RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCS-T07

Security @ Scale: Making Security Analytics Work for the Internet of Things

Peter Tran

Sr. Director- Advanced Cyber Defense
RSA Security
@breachreadiness

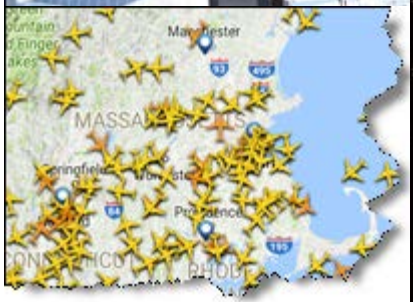
#RSAC

Applying IoT Analytics @ Scale

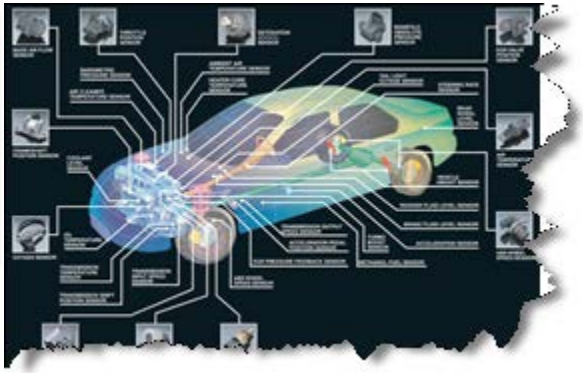
- Understand the 5 dimensions of IoT Analytics
- IoT Security Enclaves and “iZones”
- Developing IoT Volatility Monitoring Frameworks using VIX


DUBAI
SMART
CITY

Internet of Everything



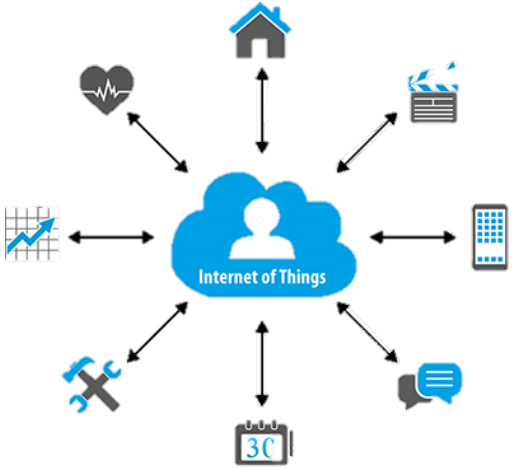
Flight Control Systems
Transit Systems
Home Devices
Health Devices



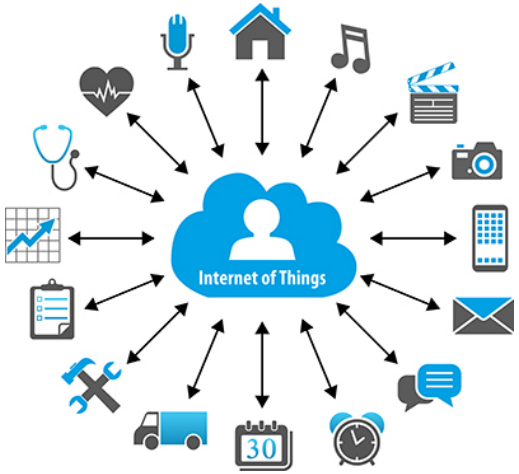
RSA

IoT Warmup – More Sensor Outputs Anyone?

6 bricks (8 studs) plus? = 915,103,765 combinations ++

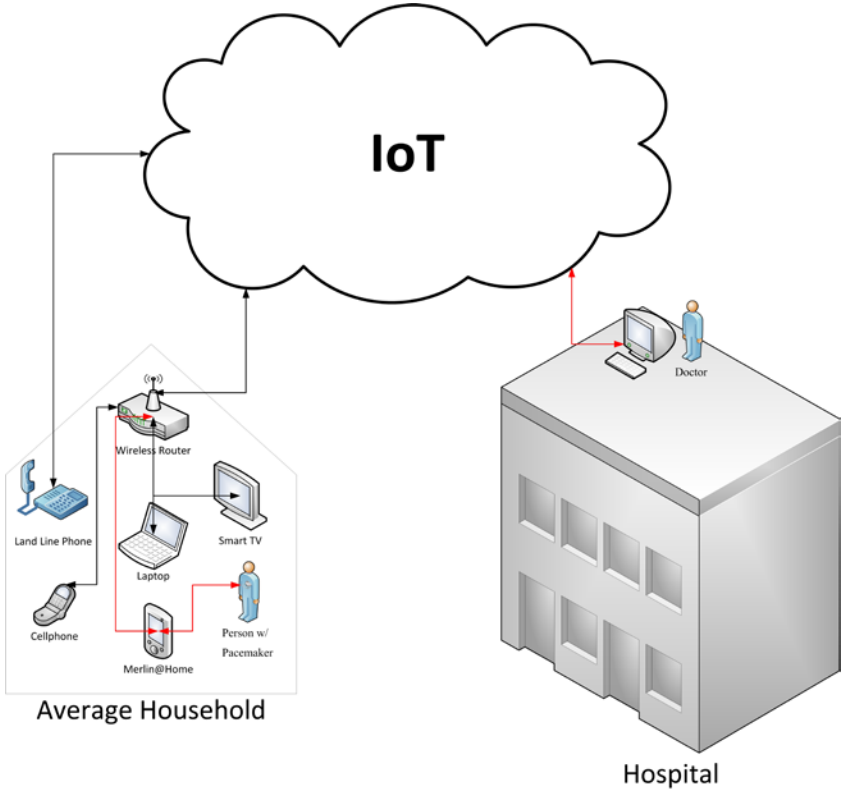


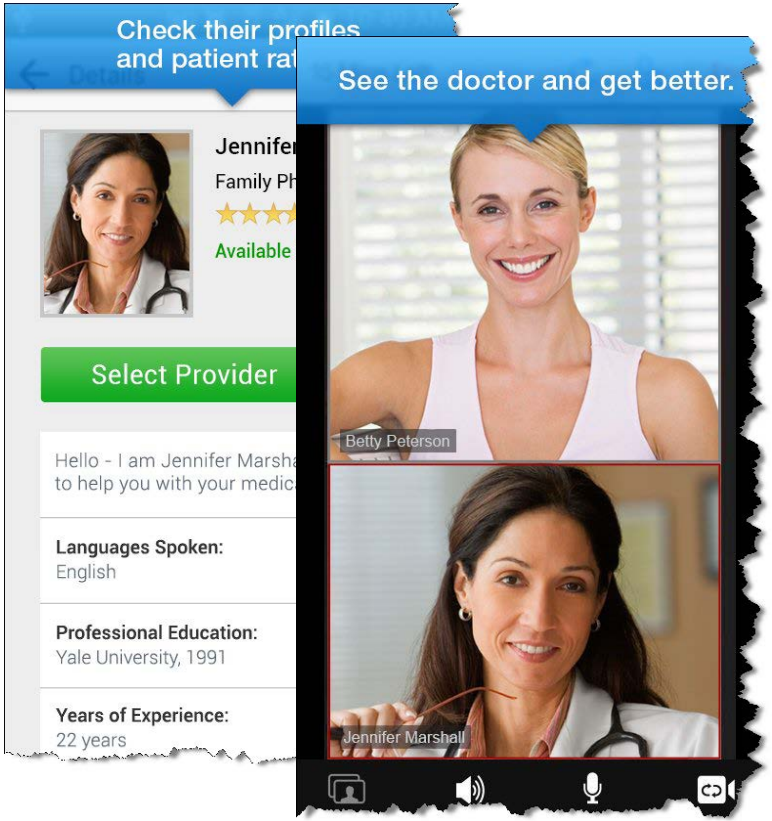
Currently ~22.9 Billion IoT Devices…



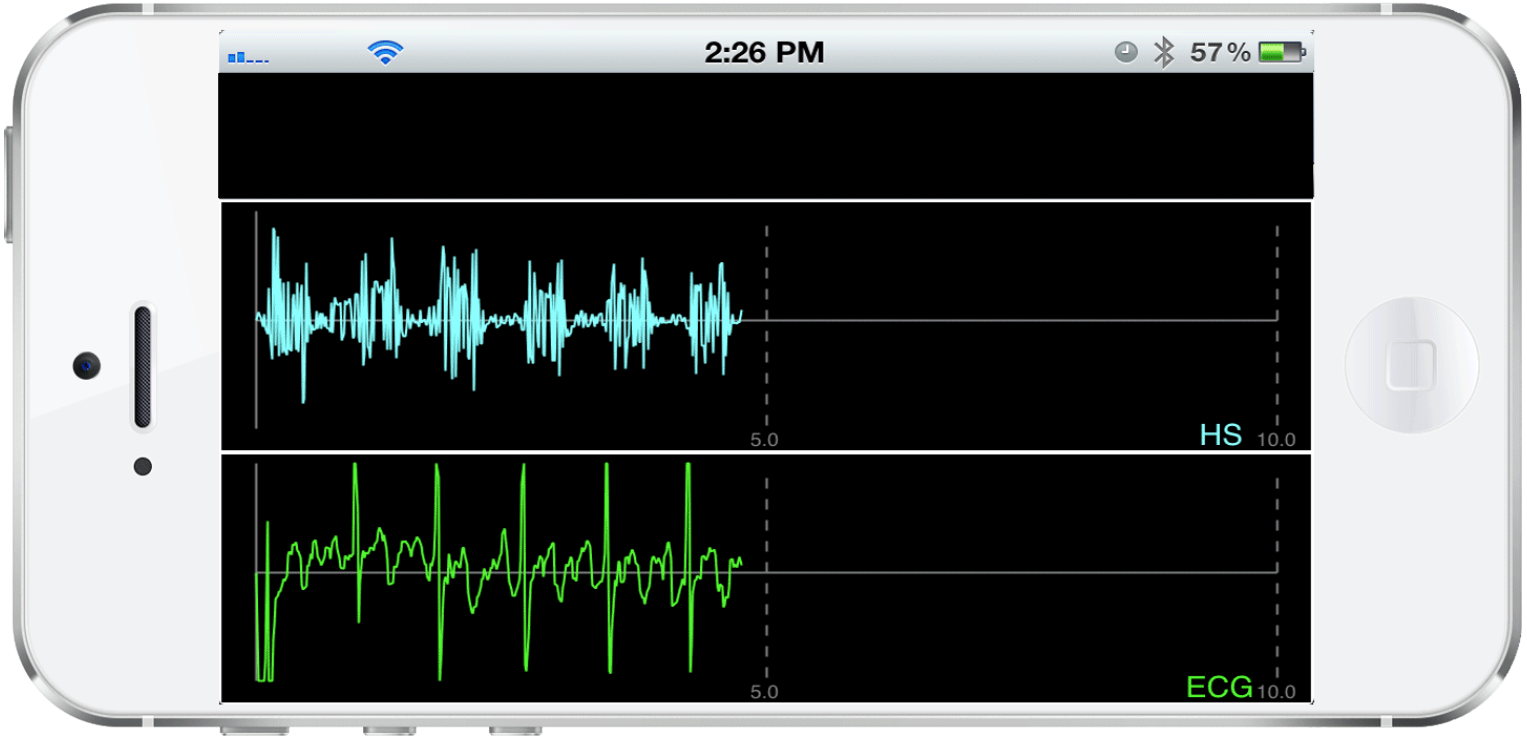
Estimated 50 Billion IoT Devices by 2020

Use Case 1: Connected Health

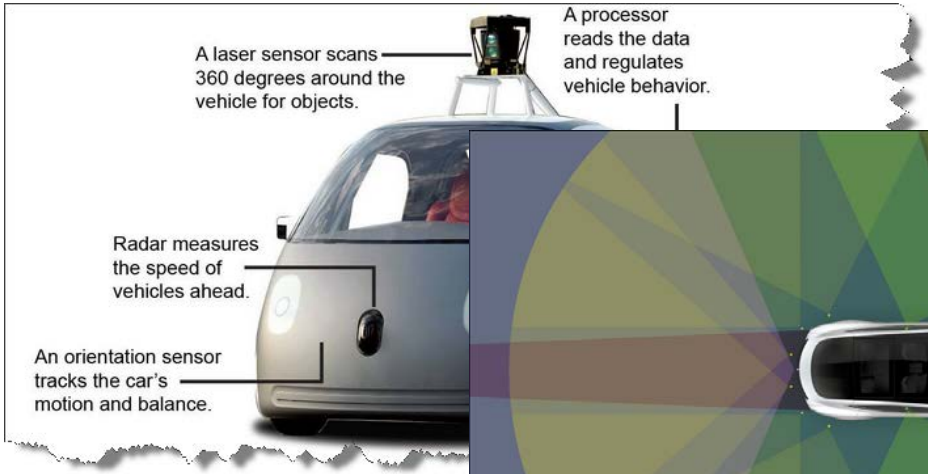




IoT Analytics- Signal to Noise….

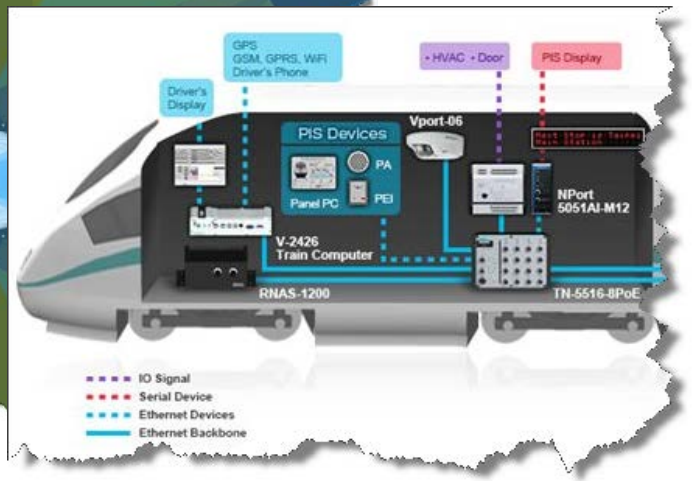


Use Case 2: Autonomous Transportation



Google Self Driving Car

Google Self Driving Car



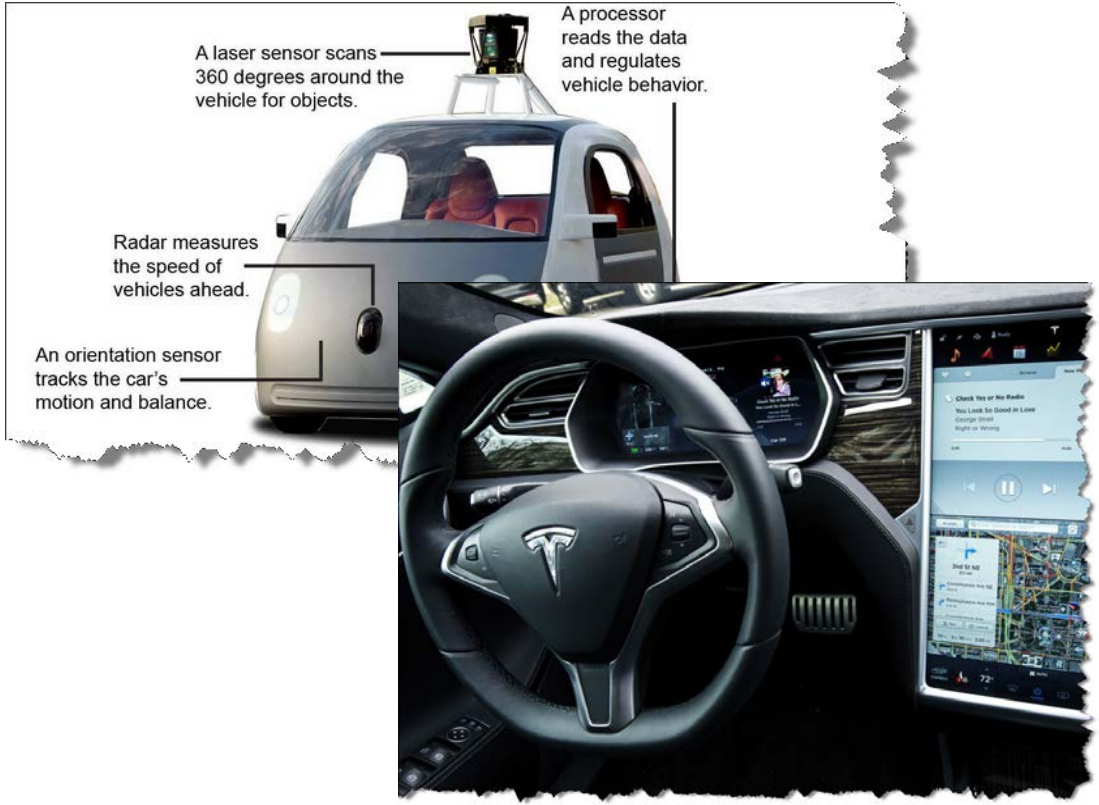
Autonomous Mass Transit

IP Enabled Automobiles

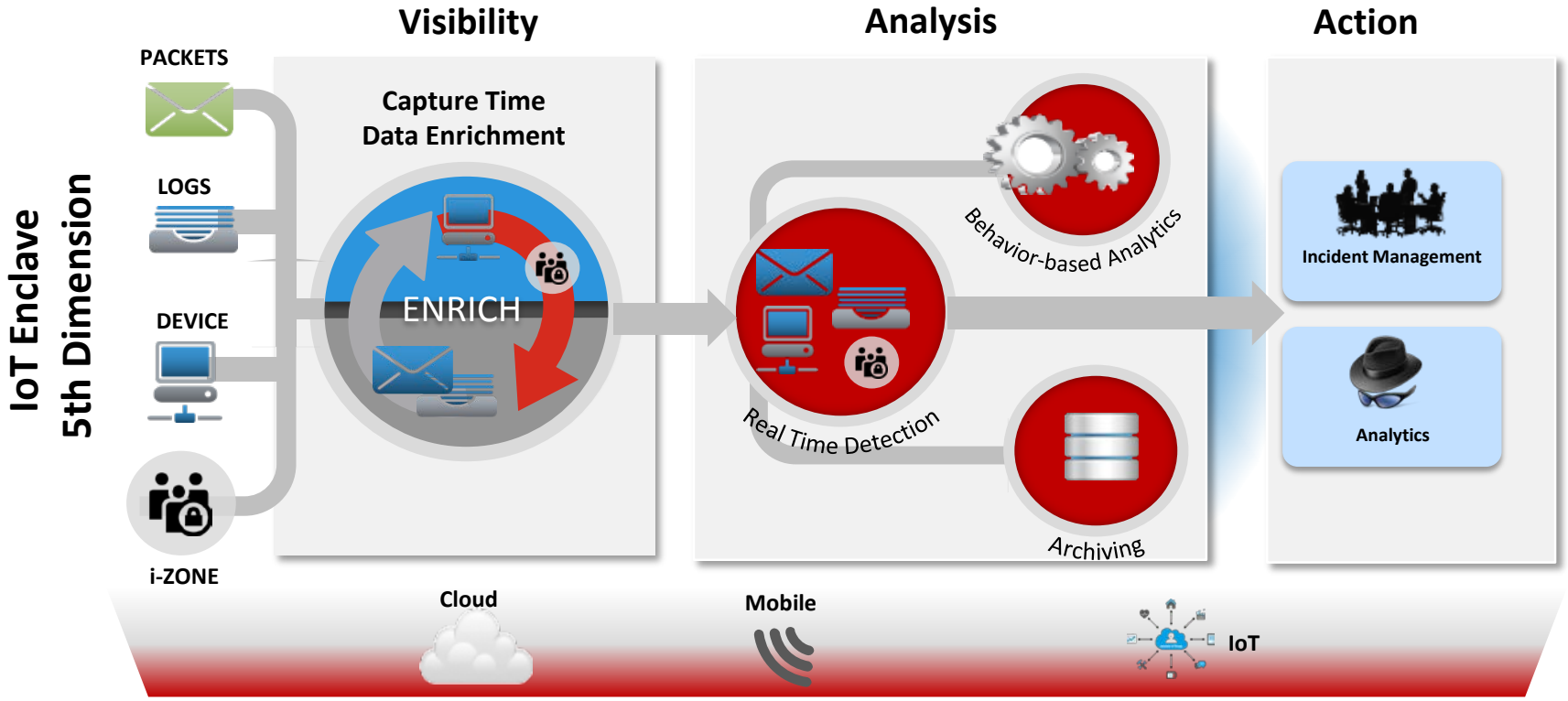
Musk is pledging that by the end of **2017, he'll produce a Tesla** that can **drive itself from Los Angeles to New York City, no human needed.**

That timeline **puts him years ahead of every other big player** working on fully autonomous cars.

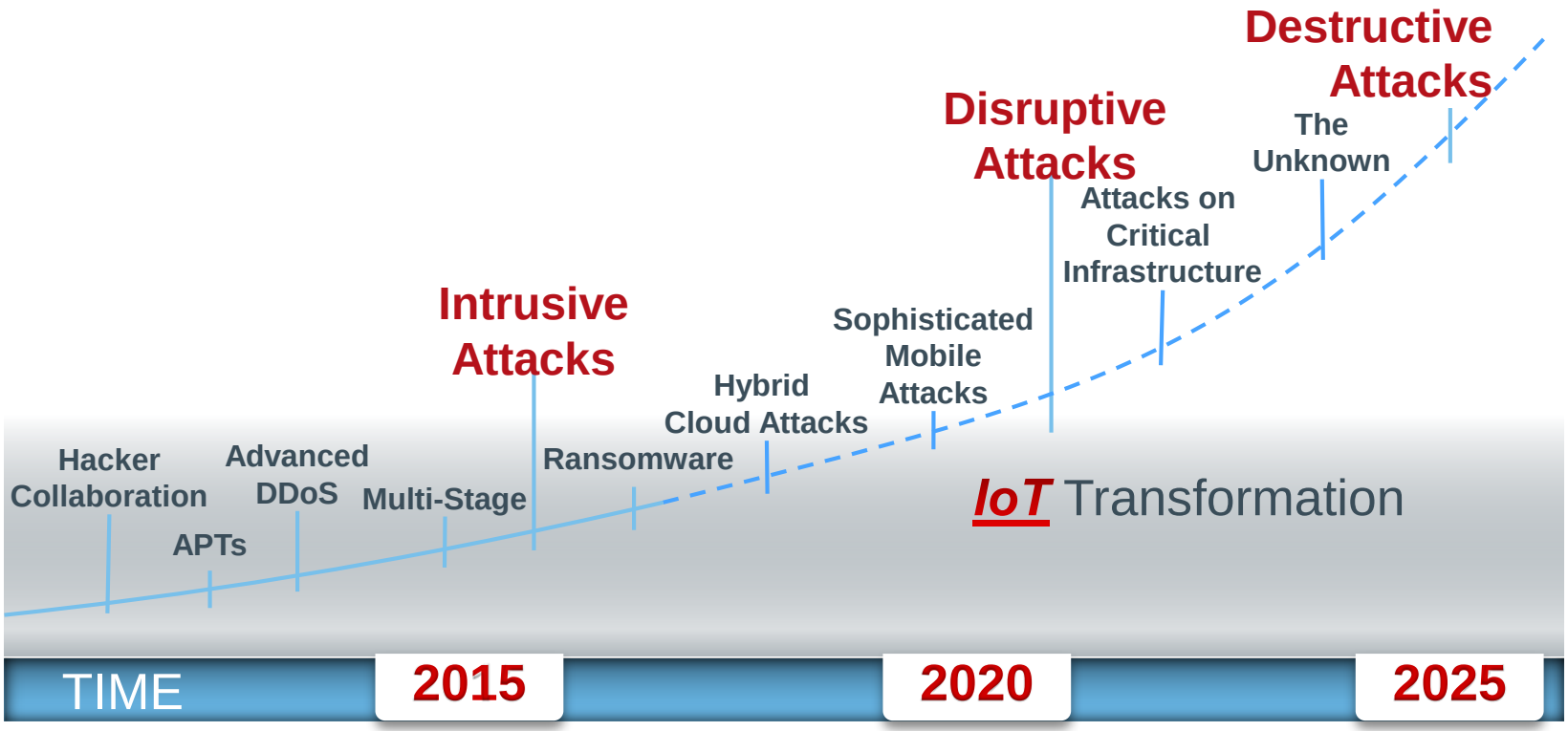
Ford is aiming for 2021, China's Baidu for 2019. Google and GM haven't given a hard date, but 2021 is a good bet.



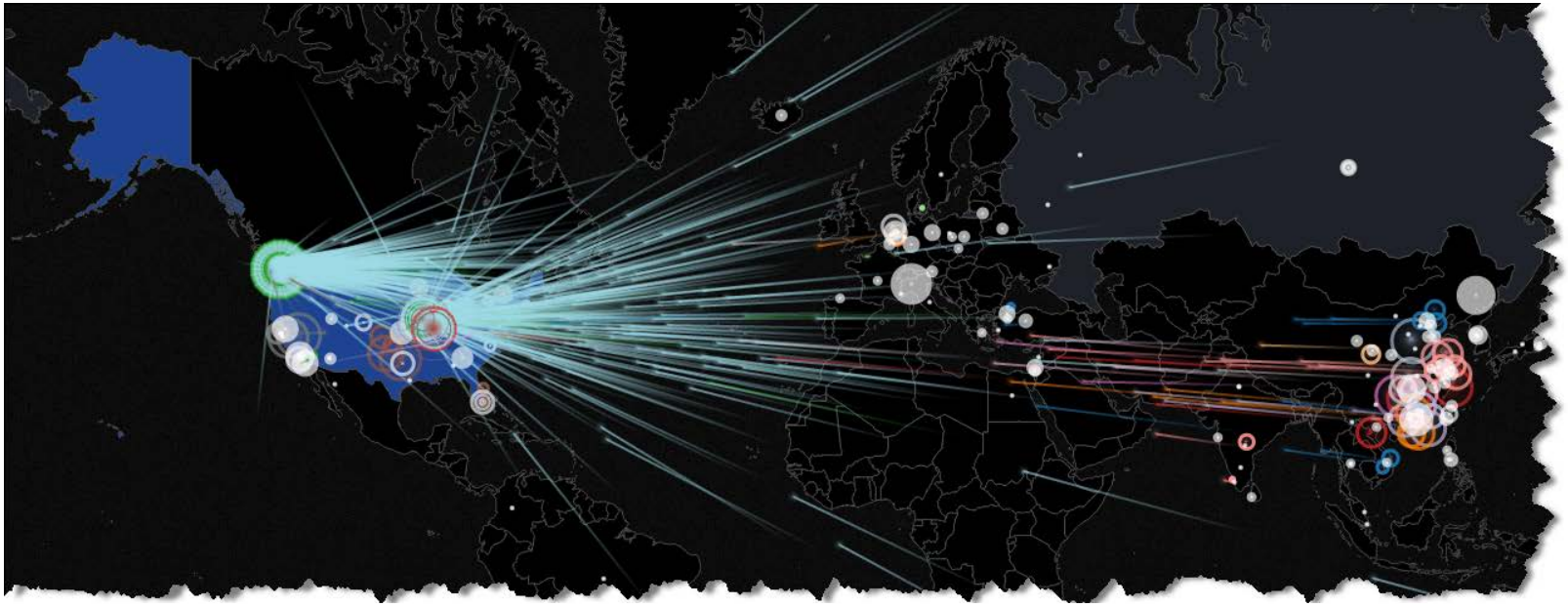
Analytics @ Scale – 5 Dimensions



IoT Attack Force Multiplier

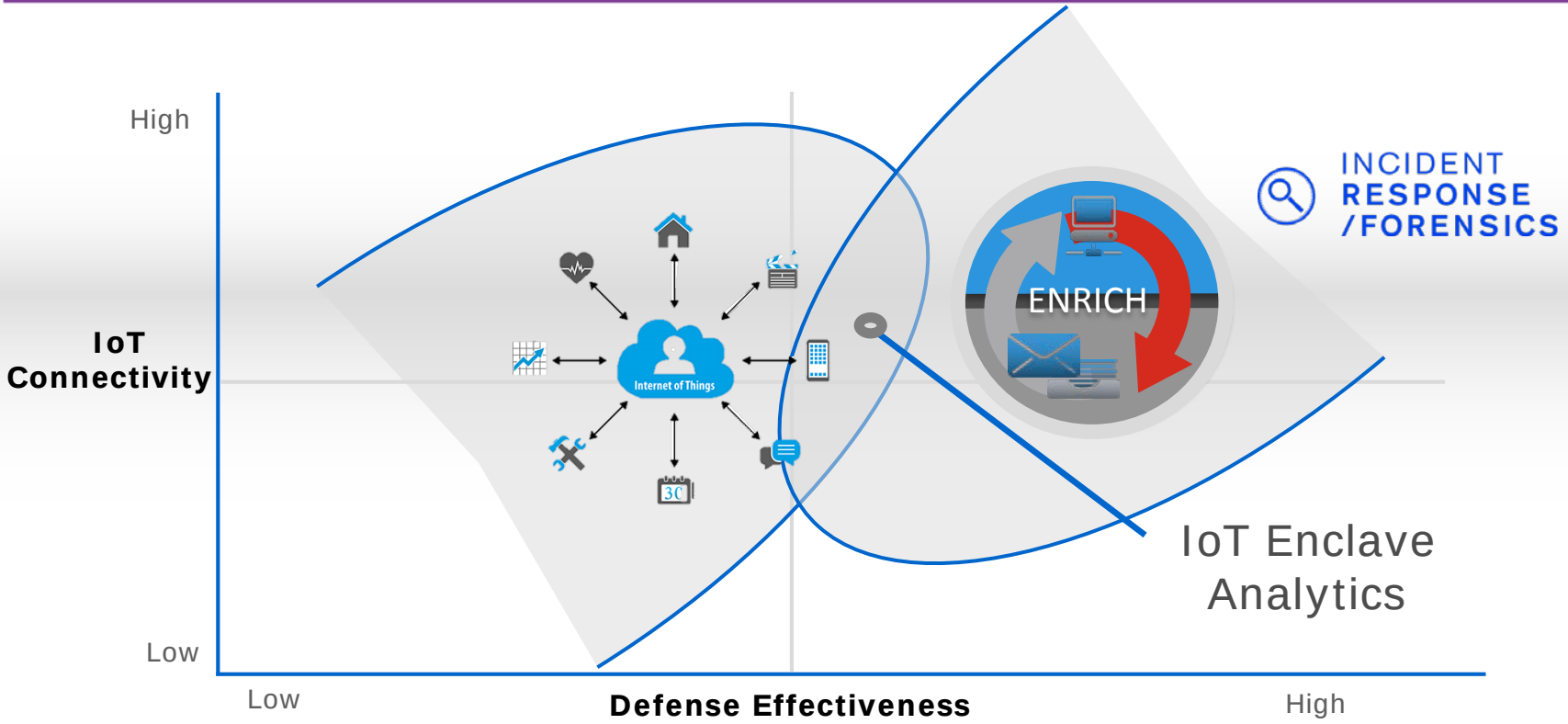


The DYN DDoS Attack Leveraging IoT

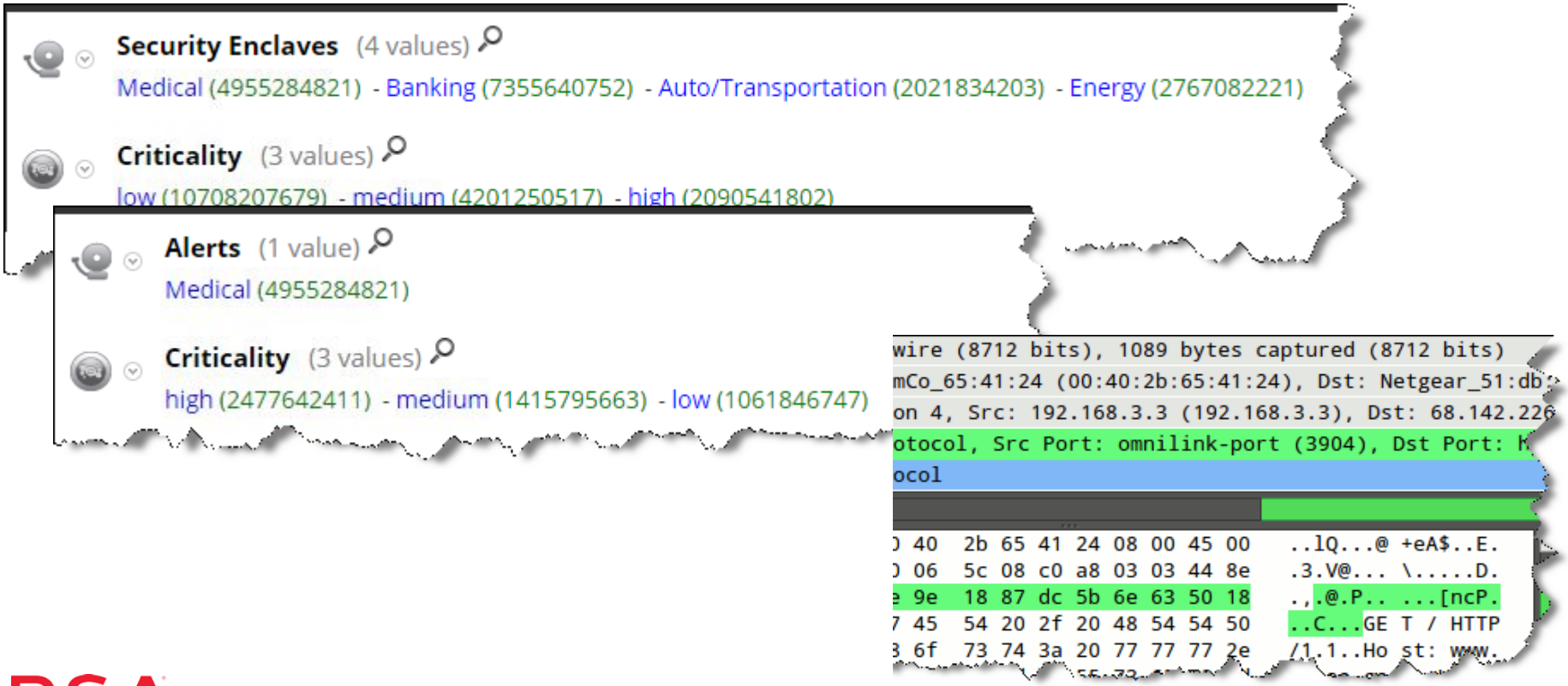


7AM	~9AM	~12PM	~1PM	~3PM
• First Attack Starts	• First Attack is Mitigated	• Second Attack Starts	• Second Attack is Mitigated	• Third attack starts and Is Immediately Mitigated

IoT Zone & Enclave Analytics



“iZones” and Enclaves



IoT and Volatility – Modeling with VIX

- **VIX** is a measure of expected volatility **calculated** as 100 times the square root of the expected variance (var) of a given data driven environment's rate of return. The variance is annualized and **VIX** expresses volatility/vulnerability in percentage points.
- The *higher the percentage points, the higher likelihood of potential vulnerability/exploitation*….

Cyber Economic VIX Formula

$$\sigma^2 = \frac{2}{T}\sum_i \frac{\Delta K_i}{K_i^2} e^{RT} Q(K_i) - \frac{1}{T}\left[\frac{F}{K_0} - 1\right]^2$$

Changes in IT Infrastructure

$$\sigma = \sqrt{\left\{\left(\frac{21{,}600}{525{,}600}\right) \times 0.066472 \times \left[\frac{61{,}920 - 43{,}200}{61{,}920 - 21{,}600}\right] + \left(\frac{61{,}920}{525{,}600}\right) \times 0.063667 \times \left[\frac{43{,}200 - 21{,}600}{61{,}920 - 21{,}600}\right]\right\} \times \frac{525{,}600}{43{,}200}}$$

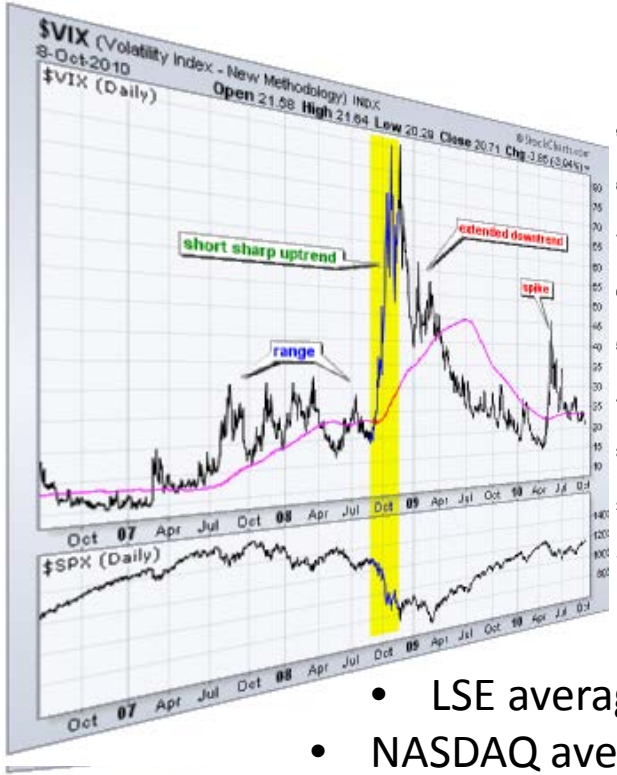
$$\sigma = 0.253610$$

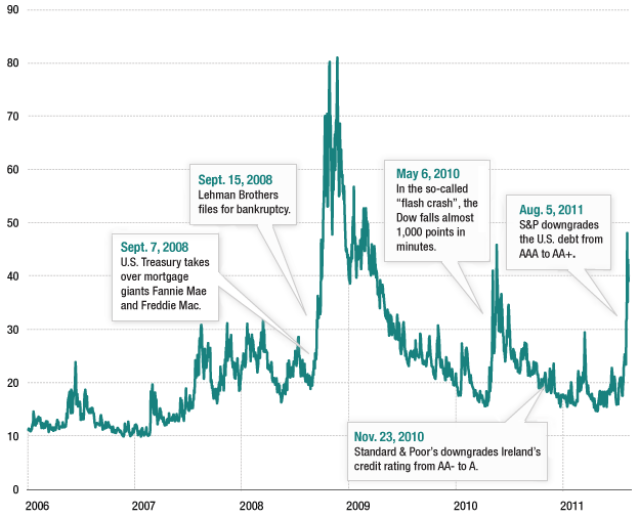
Mergers & Acquisitions

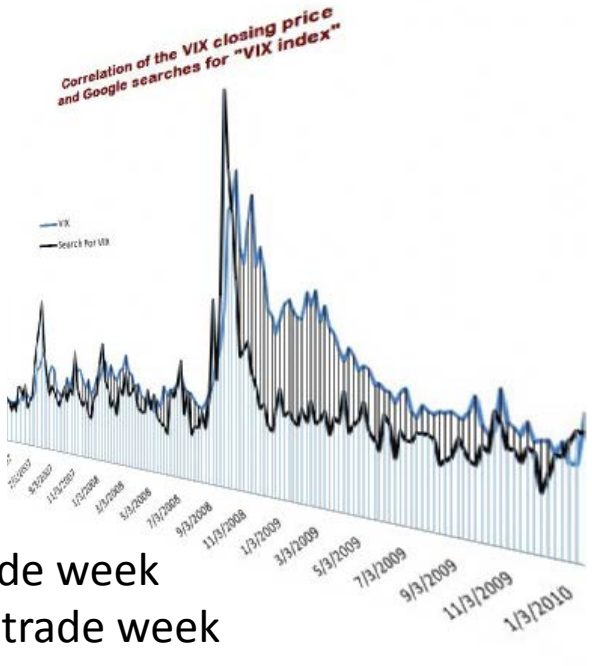
$$VIX = 100 \times \sigma = 25.36$$

Threat Intelligence

VIX – Volatility Predictors @ Scale

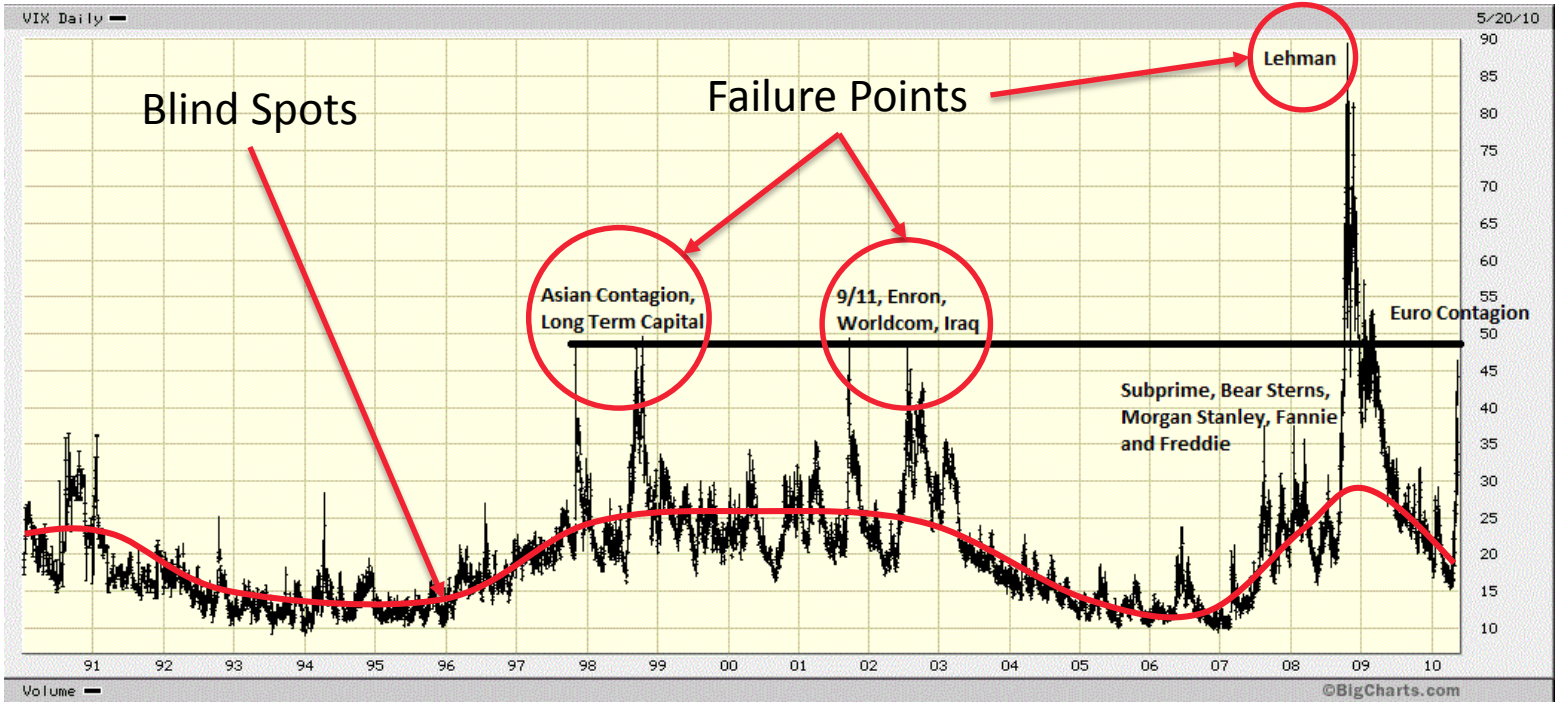




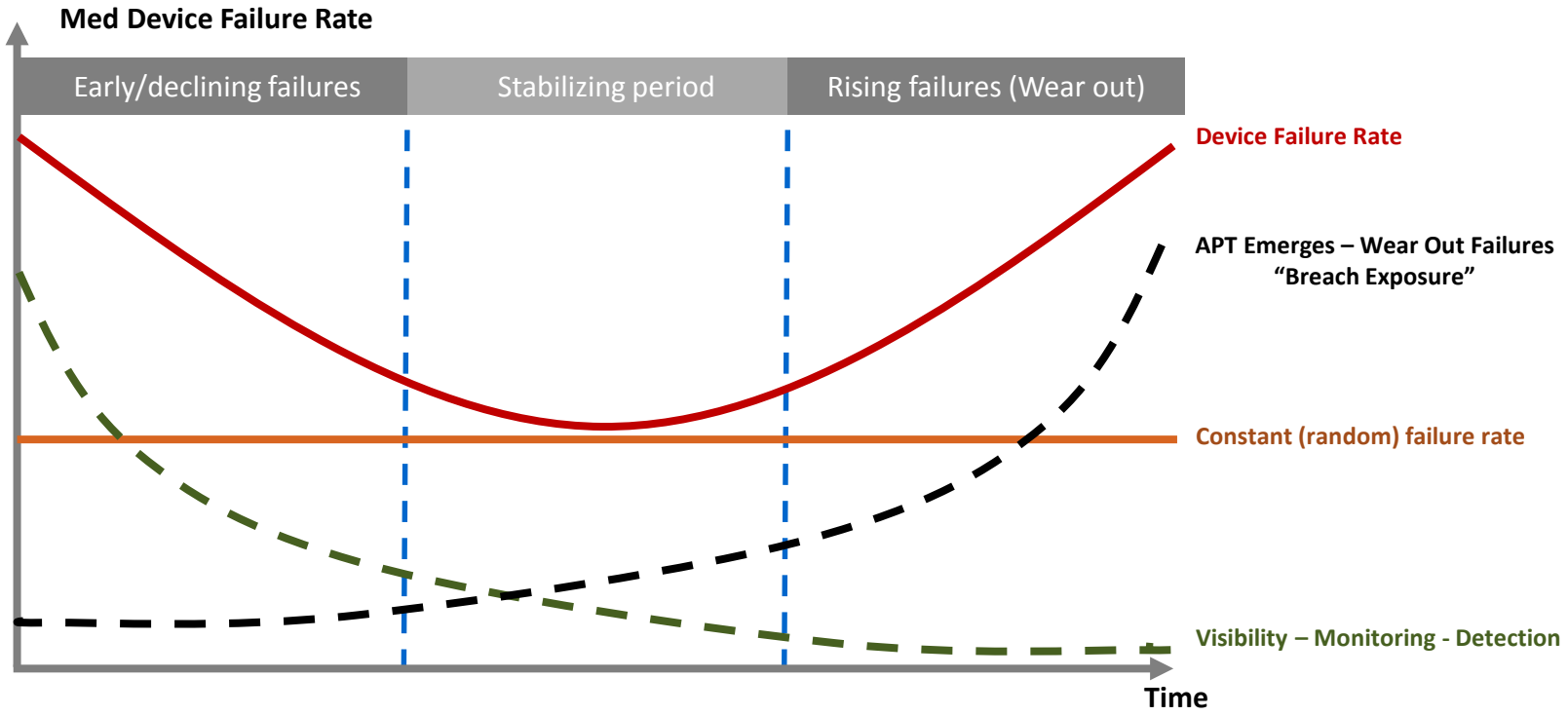


- LSE averages 5 billion transactions per trade week
- NASDAQ averages 7.5 billion transaction per trade week

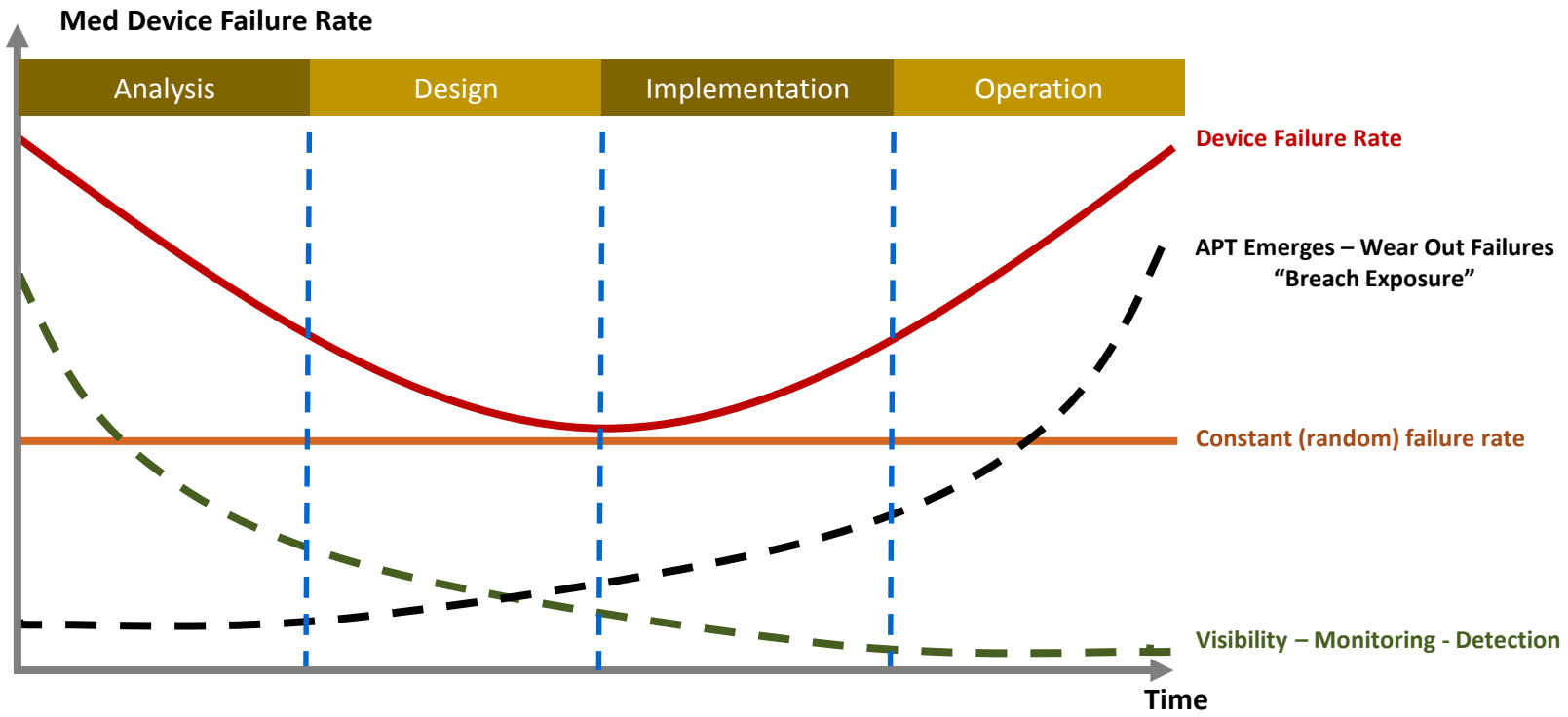
VIX – A Closer Look



Device Analytics: “The VIX Test”



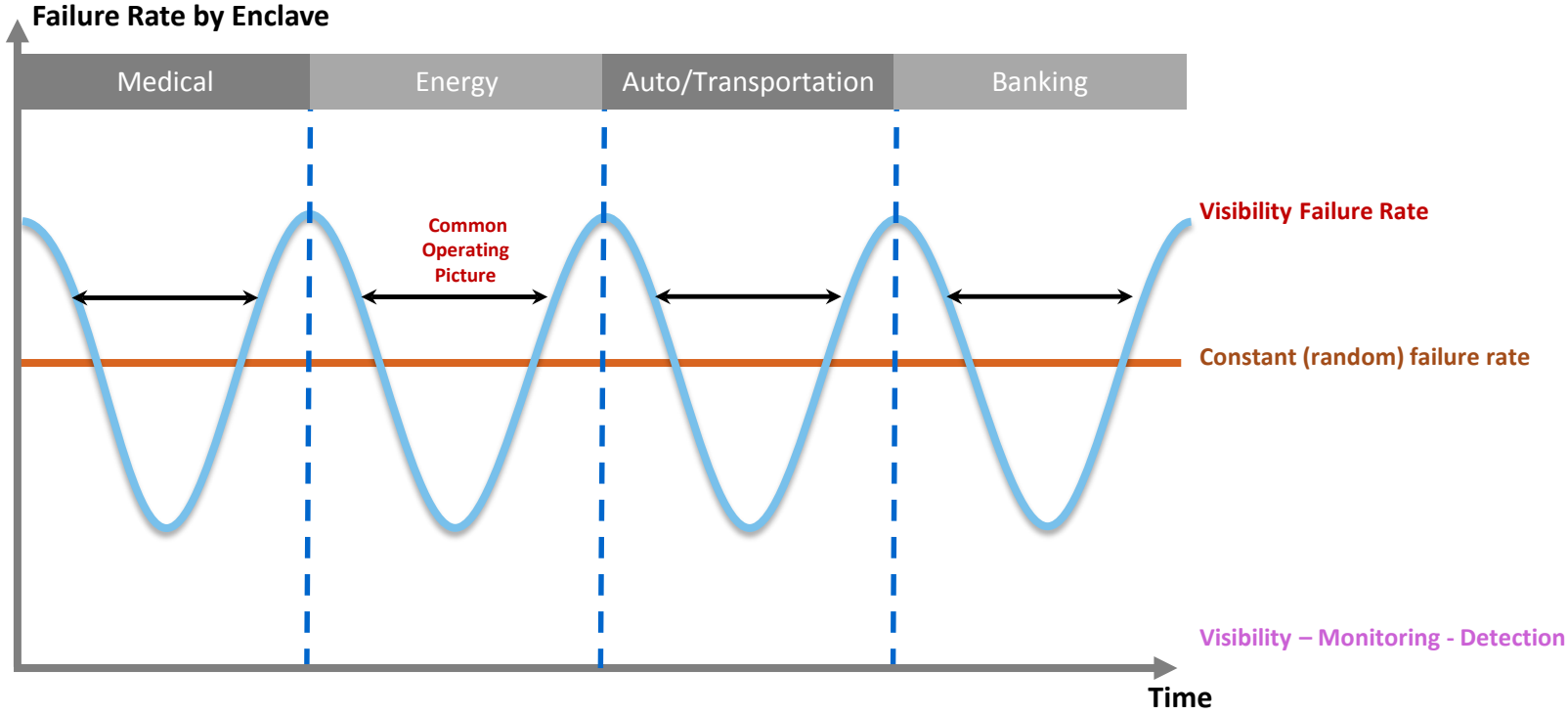
IoT Device Volatility: iZones and Enclaves



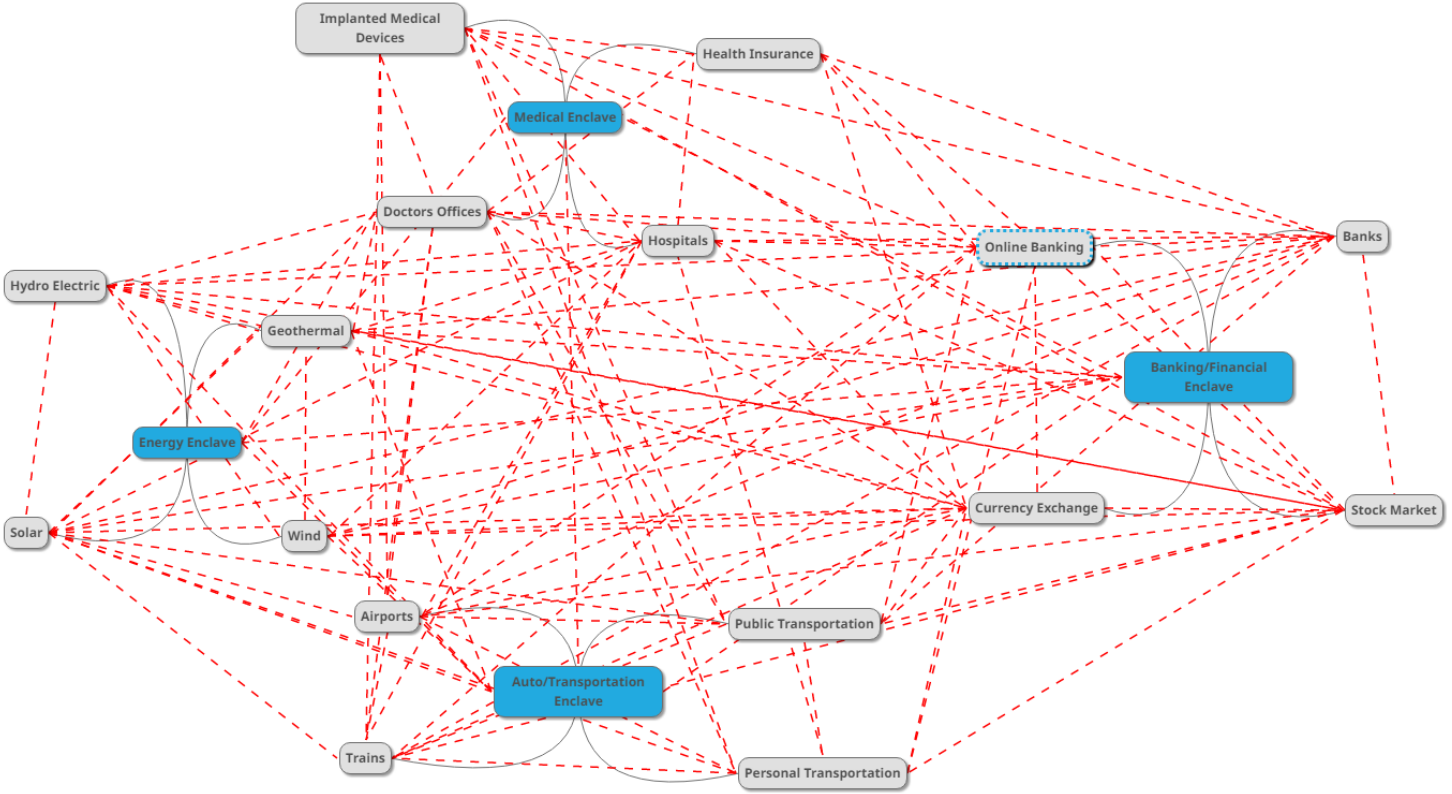
Volatility & Failures

- 747 Engine Resiliency (Length of life) ~ 30 years.
- Average flight hours for 2 million miles/year with average speed of 600 mph * 30 years = ~4,165 days or almost 100,000 hours of flight time over the course of its life.
- Failure Rate – 27 total-engine failures since 1953 (~0.42 failures per year over last 63 years.

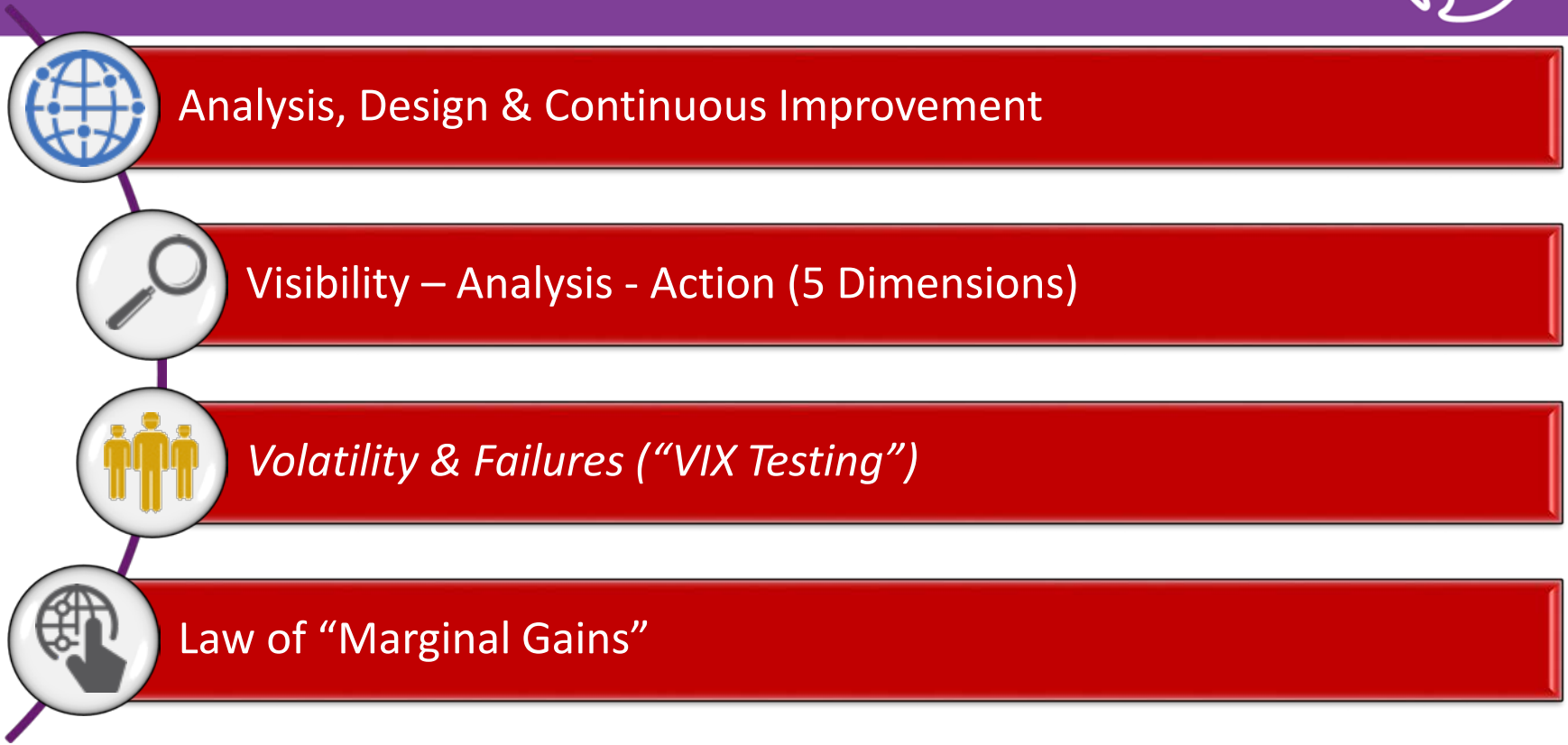
@ Scale: “Continuous Visibility”



Enclave Relationships



CRITICAL SUCCESS FACTORS



Thank You