

# RSA<sup>®</sup>Conference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: CCS-T07

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



#RSAC



Connect **to**  
Protect

**Peter Tran**

Sr. Director- Advanced Cyber Defense  
RSA Security  
**@breachreadiness**

# 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

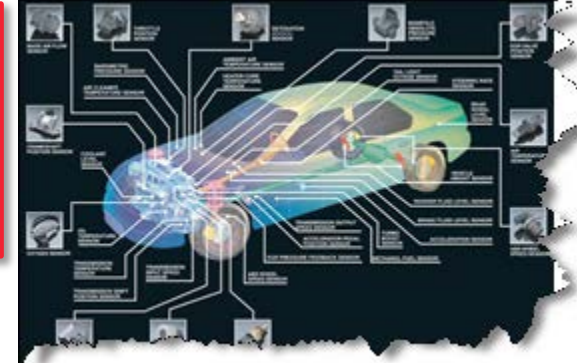


# Internet of Everything

#RSAC



Flight Control Systems  
Transit Systems  
Home Devices  
Health Devices

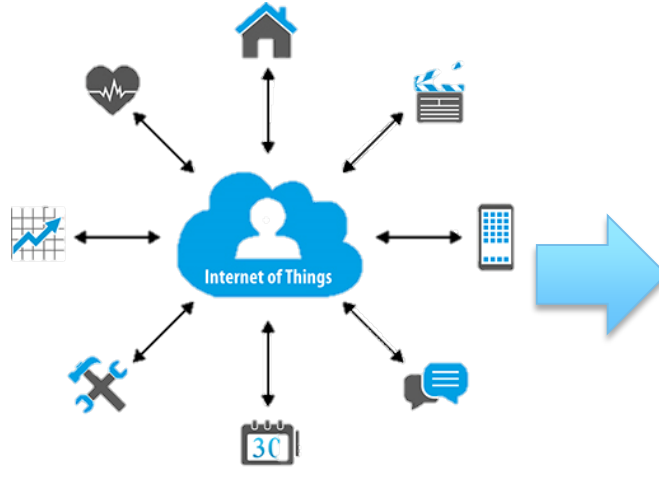




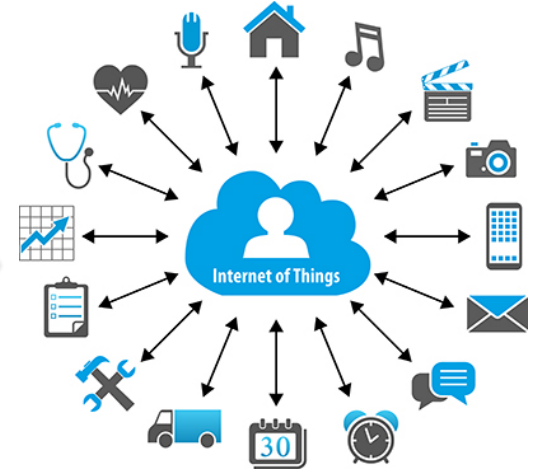
# IoT Warmup – More Sensor Outputs Anyone?



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

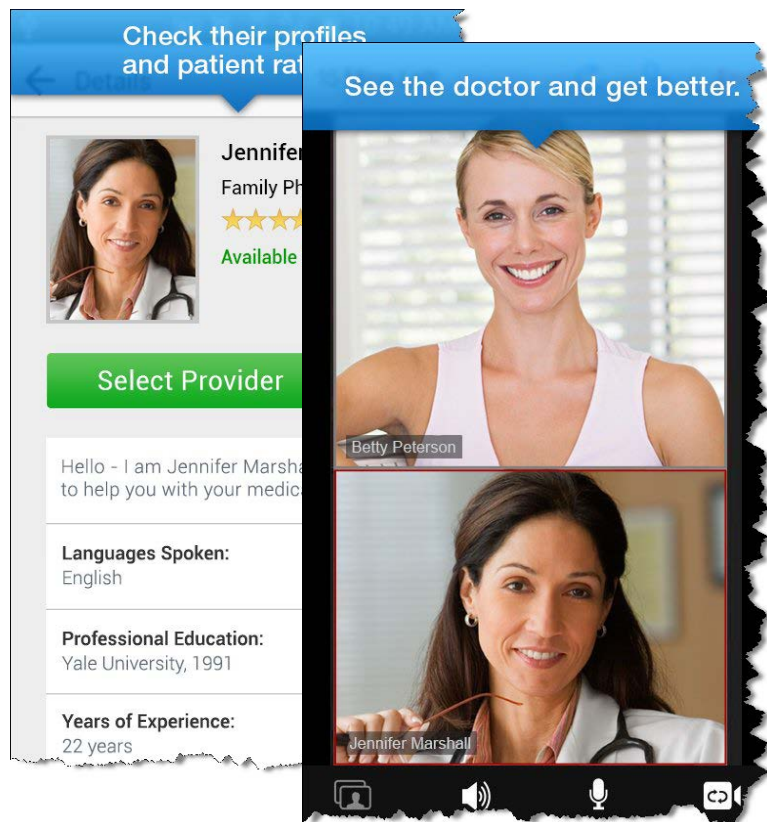
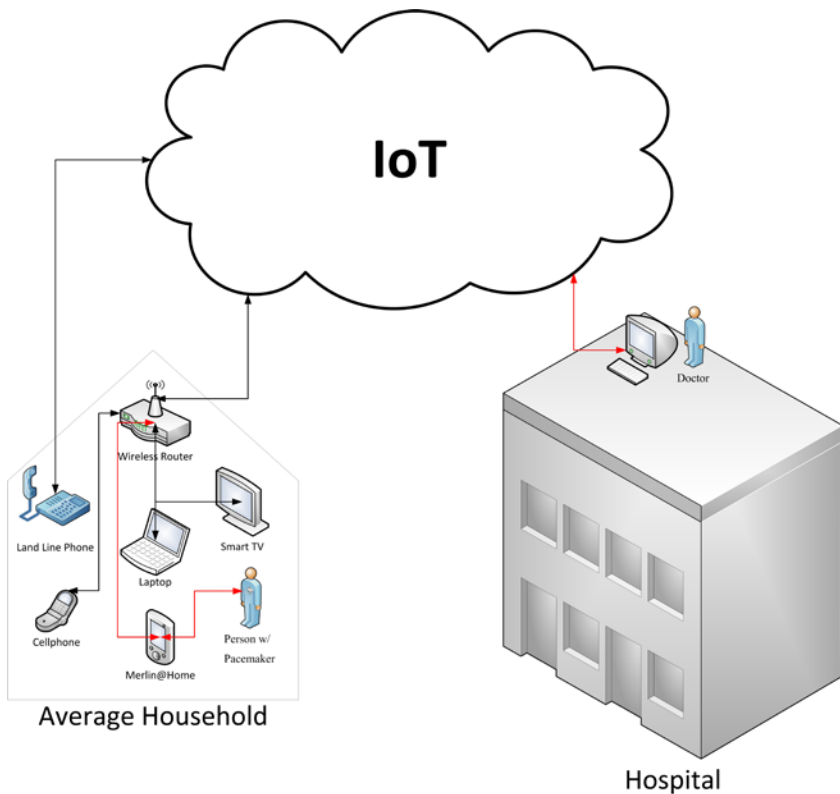


*Currently ~22.9  
Billion IoT  
Devices...*

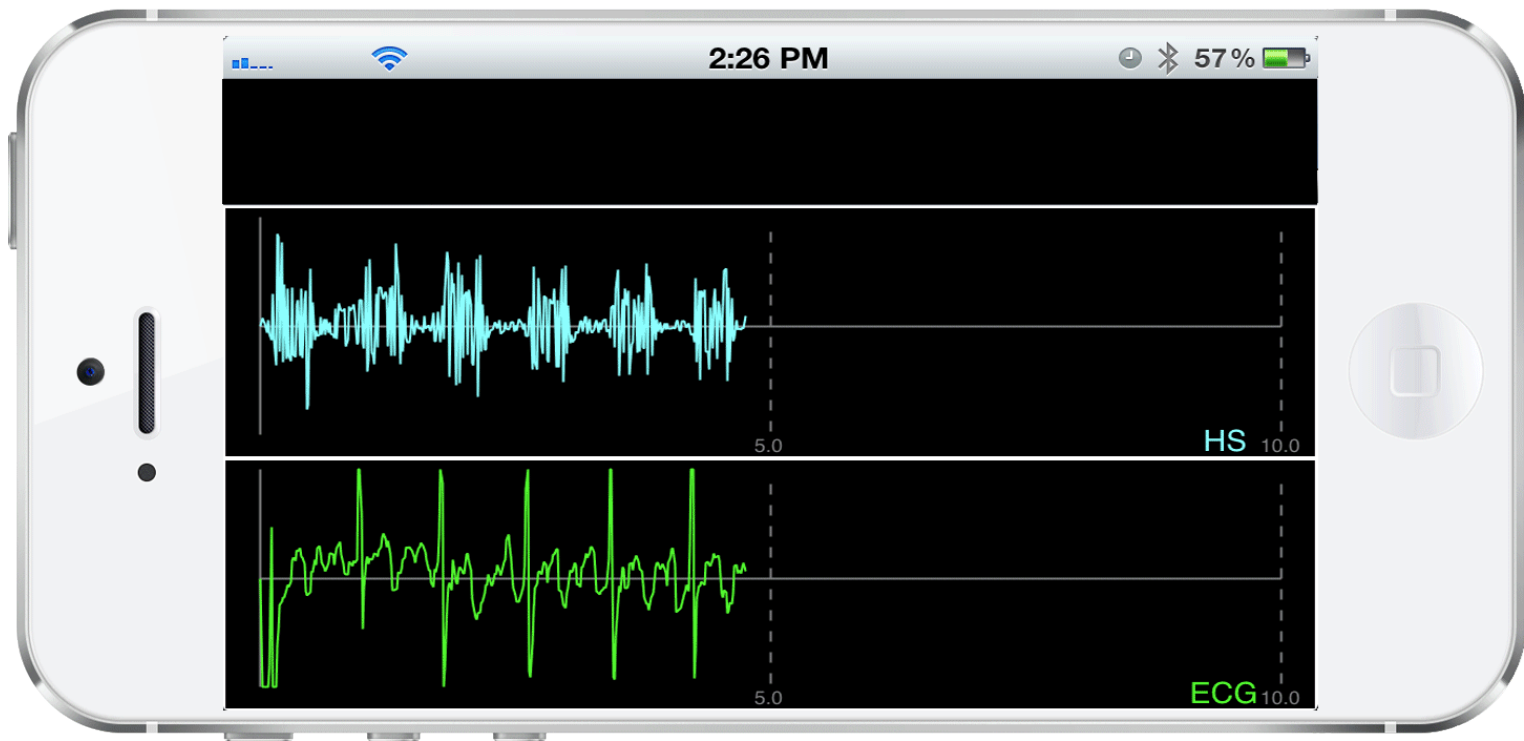


*Estimated 50  
Billion IoT Devices  
by 2020*

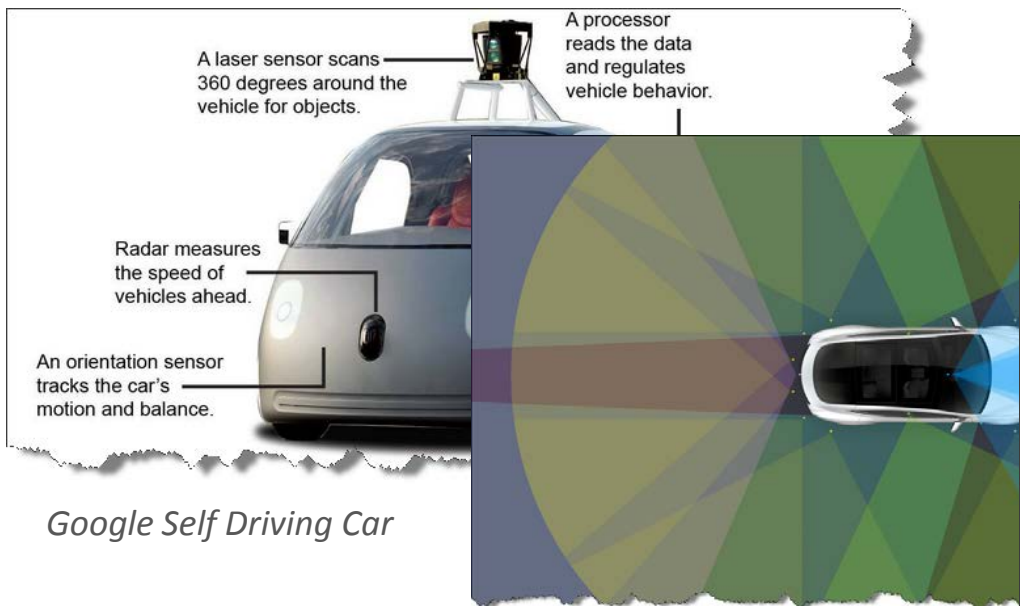
# Use Case 1: Connected Health



# IoT Analytics- Signal to Noise....

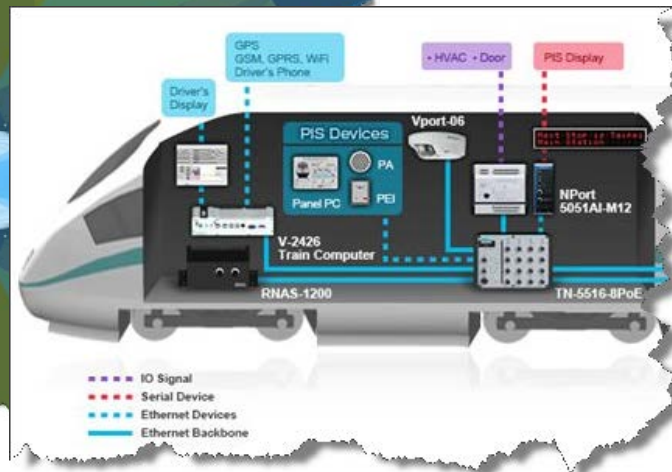


# Use Case 2: Autonomous Transportation



Google Self Driving Car

Google Self Driving Car



Autonomous Mass Transit



# IP Enabled Automobiles

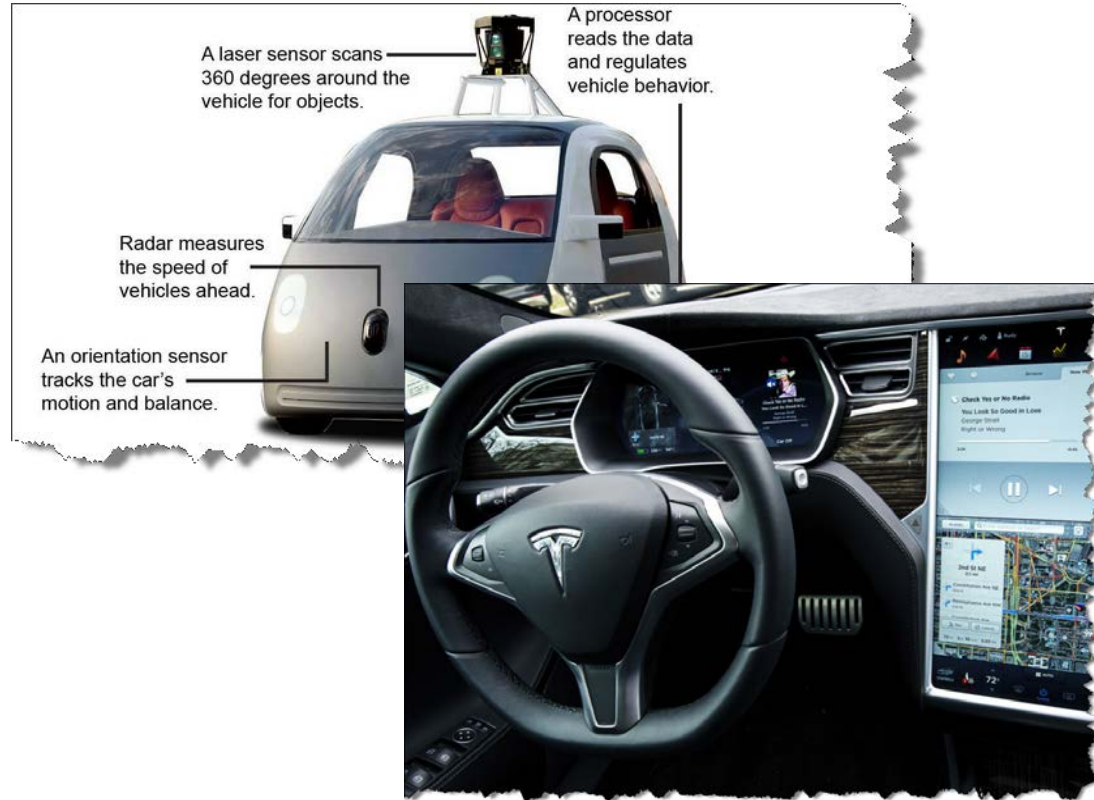
#RSAC



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.

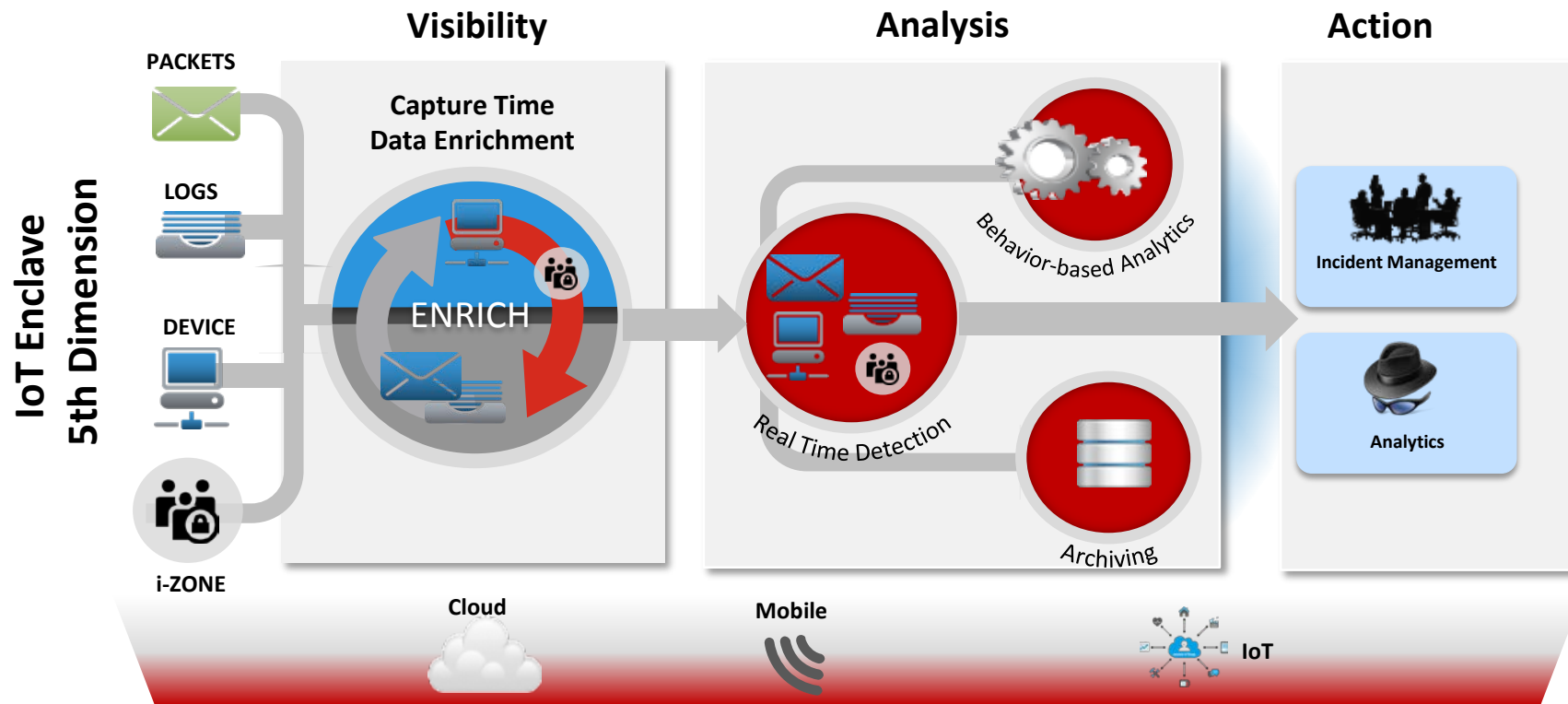
That timeline puts him years ahead of every other big player working on fully autonomous cars.

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.

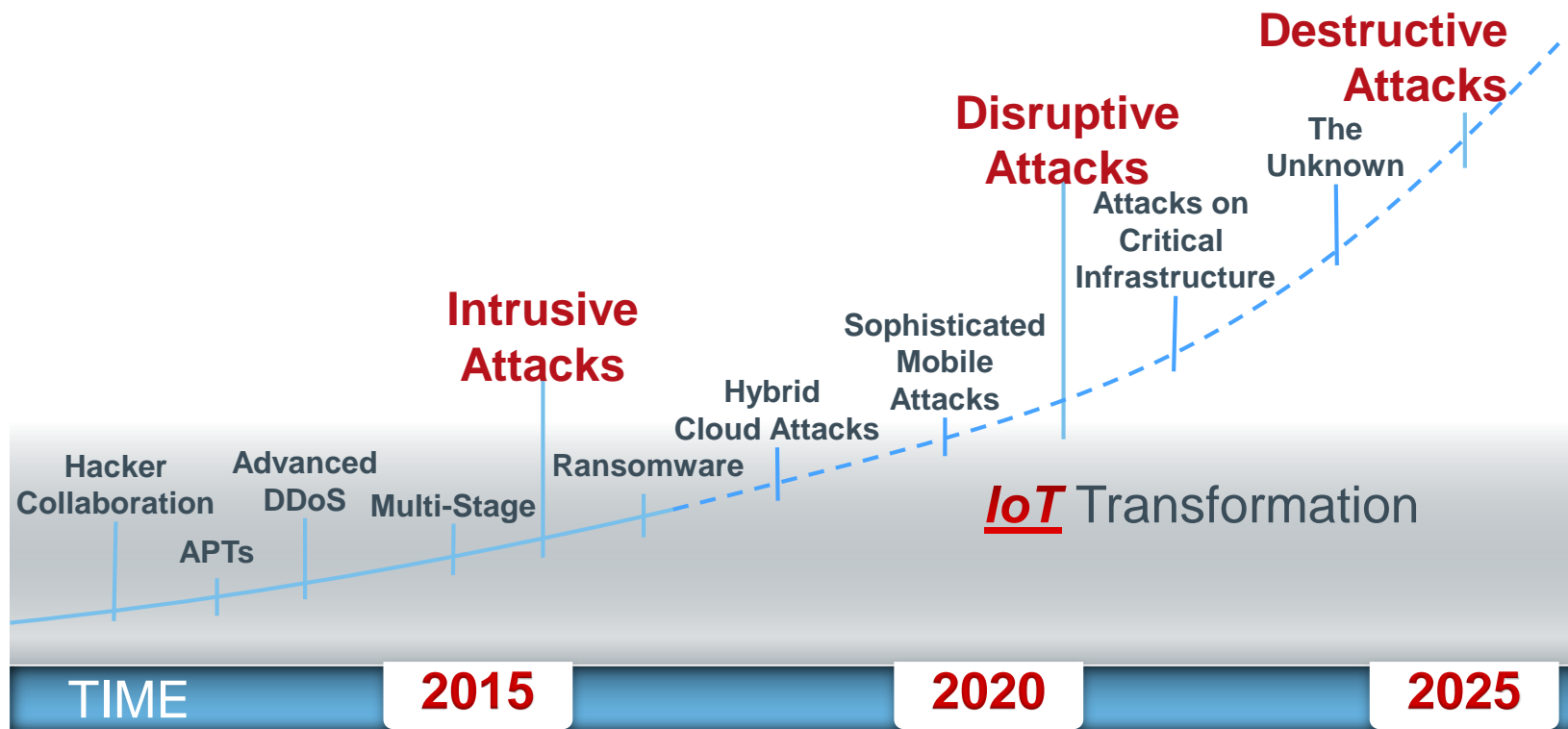


# Analytics @ Scale – 5 Dimensions

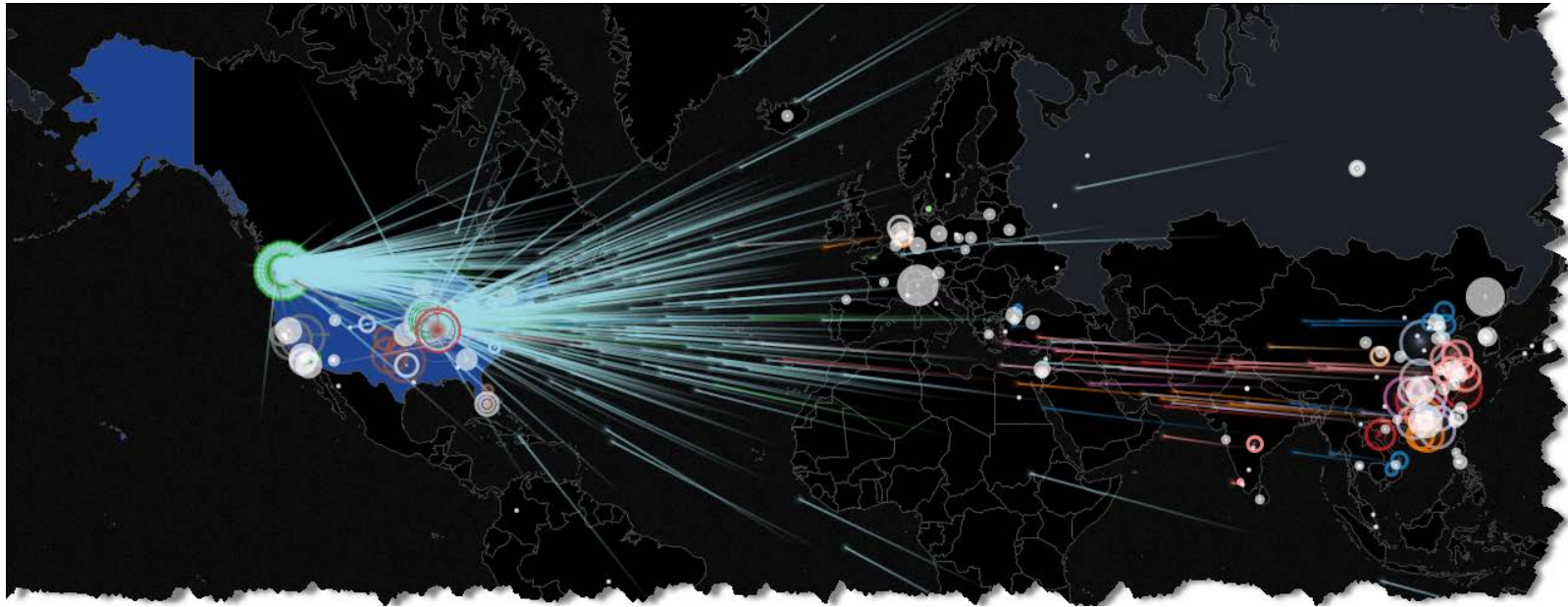
#RSAC



# 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

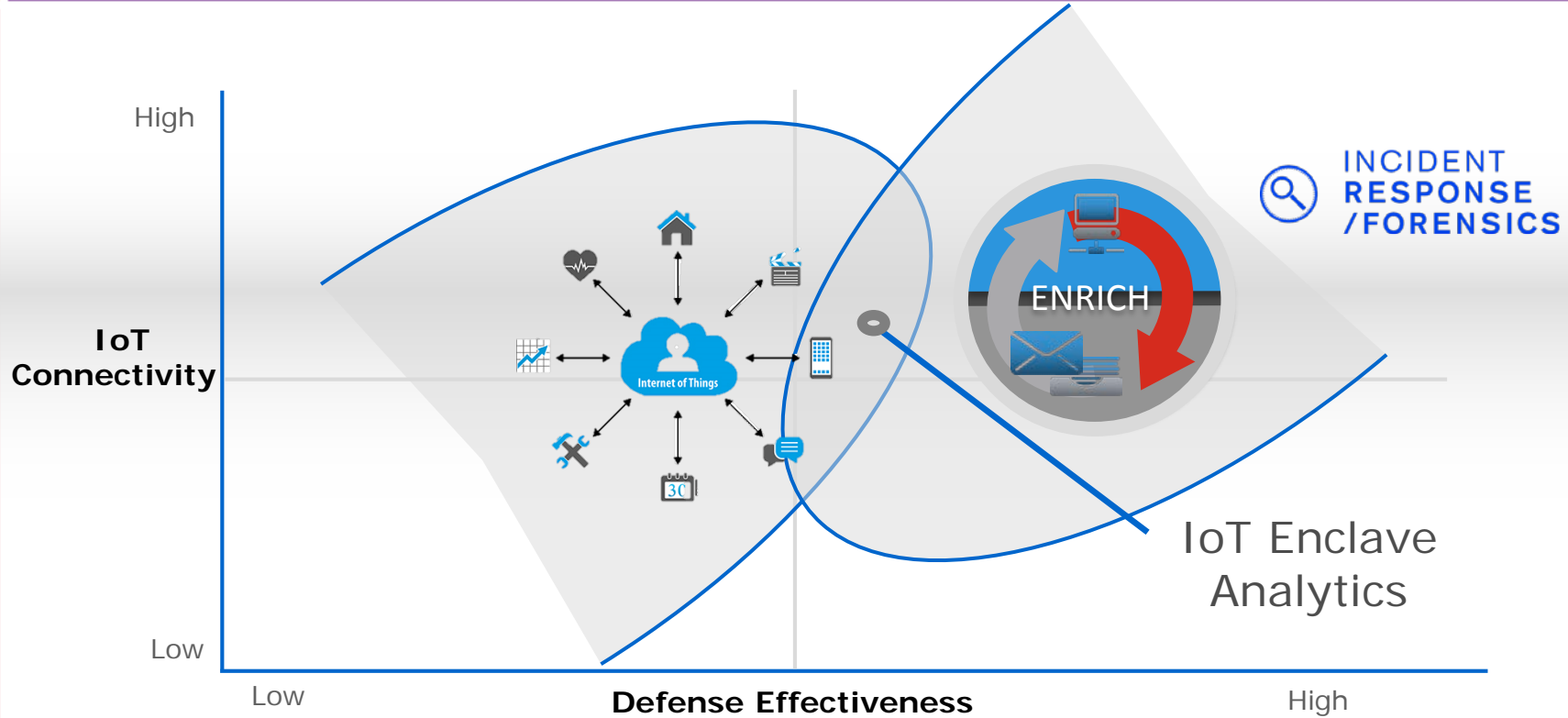
- Second Attack is Mitigated

- Third attack starts and Is Immediately Mitigated

**RSA**

RSAConference2016 Abu Dhabi

# IoT Zone & Enclave Analytics





# “iZones” and Enclaves

## Security Enclaves (4 values)

Medical (4955284821) - Banking (7355640752) - Auto/Transportation (2021834203) - Energy (2767082221)

## Criticality (3 values)

low (10708207679) - medium (4201250517) - high (2090541802)

## Alerts (1 value)

Medical (4955284821)

## Criticality (3 values)

high (2477642411) - medium (1415795663) - low (1061846747)

wire (8712 bits), 1089 bytes captured (8712 bits)  
mCo\_65:41:24 (00:40:2b:65:41:24), Dst: Netgear\_51:db  
on 4, Src: 192.168.3.3 (192.168.3.3), Dst: 68.142.226

Protocol, Src Port: omnalink-port (3904), Dst Port: K  
ocol

```

0 40 2b 65 41 24 08 00 45 00  ..lQ...@ +eA$..E.
0 06 5c 08 c0 a8 03 03 44 8e  .3.V@... \.....D.
e 9e 18 87 dc 5b 6e 63 50 18  ..,.@.P... ..[ncP.
7 45 54 20 2f 20 48 54 54 50  ..C...GE T / HTTP
3 6f 73 74 3a 20 77 77 77 2e  /1.1..Ho st: www.

```

- **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

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

$$\sigma = 0.253610$$

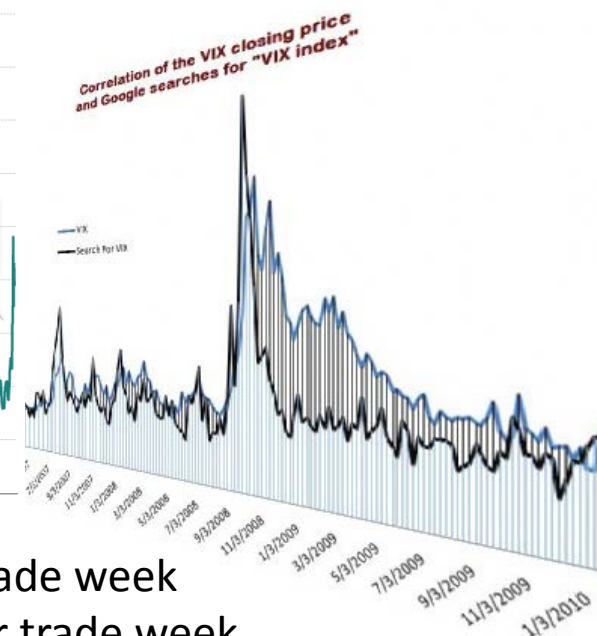
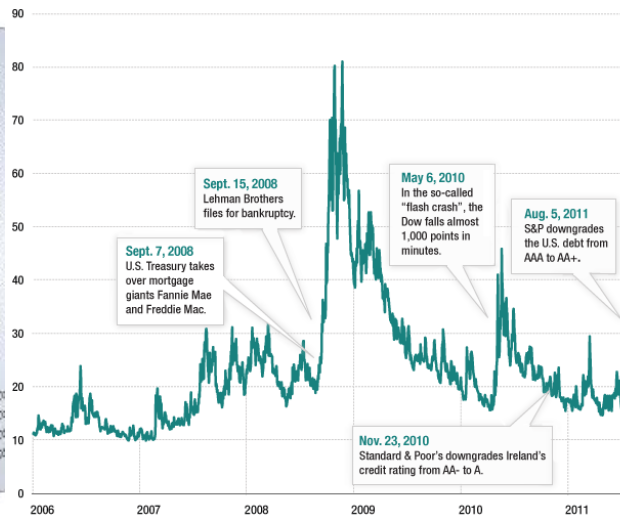
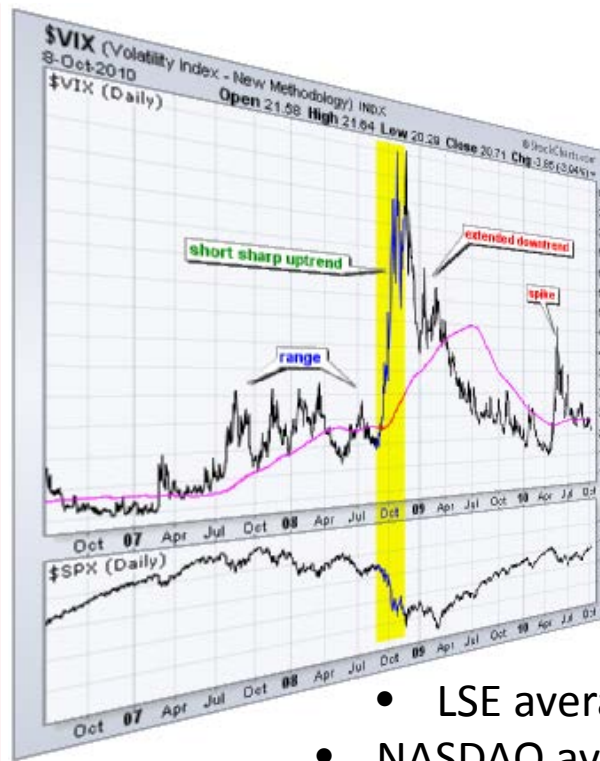
Mergers &  
Acquisitions

$$\text{VIX} = 100 \times \sigma = 25.36$$

Threat Intelligence

# VIX – Volatility Predictors @ Scale

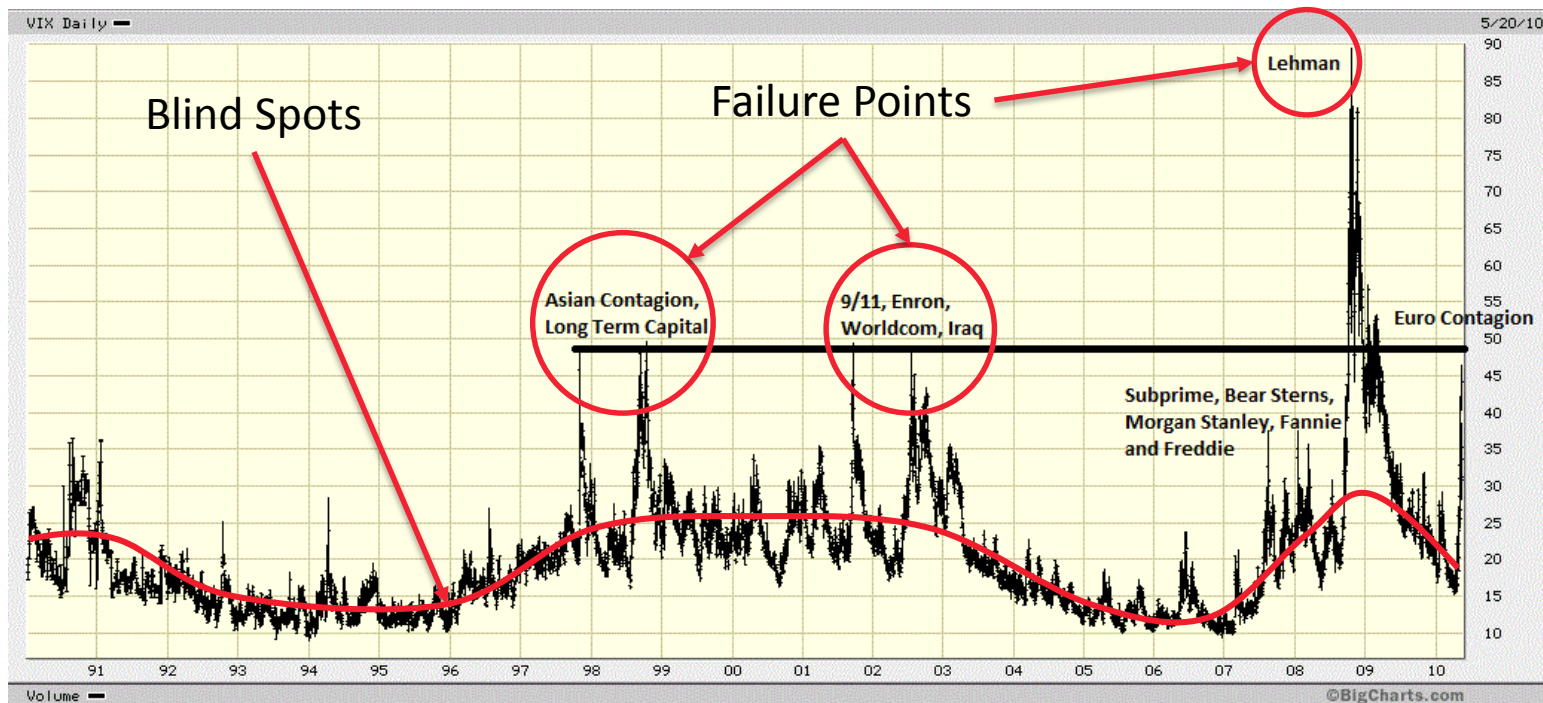
#RSAC



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

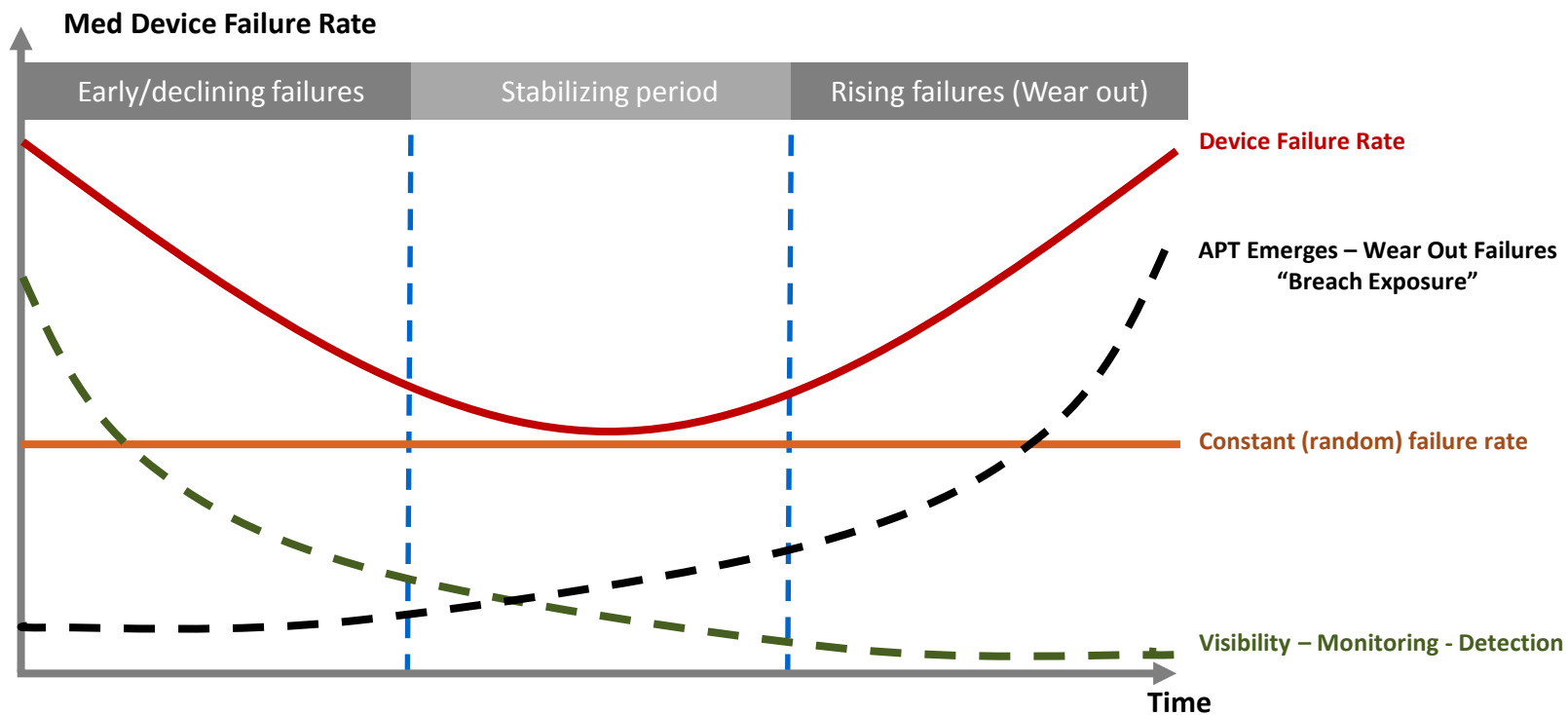
# VIX – A Closer Look

#RSAC

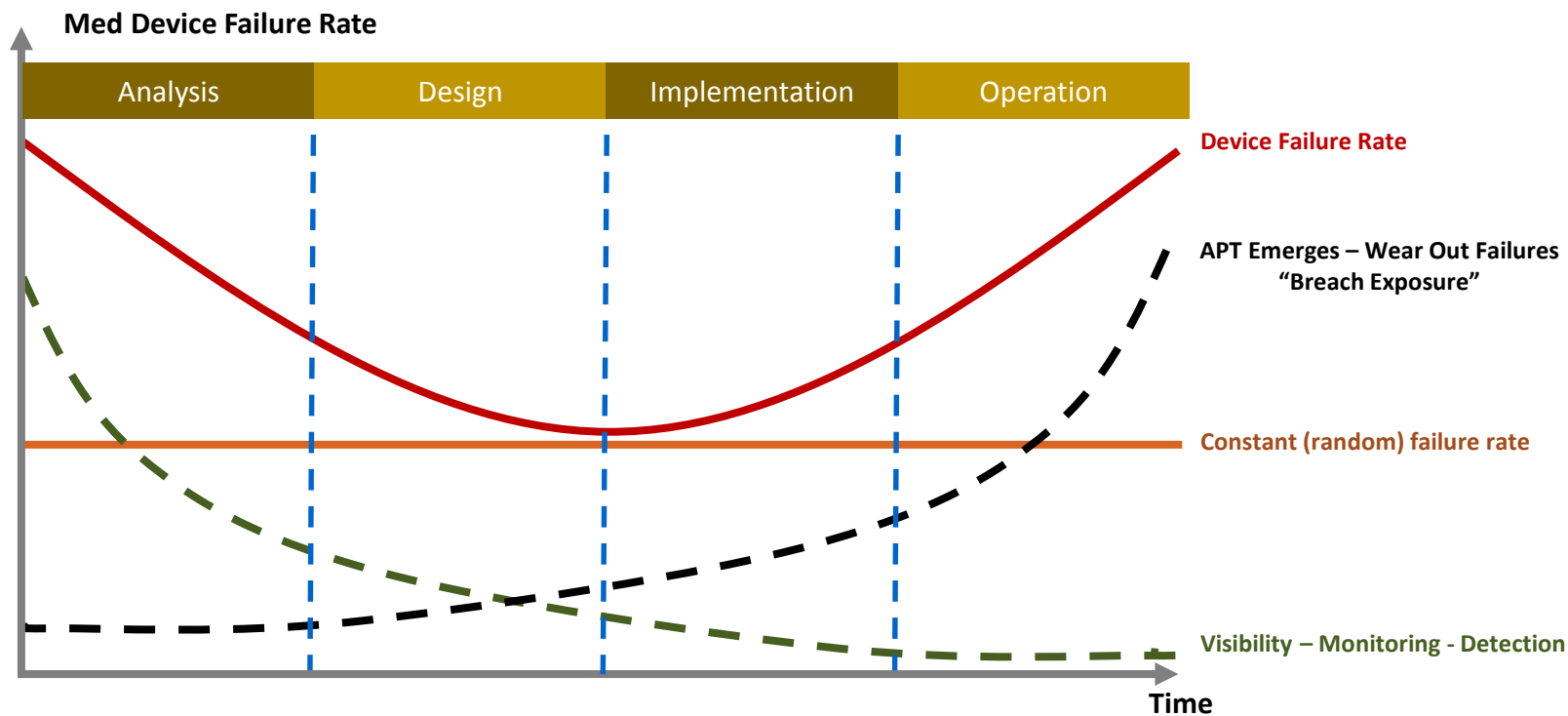




# Device Analytics: “The VIX Test”

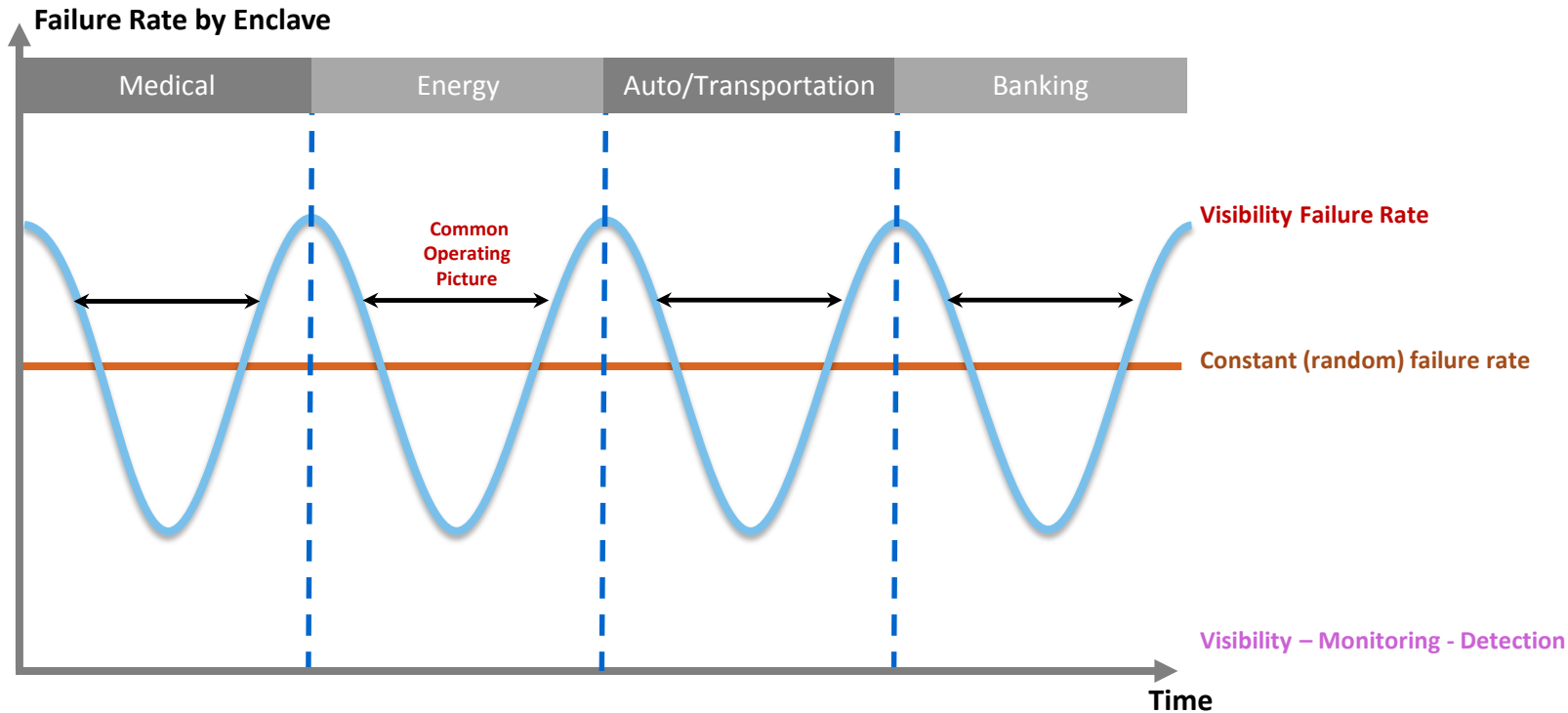


# IoT Device Volatility: iZones and Enclaves

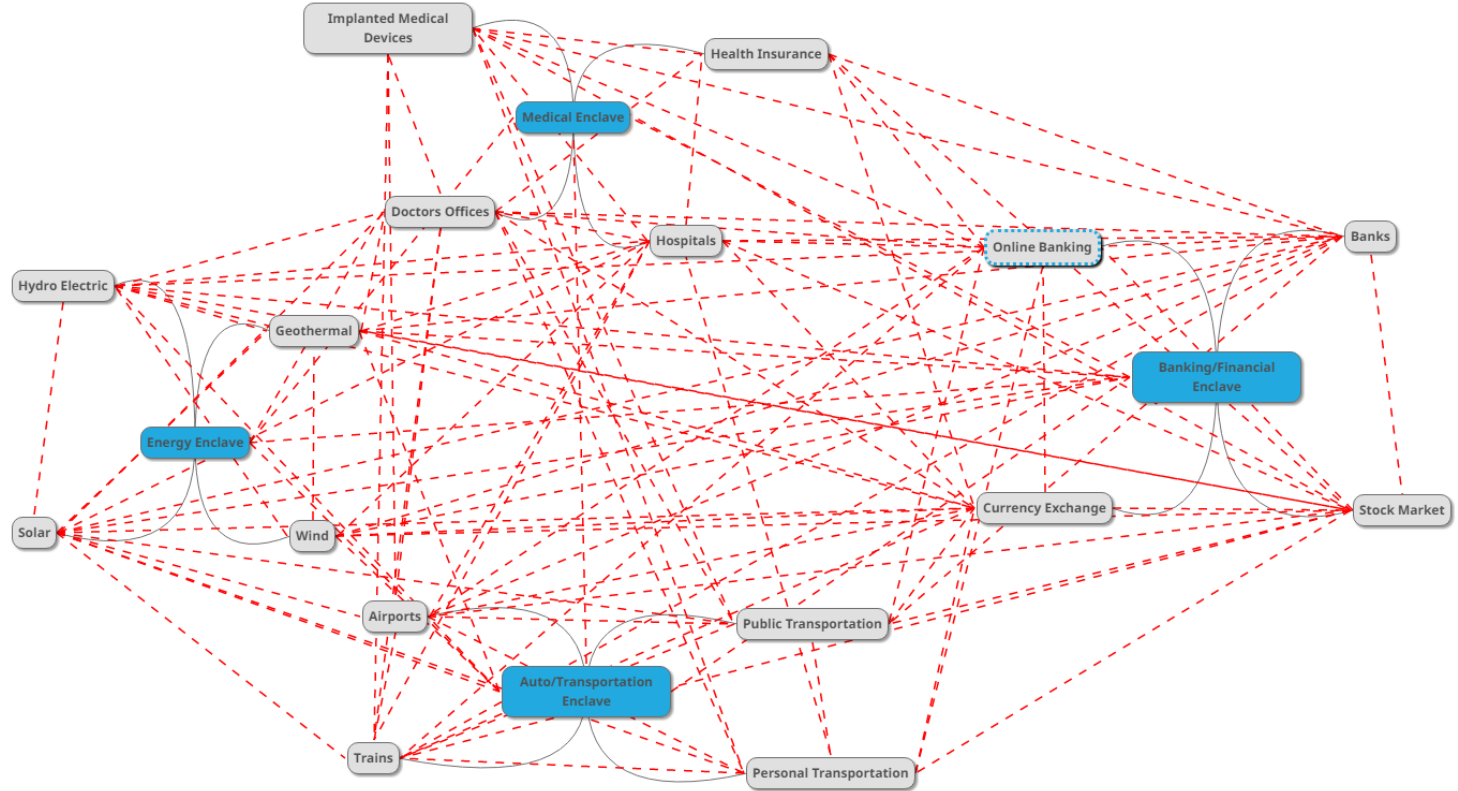


- 747 Engine Resiliency (Length of life) ~ 30 years.
- Average flight hours for 2 million miles/year with average speed of 600 mph \* 30 years = ~4,165 days or almost 100,000 hours of flight time over the course of its life.
- Failure Rate – 27 total-engine failures since 1953 (~0.42 failures per year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

# @ Scale: “Continuous Visibility”



# Enclave Relationships





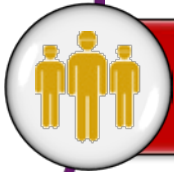
# CRITICAL SUCCESS FACTORS



Analysis, Design & Continuous Improvement



Visibility – Analysis - Action (5 Dimensions)



*Volatility & Failures (“VIX Testing”)*



Law of “Marginal Gains”

# Thank You