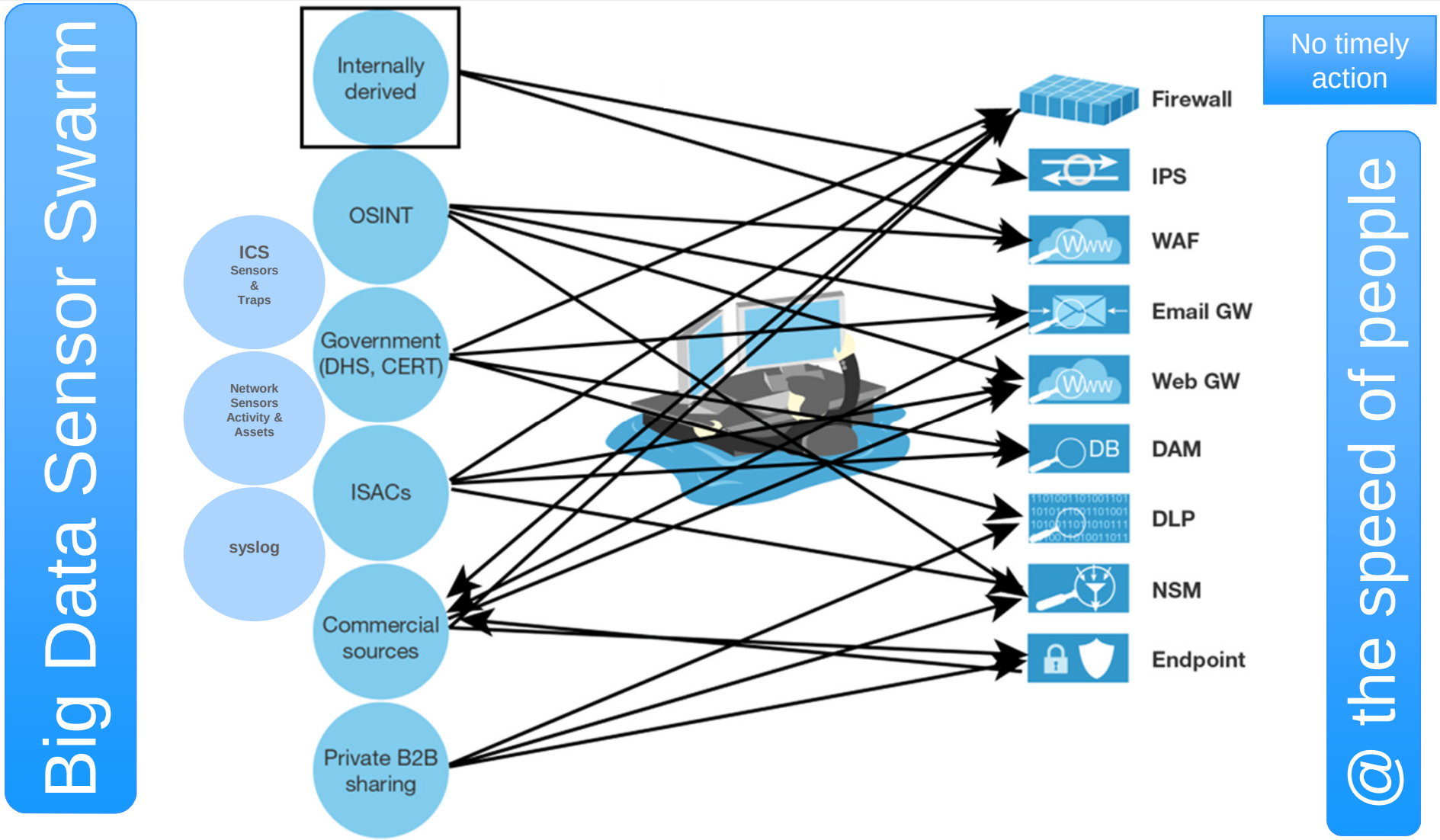
Source: SAP

Emerging Threat Landscape

- **Attack Trend is Increasing**
  - Cyberattacks: Designer Malware, Phishing, Fraud, APTs
  - Big Data model has great value but also inherently great risk.
  - BD security needs to be designed in from day 1 to achieve grid resilience.
  - Data Centric Model has to be considered for security approach

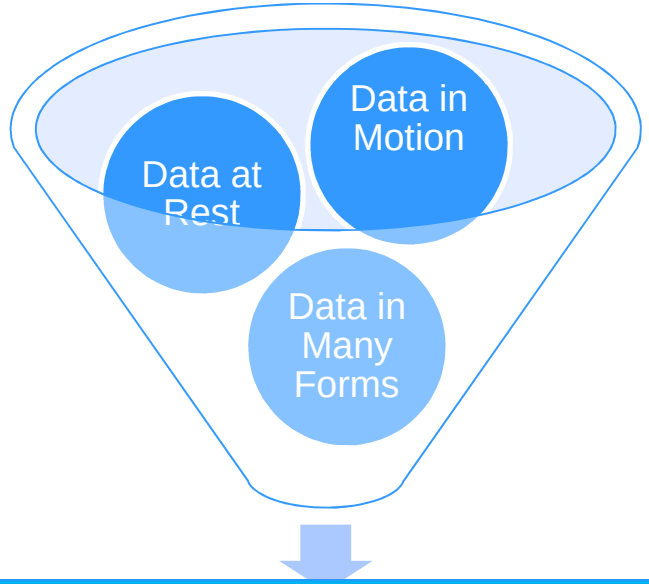
- **Threats are not just external**
- **System of Systems Architectures increase complexity**
  - Unprecedented vulnerability surface
- **Enterprise edge is no longer static**
- **CIP Compliance ≠ Security**
- **Overlay Security Layer with trust anchors**

Big Data Gridlock



The Power of Data Science

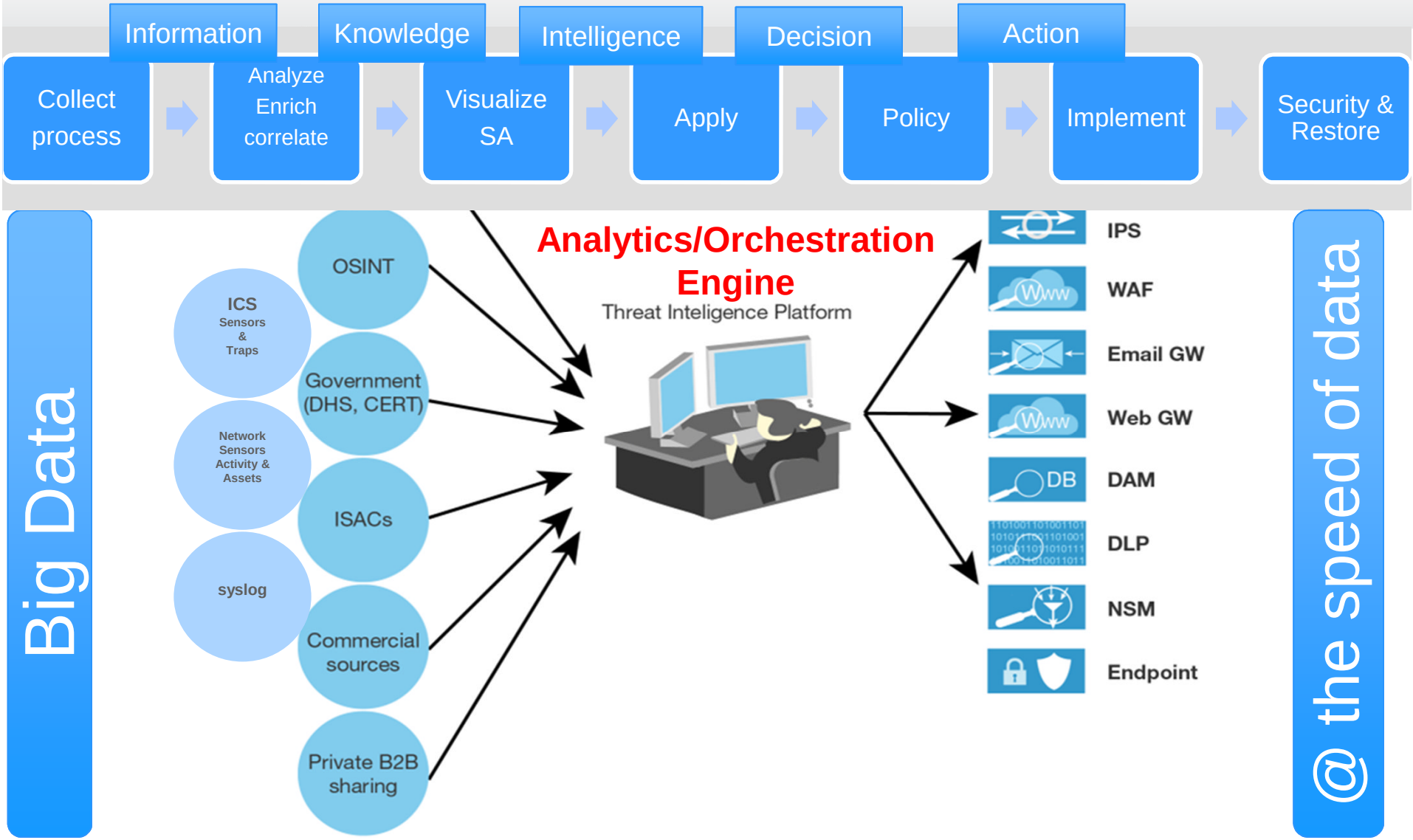
Big Security Intelligence Data



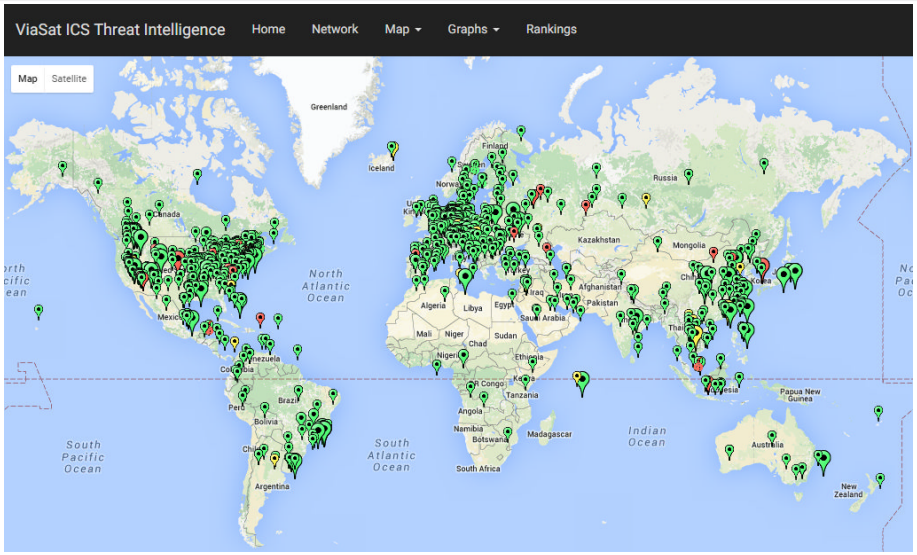
Analytics - Enrichment - Correlation
Descriptive – Predictive - Prescriptive

Smart Data

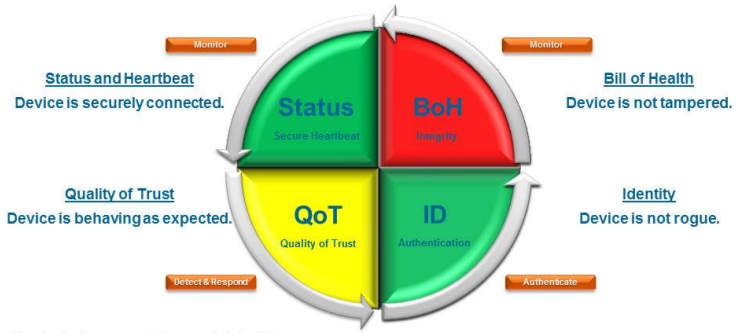
Security Intelligence Value Chain



Baseline - Detect - Analyze - Remediate

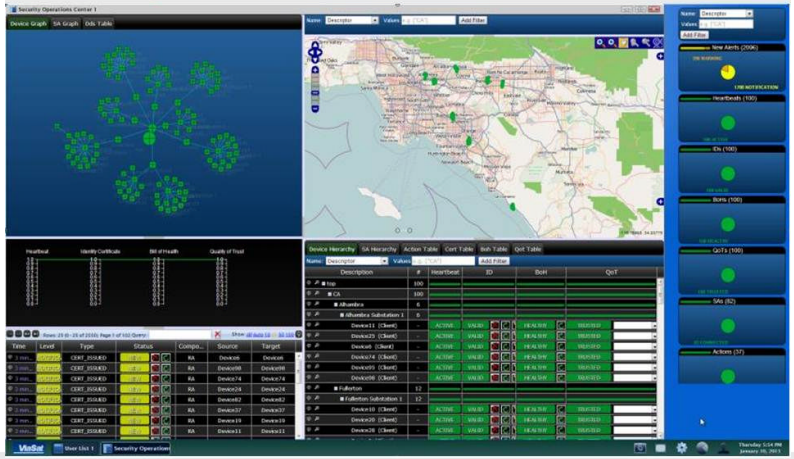


Trusted Cyber Sensor: Detect and Defend Insider Threats.

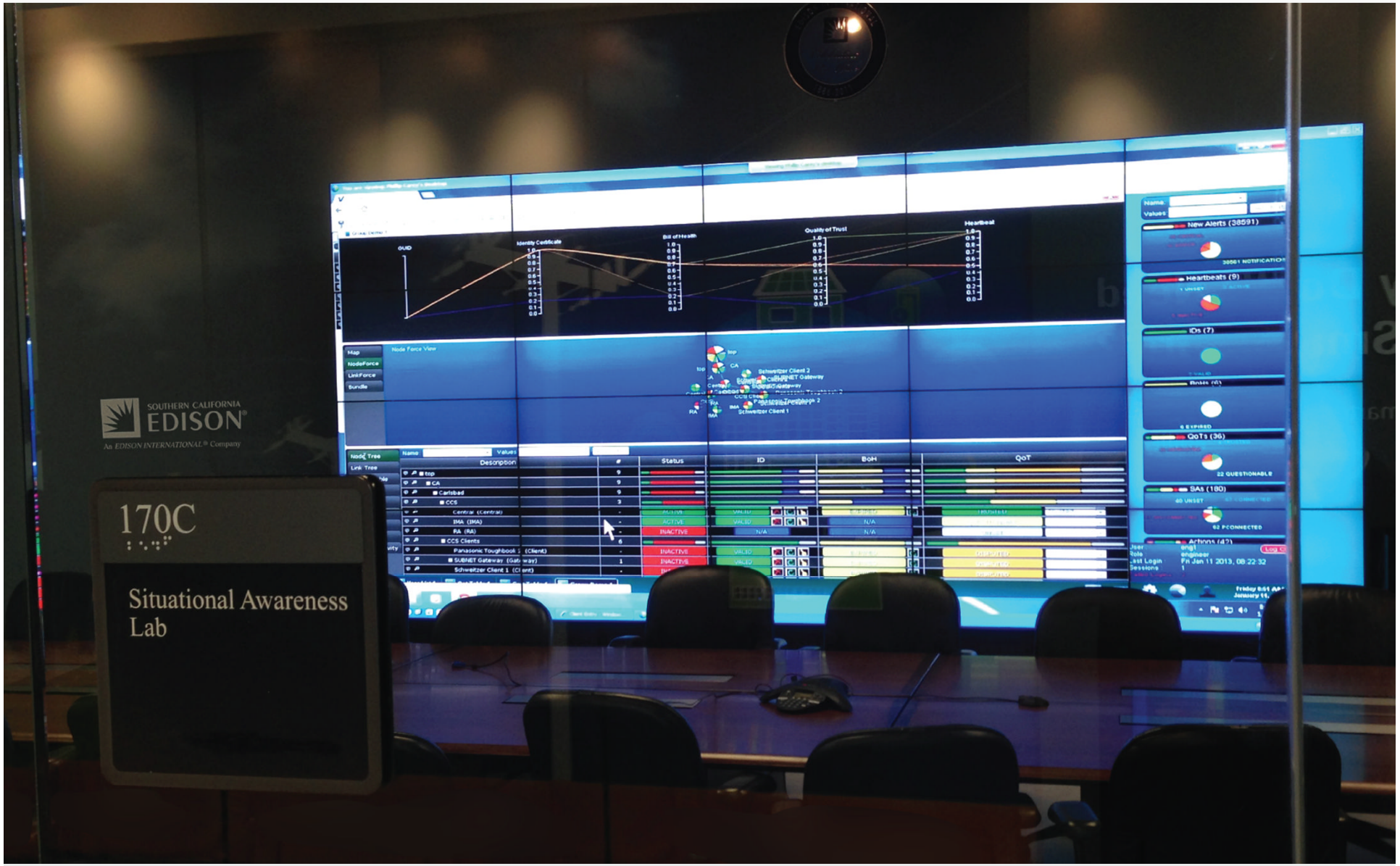


*Quadrant color represents the current state of the security attribute

Passive Network Visualization: Security You Can See™



Thank You!


SOUTHERN CALIFORNIA
EDISON
An EDISON INTERNATIONAL Company
170C
Situational Awareness
Lab