Cloud & Security & Mobile

New Security challenges for Telcos

2012 CEE-SEC(R)

Software Engineering Conference in Russia

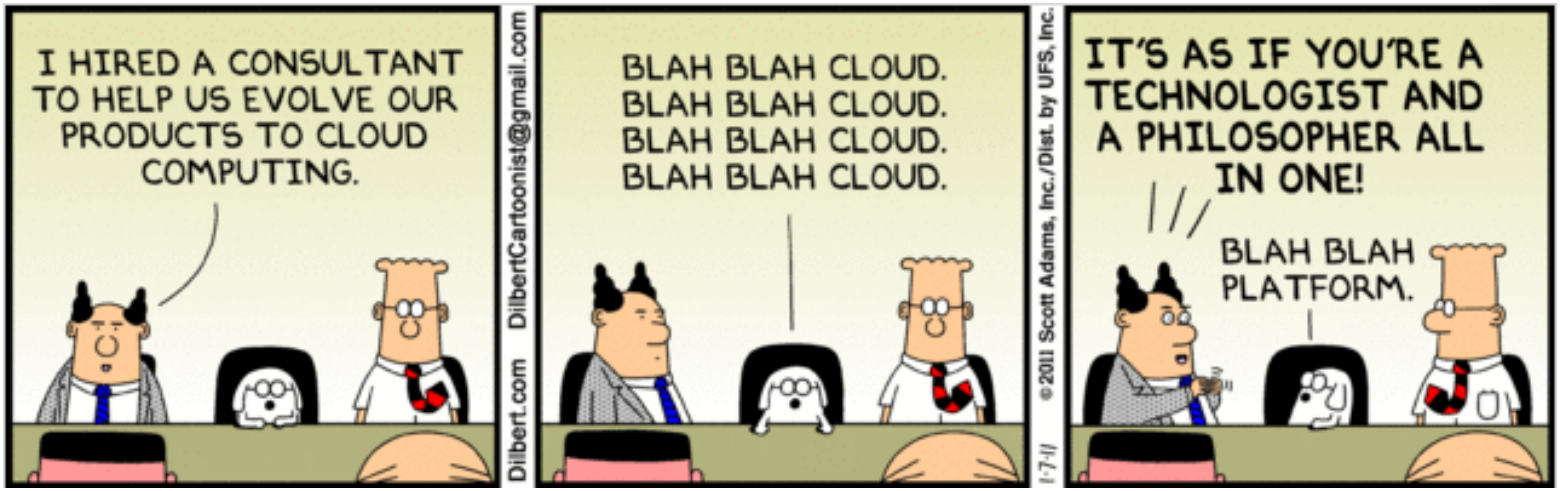
Telecoms new security challenges facing Cloud and Mobile expansion.
A new security approach

Juan Miguel Velasco
November 2012

Agenda

- ✓**CLOUD & Security. Introduction approach…**
  - A brief view of Cloud
  - Expectations & Benefits for Cloud Services
  - Security and Global Threaths situation
- ✓**Telco World evolution**
  - Telco traditinal business
  - New devices and mobile expansion
  - Cloud & Telco
- ✓**Cloud as a Security Tool vs Cloud Threats**
  - Mobile threats
  - Cloud threats
  - Security alternatives

Cloud, no need for the standard introduction …. **But…**

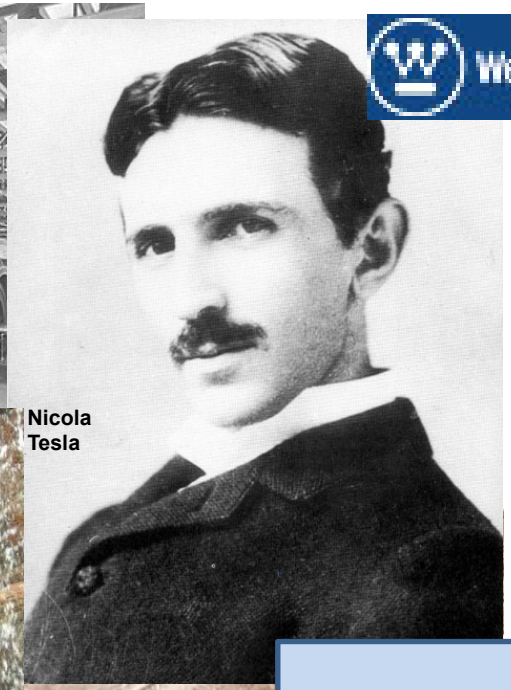


Source: Dilbert.com 2011.Dilbert ©2012, Universal Uclick

19th Century

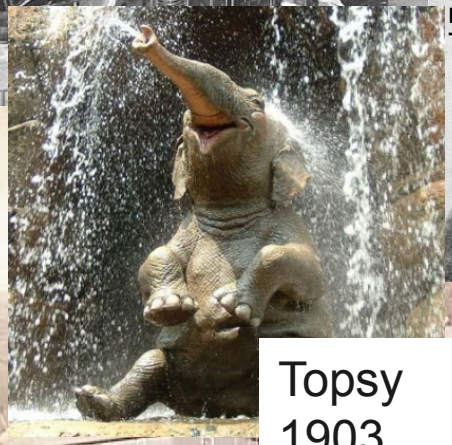
01 The War of Currents: AC / DC

Cloud Electricity from 1900 to 1930

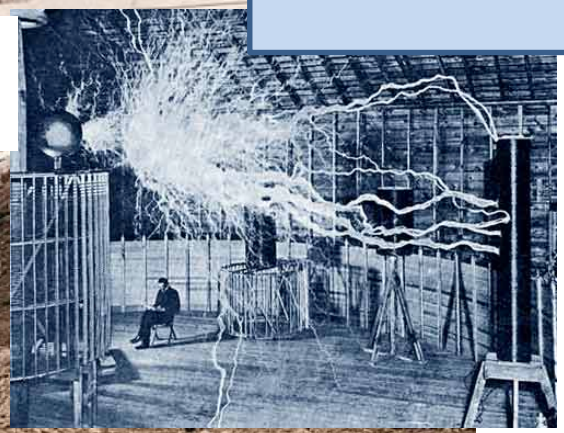


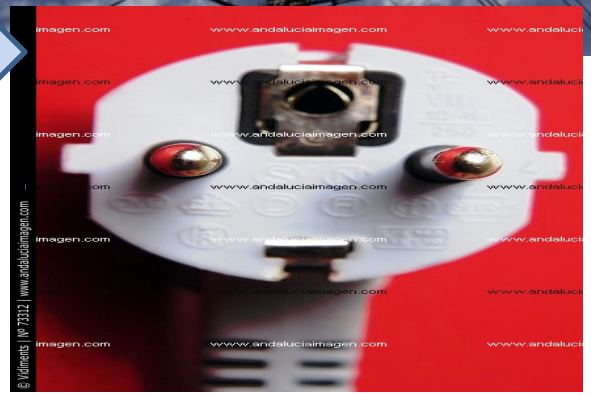
Nicola Tesla

Westinghouse



Topsy 1903



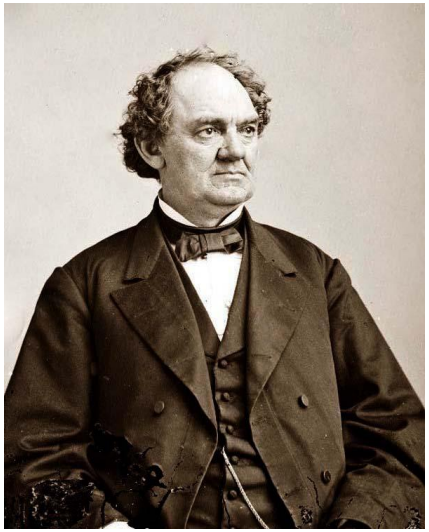


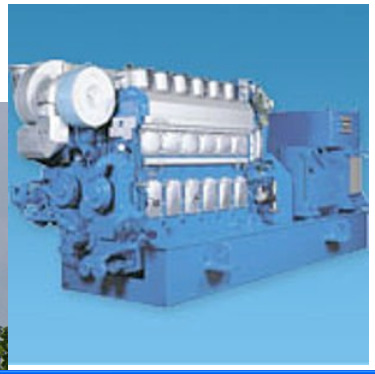
imagination at work

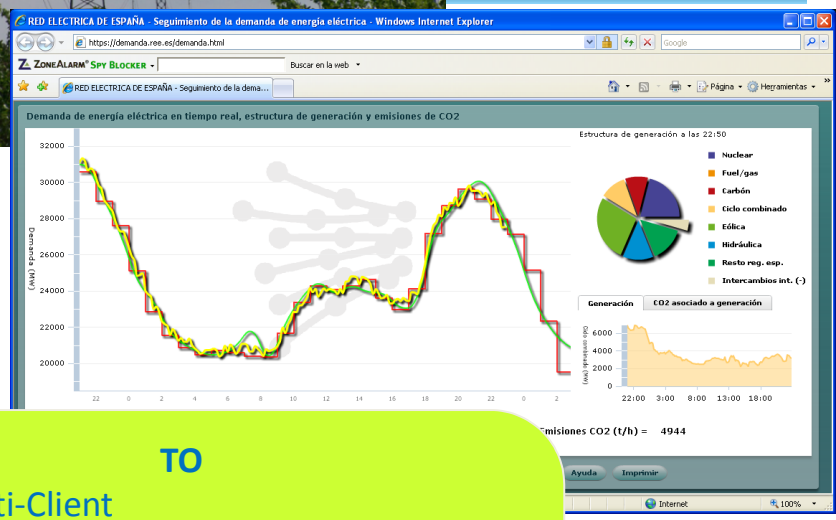
20th Century

01 Cloud Introduction– Electricity Cloud

Electricity revolution vs Cloud Revolution







1890 – Anonymous Enterprise:
"Our Business doesn't need any external current at all, we are autonomous"

FROM

- No multi-client
- Limited Generation
- No standardization
- High investment required
- Dedicated technical team required
- Local scope

TO

- Multi-Client
- Standard API (AC/DC – Voltage 110V-220V)
- Pay – per – Use
- 24x7 always on
- Remote management & support
- Unlimited service
- Worldwide service

http://www.ree.es/operacion/curvas_demanda.asp

How to find eficency with IT infrastructures?

IT evolution Cloud as IaaS / SaaS

IT Infrastructures

Aplications

SW Base & Middleware

IT Equipment

DataCenter Infrastructures

First Approach to Cloud

Manteinance consolidation
Operations consolidation

Support Consideration
Standarazation
Software free

HW Consolidation
Virtualization

Cooling Consolidation
Free Cooling
Cold / Warm corridor

Transformation

SaaS
IaaS
Services Centers

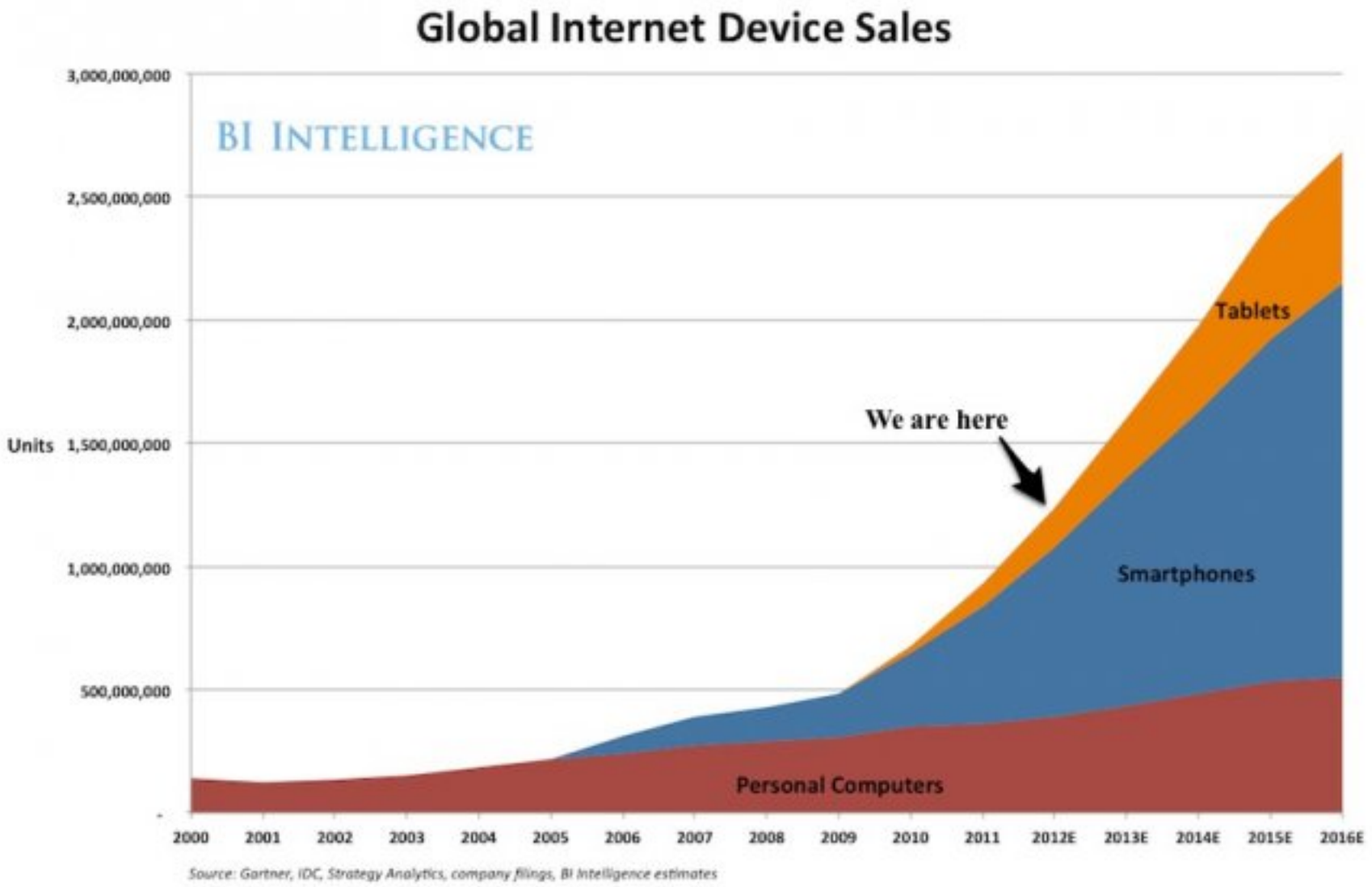
Private Cloud (Sharing for Gov only)

DataCenter Consolidation

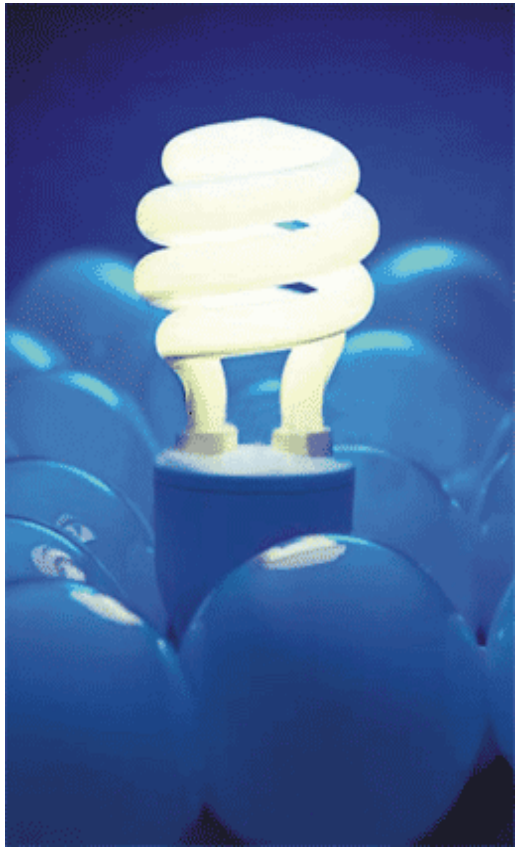
Cloud is NOT a technology is a market transformation

In 2020, people will interact each day with more than 70 devices connected to Internet. Nowadays we interact with less than 10 devices connected. The M2M phenomenom will boots Cloud and Internet users and bandwidth use.
From 1 billion users today to 3 billion devices connected in 5 years

By 2014 will be more connected devices to Internet than people on Earth



Cloud answer for:
Efficiency



Cloud, as Hosting services evolution

Collocation / Hosting 2000

Hosting Virtualization 2008

First move from classic servers to virtual servers
Sharing resources Storage, network, administration
Provisioning in hours not days

IaaS Private Cloud 2010

From days to minutes in provisioning
Network, Operating Systems, Applications,
Storage, everything onDemand
Private Cloud iterations

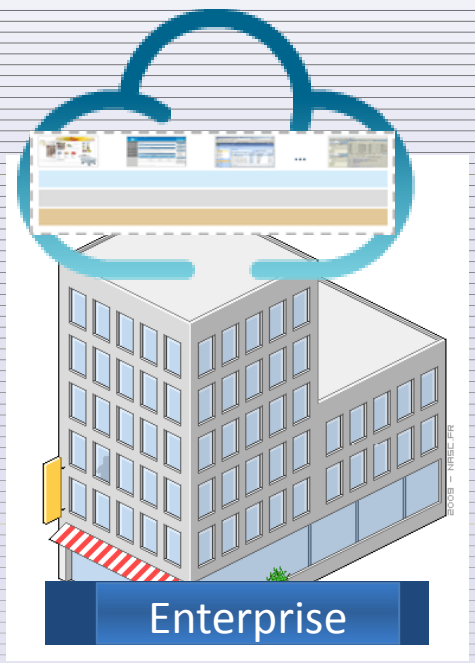
Public Cloud Services 2011

Evolution from IaaS – Private to Public
DataCenter merge and consolidation
Provisioning Portal – Full Mngmt
New API for Cloud and mobile

Mobility as an answer for :
Availability

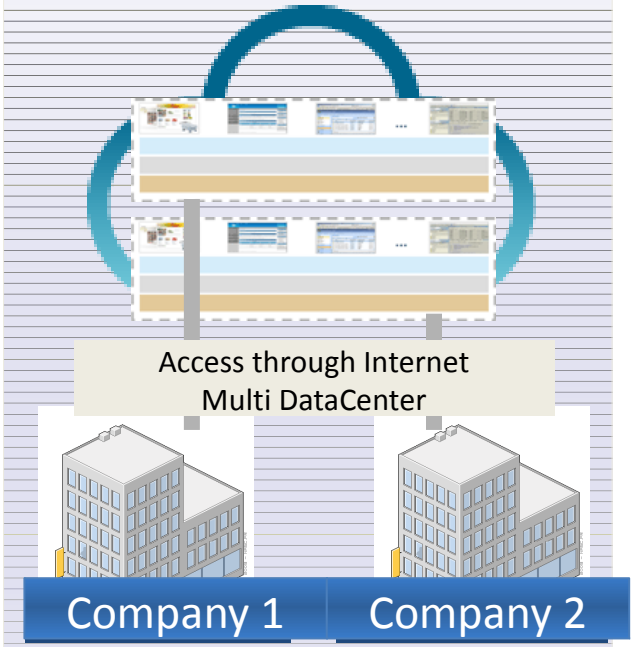
Cloud Models

Private Cloud



- High investment required
- Obsolescency risk
- Few operation cost optimization

Public Cloud



- Best scalation offering
- Lower costs
- Security concerns

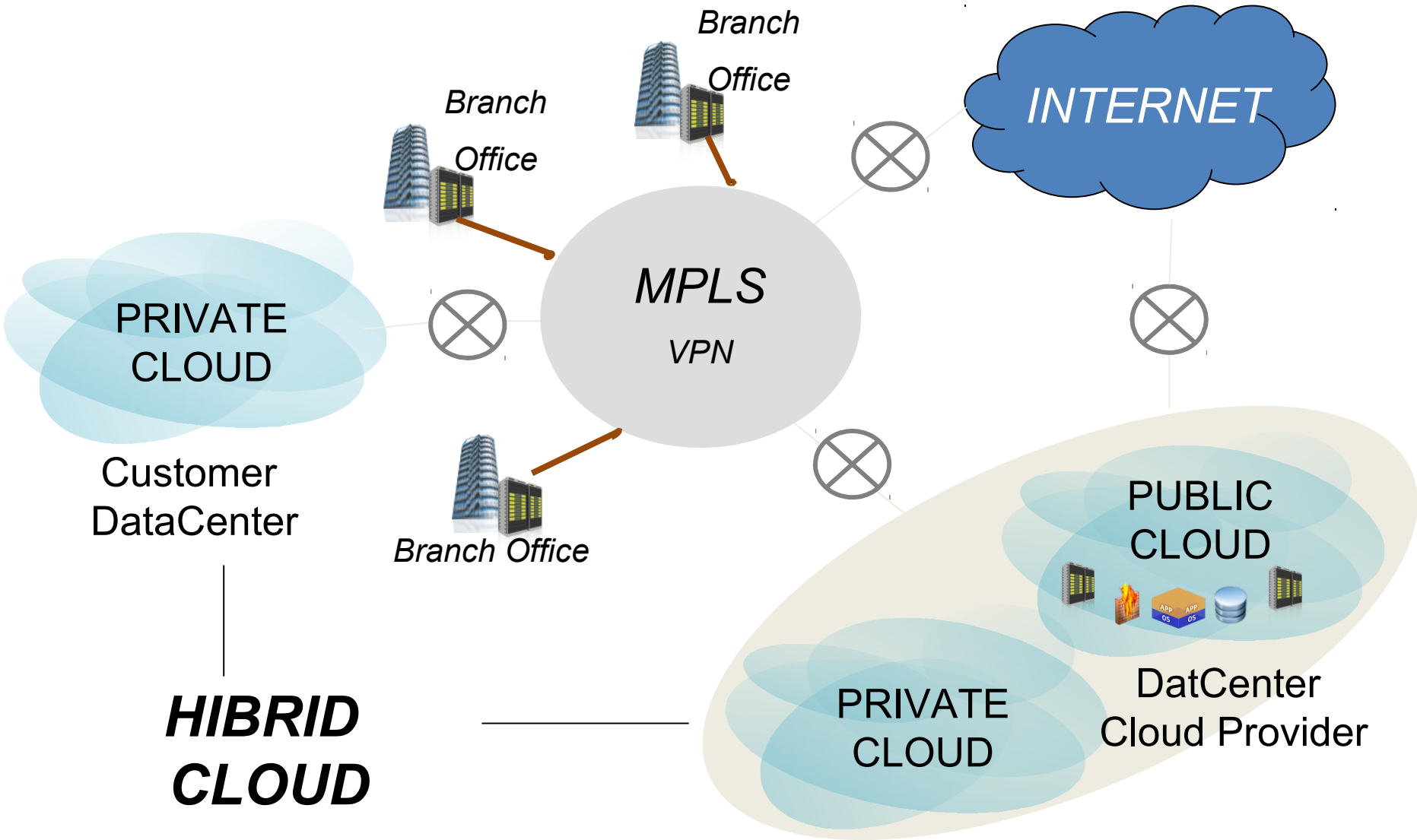
Hibrid Cloud

Private Cloud

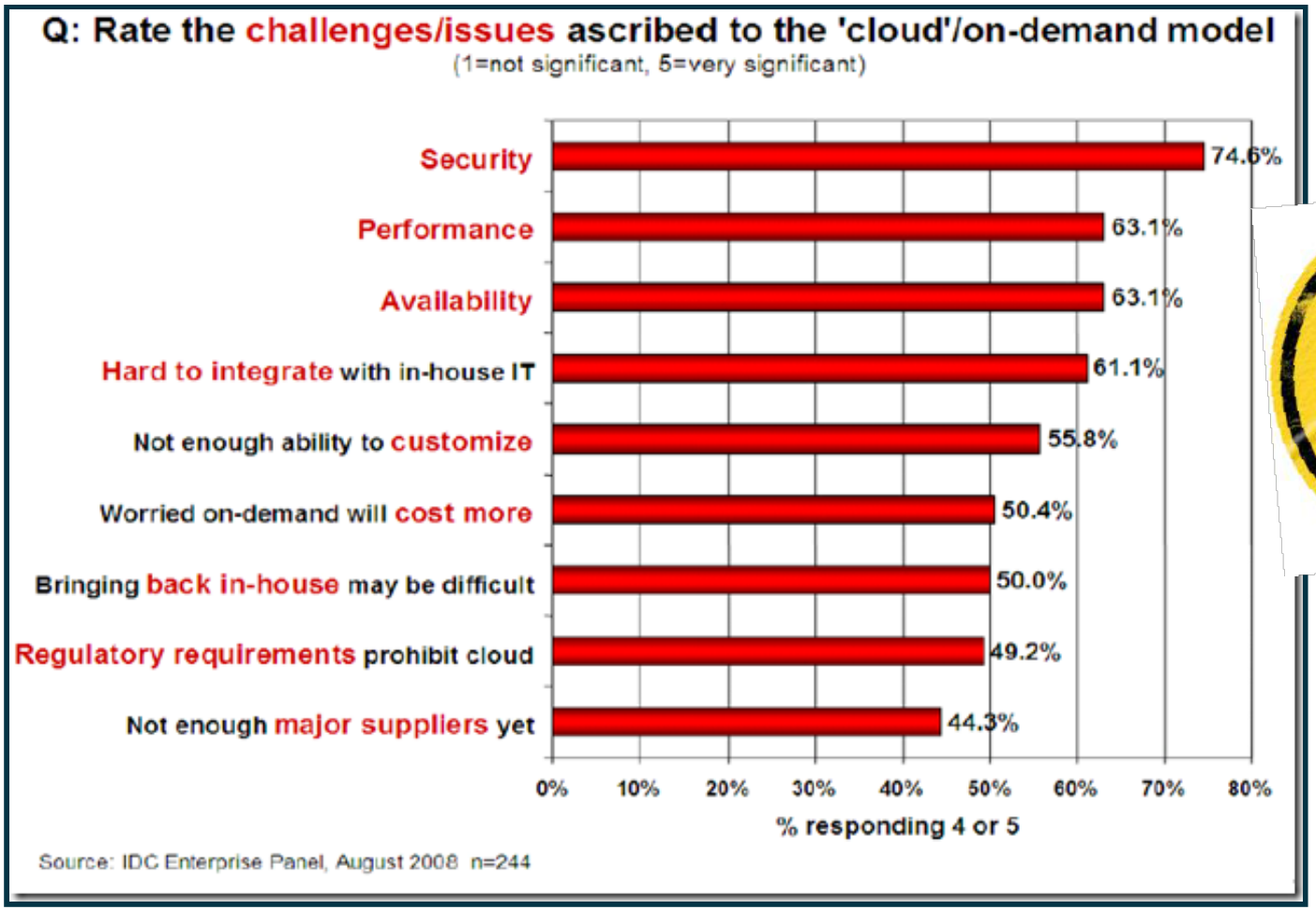
Enterprise

Public Cloud

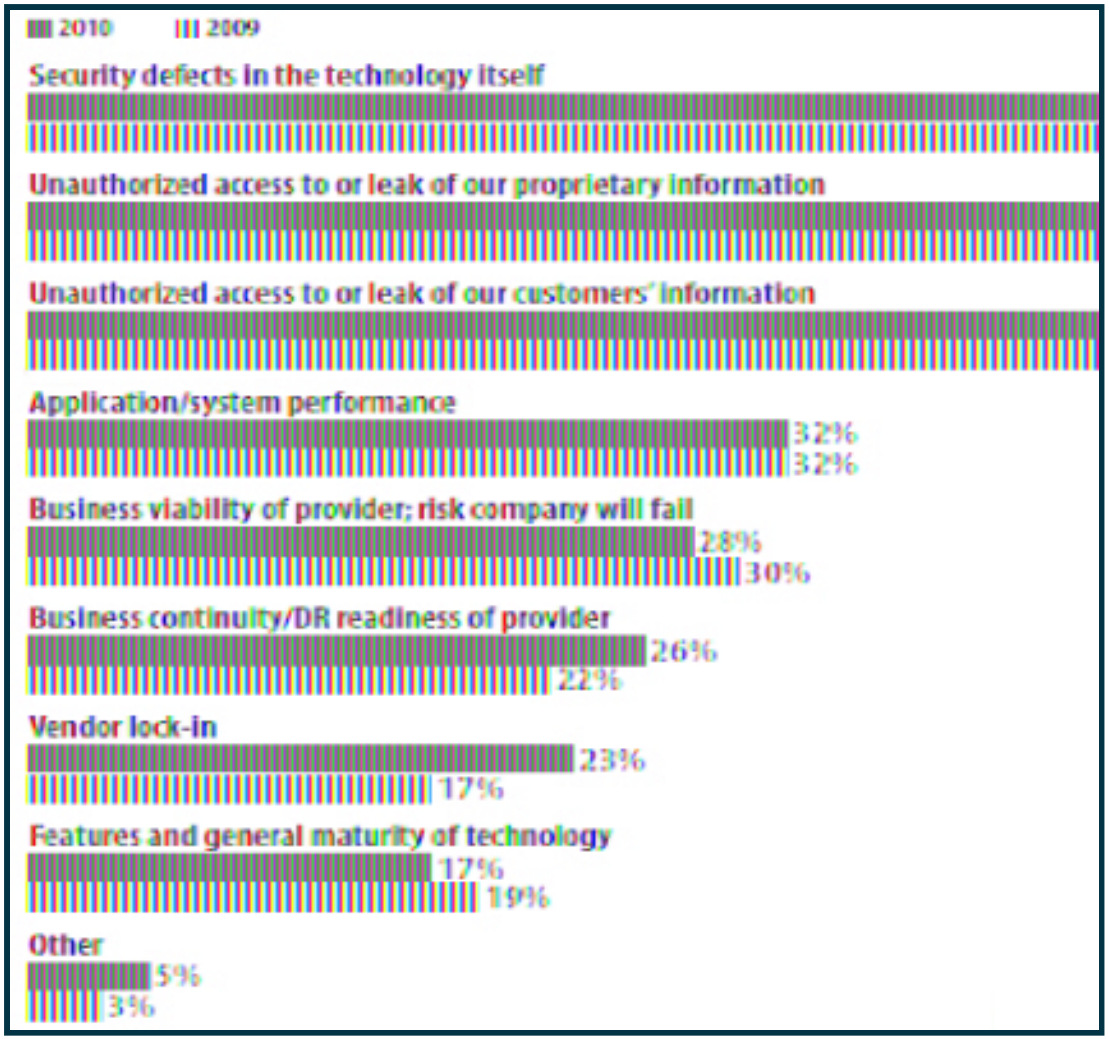
Global View for Cloud Models



CLOUD Security concerns



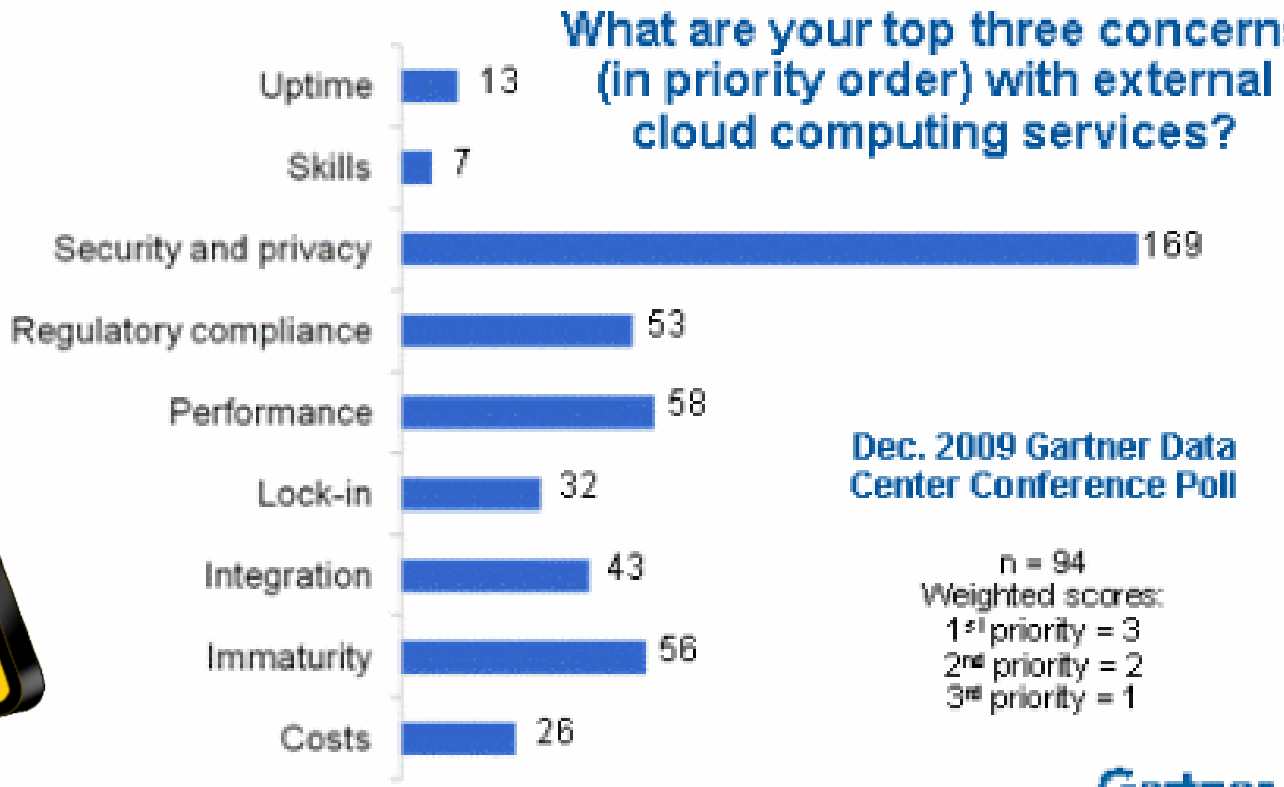
Cloud Security priorities



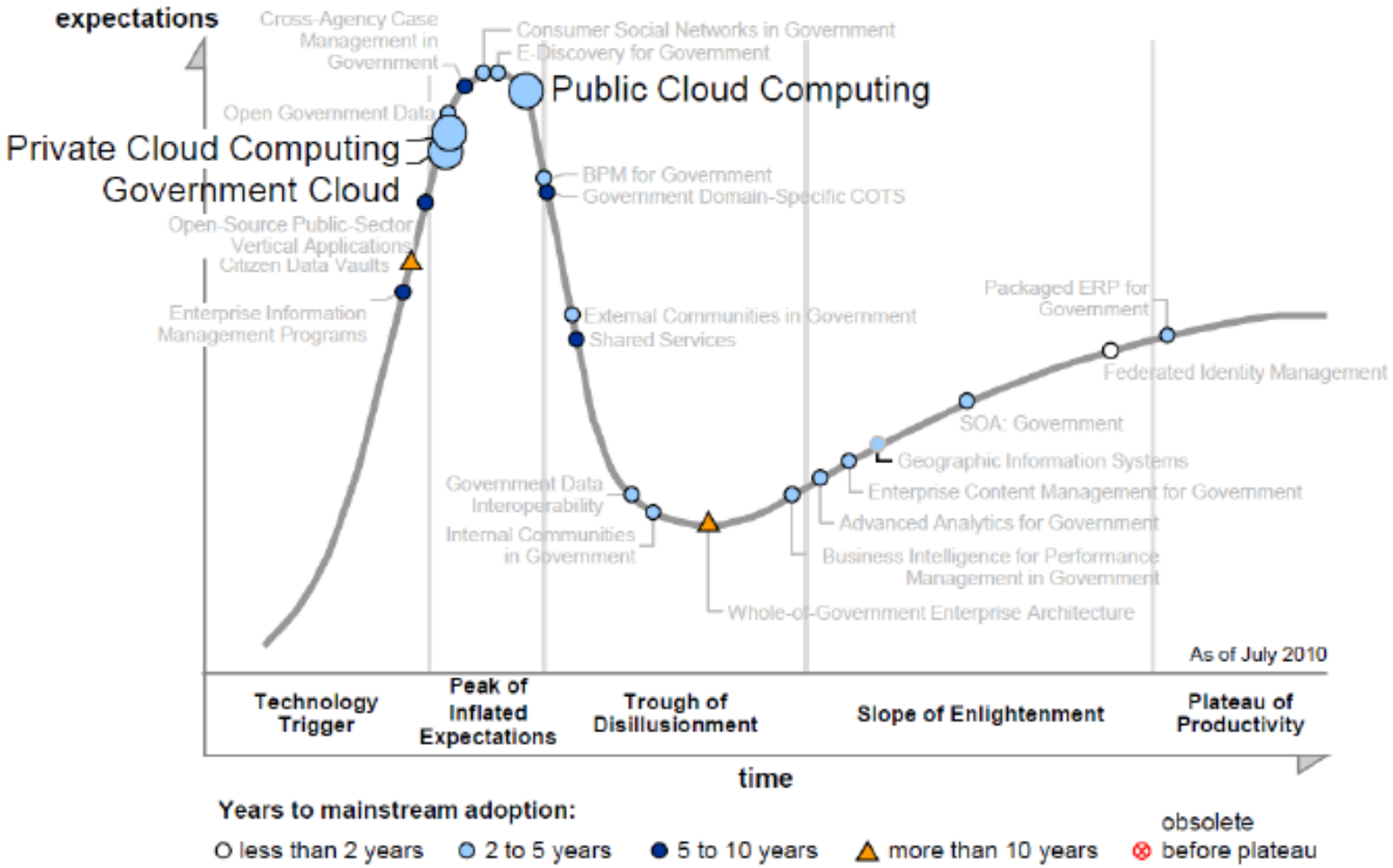
Fuente: InformationWeek Analytics, State of Cloud 2011: Time for Process Maturation

Concerns about Public Cloud (not private Cloud?)

Concerns With Public Cloud Computing



Cloud Computing in the Hype Cycle for Government Transformation, 2010



(From: "Hype Cycle for Government Transformation, 2010," 20 July 2010

Gartner

What Control Mechanisms Does the Vendor Provide?

- Identity and access management
  - Federation, strong authentication, access and roles
  - How to verify who has access to what and who has done what?
- Data confidentiality protection
  - Encryption of data at rest and in transit
  - How do you manage encryption keys?
- Monitoring and alerting
  - DLP, IPS, SoD, DAM
  - How do you perform an audit?
- Discovery and investigation
  - How do you do forensics in multiple jurisdictions?
  - What is a business record?
  - Don't forget law enforcement access

If they don't build it in, you can't use it.

Gartner

CLOUD Security Cycle

Gartner

La Aceleración de los Ataques Avanzados Dirigidos

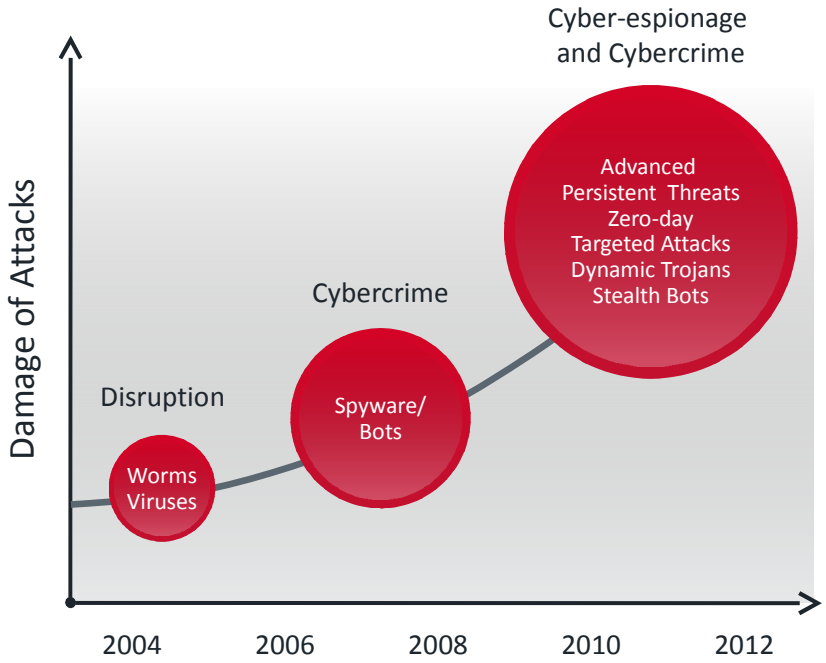
Number of threaths **x5** in 4 years

Nature of threats and attacks change:

- From general and diverse to persistent, avanced and oriented

Avanced attacks grow

- High victims level profile (i.e, RSA; Symantec, Google)
- Great variety of new APTs like Aurora Operation, Shady RAT, GhostNet, Night Dragon, Nitro



"Organizations face an evolving threat scenario that they are ill-prepared to deal with….advanced threats that have bypassed their traditional security protection techniques and reside undetected on their systems."

Gartner, 2012

Source re ye

APT Attacks. Attacks profile has increased

News

Symantec confirms source code leak in two enterprise security products

Hacking group discloses source code segments used in Symantec's Endpoint Protection 11.0 and Antivirus 10.2

By Jaikumar Vijayan
January 6, 2012 06:42 AM ET

9 Comments

Computerworld - Symantec late Thursday confirmed that source code used in two of its older enterprise security products was publicly exposed by hac

LulzSec, Sony, And The Rise Of A New Breed of Hacker

SHARE THIS STORY

Like Sign Up to see what your friends like.

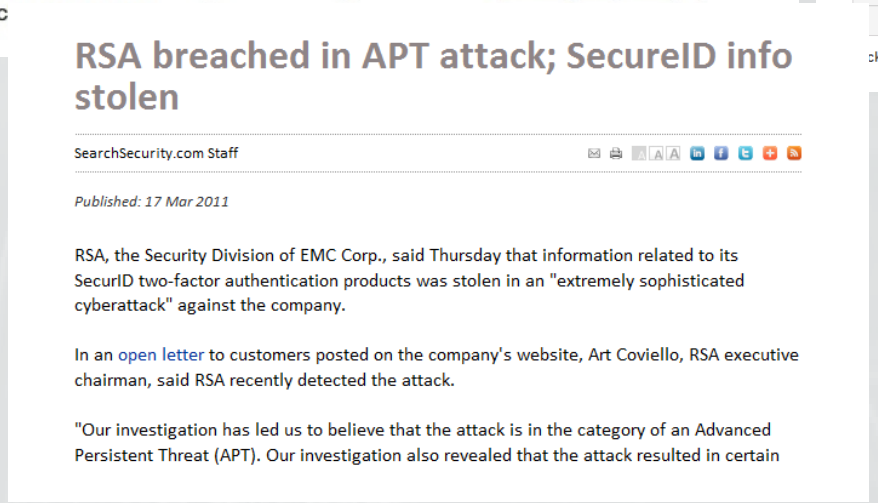
6 share | 11 tweet | 1 email | 20 comment

Get Technology Alerts

Sign Up

NEW YORK -- When a new hacking entity calling itself LulzSec claimed credit for a barrage of recent attacks on Sony and several other companies, many cyber-security experts found themselves grasping for a term to describe the attackers.

Hackers often divide themselves into two groups -- the "black hat" hackers, who exploit the vulnerabilities of their victims for profit, and the "white hat" hackers, who point out those weaknesses so that the vulnerable can take the proper measures to protect themselves. Yet as several experts pointed



RSA breached in APT attack; SecureID info stolen

SearchSecurity.com Staff

Published: 17 Mar 2011

RSA, the Security Division of EMC Corp., said Thursday that information related to its SecurID two-factor authentication products was stolen in an "extremely sophisticated cyberattack" against the company.

In an open letter to customers posted on the company's website, Art Coviello, RSA executive chairman, said RSA recently detected the attack.

"Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT). Our investigation also revealed that the attack resulted in certain

New Zero-Day Adobe Attack Under Way

Adobe working on emergency patch for Adobe Reader and Acrobat 9.x for Windows

Dec 06, 2011 | 11:18 PM | 0 Comments

By Kelly Jackson Higgins
Dark Reading

Adobe Reader and Acrobat are under siege once again, this time via targeted attacks exploiting a previously unknown flaw in the software that lets an attacker crash the app and wrest control of the victim's machine. Adobe plans to issue an out-of-band update by next week for Windows-based systems only.

source re ye

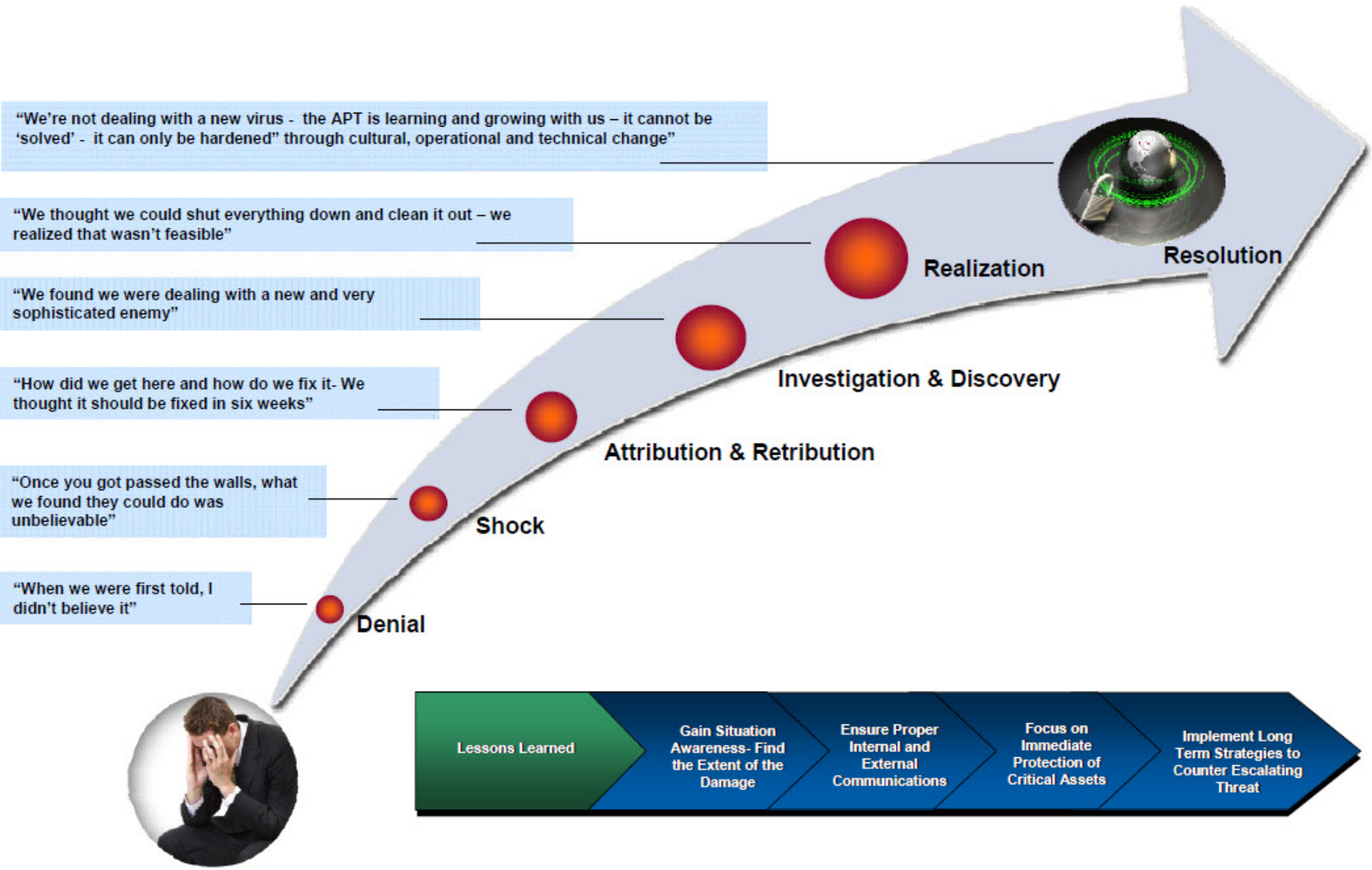
2012 CEE-SEC(R)
Software Engineering Conference in Russia

APTs GOALs. Motivation

Advanced Persistent Threats (APTs) are created by different organizations from hackers like Lulzsec, Anonymous,etc. Also by Federeal Goverments like CIA, Mossad, etc.Their main motivation are:

- **Goverment**
- **Economical**
- **Technical**
- **Military**

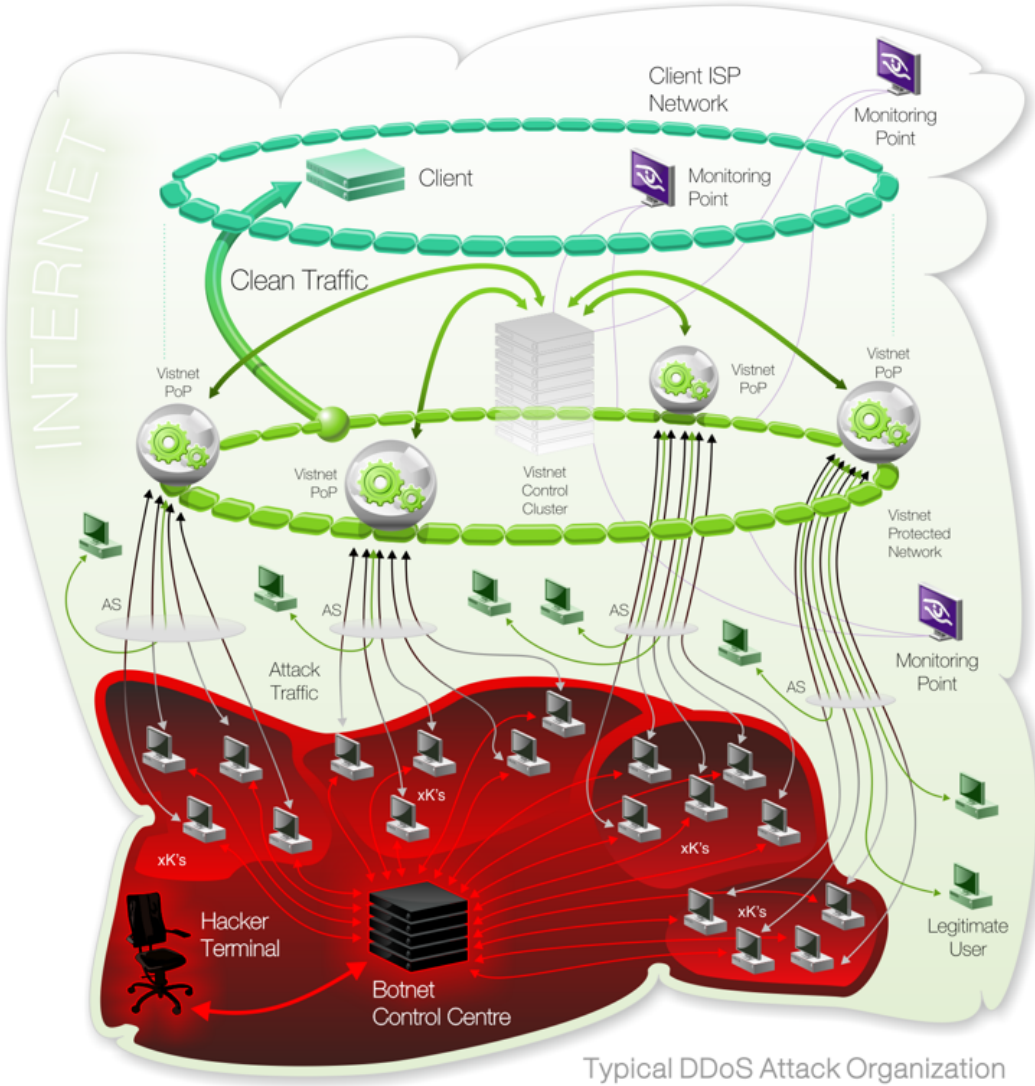
APT Case Study



APT LyCicle. Goals and Operations

Step 1	• Discovery (Perimeter/ Network)
Step 2	• Initial Network intrusion
Step 3	• Established a “backdoor” into the Network
Step 4	• Getting all type of credentials
Step 5	• Installation of malware tools. All kind
Step 6	• Data Link / Privileges escalation
Step 7	• Infection extension and expansion

DDoS the increasing threat, and persistent



Typical DDoS Attack Organization

- zón 1 • Universal
- zón 2 • Cheap
- zón 3 • Eficiency
- zón 4 • No pushment
- zón 5 • Big Impact
- zón 6 • Easy to replicate
- zón 7 • Underestimate

DDoS the increasing threat, and persistent

Attack Motivations Considered Common or Very Common

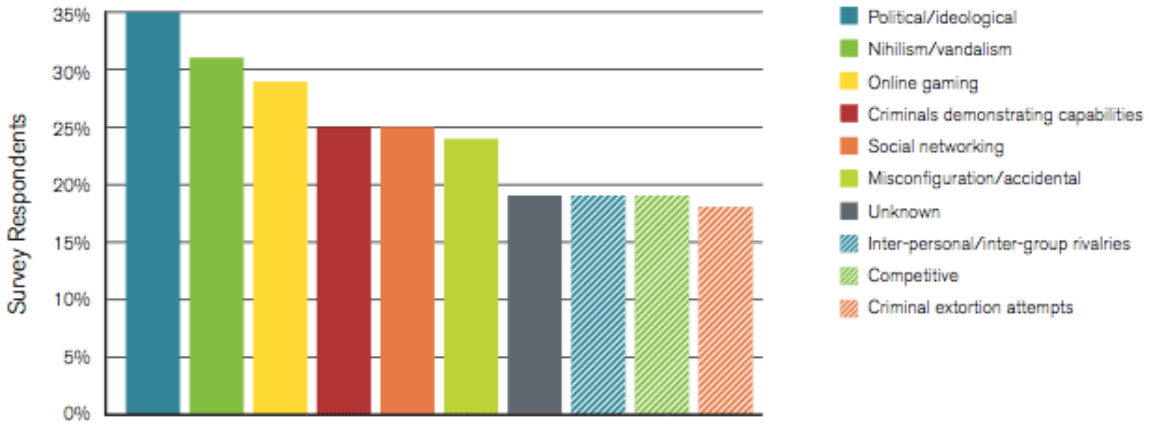


Figure 20 *Source: Arbor Networks, Inc.*

Average Number of DDoS Attacks per Month

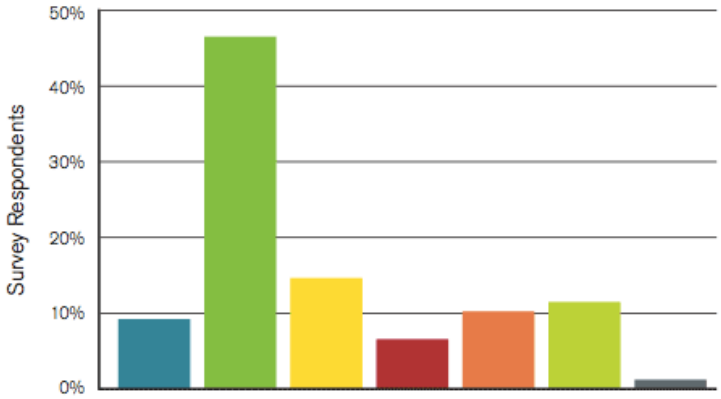
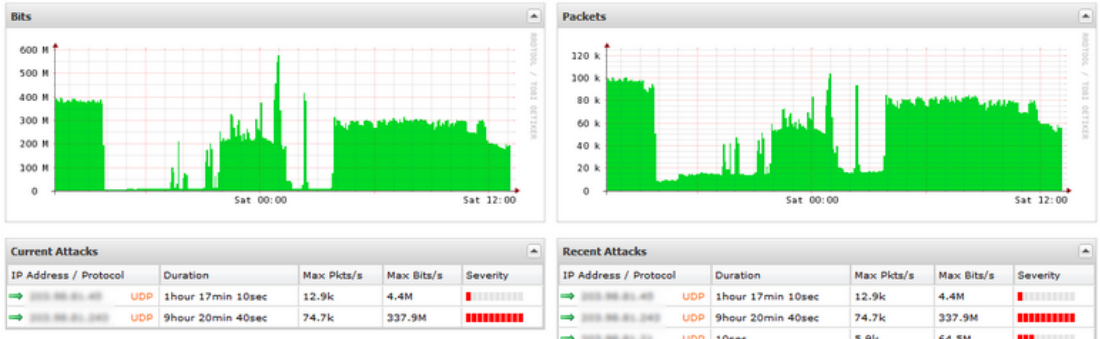
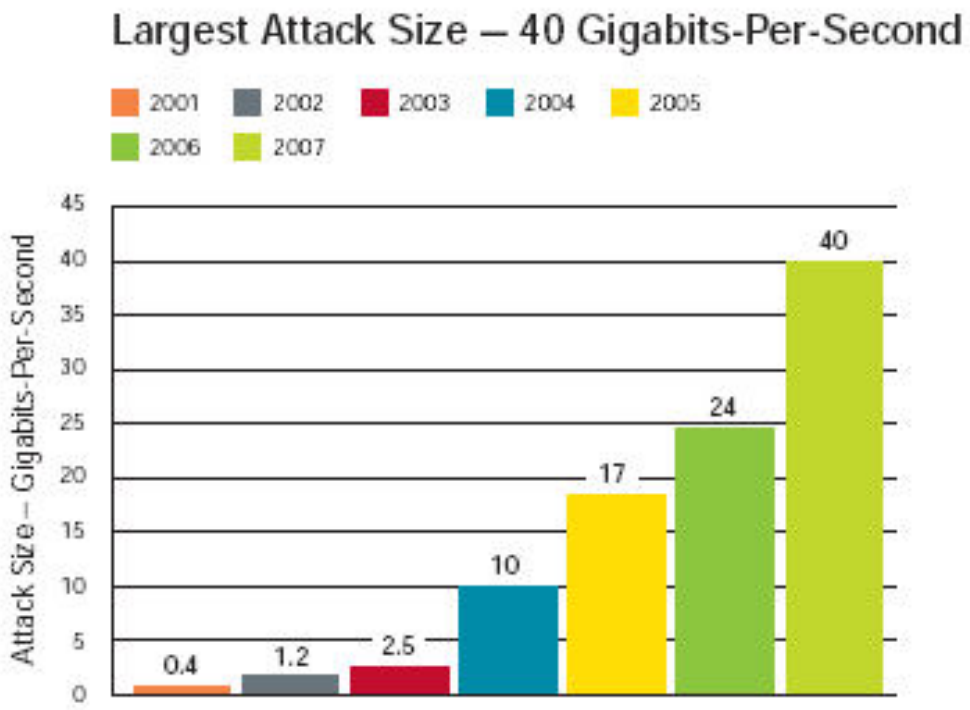
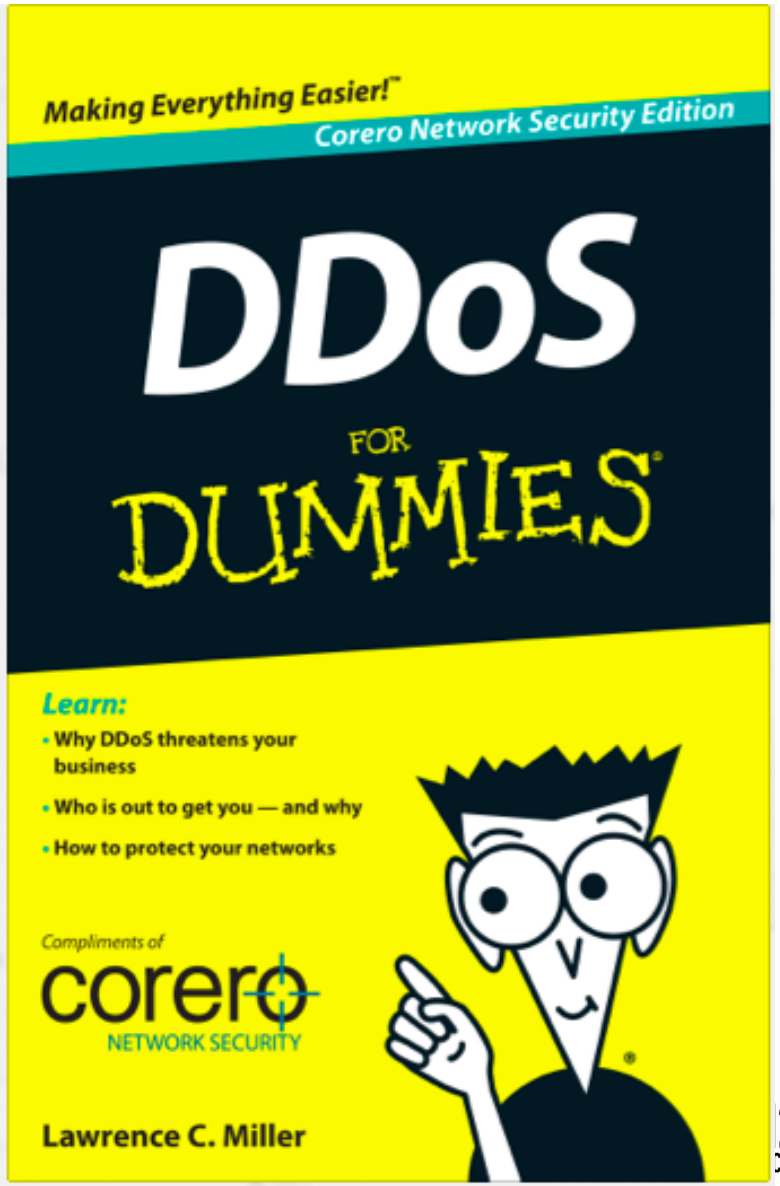


Figure 17 *Source: Arbor Networks, Inc.*



DDoS the increasing threat, and persistent





http://ww2.corero.com/lp/ddos/ddosfordummies-ebook.html

CLOUD as Security Ally

Services & Solutions

Anti-Fraud

Brand Watch

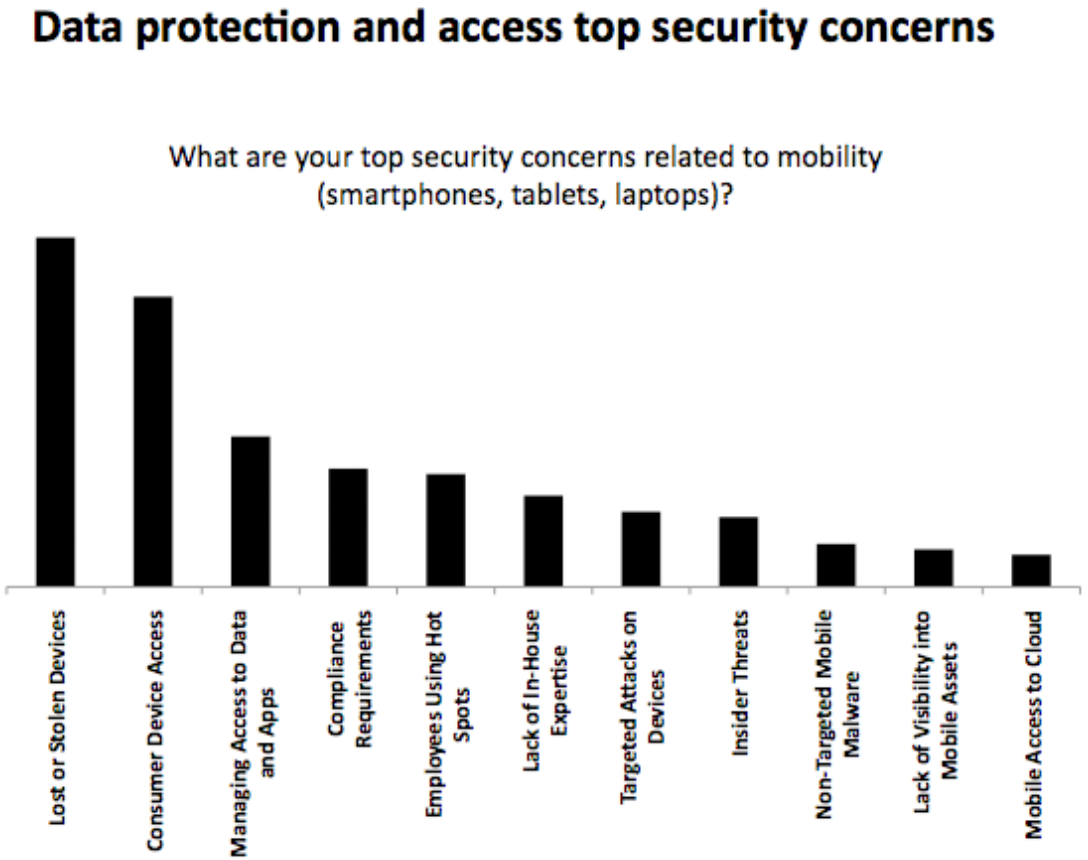
Email Security

Web Security

Source Code Vulnerability Analysis

Vulnerability Manager

Risk Mobile



Fuente: http://searchmobilecomputing.techtarget.com/ (2011)

BYOD `Bring Your Own Device´

BYOD and consumerization, is one based on the desire of employees to use their own mobile devices (phones, smartphones, tablets, laptops ...) in the workplace and access to information from this company, such as the corporate email, DB or file servers.

It is a reality accepted by IT departments, in the post-pc

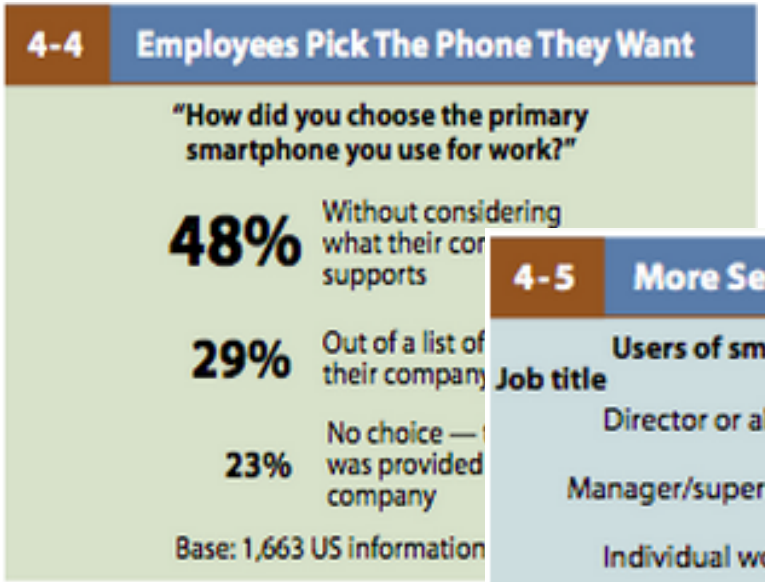
According to a survey of CISCO over 90% of CIOs surveyed said they permit, even doing the "blind eye," the use of mobile devices owned by employees to access their data.

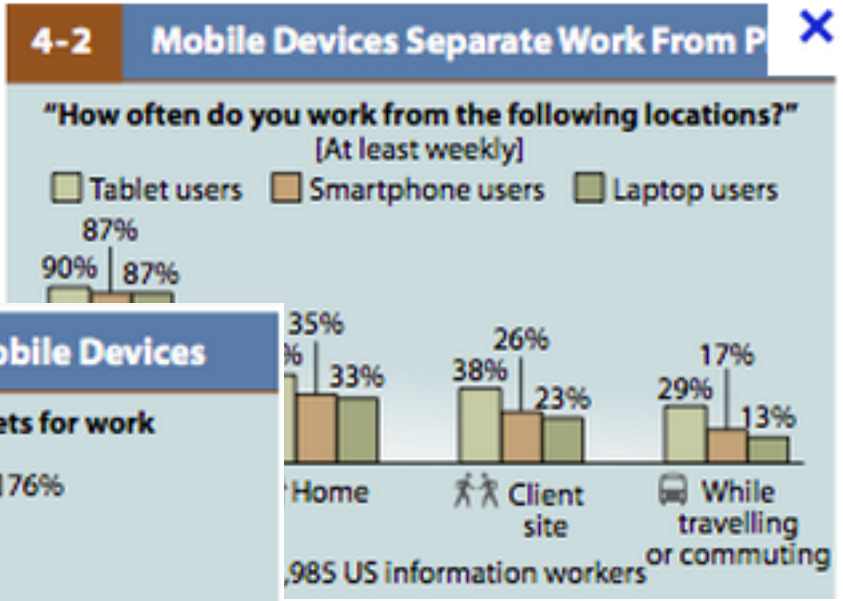
Of the principals surveyed more than two thirds have overcome fears this trend and see it as something positive for the organization.

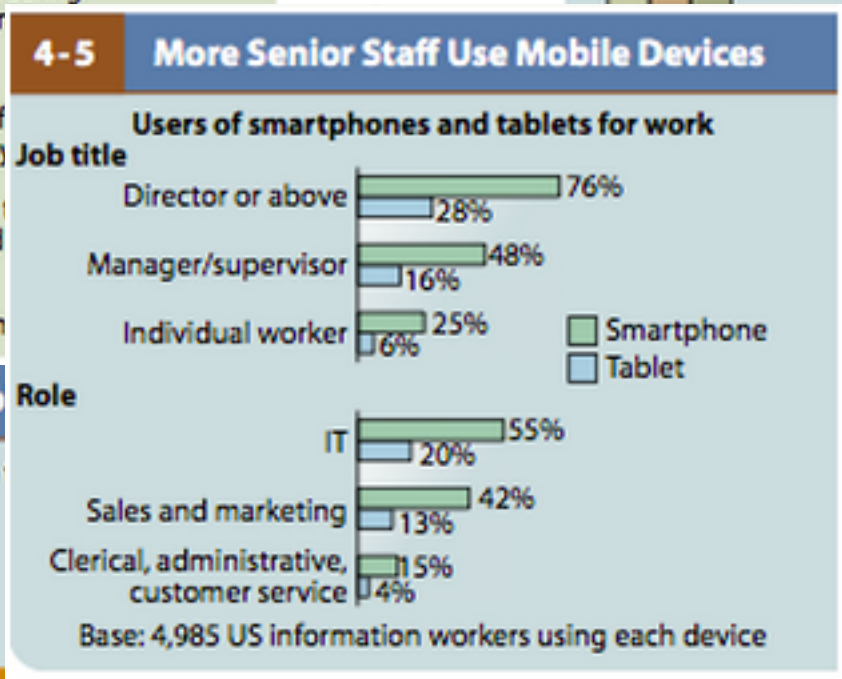
Yet another study, this time from the company BT, puts out the lack of vision of the potential risks of this practice on the part of employees, as only one in four sees risk in using their own devices, when almost 40% of companies have experienced security incidents related to this issue.

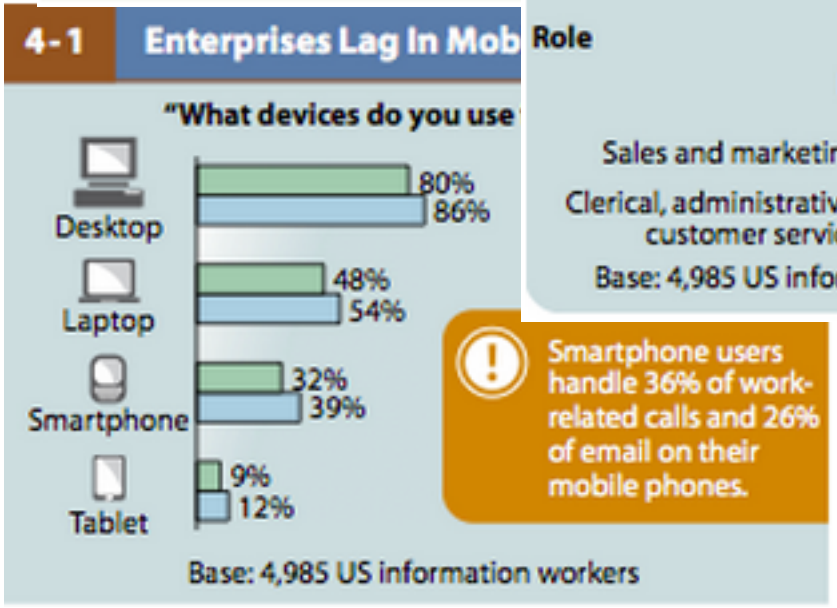
BYOD the New Threat door

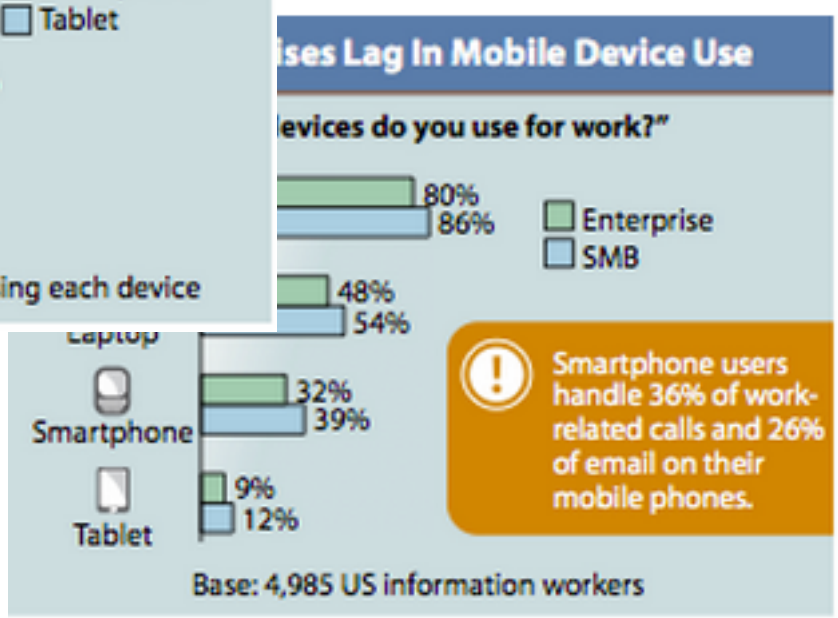
BYOD `Bring Your Own Device´





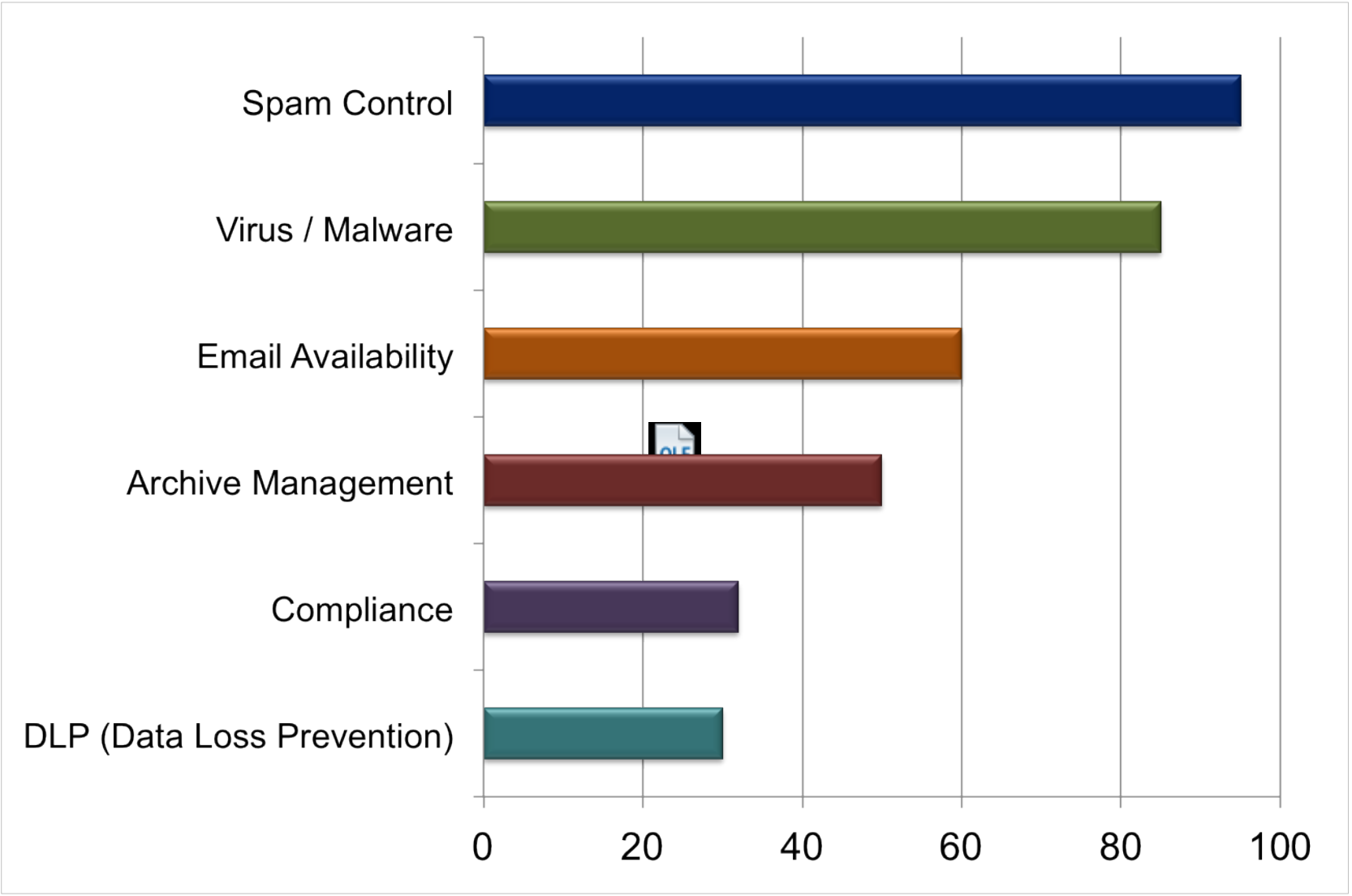




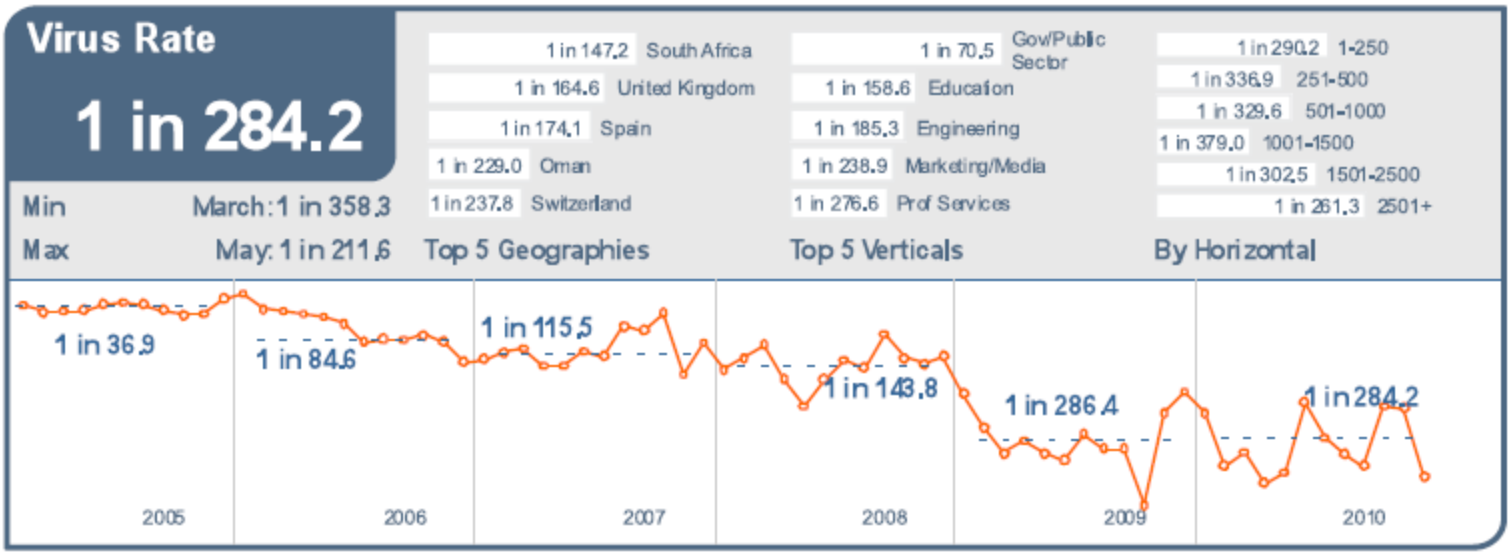


Email Security

- **Security Challenges of Email in the Cloud**



In 2010 one in every 284 emails contained malware.
1 out of every 445 emails is Phishing (posing as official or institutional)

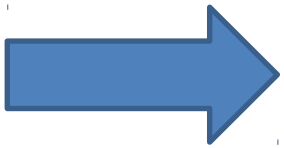


Seguridad email, DLP & Encryption

Security for customers and employees

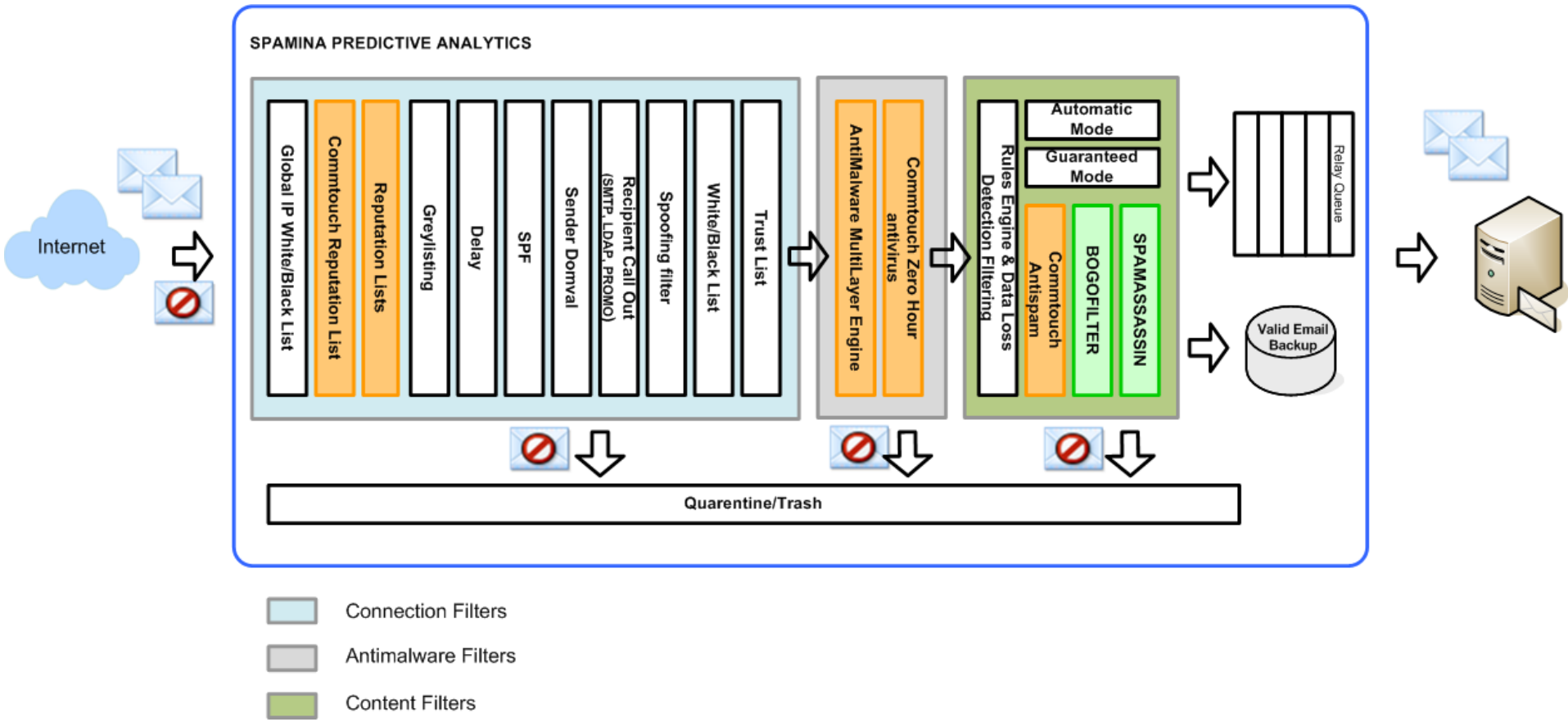
- Email is a strategic tool for organizations that must be protected and accessible at all times.

- Productive business processes are dependent on Email.

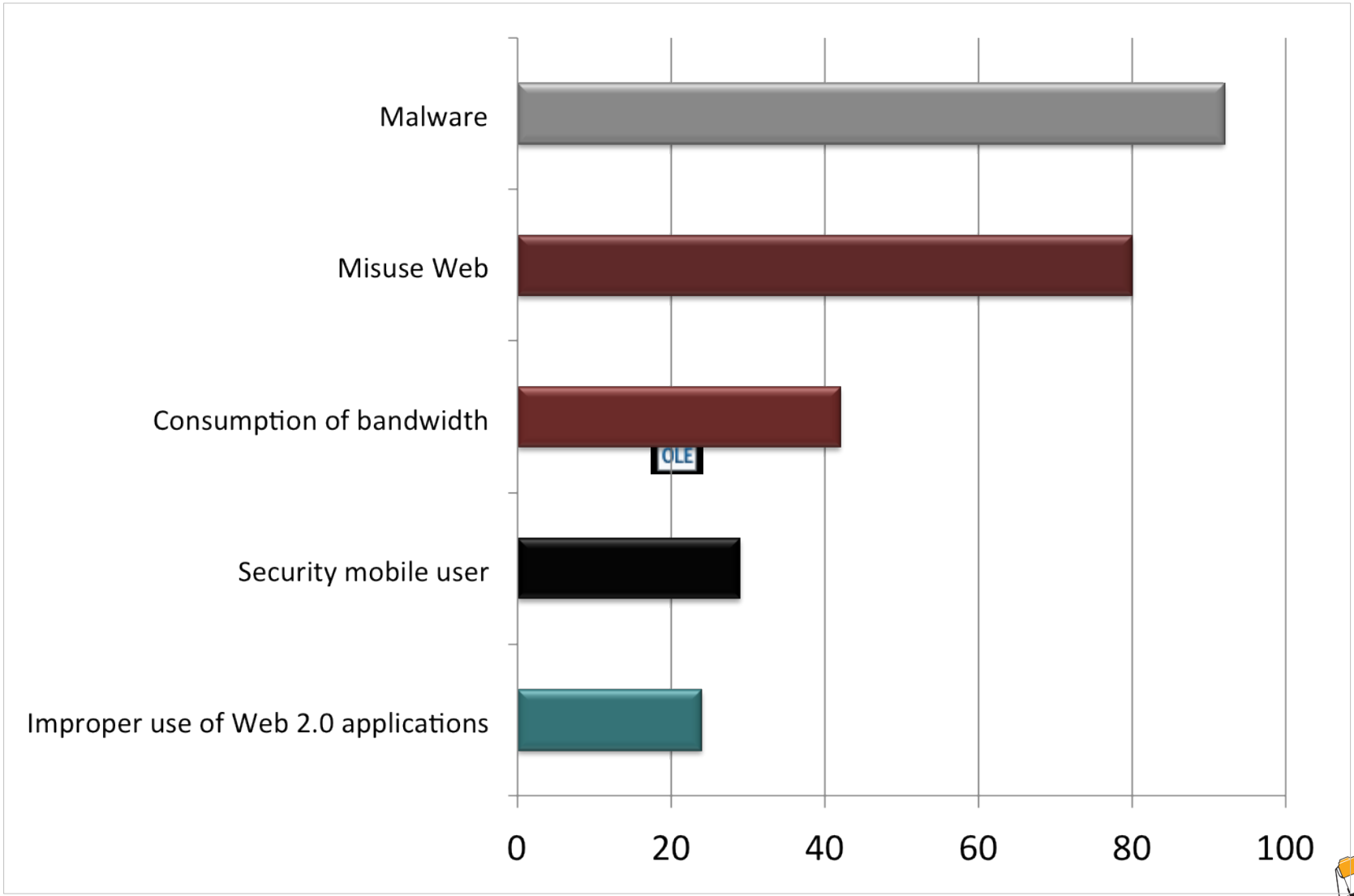


Seguridad email, DLP & Encryption

Security for customers and employees

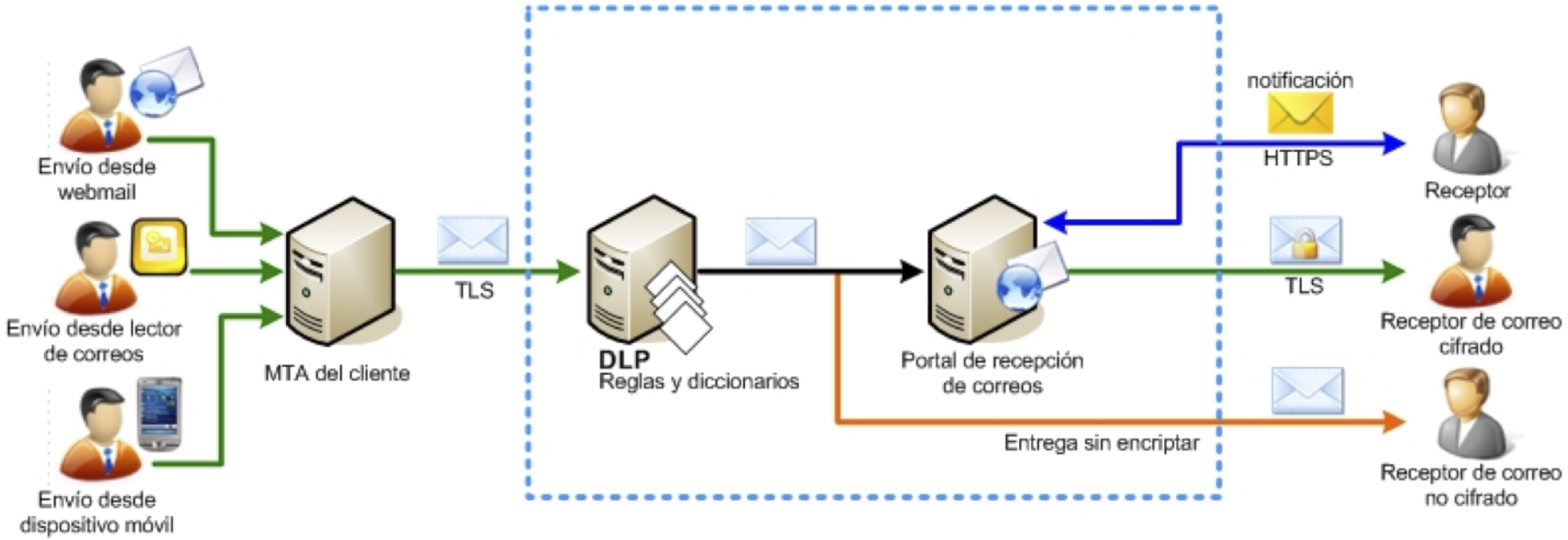


Security Challenges of Web traffic in the Cloud

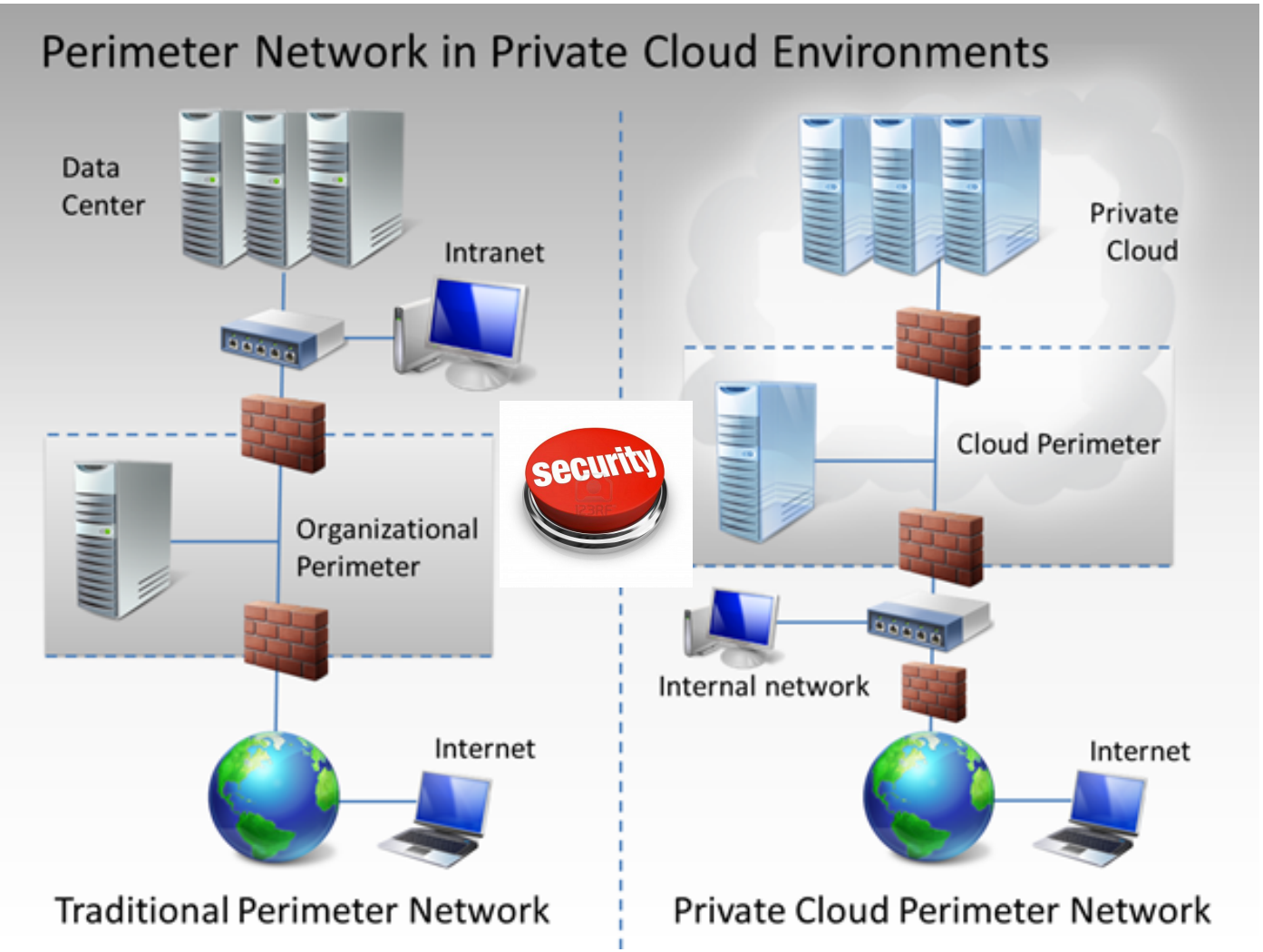


Seguridad email, DLP & Encryption

Security for customers and employees



El perímetro. Seguridad Cloud y Cloud para Seguridad

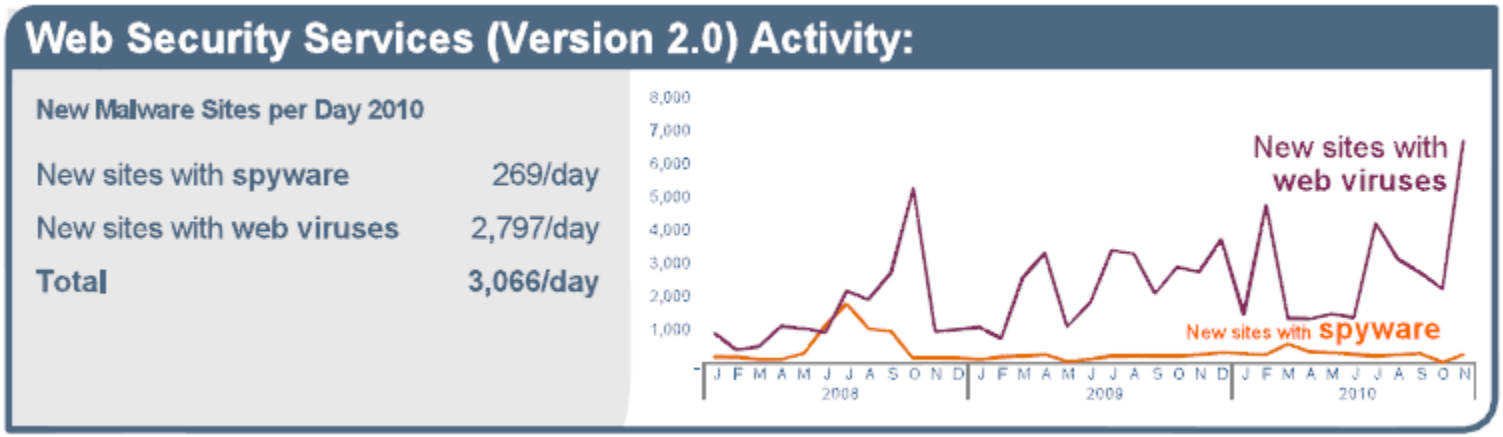


- El Cloud debe asumir un papel protagonista como el tercer perimetro.
- Debe ser una extensión de nuestro perimetro exterior, asumiendo nuestra política y reglas
- Debe aportar comuniaciones limpias a nivel básico
- Debe ser proactivo

Seguridad Navegación Internet

Security for remote users

In 2010 the number of blocked sites containing malware are increasing 24.3% over 2009.
SEO attacks (breaking news). Top 100 search 25% malicious url.
Fake Antivirus. Combined with SEO attacks
Exploiting vulnerabilities, use of social networks, etc.



Seguridad Navegación Internet

Security for remote users

What sites are my employees visiting?
How much time do my employees to connect
to social networks?
How does this affect the productivity of employees?

Seguridad Navegación Internet

BandWidth Consumption

Increased use of repositories of documentation on the Web (Zyncro, Dropbox, etc ...)
Increased corporate cloud solution (Salesforce, etc ...)
Increased loading of documents with images, videos, multimedia, etc ...
Exponential growth in streaming
New content ✳ new demand

Seguridad Navegación Internet

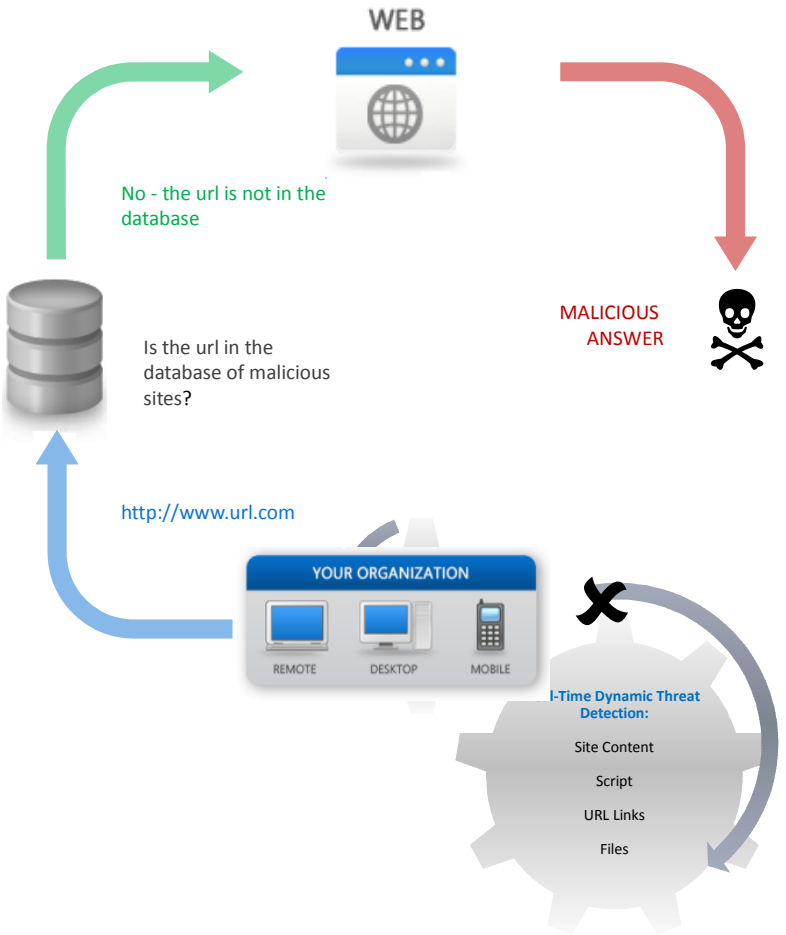
Security for remote users

- Users need secure connectivity wherever they are, in the office, a hotel, on a client, etc ...
- Employees use the devices to connect to the Internet when away from the office
- New types of employees: Telecommuting, freelance, etc ...
- New devices, Tablets, Notebooks, smartphones, mobile connectivity to facilitate
- Based security appliances use is inefficient
- Mobility implies that the evolution of appliance-based security must evolve to Cloud

Internet Access Security

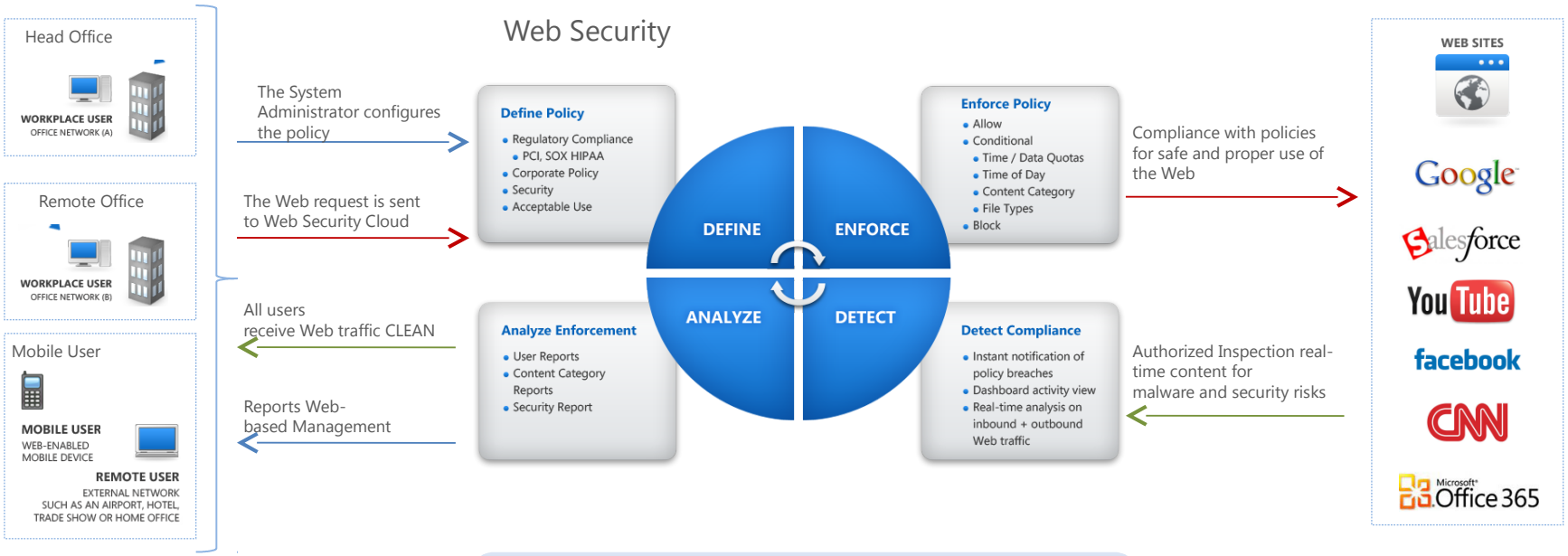
Web 2.0

- The content of the sites is dynamic. Traditional filtering methods are no longer valid
- The dynamic content of bbdd sites means the knowledge of the traditional model does not work
- Leaks of confidential information



Internet Access Security

Internet Access Security



The ability of 360 degrees SaaS enables customers to easily define their policies, enforce them automatically, proactively detect malware or offensive and analyze Web usage through reporting

FEATURES AND BENEFITS

- Disposal of investment in infrastructure and maintenance
- URL filtering and anti-malware, providing navigation safety
- Control of the misuse of the Internet, blocking access to websites unrelated to work
- Web traffic filtering and applications to remote users
- Control bandwidth, restricting access to sites such as YouTube.com
- Data leak prevention, preventing the output files through Web
- Implementation of regulations, facilitating compliance with company policies
- Access historical traffic logs without loss of granularity

Code Vulnerabilities. Cloud security (layer 7)

Fuente: WASC (Web Application Security Consortium)

'95 % of Internet attacks goes against the Application'

More than 90 % of Internet vulnerabilities are inside the code

'The code attacks has high impact and consecuensec for Enteprise, and also legal consecuences

Internet Application attacks type

Distribution of code attacks by sector

Distribution of code attacks by type

Detección del lenguaje a procesar

Análisis léxico

Análisis sintáctico

Generación del modelado de la arquitectura software del aplicativo

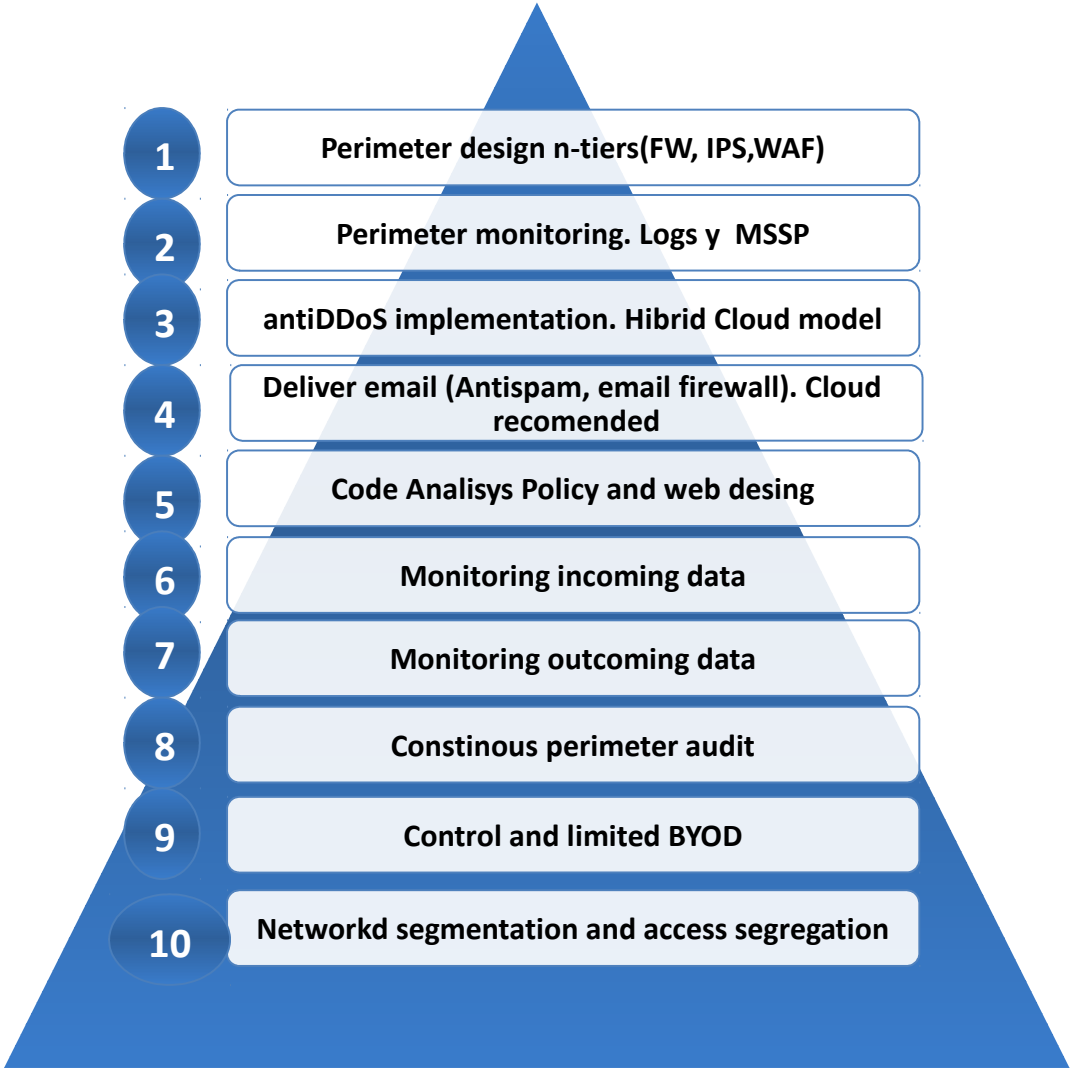
Análisis del flujo de datos

Detección de patrones vulnerables

Discriminación de falsos positivos

Comunicación de las posibles vulnerabilidades encontradas

APTs. Defense Guide for Telco



Juan Miguel Velasco López-Urda
juanmiguel.velasco@gmail.com
@juanmivelasco

2012 CEE-SEC(R)
Software Engineering Conference in Russia