RSA CONFERENCE CHINA 2011
NOVEMBER 2-3 | CHINA WORLD HOTEL | BEIJING

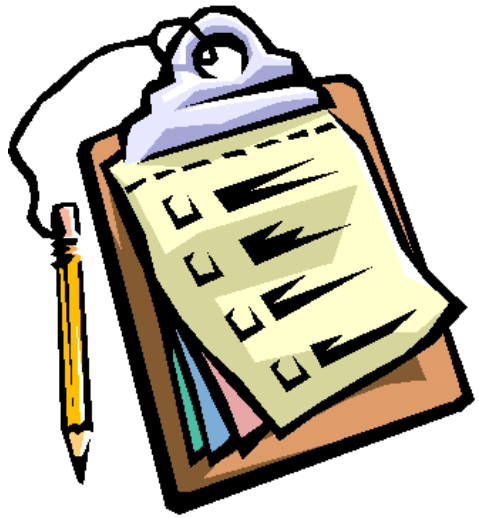
the adventures of

Social Media, Mobility And The Cloud, Oh My!

Dr. Hongwen Zhang
President and CEO
Wedge Networks Inc.

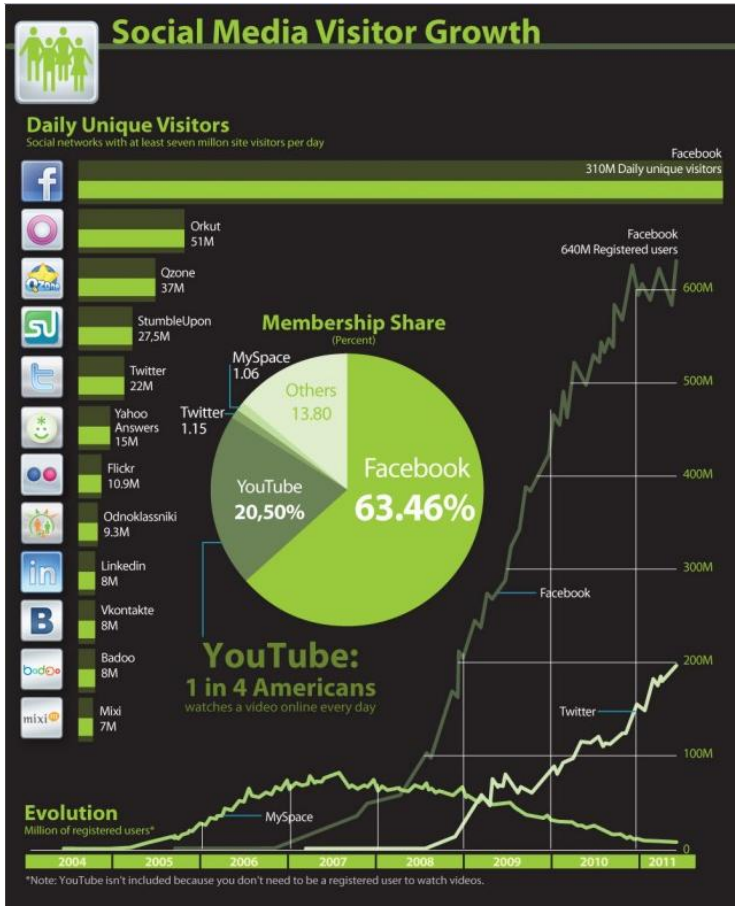
AGENDA

- The New Internet
  - The Rise of Social Media
  - The Rise of Mobile Internet
  - The Rise of Cloud Computing
- The Attack Vectors
  - Threats That Ride On the Trends
  - New factors – HTML5 and IPv6
  - “The Large Scale Security Issues”
- The Solution
  - Deep Content Inspection
  - Use cases of DCI
- Questions?



The New Internet

THE RISE OF SOCIAL MEDIA



Source: [The Growth of Social Media: An Infographic]

- One in every nine people on Earth is on Facebook
- How is our life consumed:
  - 700 billion minutes per month on Facebook
  - 2.9 billion hours per month (326,294 years) on YouTube
  - 190 million average Tweets per day
- Google+ was the fastest social network to reach 10 million users at 16 days (Twitter took 780 days and Facebook 852 days)

THE RISE OF SOCIAL MEDIA

人人网 renren.com

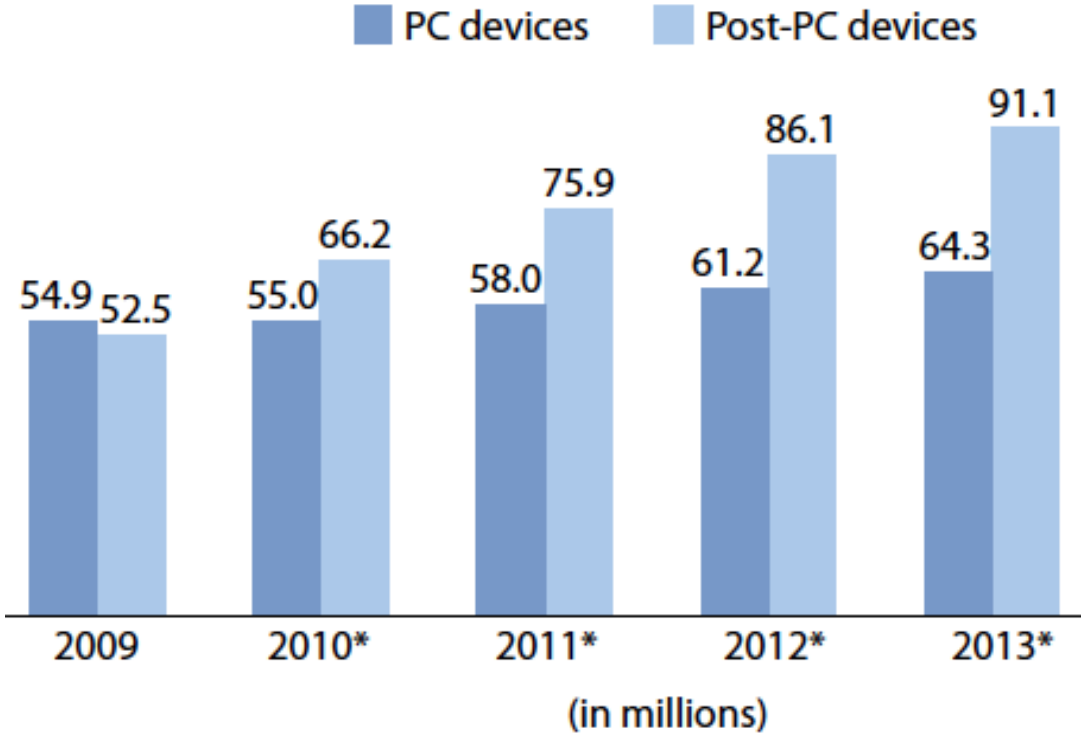
新浪微博

YOUKU 优酷 世界都在看

China Specific Stats

- Renren: 140 Million Chinese Users (Aug 2010)
- Youku: 100 Million Users
- Weibo: 80 Million Users (Feb 2011)

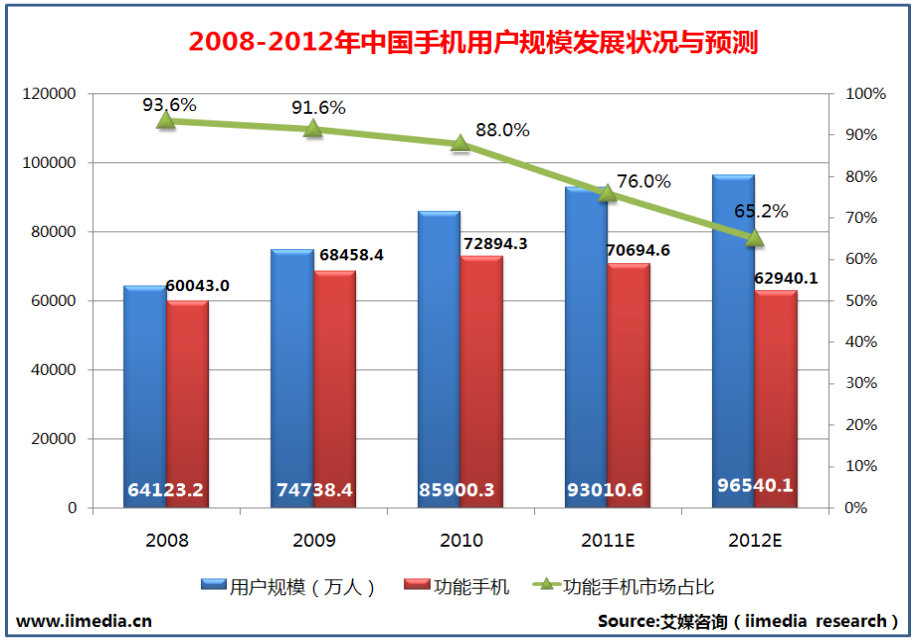
THE RISE OF MOBILE INTERNET

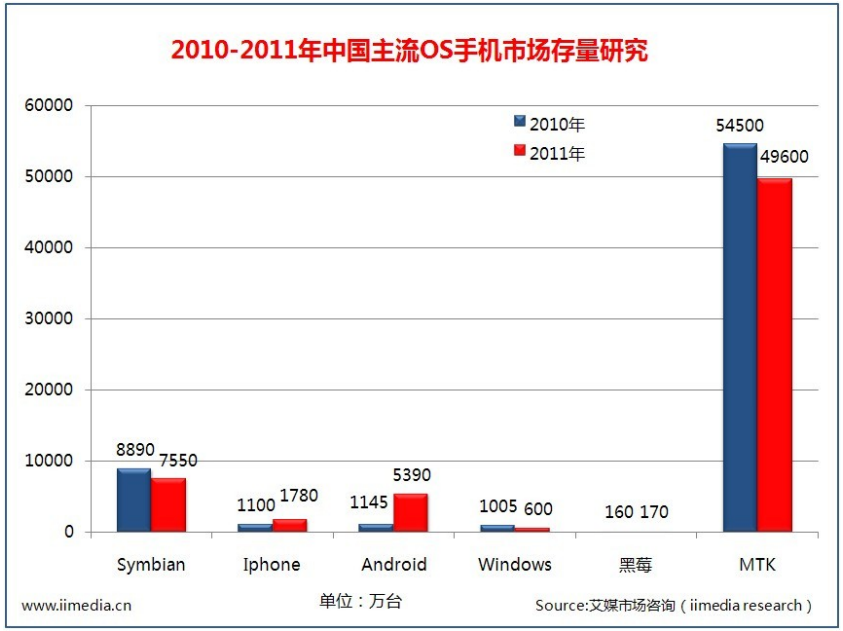


Source: Forrester

"… the countries we're getting into now are ones that don't really use computers at all. The predominant ways people are connecting in Africa, in India, is through their mobile devices. … we now have over 350 million mobile users. Within another year or two, we'll be a mobile company, with 1/2 mobile users." – *Erick Tseng, Facebook Mobile Chief*

THE RISE OF MOBILE INTERNET

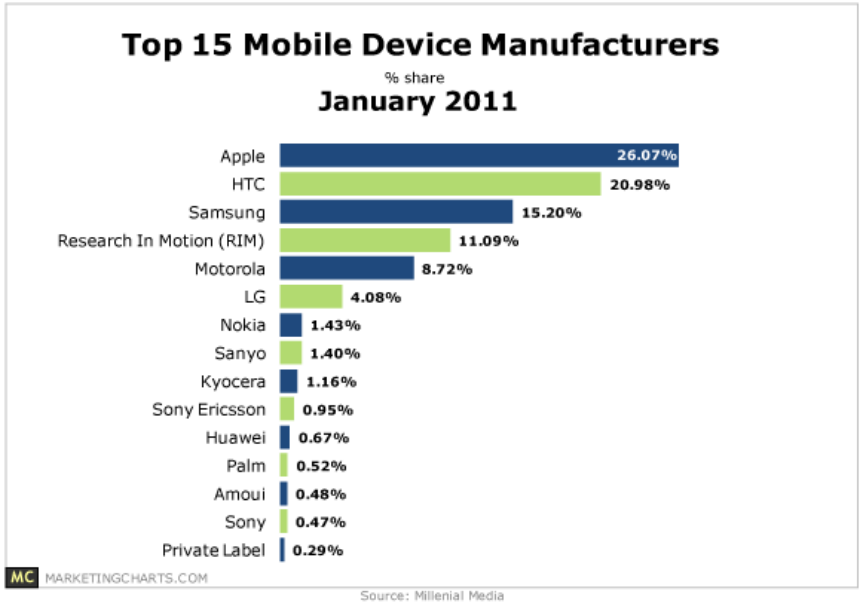


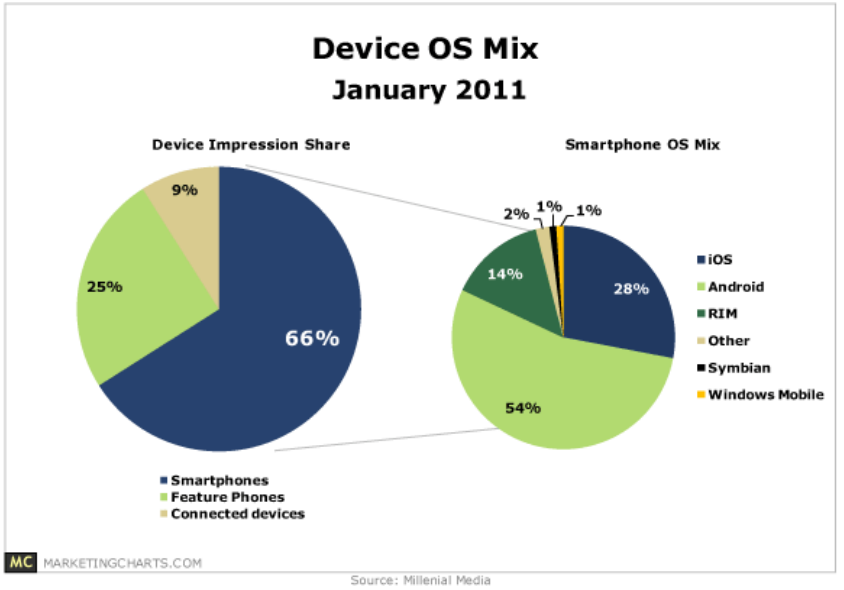


ALWAYS ON, ALWAYS CONNECTED

- *"… at any given time, there are 670,000 concurrent HTTP sessions in a single metro area"* – administrator of a provincial mobile data network in China
- HTML5 keeps two way communication sessions

DIFFERENT MOBILE DEVICES



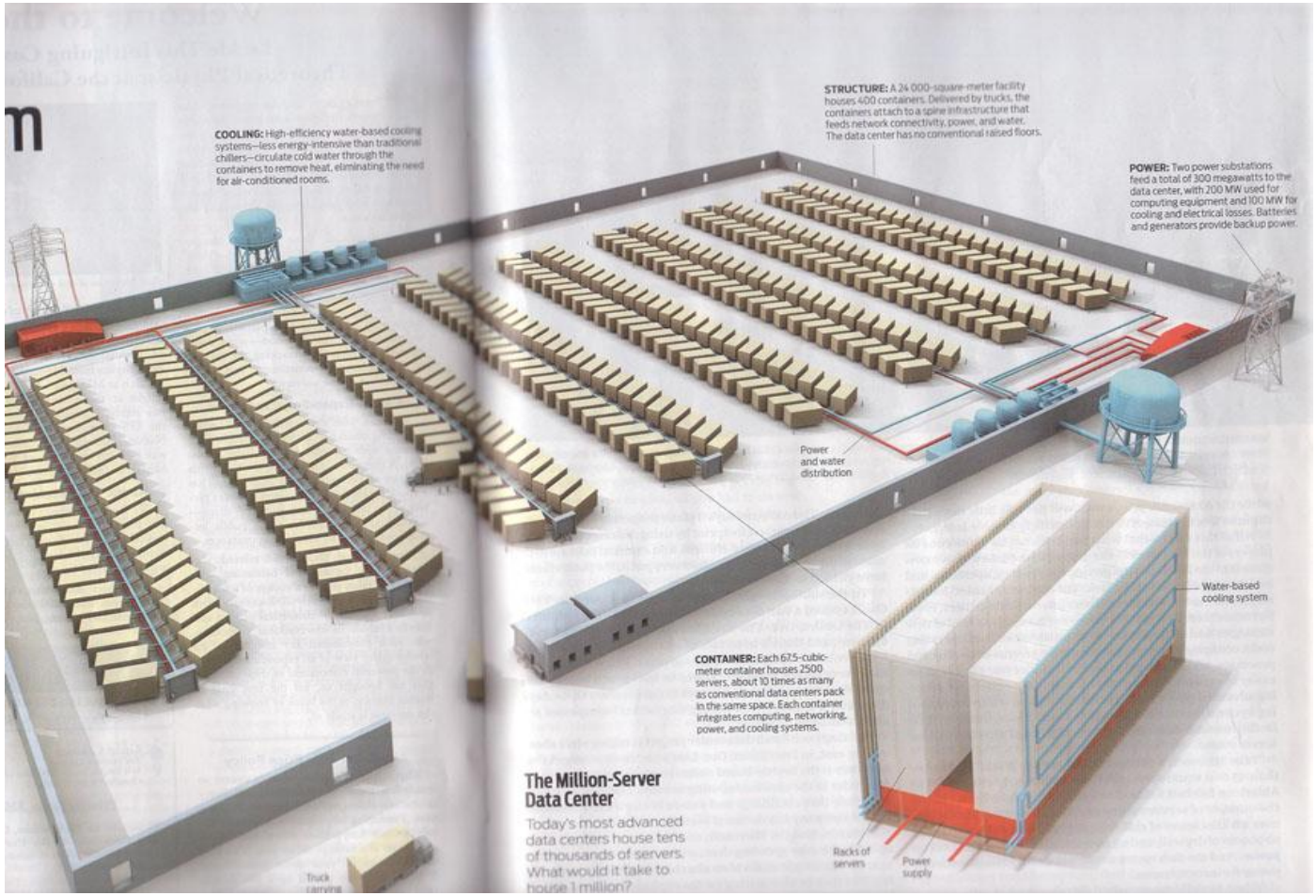


Top Smartphone Platforms
3 Month Avg. Ending Apr. 2011 vs. 3 Month Avg. Ending Jan. 2011
Total U.S. Smartphone Subscribers Ages 13+
Source: comScore MobiLens

	Share (%) of Smartphone Subscribers		
	Jan-11	Apr-11	Point Change
Total Smartphone Subscribers	*100.0%*	*100.0%*	*N/A*
Google	31.2%	36.4%	5.2
Apple	24.7%	26.0%	1.3
RIM	30.4%	25.7%	-4.7
Microsoft	8.0%	6.7%	-1.3
Palm	3.2%	2.6%	-0.6

Ref. comScore

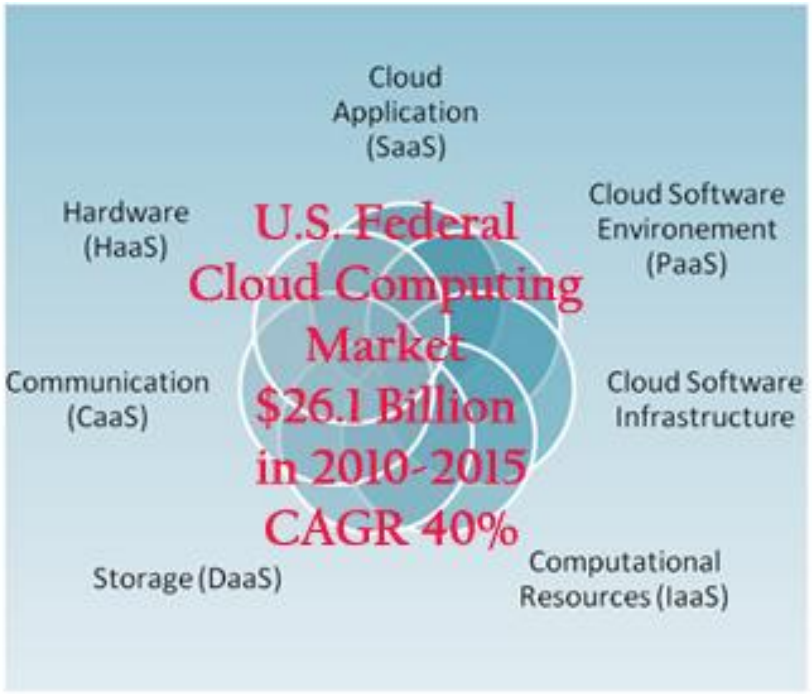
THE RISE OF CLOUD COMPUTING



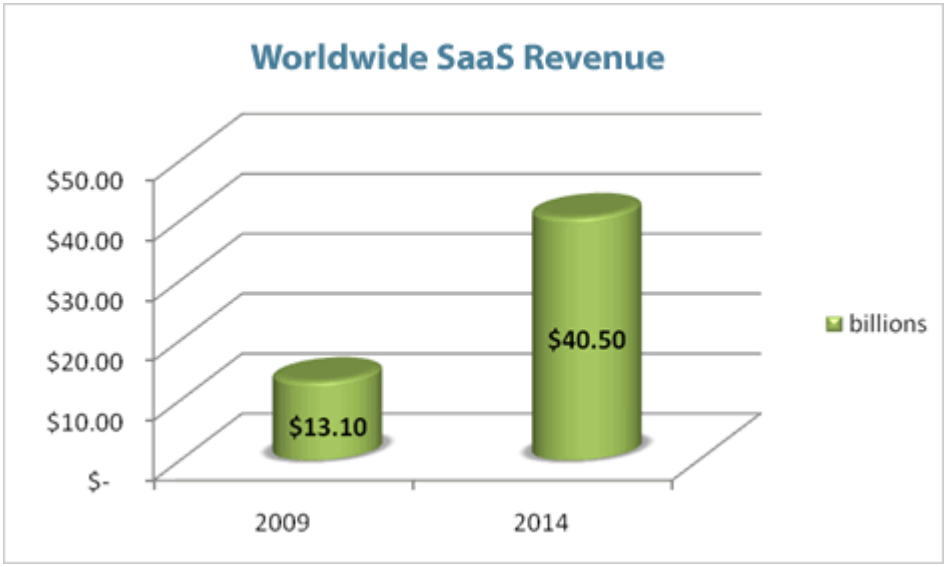
The Giant Cloud

Source: IEEE Spectrum Jan, 2009

MARKET GROWTH



Source: Market Research Media



Source: IDC

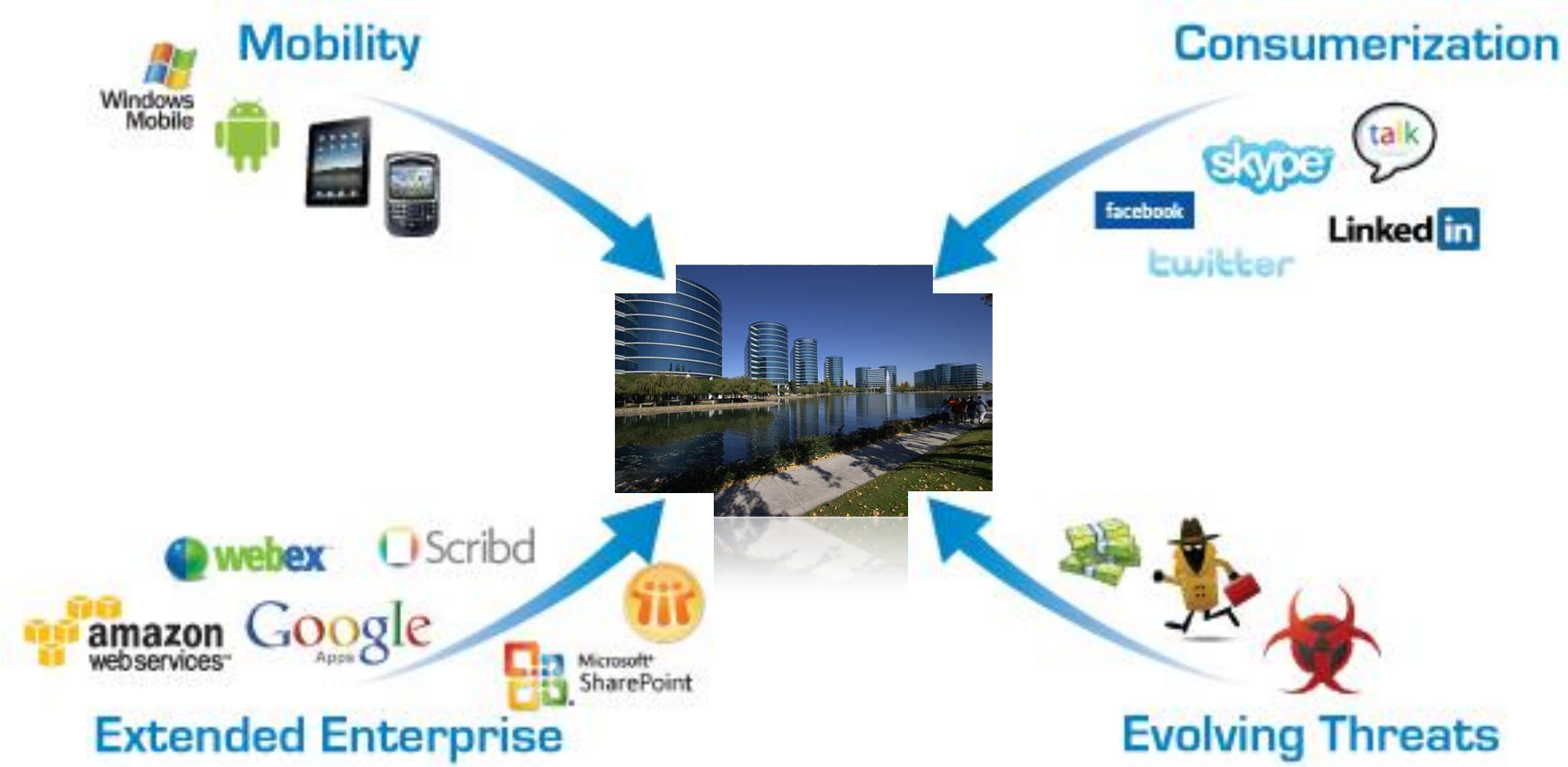
- "…CHT will spend USD$6.2B to build out Cloud Computing Centers …"
- "… We are building 5 Cloud Computing clusters …"

THE BIG PICTURE

- **Content**: dynamic and large scale multi-sources
- **Source**: decentralized and large scale aggregation
- **Access**: mobile and large scale concurrency

Increasing Attack Vectors: What Does This Mean?

EVOLVING THREATS



COMPLEX DELIVERY METHODS

How Malicious Activity Spreads

- Speed Of Transmission
- Trusted Source Manipulation
- Reach of Transmission
- Data Harvesting

INCREASED VECTORS FOR DATA COMPROMISE

- **GPS** – used for E911, but can also be used to know where you are
- **Signaling** – used by operator to control device, deliver text messages, indicators
- **Voice** – used for the main function of voice communication
- **Cellular Data** – used for applications when not in Wi-Fi zone
- **Local Area** (Wi-Fi) – used for applications and in some cases voice when in Wi-Fi zone
- **Personal Area** (Bluetooth) – used for device to accessory or device to device communication
- **Near Field** (future) – used to pay. Think Esso Speedpass

Any entry / exit point for data could potentially be compromised…

CLOUDY SKY

- No boundary to defend

NEW FACTORS: HTML5, IPv6

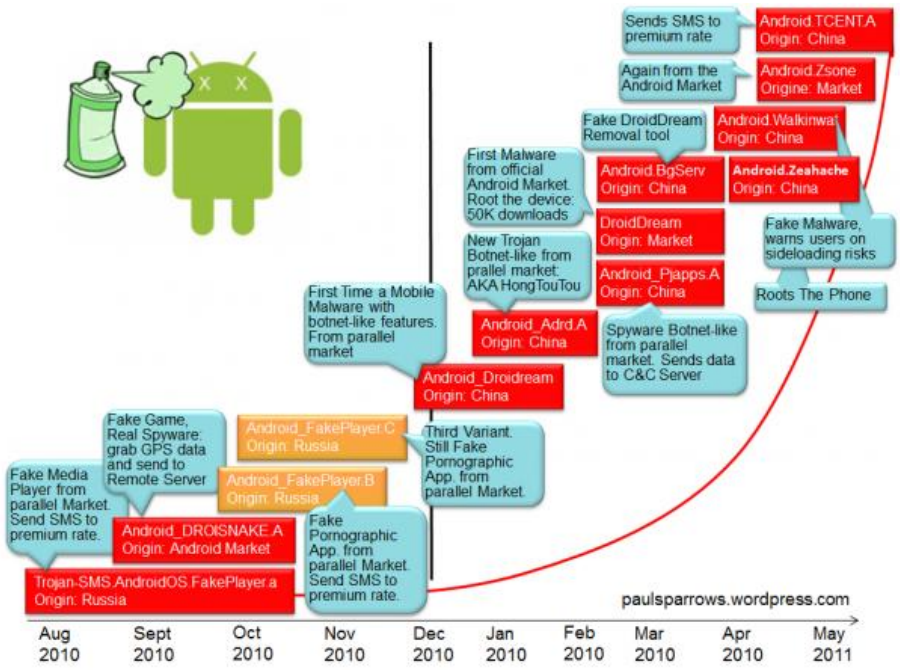
- New structure for content
- Known malware undetected within Websocket
- Large amount of two way concurrent sessions

- Render IP reputation based approach useless due to the lack of history
- Huge search space that will slow down the inspection engines

LARGE SCALE VULNERABILITY

- Enemy is within: breach of the “Trust Networks”
- Underprivileged mobile end points are the weakest links
- “Ease of access” of cloud services applies to everyone, good or evil
- Obsolete defense due to emerging standards

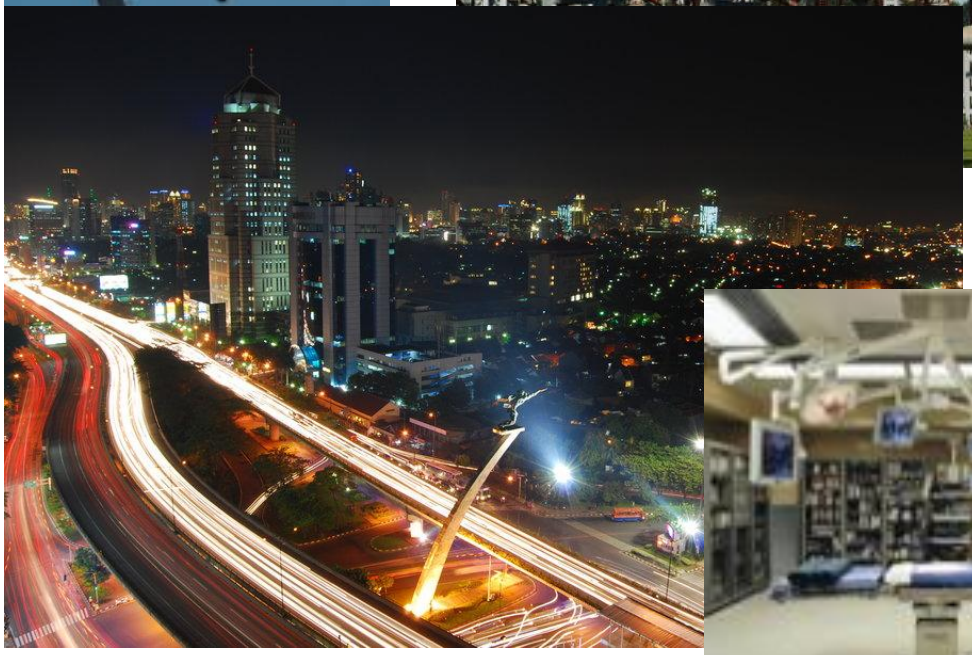
LARGE SCALE SECURITY OUTBREAKS

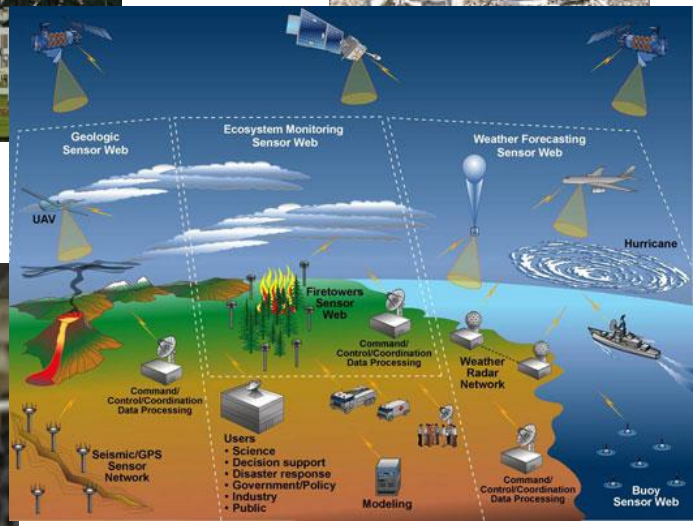


Ref: paulsparrow.wordpress.com

- Fake joke worm wriggles through Facebook (May 21st, 2011)
- 400% increase in mobile malware in 7 months
- “0.48% of mobile devices are infected. 30% of micro-blog sites contain malware”
- “1/3 of my computing resources are consumed by content based DDoS”
- Survey of SaaS providers: 46% major security issues; 36% minor security issues; 18% do not know.
- Texas Controller’s Office: 3.5M records; WordPress: 18M records; Sony PlayStation Networks: 77M records
- The “flocking behaviour” of attacks – conspiracy theory

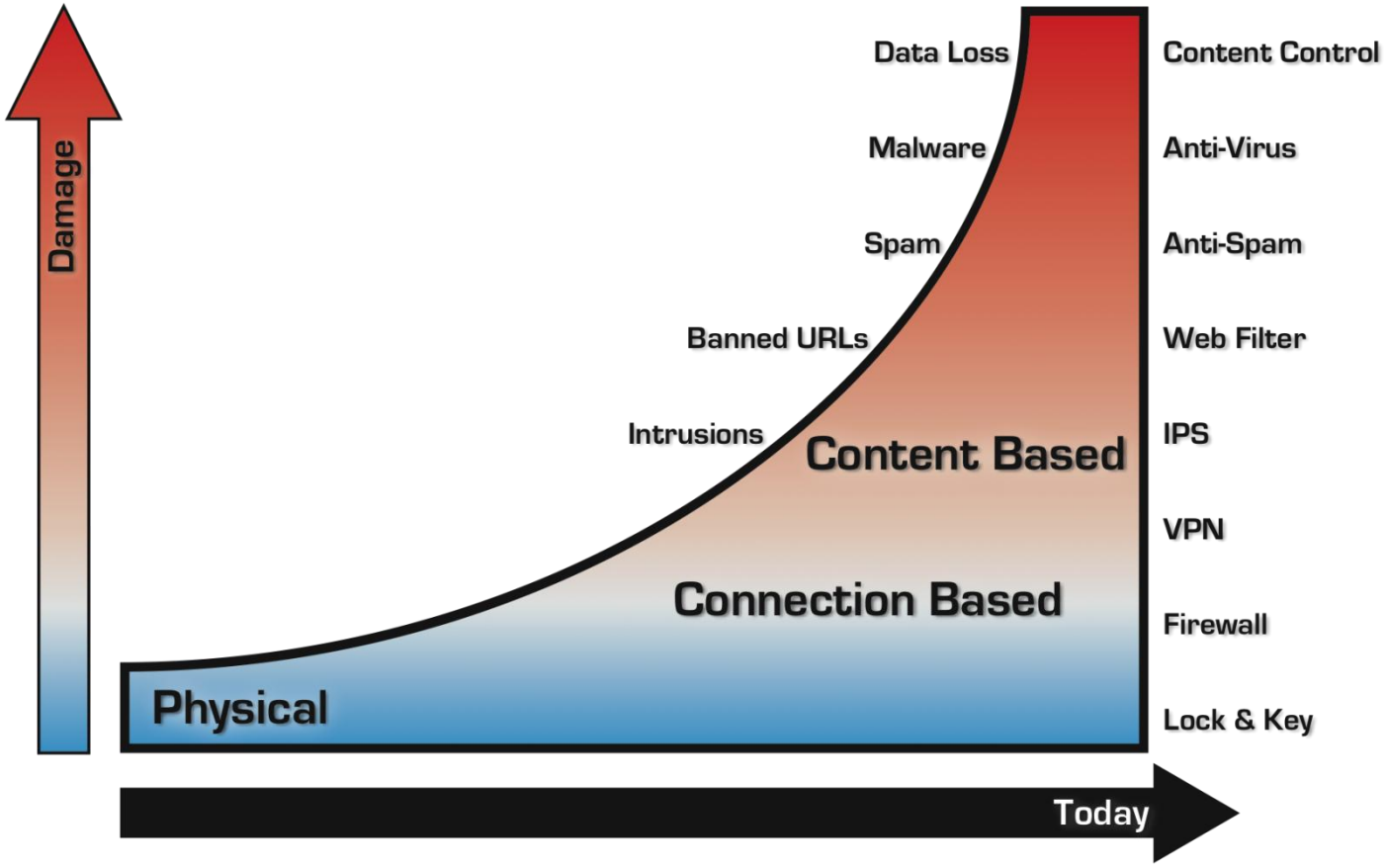
OTHER LARGE SCALE SECURITY TARGETS





The Solution

DANGEROUS CONTENT



Most threats come through CONTENT

- Dynamic Content
- High Performance
- Complex Traffic

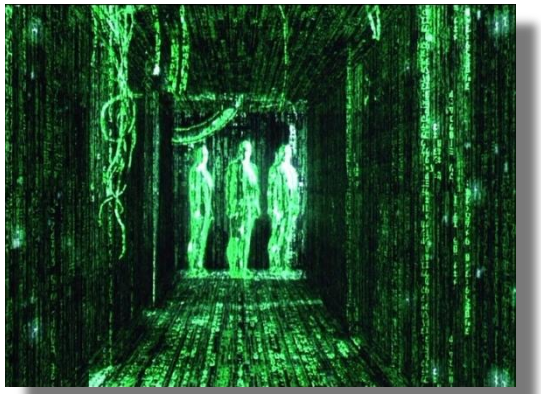
STOP THE TRANSMISSION OF MALICIOUS CONTENT

In the Middle Ages, we had to boil water for cleanliness and safety…
Today, we expect clean and safe water coming out from our taps…
Internet traffic should not be any different!

DEEP CONTENT INSPECTION

Goal: 100% visibility of content, not just packets or application types

Deep Packet Inspection

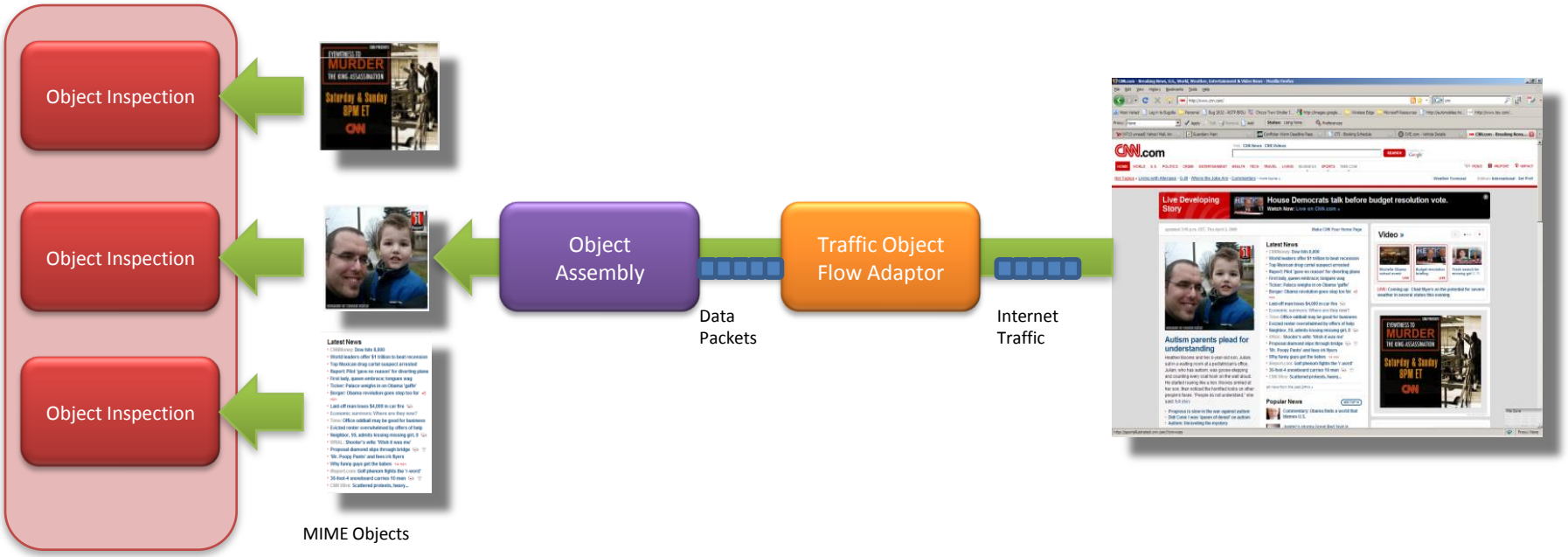


Deep Content Inspection

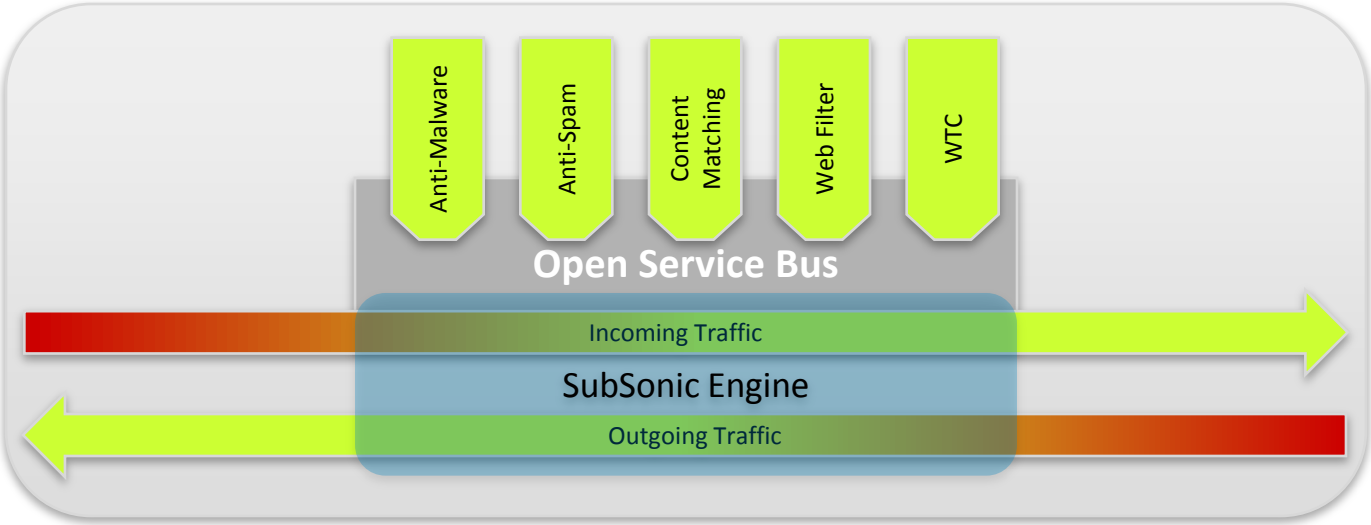
Requirements

- Visibility of the whole application session and data-in-motion (the content vs. individual packet)
- Intelligence to understand the intent of content
- Content independent of protocol

HOW IS CONTENT INSPECTED?



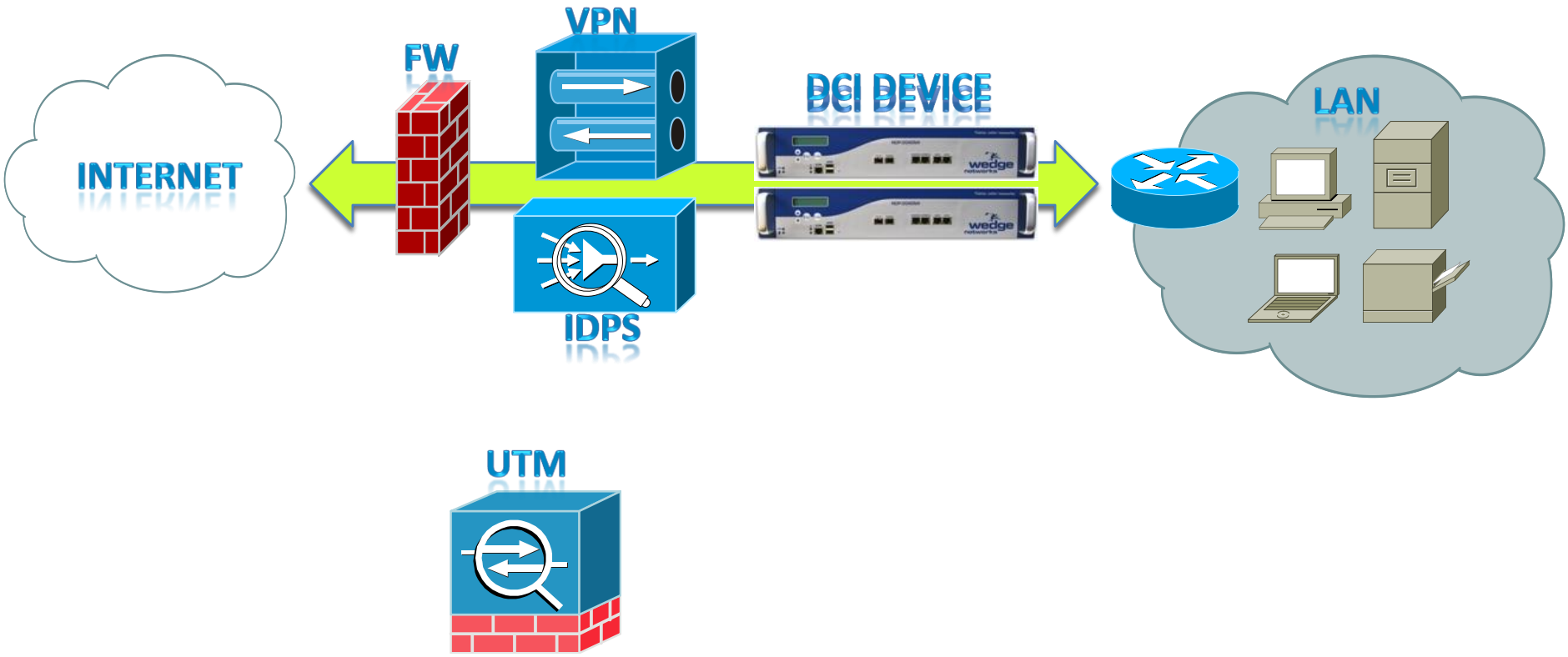
HOW IS SECURITY ENFORCED?



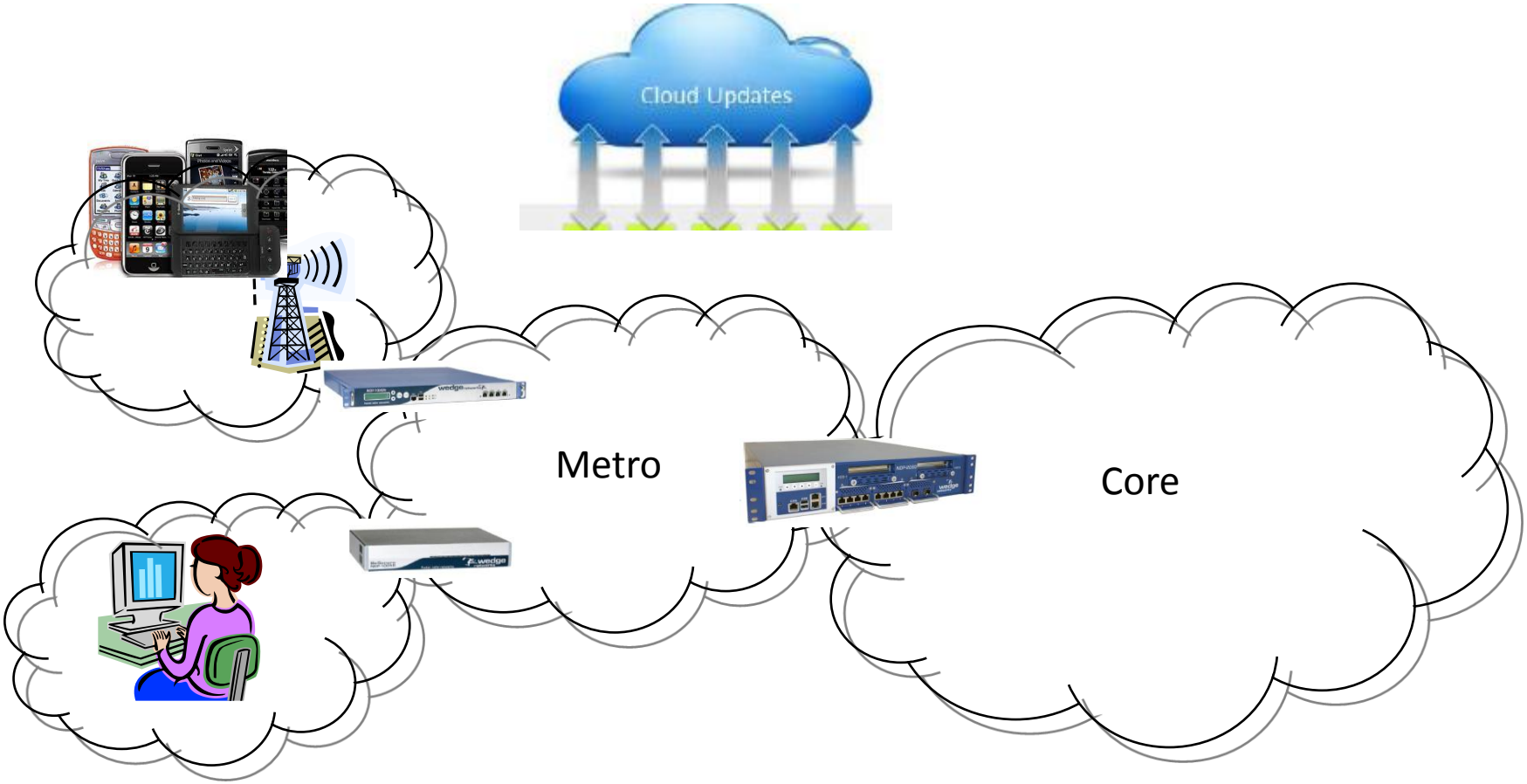
Open Services Bus

- Allows Any Engine to be Implemented
- Scan Once Apply All Services
- Applied Across Multiple Protocols
- Multiple Best of Breed Party Signature / Heuristics Engines

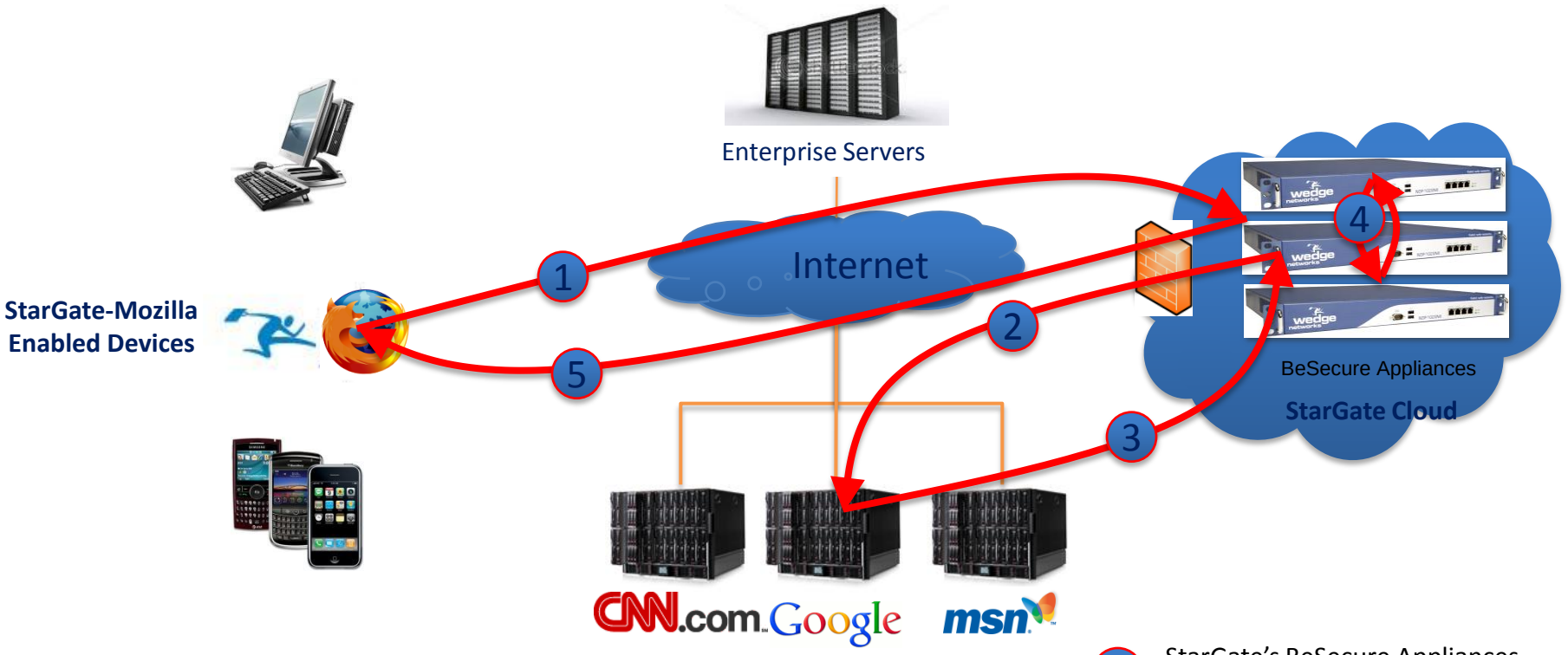
WHERE IS IT LOCATED?



WHERE IS IT LOCATED?



WHERE IS IT LOCATED?

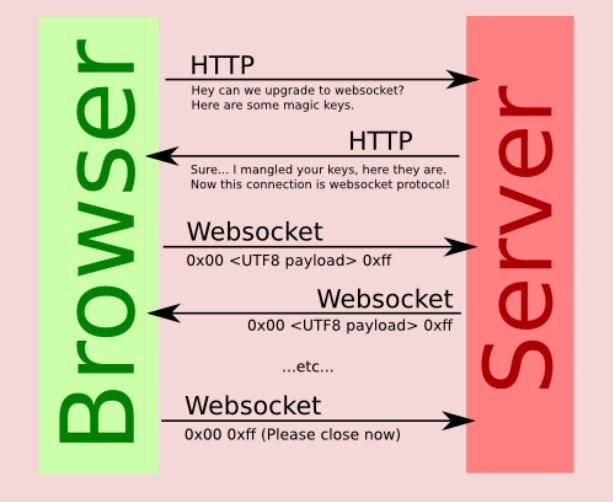


1. StarGate-Mozilla Browser issues www.google.com to StarGate Cloud
2. StarGate Cloud fetches www.google.com content
3. www.google.com content is sent to StarGate Cloud
4. StarGate's BeSecure Appliances scans www.google.com content
5. Clean "www.google.com" content is delivered

DCI: USABILITY REQUIREMENTS

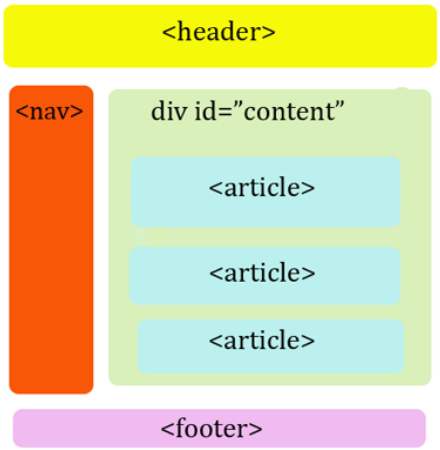
High Performance • High throughput • Low latency • Scalability	High Security Accuracy • Best-of-breed detection analytics • Frequent updates to automatically adapt to new threats
Network Equipment • Plug&Play in existing networks • Multitude of HA/LB options	Managed Device • Flexible/adaptive DCI policy • Event reporting/Dashboard/Threat notification • Firmware field updating. • Web, CLI, SNMP management interfaces

USE CASE: HTML5



- New structure for content
- Known malware undetected within Websocket
- Large amount of two way concurrent sessions

Ref: http://warmcat.com



SUMMARY

- The new internet: large scale content creation, aggregation, and distribution
- The large scale security issues
- DCI as a solution

Questions?

Thank You

Dr. Hongwen Zhang
President & CEO
Hongwen.Zhang@WedgeNetworks.Com
Tel. +1.403.441.2030