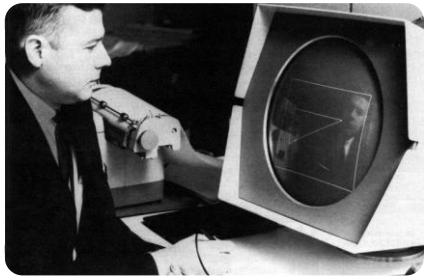
2016 FEDERAL FORUM

Security

Dr. Chip Copper
Strategic Technologist

Presented by BROCADE Produced by fedscoop

Computing & Computers








Computers have evolved tremendously

National Academy of Engineering

Grand Challenges for 21st Century

- Make solar energy economical
- Provide energy from fusion
- Develop carbon sequestration methods
- Manage the nitrogen cycle
- Provide access to clean water
- Restore/improve urban infrastructure
- Advance health informatics
- Engineer better medicines
- Reverse-engineer the brain
- Prevent nuclear terror
- **Secure cyberspace**
- Enhance virtual reality
- Advance personalized learning
- Engineer tools of scientific discovery

25% Believe that the appropriate security measures are in place to support their agencies' needs

25% Do not believe that the appropriate security measures are in place to provide the appropriate level of protection

50% Not sure where their organization fits in regards to having the appropriate security measures in place

SOURCE: MARKET CONNECTIONS - IS DATA AS SAFE AS AGENCIES THINK IT IS?

62% Associate SSL as their primary encryption measure within their particular agency

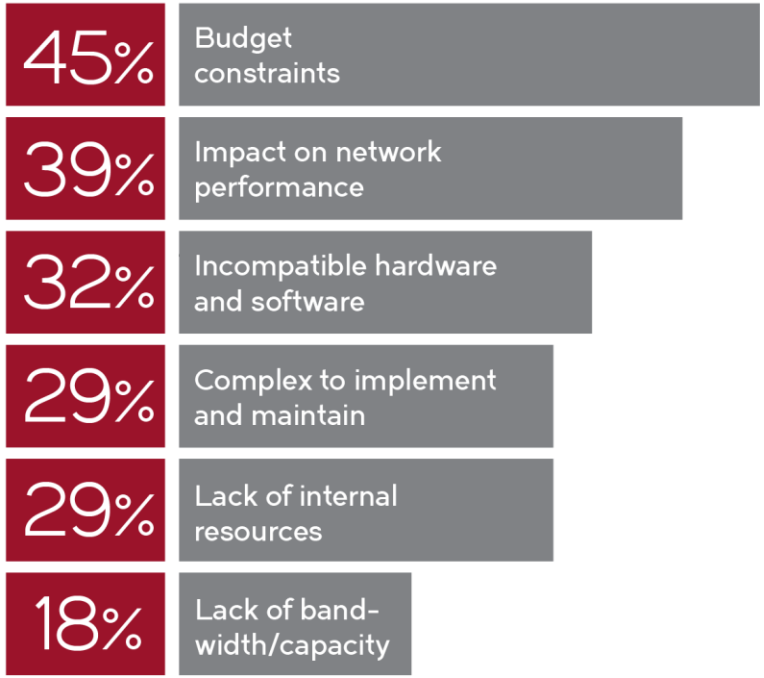
9% Have **NO** idea what security measures are in place to protect any form of agency-specific data

32% Believe that moving forward 256 bit encryption is a requirement for protecting sensitive, secret and top secret data sets

SOURCE: MARKET CONNECTIONS - IS DATA AS SAFE AS AGENCIES THINK IT IS?

WHY AGENCIES DON'T ENCRYPT THEIR DATA

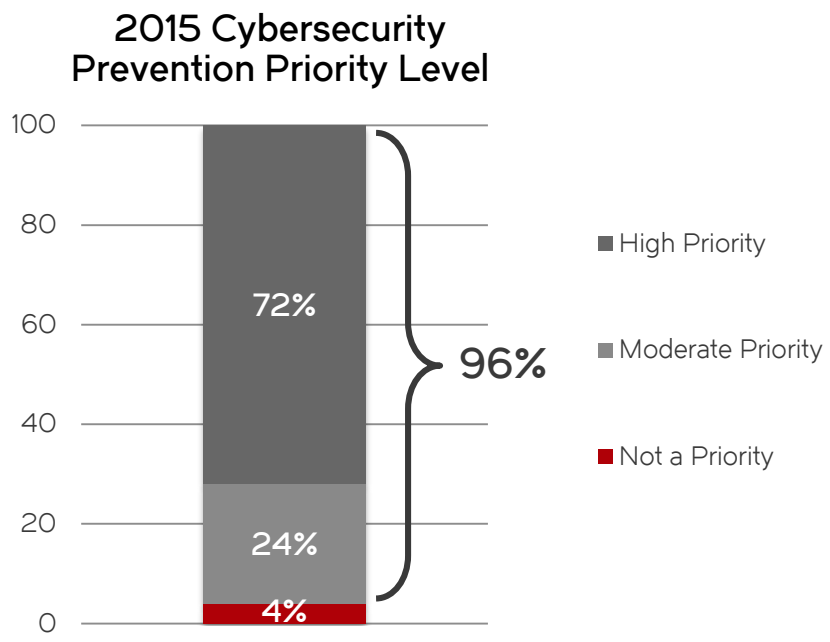
Of the one-quarter of agencies that do not encrypt their data, the top reasons are:

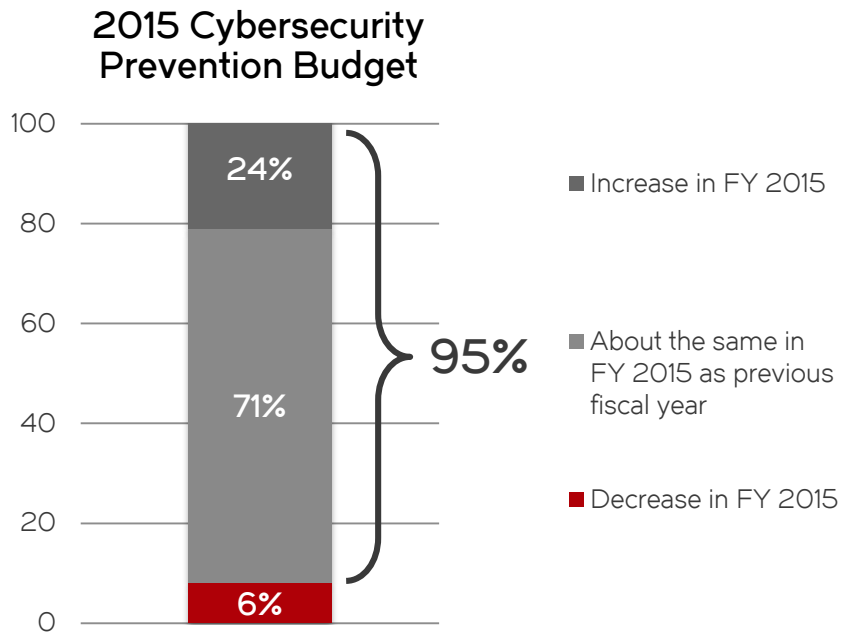


SOURCE: MARKET CONNECTIONS, INC.

Agency Cyber Priorities & Budgets

Agencies' cybersecurity priorities for 2015 include a widespread focus on prevention (72%), and budgets reflect this





Q What are your agency's cybersecurity priorities for 2015 with regard to prevention?

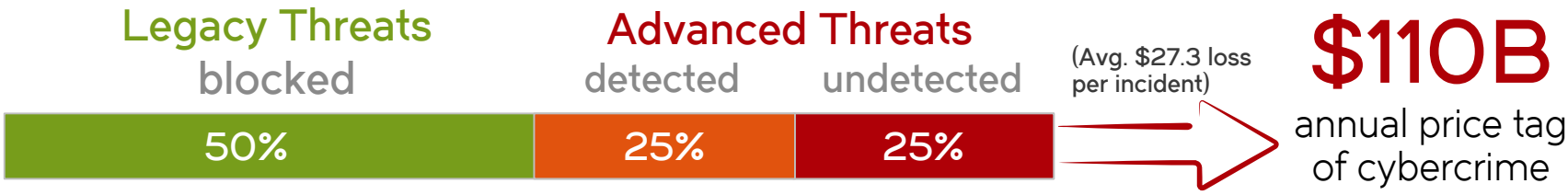
To the best of your knowledge, in each of the following areas did your agency's cybersecurity budget increase, decrease, or stay about the same as the previous fiscal year?

SOURCE: MARKET CONNECTIONS, INC.

General Threat Landscape

>3,000,000,000,000

threats annually



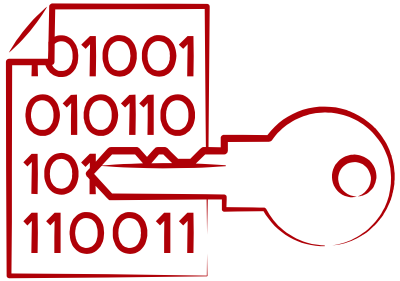
1.6B
number of records lost globally in 2014

$236M
recovery cost of Target breach (so far)

15B
connected devices in 2015

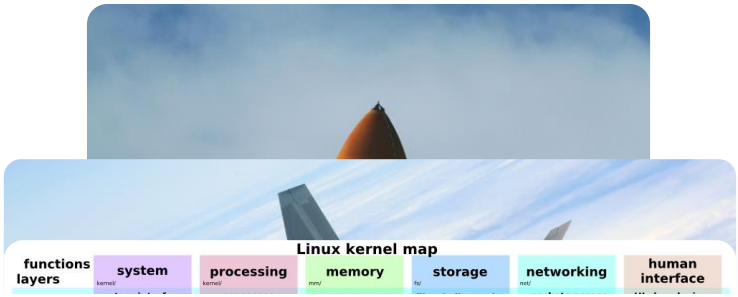
Current State

- More connected devices → more value → added risk
- Security posture hasn't magically just improved
  - In many cases in fact it has regressed
- Heterogeneous security paradigms
  - Device-end data is processed out of band
  - Dubious infrastructure security posture



Complexity Is Increasing

- Space Shuttle: ~400K LOC
- F22 Raptor fighter: ~2M LOC
- Linux kernel 2.2: ~2.5M LOC
- Hubble telescope: ~3M LOC
- Android core: ~12M LOC
- Future Combat System: ~63M LOC
- Connected car: ~100M LOC
- Autonomous (?) vehicle: ~300M LOC

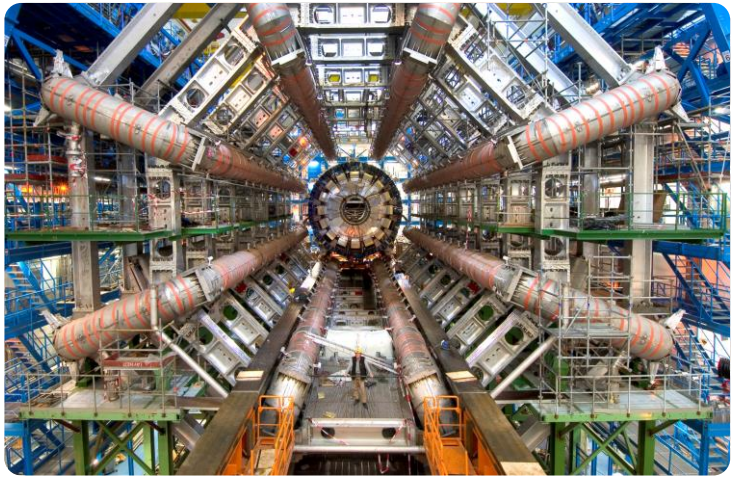


- Autonomous vehicle: ~300M LOC

- Facebook: 50M LOC

facebook

- Large Hadron Collider: 60M LOC



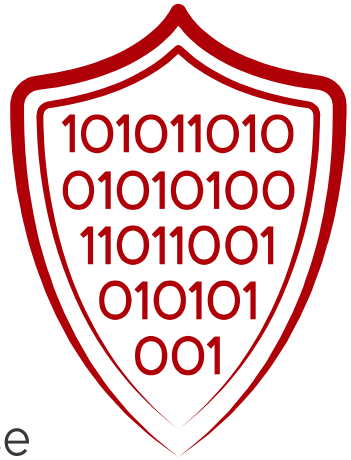
E.g., Connected Vehicle

- Hackable?
- Concept hacks
- Drivetrain exploits
- Notice the speed and gear position?

Infrastructure
→ VPN to backend
→ 1-N exploits

Currently, Security Is *Static*

- Our systems are actively passive
- Need to know all the attack cases ahead of time
  - Presumptuous design
- Best case: Don't be the worst to fail!
- Static security used to be enough: no longer the case



BROCADE

So, What Are We Doing About It?

Many Types of Security Companies

Denial of Service Mitigation

f5 / defense.net · VERISIGN · Symantec · Akamai · neustar · ARBOR NETWORKS (The Security Division of NETSCOUT) · PROLEXIC (DDoS Attacks End Here.)

Realtime Fraud Detection

iovation · ThreatMetrix · ca technologies · DELL / EMC² / RSA · Guardian Analytics · AMERICAN EXPRESS / Accertify · IBM / Trusteer (an IBM Company)

End Point Security / Malware Inoculation

CISCO · SOPHOS · Barracuda · Check Point SOFTWARE TECHNOLOGIES LTD. · KASPERSKY lab · TREND MICRO · Menlo Security · Symantec

Application Security

Symantec · Barracuda · CISCO · hp · QUALYS (On Demand Security) · TINFOIL SECURITY · IBM · WhiteHat SECURITY · VERACODE · TREND MICRO

Identity & Access Management

ca technologies · oneID · authentify · VERISIGN · covisint · Centrify · NetIQ · okta · IBM · gemalto · DELL / EMC² / RSA

Security Analytics / Threat Intelligence

ArcSight · hp · DELL / EMC² / RSA · intel · QUALYS (On Demand Security) · LogRhythm (The Security Intelligence Company) · CYLANCE · BELDEN · tripwire · CYPHORT · ALIEN VAULT

Insider Threat Prevention / DLP

IONIC SECURITY · ca technologies · DELL / EMC² / RSA · websense · CISCO / OpenDNS · Symantec

Cloud Security

BlueCoat · CLOUDFLARE · Symantec · zscaler · intel Security / McAfee · bitglass · CipherCloud (Trust in the Cloud)

Security Orchestration & Workflow Management

cybereason · csg INVOTAS · proofpoint / NETCITADEL (INTELLIGENT NETWORK SECURITY) · splunk> · Triumfant

Network Security Monitoring

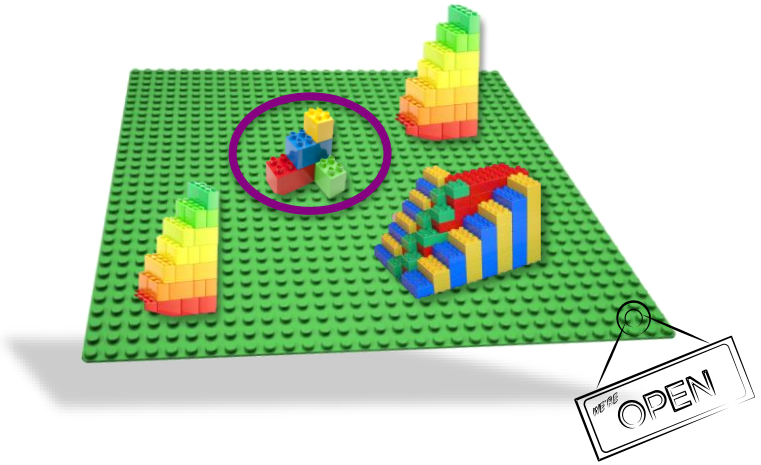
paloalto NETWORKS · JUNIPER NETWORKS · CISCO · JAVELIN · csg INVOTAS · BlueCoat · FORTINET · aruba NETWORKS · Check Point SOFTWARE TECHNOLOGIES LTD. · broala · <VA> vARMOUR · FireEye · Barracuda · illumio · TippingPoint

Platform to Enable Security Innovation

Security

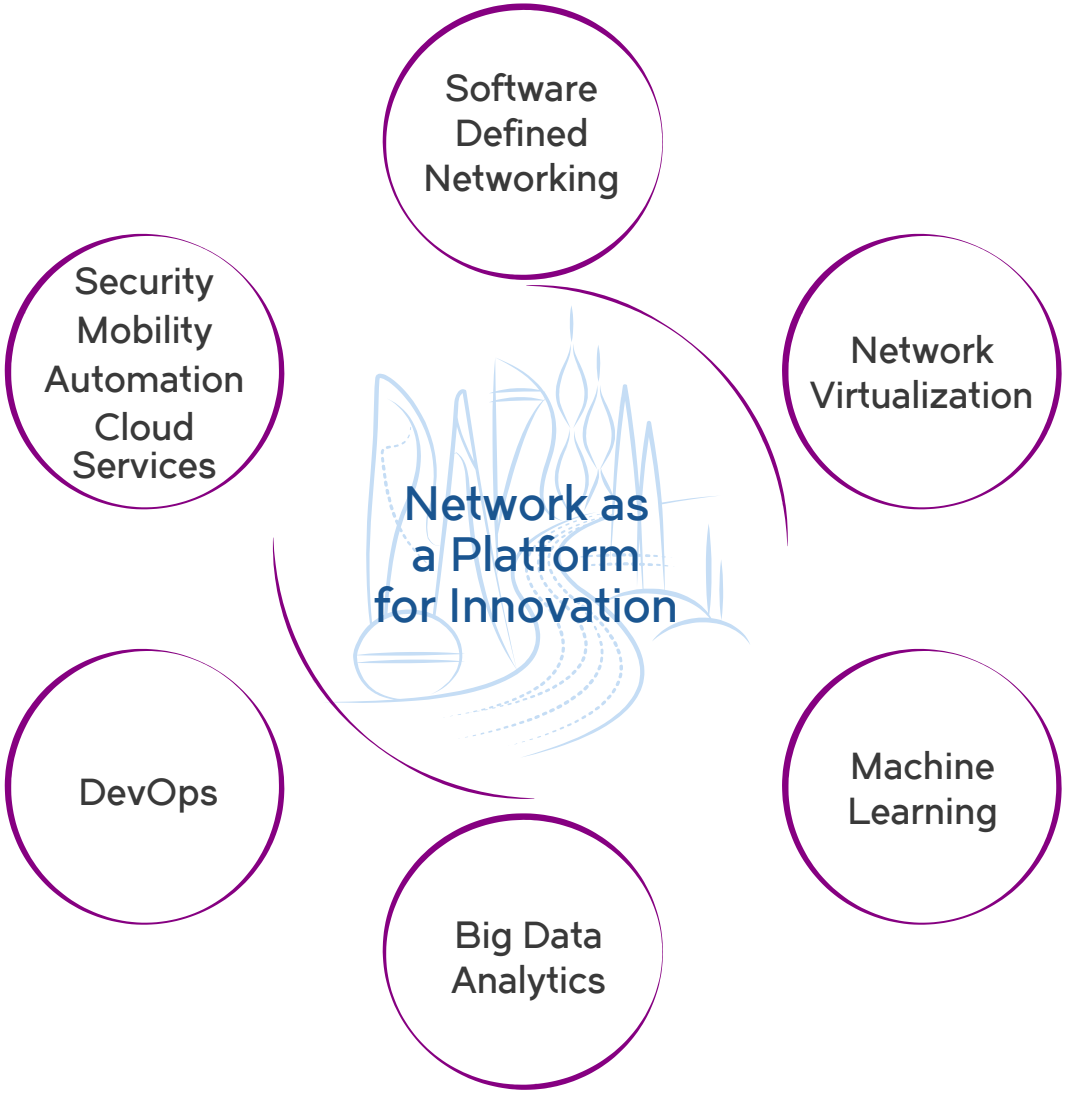
Network Security Solutions Today

Brocade Open Platform for Network Security Innovation

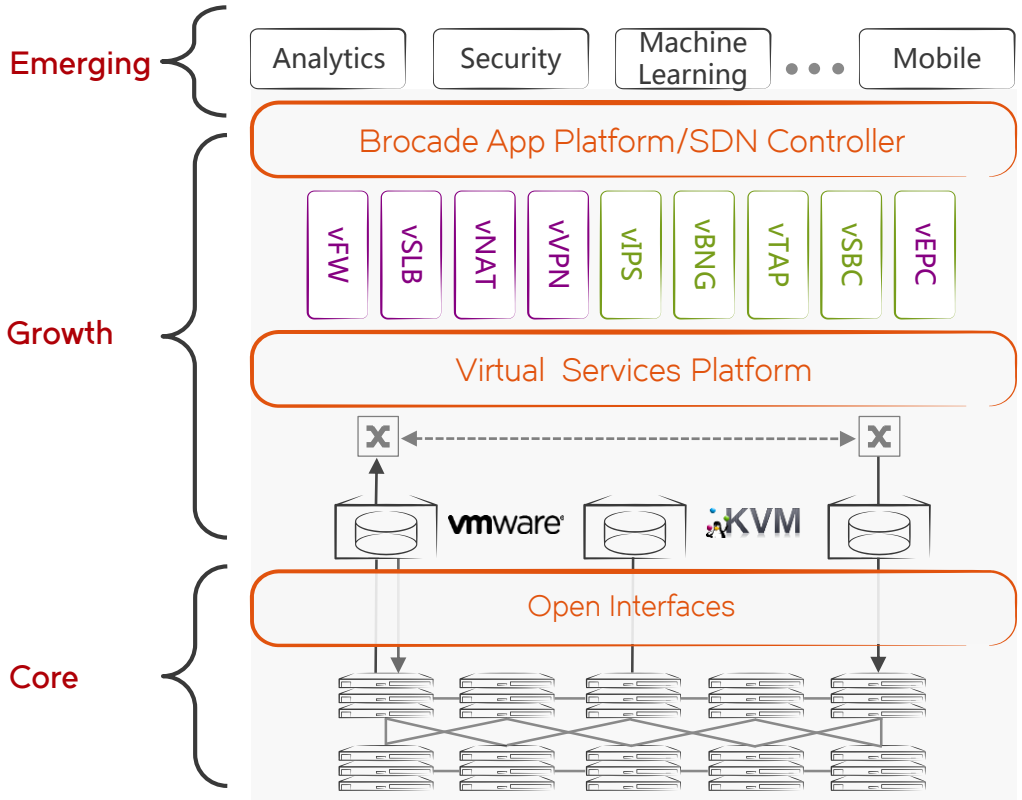


Lead the core network-based security capabilities

Network as a Platform for Innovation



Brocade Technology Stack



SDN Applications / Automation

- Brocade SDN Controller, Orchestrator
- Network, Security, Analytics, Mobility Apps
- DevOps

Virtualized Network Services

- vRouter, vNAT, vADC, vFW, vCPE, vEPC…
- Vyatta Network OS

Network Virtualization

- EVPN
- VTEP
- Service Chaining

High-Performance HW Infrastructure

- DC SAN
- DC Ethernet and IP Fabrics
- DC Routing
- Campus Switching
- Wireless & Small Cell

Machine Learning:
A Foundational Technology at Brocade

Theory

- Breakthrough representations for network data
- Innovative deep neural network architectures
- New applications of reinforcement learning
- Solid mathematical foundations

Algorithms

- Knowledge-Defined Networking
- Deep neural networks predict/ recognize APT activity
- Optimal (risk aware) control discipline
- Conventional statistical techniques where appropriate
- Dynamic/on-line vs. static

ML @ BRCD

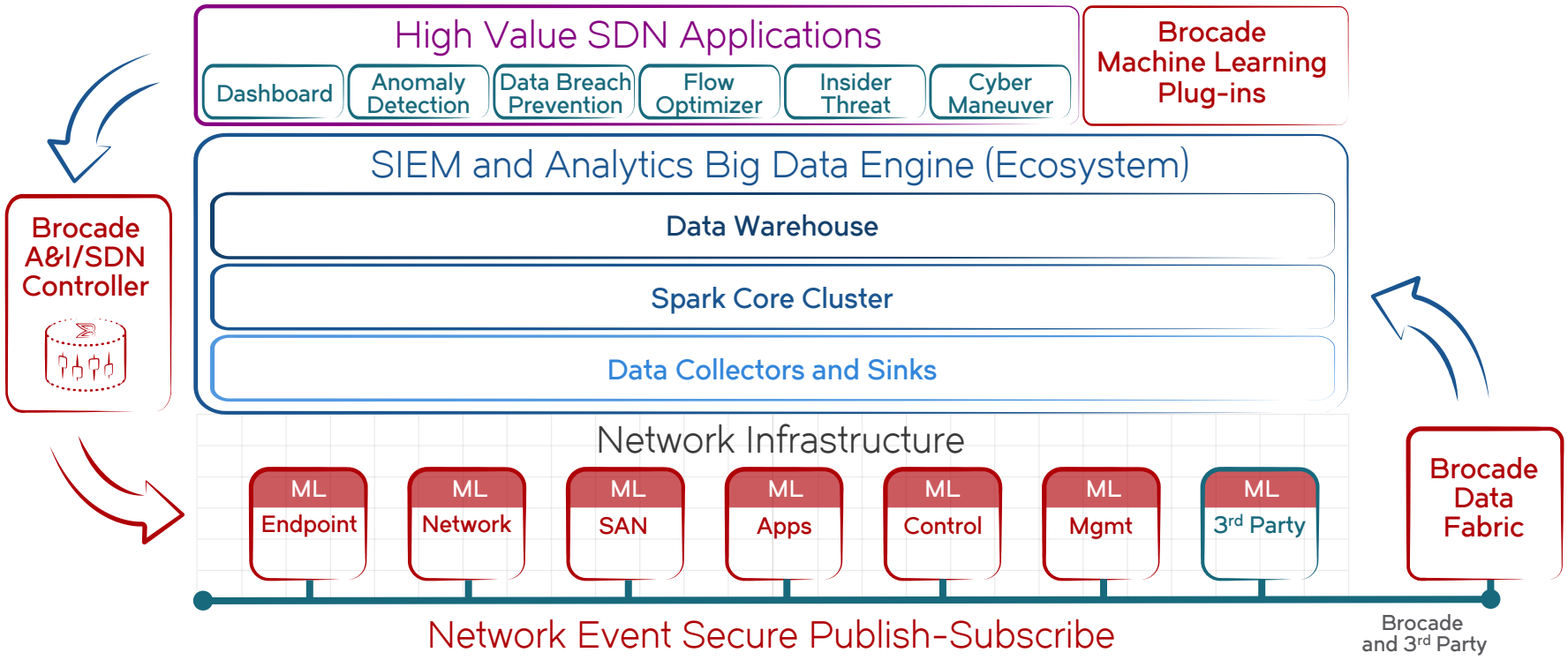
Implementation

- Integration of Brocade ML with the Brocade Data Fabric, Brocade SDN Controller, and the Brocade Open Platform for Network Security Innovation creates a new kind of predictive, actionable, and real-time intelligence
- Uniform support across all Brocade product lines
- Complete OODA loop

Ecosystem

- Open Source, data and models where possible
- Provide/receive data/intelligence to/from partners
- Integration with DISA CMRS mission partners
- Industry and academic partnerships

Brocade Data Fabric and ADP2*



*ADP2: ANOMALY DETECTION, PREVENTION AND PREDICTION

Two Types of Security

Static Security

- Designed for known attacks
- Tailored to specific abuse cases
- Need to know adversary profiles ahead of time
- Manual patching and update
- Inflexible un-scalable
- Best case: just “detect”
- Yet absolutely necessary

Dynamic Security

- Data- and analytics-driven
- Adjusts based on runtime security posture of the system
- Adaptive, active, and learning
- Self-organizing, automated
- Proactive, self-defending
- Predicts attacks
- Improves with scale

Machines and humans are becoming more similar

Real action is in Dynamic Security

Static Security Building Blocks

- Assets, attack tree, VATA
- Identity, authentication, authorization
- Cryptography (confidentiality, integrity, authenticity, non-repudiation)
- Attestation, verification, run-/load-/crash-time integrity validation and measurement
- …

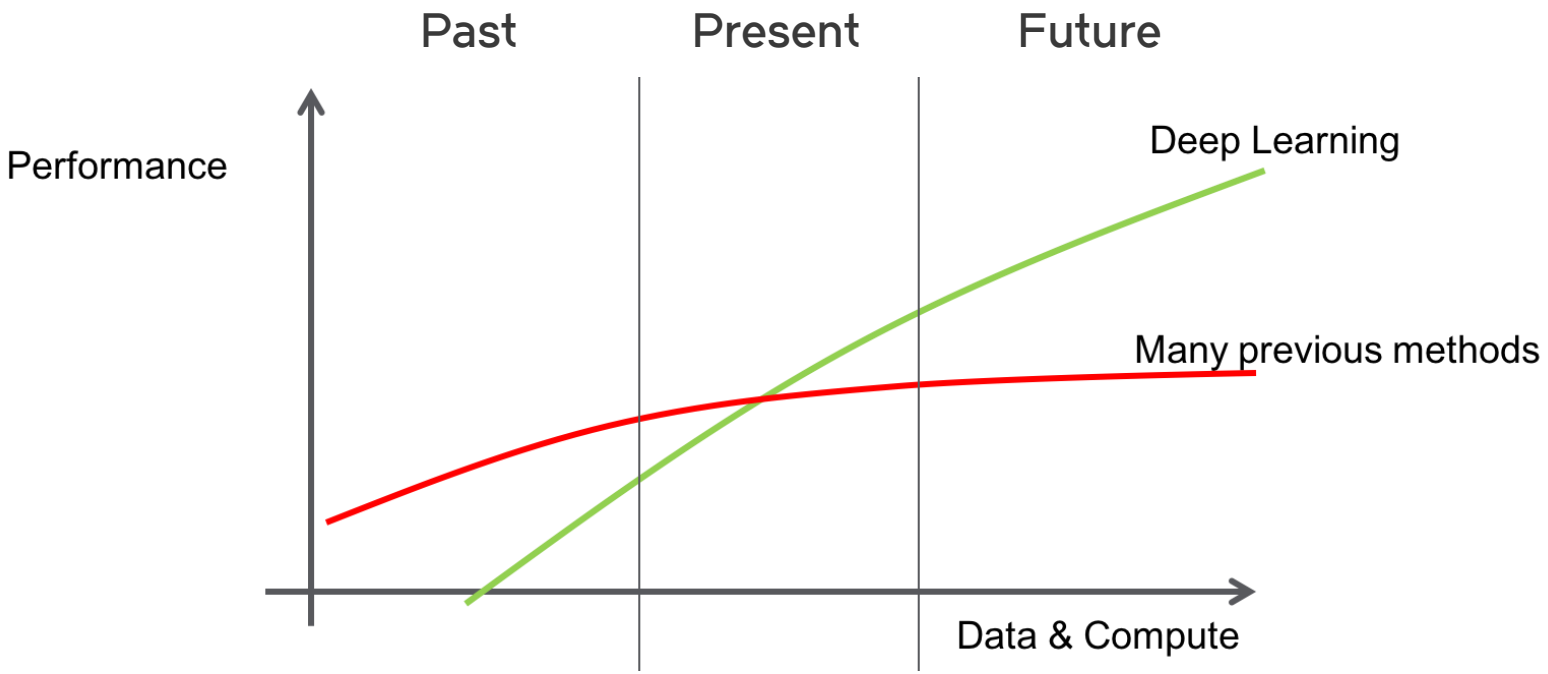
Dynamic Security Building Blocks

- AI
- AI + Big Data + Analytics
- AI + Big Data + Analytics + ML/DL
- Data → Information → Actionable Intelligence (AI?)
  - **Action** is the next big thing
  - Professor Karl Friston, University College London
  - "Order of Magnitude Labs", etc.

Dynamic Security

Dynamic Security & Data

- Dynamic Security **in theory** improves with scale
- IOT = more data



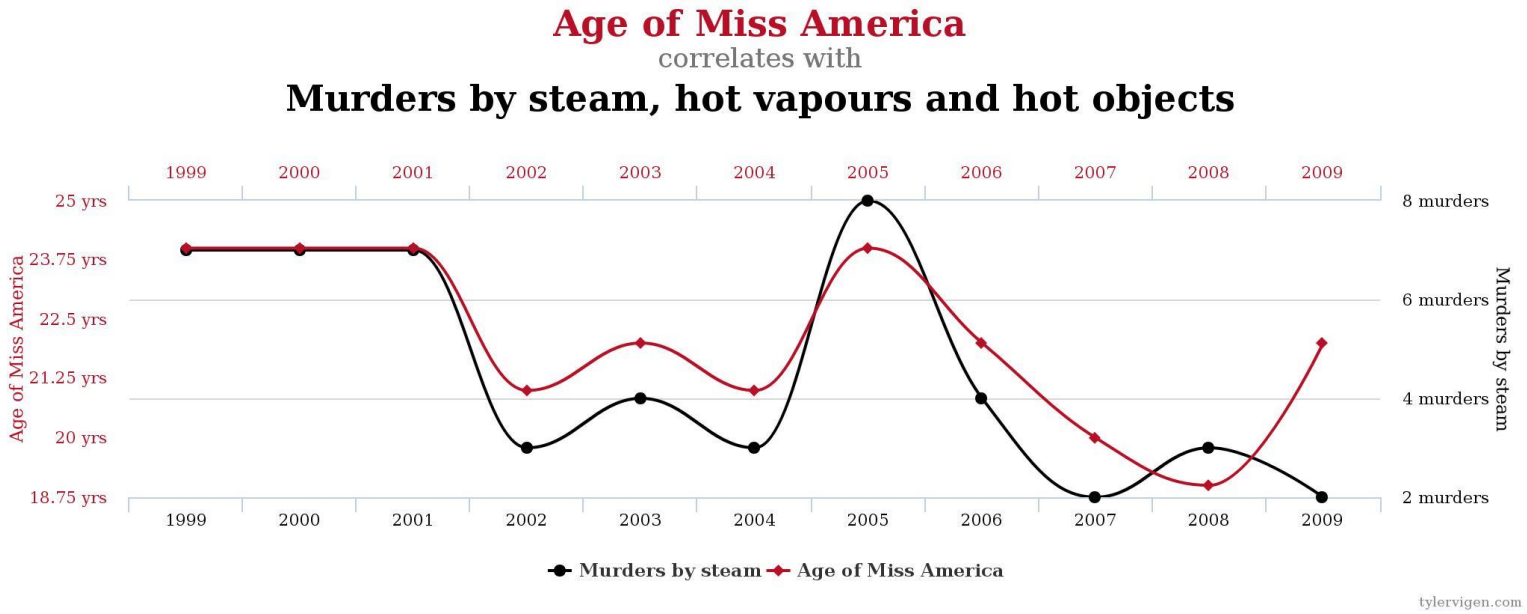
SLIDE COURTESY OF ADAM COATES, BAIDU RESEARCH

Challenges

- Baselining
  - Curse of dimensionality
- We have Operating Systems
  - We need Cooperating Systems
  - Among mutually-distrusting actors
- Privacy
  - Data sharing: digital equivalent of cognitive dissonance
  - DataHub @MIT CSAIL: very promising project
    - Sandy Pentland, Thomas Hardjono, et al.

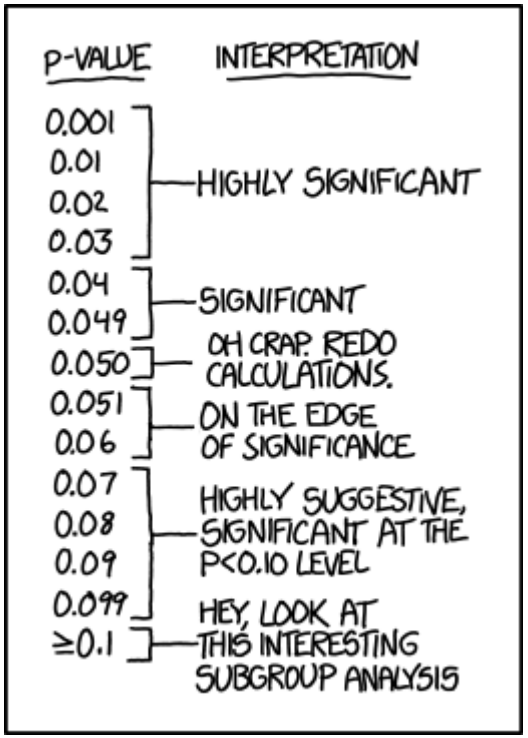
Challenges (Cont.)

- Simple correlations



Challenges (Cont.)

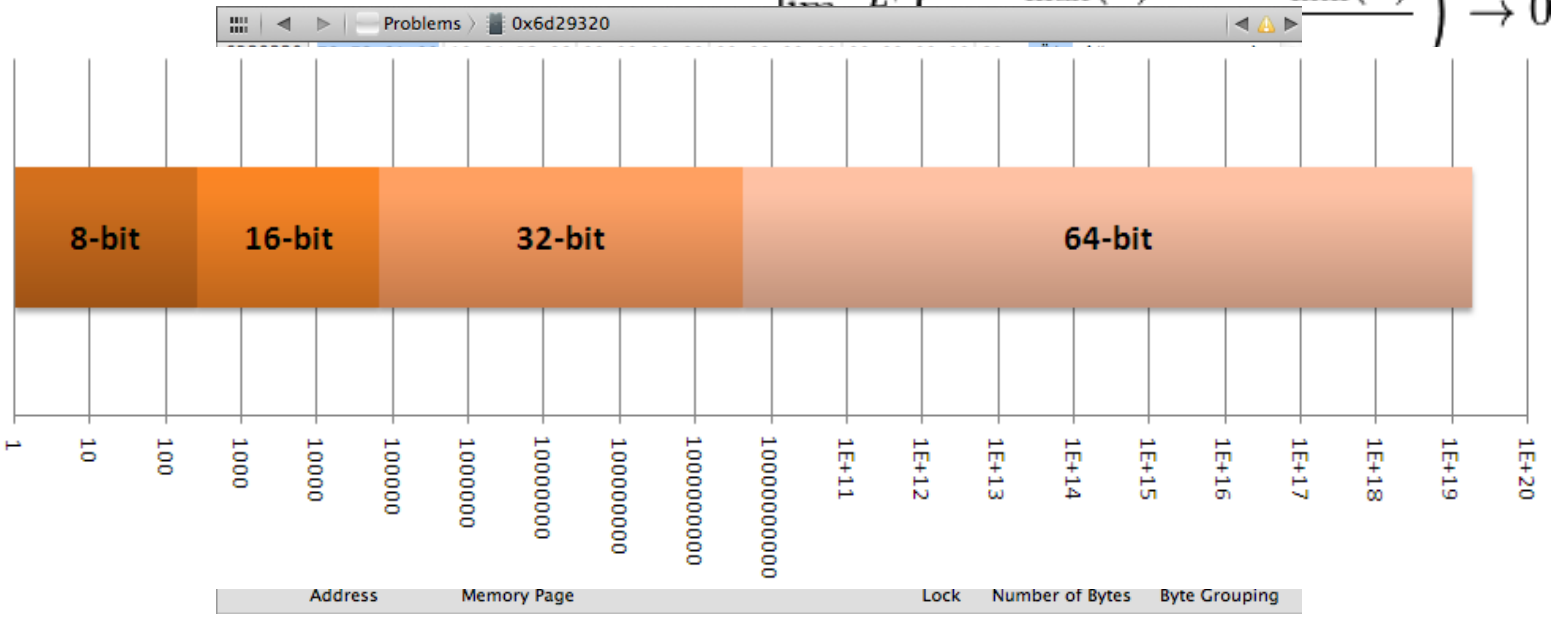
- Simple correlations
- Statistical significance



Challenges (Cont.)

- Simple correlations
- Statistical significance
- Combinatorial explosion of state-space
  - AKA Curse of Dimensionality

$$\lim_{d \to \infty} E\left(\frac{\text{dist}_{\max}(d) - \text{dist}_{\min}(d)}{\text{dist}_{\min}(d)}\right) \to 0$$



Challenges (Cont.)

"If you torture data long enough, it will confess to anything you'd like."

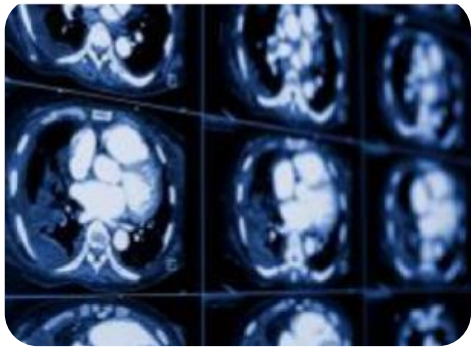
R.H. Coase, British Economist

Generic Use Cases

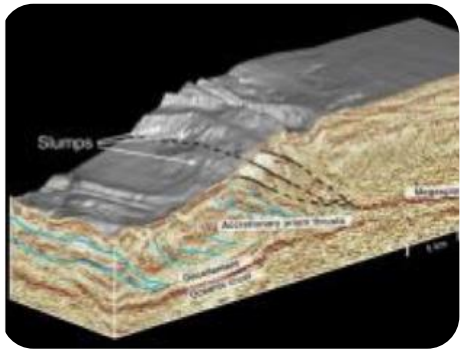
Social Media

Security, Defense, and Intelligence

Consumer Electronics



Medical



Energy

Media & Entertainment

Cyber Analytics Use Cases

- Scalable training of large datasets (logs, traffic, etc.)
- Real-time network anomaly detection
  - Deep packets, edge logs, etc.
  - DDoS, malware
- Botnet detection
  - Zombie hosts, command and control, targets
- Host malware detection
- Internal fraud detection
- …and applying predictive modeling to all the above

BROCADE

Thank you