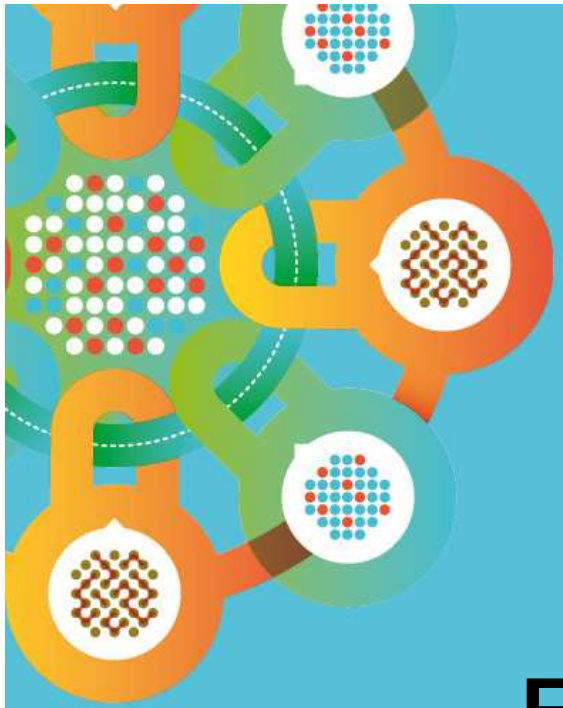


IBM Forum Segrate - Milano

18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

Fabio Panada

I risultati della ricerca X-Force nelle soluzioni IBM

IBM X-Force 2011
Trend and Risk Report

IBM

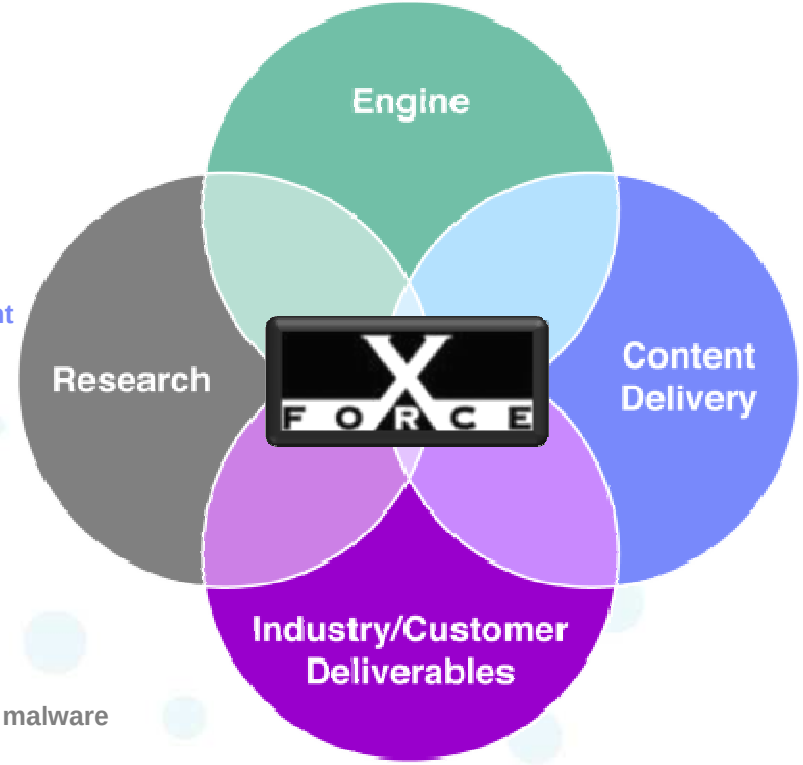
IBM X-Force Mission Statement

- **Research** & evaluate vulnerabilities and security issues
- **Develop** assessment & protection technology for IBM products / services
- **Educate** the media and user communities on emerging security issues.

IBM X-Force Research and Development

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development



Content Delivery

- Continue third party testing
- Execute to deliver new content streams for new and existing engines
- Develop new protocol parsers

Research

- Support content streams
- In-house reverse engineering and malware analysis teams
- Expand current capabilities in research to provide industry knowledge to the greater IBM

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

The world's leading security R&D organization

We have a lot of data…

IBM X-Force® Research and Development

- **Research and evaluate threat and protection issues**
- **Deliver security protection for today's security problems**
- **Develop new technology for tomorrow's security challenges**
- **Educate the media and user communities**

X-Force Research

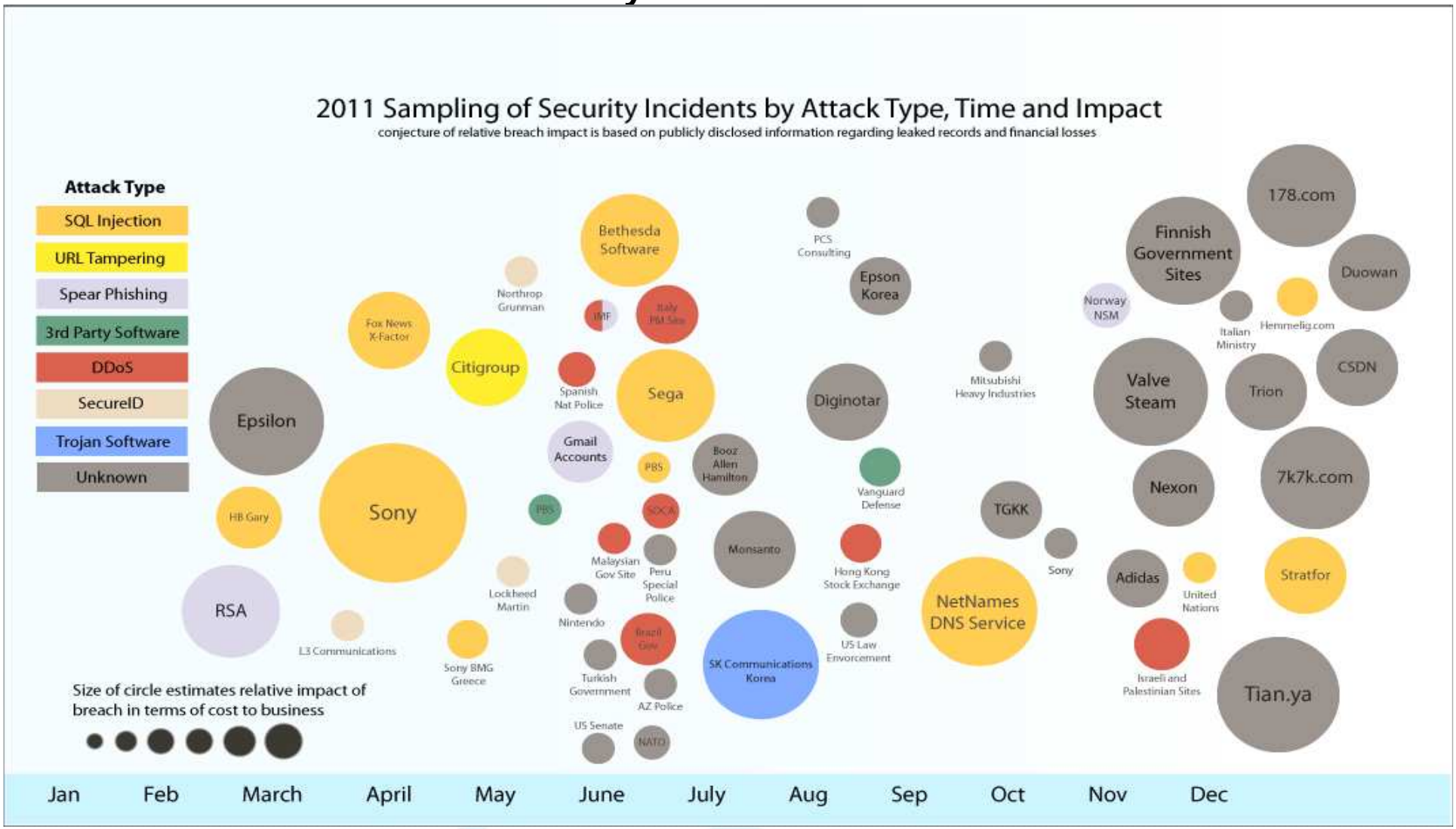
15B	analyzed Web pages & images
40M	spam & phishing attacks
60K	documented vulnerabilities
9B+	of security events daily
1M+	of unique malware samples

Provides Specific Analysis of:

- **Vulnerabilities** & **exploits**
- **Botnet** command and control
- **Malicious**/Unwanted websites
- Spam and phishing
- **Malware**
- **Emerging trends**

Cyber breaches are having a growing impact

"The Year of the Security Breach" – IBM's X-Force® R&D



Last 4 Days of August 2012

Aug 27	?	AMNESTY INTERNATIONAL	A blog site belonging to Amnesty International - Livewire (livewire.amnesty.org) is targeted by hackers who post fake blog posts, including one that took a strong pro-Syrian government stance.[27]	Unknown	Organization: Human Rights	Hacktivism
Aug 27			Hackers claiming allegiance to the Anonymous deface the website of Peter Hain, a former British cabinet minister in solidarity with WikiLeaks founder Julian Assange.[28]	Defacement	Organization: Politics	Hacktivism
Aug 27		INTERPOL	The website of the Interpol is the target of a distributed denial-of-service attack launched by Anonymous hackers as part of Operation Free Assange (#OpFreeAssange).[29]	DDoS	Law Enforcement	Hacktivism
Aug 27		GlobalCerts	A hacker called Stun AKA @S7UN hacks GlobalCerts (GlobalCerts.net), a firm that offers secure messaging and other similar solutions. The leak contains 1,249 records, several of which, with clear text passwords.[30]	SQLi?	Industry: Information Technology	Hacktivism
Aug 27		AVX	Anonymous Hackers hit the website of electronics manufacturer AVX as part of the attack campaigns dubbed #OperationGreenRights and #OpColtan. The attack leaves over 2,900 of the sites clients details exposed.[31]	SQLi	Industry: Technology	Hacktivism
Aug 27	?	TVB	Hackers are suspected of attacking with a DDoS TVB's Miss Hong Kong beauty pageant server, thwarting the broadcaster's attempt for online voting.[32]	DDoS	Industry: Media	Cyber Crime
Aug 27	Ibrahimshah Shahulhamee	TOYOTA	Toyota's U.S. manufacturing company accuses a fired computer worker (Ibrahimshah Shahulhamee) of cracking into its proprietary plans for parts prices and designs on 23 August, downloading the information and sabotaging Toyota's internal computer software.[33]	Unauthorized Access	Industry: Automotive	Cyber Crime
Aug 28			Members of Cyb3rSeC Crew claim the hack of cronicadelquindio.com (a Colombian news web site) and dump 9,197 records with usernames, e-mails and hashed passwords.[34]	SQLi?	News	Cyber Crime
Aug 29			In name of Operation Ukraine, the Anonymous hack the Civil Society and Government web portal (civic.kmu.gov.ua) and publish its entire database, consisting of tens of email addresses, birth dates, IP addresses, usernames and password hashes.[35]	SQLi	Government	Hacktivism
Aug 29			NullCrew continue to show their support for #OpFreeAssange, hacking the databases of the Africa College site (africacollege.leeds.ac.uk) owned by the University of Leeds. The leak contains database details and over 100 email addresses, password hashes and usernames.[36]	Unknown	Education	Hacktivism
Aug 29	?	UCL	In name of #OpFreeAssange, unknown hackers dump on pastebin a database of the Dundee University (dundee.ac.uk). The database contains 300 users with email and their home address. Inside the same attack, the unknown hackers also dump some details from the University College London (ucl.ac.uk) and few admin logins from the University of Leeds (leeds.ac.uk).[37] (Original link no more available).	SQLi	Education	Hacktivism
				Unknown	Education	Hacktivism
				Unknown	Education	Hacktivism
Aug 30	?	RasGas	Ras Laffan Liquefied Natural Gas Co., a Qatari LNG producer, shuts down part of its computer systems targeted by an unidentified malware, probably Shamoon.[38]	Shamoon Malware	Industry: Energy	Cyber Warfare
Aug 30		PHILIPS	AoS AKA@AnonOpsSweden announces that Electronics giant Philips is hacked for the second time in a month and its databases raided. According to the hackers, over 200,000 emails with usernames and encrypted passwords were leaked.[39] Even in this case the company claims that old data have been leaked.[40]	SQLi?	Industry: Technology	Hacktivism
Aug 30			The Anonymous hack blizzard.com.ua, an Ukrainian based gaming community and dump over 19,000 accounts that have further details.[41]	SQLi	Online Gaming	Hacktivism
Aug 30		POLICE	In name of #OpAssange, a hacker using the handle @0x00x00 leaks several data from police.uk and 3 of its subdomains (police.uk, herts.police.uk, nottinghamshire.police.uk). Leaked data includes 97 records consisting of usernames, passwords, email addresses and names belonging to officers, and also hundreds of records consisting of login and contact details.[42]	SQLi	Law Enforcement	Hacktivism
Aug 30		SIEMENS	In name of #OpGreenRights and #OpColtan, the Anonymous (@OpGreenRights) dump Siemens Switzerland (siemens.ch) and Fujitsu General Brazil (fujitsu-general.com.br) resulting in data from server databases leaked.[43]	SQLi	Industry: Technology	Hacktivism
		FUJITSU GENERAL		SQLi	Industry: Technology	Hacktivism
Aug 30	Islamist group Boko Haram (Claimed)		The details of about 60 Nigeria State Security Services Operatives remained on the comments section of a local news site for days before being deleted. The information published included names, ID numbers, bank details and addresses. Militant Islamist group Boko Haram is suspected to be behind the leak.[44]	Unknown	Law Enforcement	Cyber Warfare
Aug 31			NullCrew hackers once again show their support for Julian Assange. This time, they claim to have breached data.gov.uk, a UK government project that provides citizens with non-personal data which can be freely re-used. The leak consists in a 700 megabyte archive that holds numerous .cvs files which contain all sorts of information.[45]	SQLi	Government	Hacktivism
Aug 31		LADA	After the announce the hack, Nullcrew publishes the database of the Russian based auto company Lada (lada-auto.ru). Account details that have been leaked include usernames, emails and hashed passwords (1,404 emails and about 600 accounts without emails).[46]	SQLi	Industry: Automotive	Hacktivism
Aug 31		PHILIPS	For the third time in this month, Philips is targeted by hackers. This time the victim is advance.philips.com, a subdomain for light technology. The data, leaked in name of #OpColtan, contains approximately 65 records.[47]	SQLi	Industry: Technology	Hacktivism

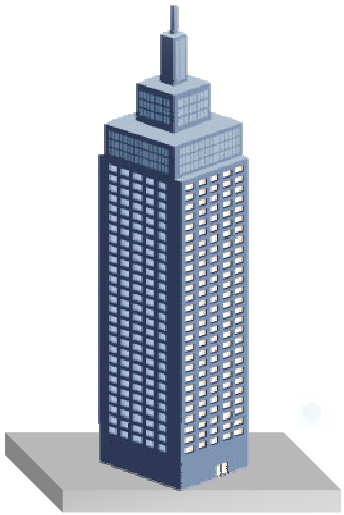
Key drivers affecting the security software business

It is no longer enough to protect the perimeter – sophisticated attacks are bypassing traditional defenses, IT resources are moving outside the firewall, and enterprise applications and data are becoming distributed across multiple devices

1. Advanced Threats

Sophisticated, targeted attacks, designed to gain continuous access to critical information, are increasing in severity and occurrence.

Advanced Persistent Threats
Stealth Bots Designer Malware
Targeted Attacks Zero-days



Enterprise Customers

2. Cloud Computing

Security is one of the top concerns of cloud, as customers drastically rethink the way IT resources are designed, deployed and consumed.

IBM SmartCloud
vmware salesforce

3. Mobile Computing

Managing employee owned devices and securing connectivity to corporate applications are top of mind as CIOs broaden their support for mobile devices.

Windows Phone

4. Regulations and Compliance

Regulatory and compliance pressures continue to mount as companies store sensitive data and become susceptible to audit failures.

PCI Security Standards Council HIPAA Sarbanes-Oxley Financial and Accounting Disclosure Information

Key Messages from the 2011 Trend Report

- **New Attack Activity**
  - Rise in Shell Command Injection attacks
  - Spikes in SSH Brute Forcing
  - Rise in phishing based malware distribution and click fraud
- **Progress in Internet Security**
  - Fewer exploit releases
  - Fewer web application vulnerabilities
  - Better patching
- **The Challenge of Mobile and the Cloud**
  - Mobile exploit disclosures up
  - Cloud requires new thinking
  - Social Networking no longer fringe pastime

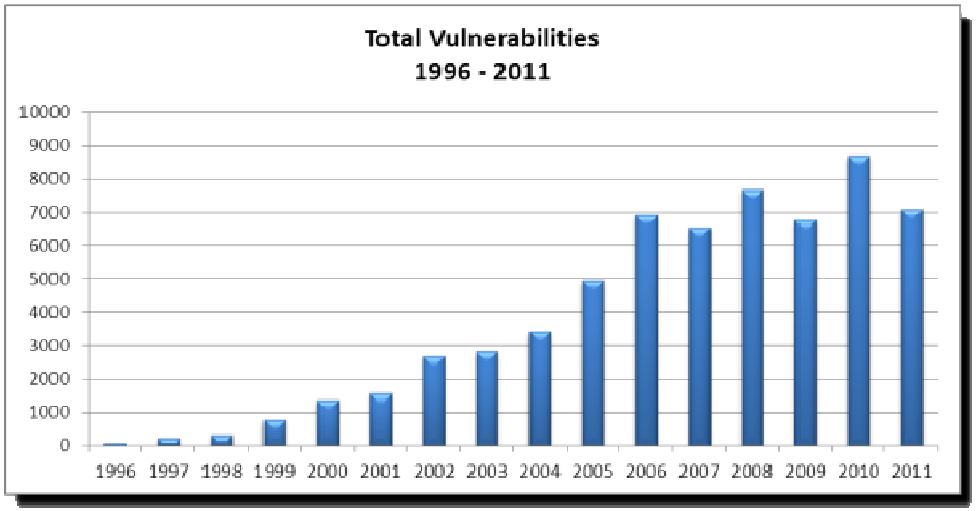
- Our statistics demonstrate some improvements in Internet software security, but attackers adapted their techniques in response. As a result, we saw several new attack trends emerge.

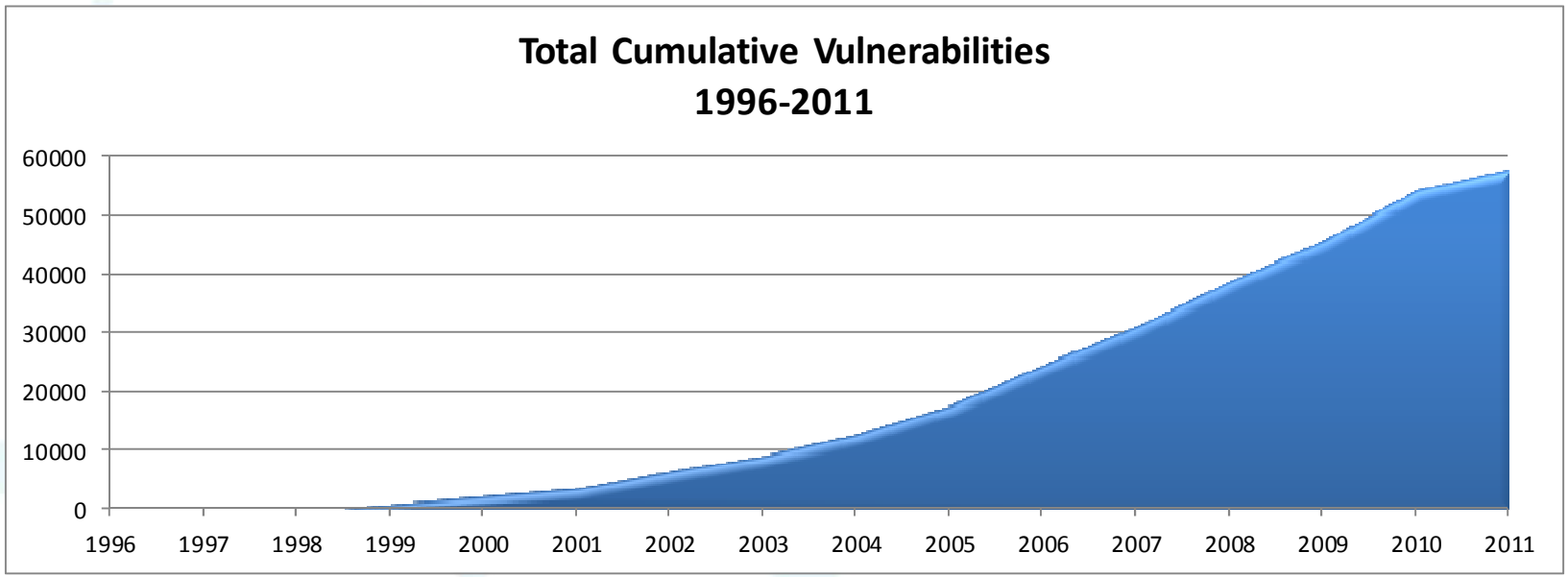
- It has become a sport for attackers to steal as many user names and passwords from a website as they can... and post them publicly..
- The emergence of cloud and the proliferation of mobile devices creates additional challenges for enterprise security.

2010 Up, 2011 Down – In 2012 the Trend Will Continue – probably

Public Vulnerability Disclosures

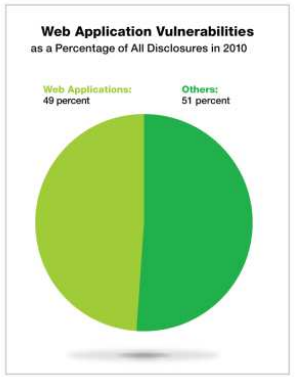
- 2010 = highest # of vulnerabilities
- **2011 = down ~17.5% YoY**
  - Web applications continue to be the largest category of disclosure.
- 2011 had less vulnerability disclosures than 2010.
  However some categories increased.
- **1H 2012 Update**: = 4,000

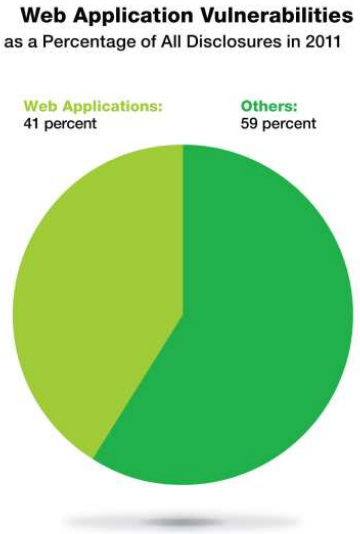




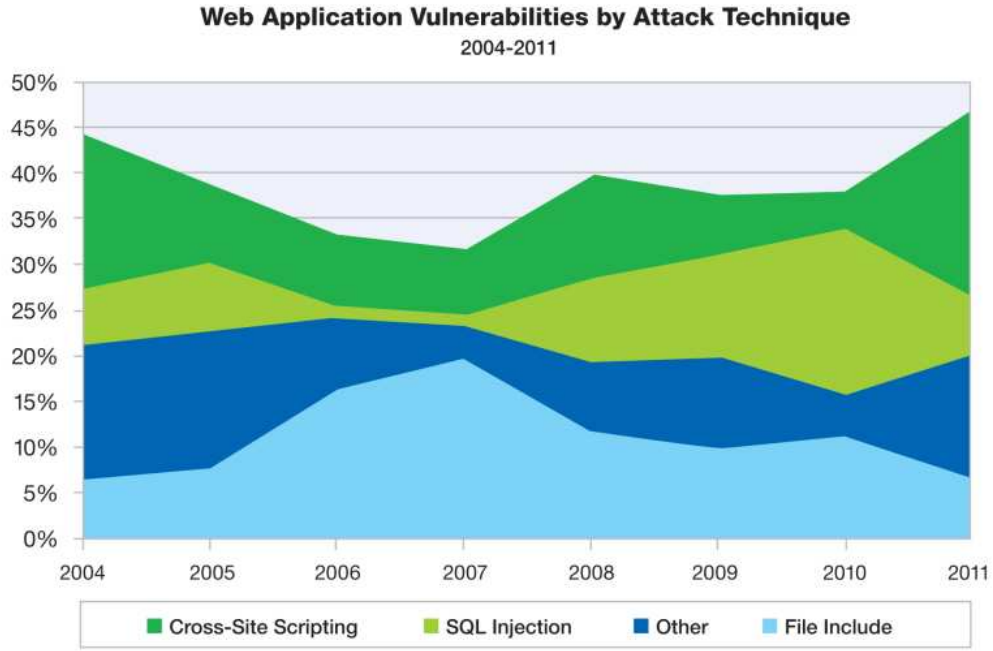
Decline in web application vulnerabilities

- In 2011, 41% of security vulnerabilities affected web applications
  - Down from 49% in 2010
  - Lowest percentage seen since 2005



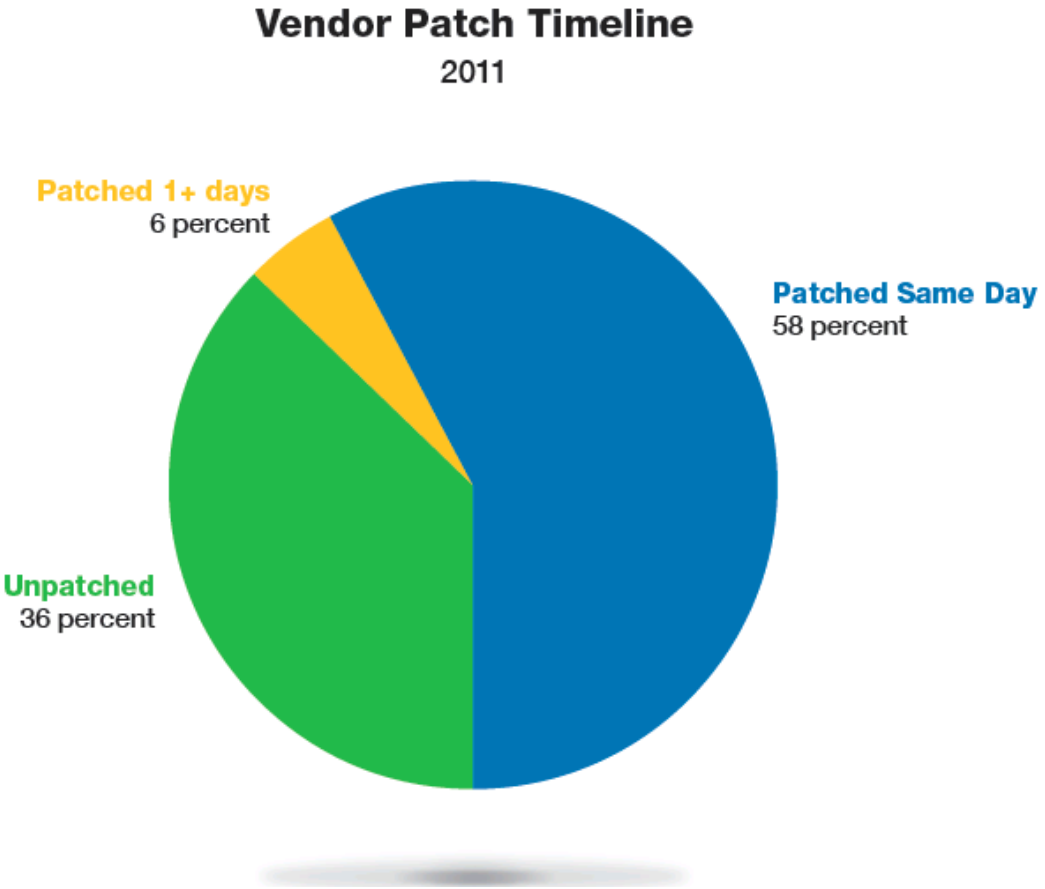


Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Patching Improved in 2011



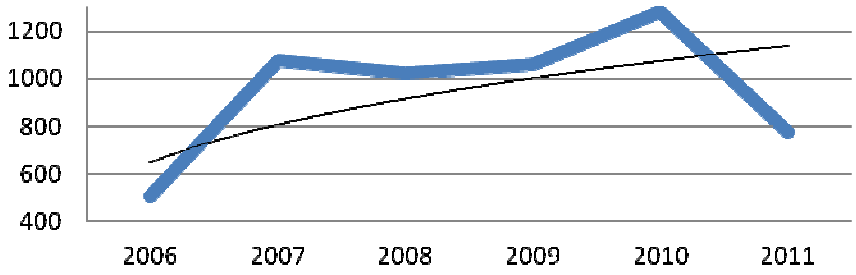
	2011	2010	2009	2008	2007	2006
Unpatched %	36.0%	43.3%	45.1%	51.9%	44.6%	46.6%

We Track All Public Exploits…

Public exploit disclosures up in 2010 down in 2011

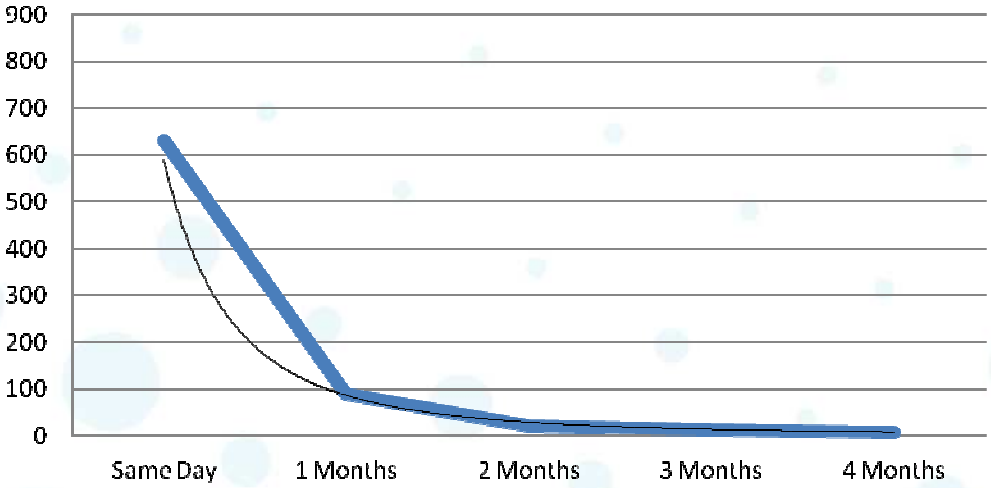
- Approximately **14.9%** of the vulnerabilities disclosed in 2010 had public exploits, which is down slightly from the **15.7%** 2009.
- **2011** has seen less public exploits than 1H 2010
- The vast majority of public exploits are released the same day or in conjunction with public disclosure of the vulnerability.

True Exploits Released 2006-2011



True Exploits	504	1078	1025	1059	1280	778
Percentage of Total	7.3%	16.5%	13.4%	15.7%	14.9%	11.0%

2011 Exploit Timeframe



Exploit Timing	0 Days	1 Month	2 Months	3 Months	4 Months
0 Days	852	308	23	12	6

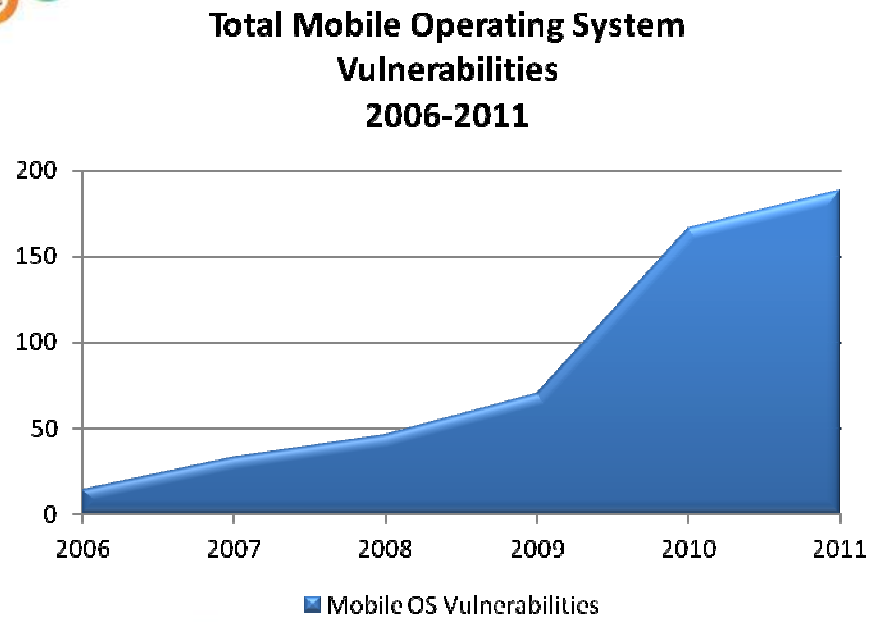
1H 2012 Update = 439

got root?

Challenging exploits: more vulnerabilities in widespread category

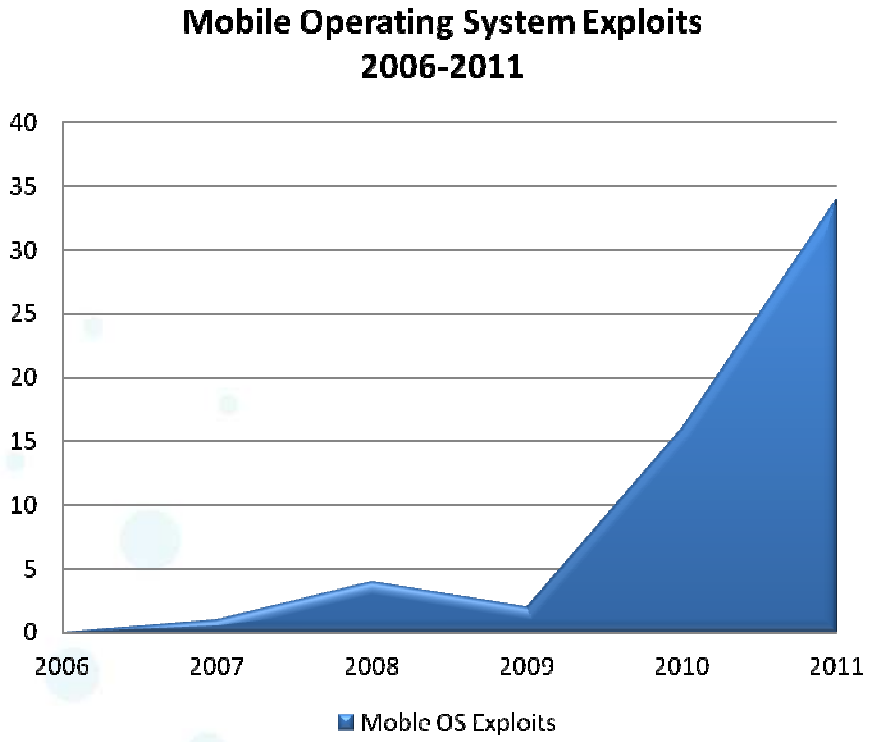
- 34 X-Force alerts and advisories in 2011
  - 16 fit the critical category
    - easy to exploit, sweet spot for malicious activity
    - most currently being exploited in the wild
  - 12 harder to exploit but high value
    - This number higher than previous years

Source: IBM X-Force® Research and Development



Continued interest in mobile vulnerabilities as enterprise users bring smartphones and tablets into the work place (BYOD)

Attackers finally warming to the opportunities these devices represent



MAC malware

Source: IBM X-Force® Research and Development

Source: IBM X-Force® Research and Development

In 2011, we started seeing Mac malware with functionalities that we've only seen before in Windows malware. This may indicate that cyber criminals are now becoming aware of how profitable targeting OS X might be.

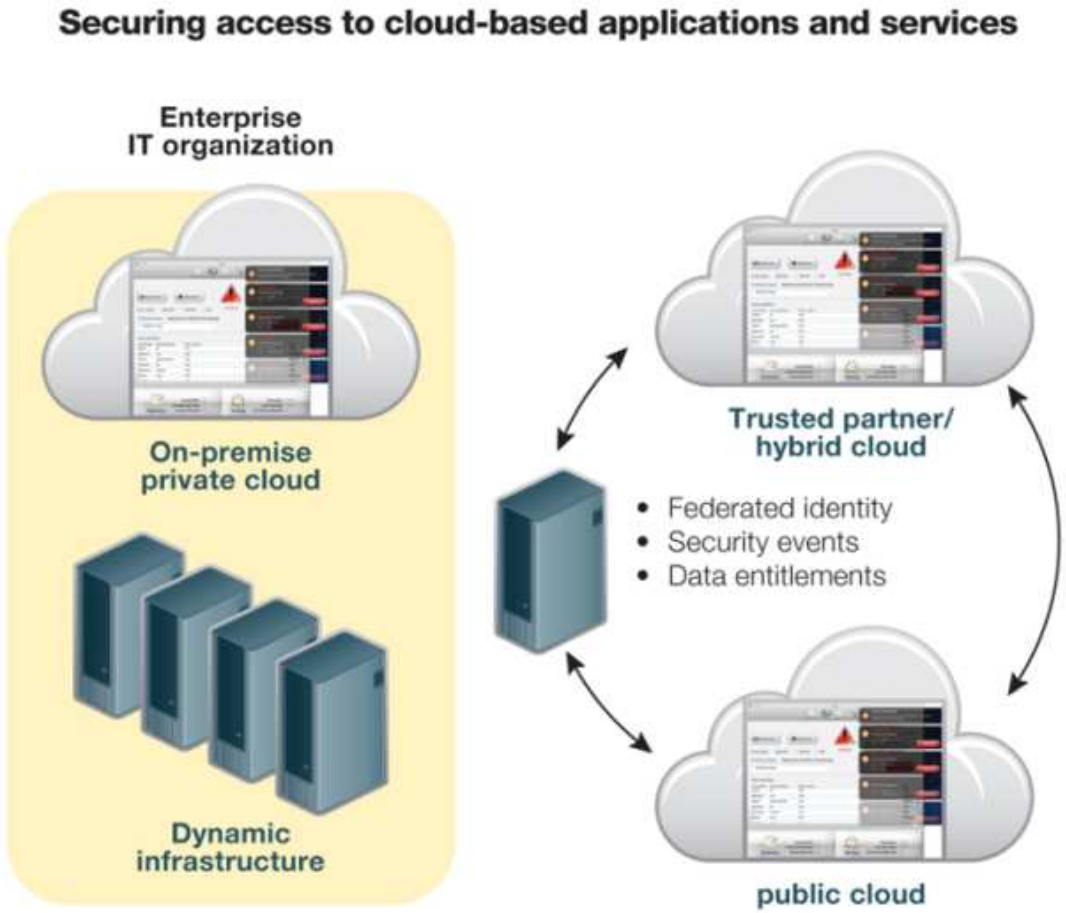
In April, 2012 security professionals identified that a new piece of malware, Flashback, had infected more than half a million Apple computers in what was the largest scale attack on Mac OS X computers to date.[1]

Mac computers can also carry malware that could infect Windows PCs.

Note[1] - Source: eWeek.com

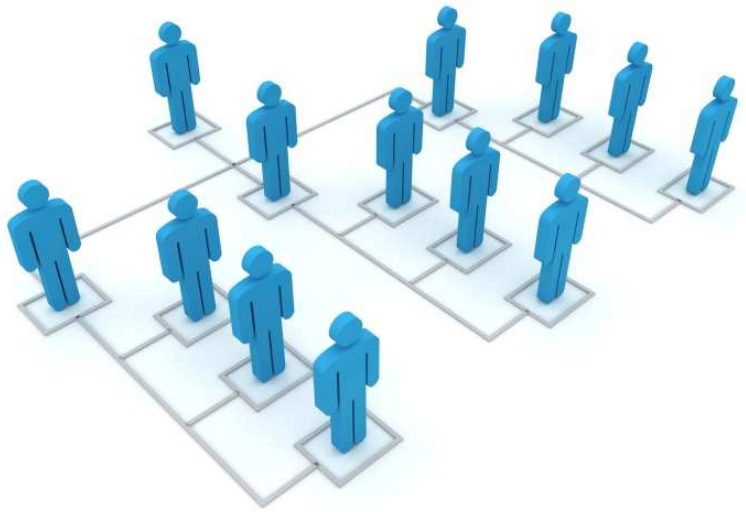
Challenges of cloud security

- We saw a number of high profile cloud breaches in 2011 affecting well-known organizations and large populations of their customers
- Cloud computing offers new possibilities and new security challenges. These challenges range from governance, through to securing application and infrastructure. Fundamentally it is important to be able to assure the security of these new models in order to build trust and confidence

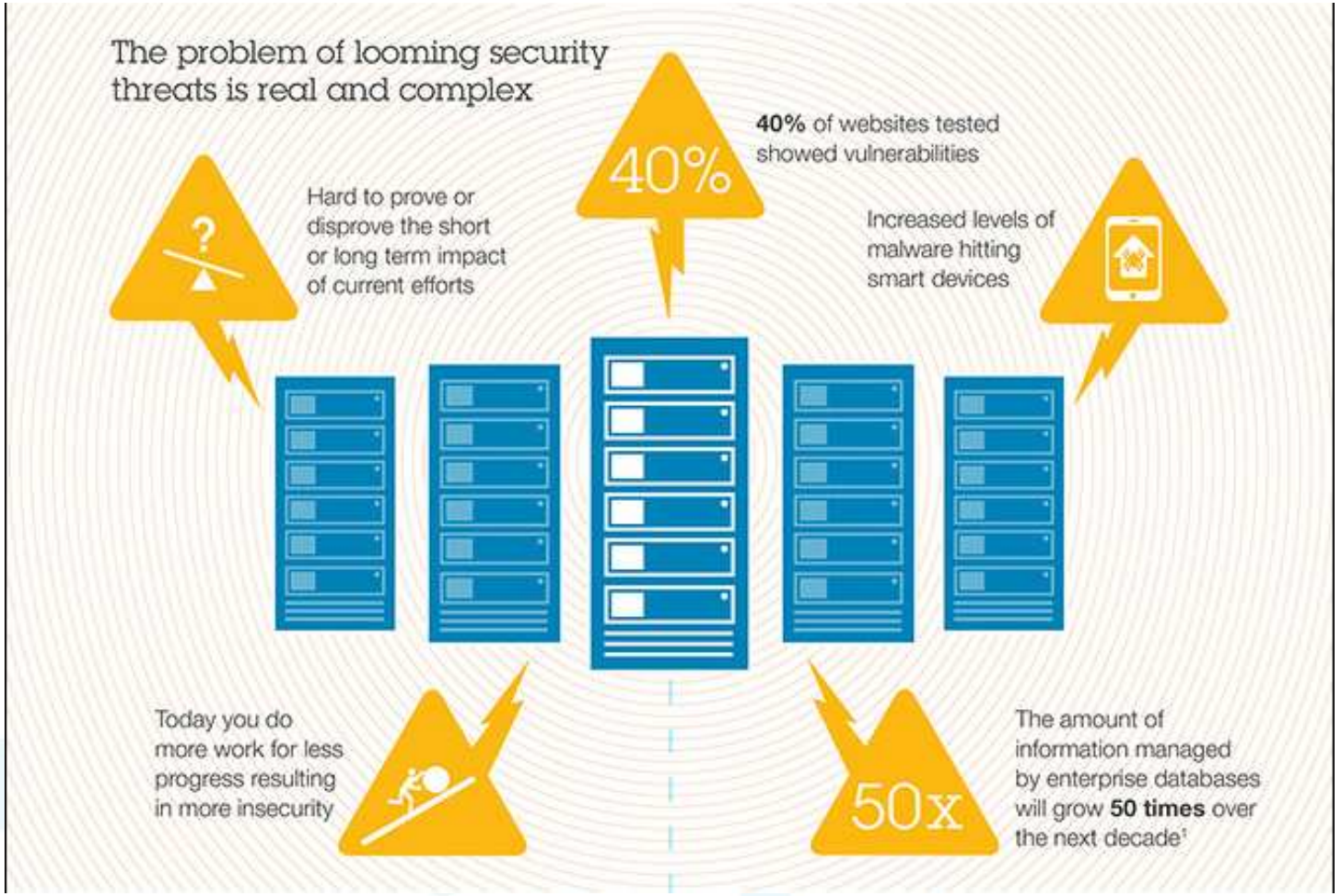


Social Networking – no longer a fringe pastime

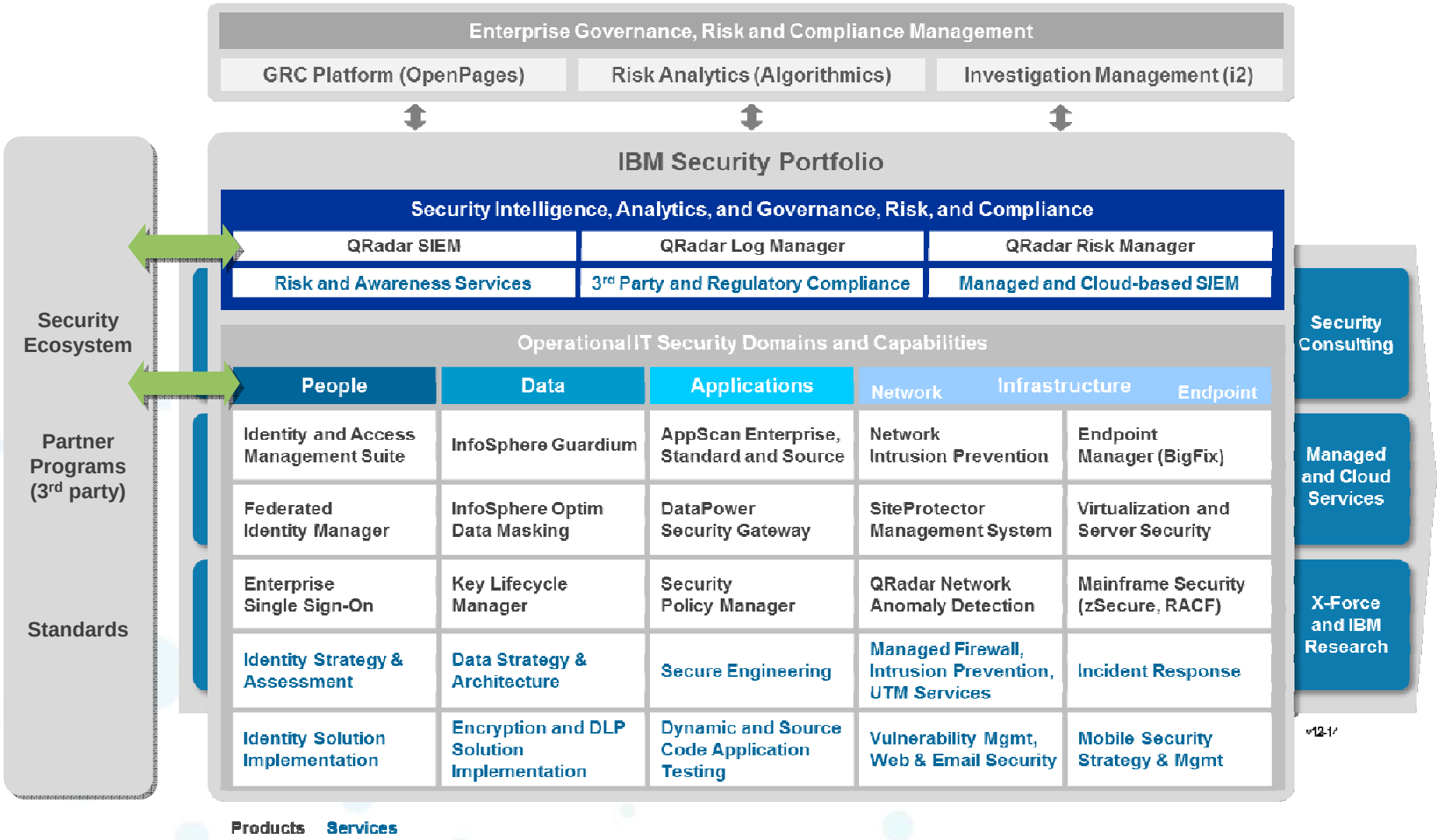
- Attackers finding social networks ripe with valuable information they can mine to build intelligence about organizations and its staff:
  - Scan corporate websites, Google, Google News
    - Who works there? What are their titles?
    - Create index cards with names and titles
  - Search Linkedin, Facebook, Twitter profiles
    - Who are their colleagues?
    - Start to build an org chart
  - Who works with the information the attacker would like to target?
    - What is their reporting structure?
    - Who are their friends?
    - What are they interested in?
    - What are their work/personal email addresses?



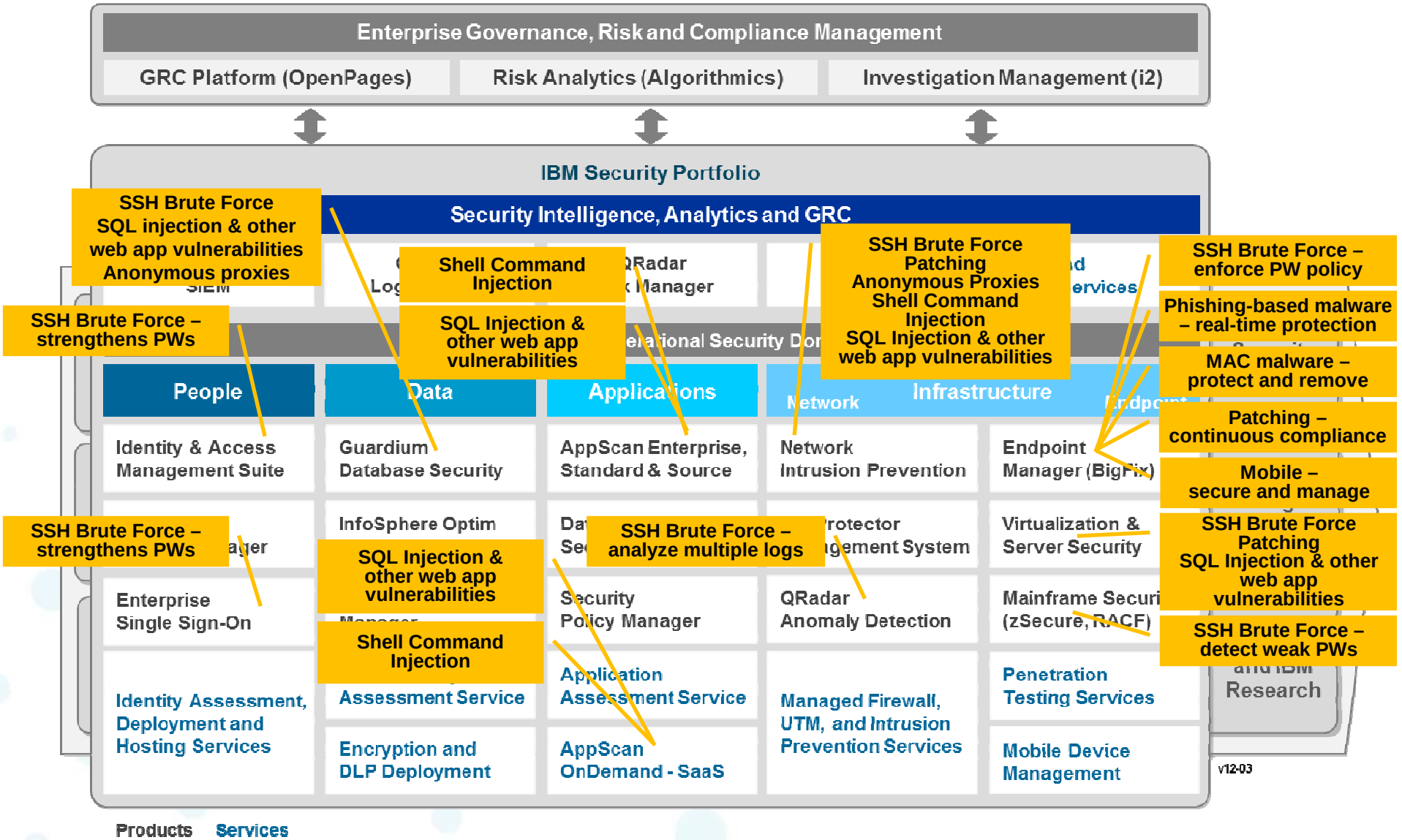
Are we more secure today than we were yesterday ?



Comprehensive portfolio across security domains



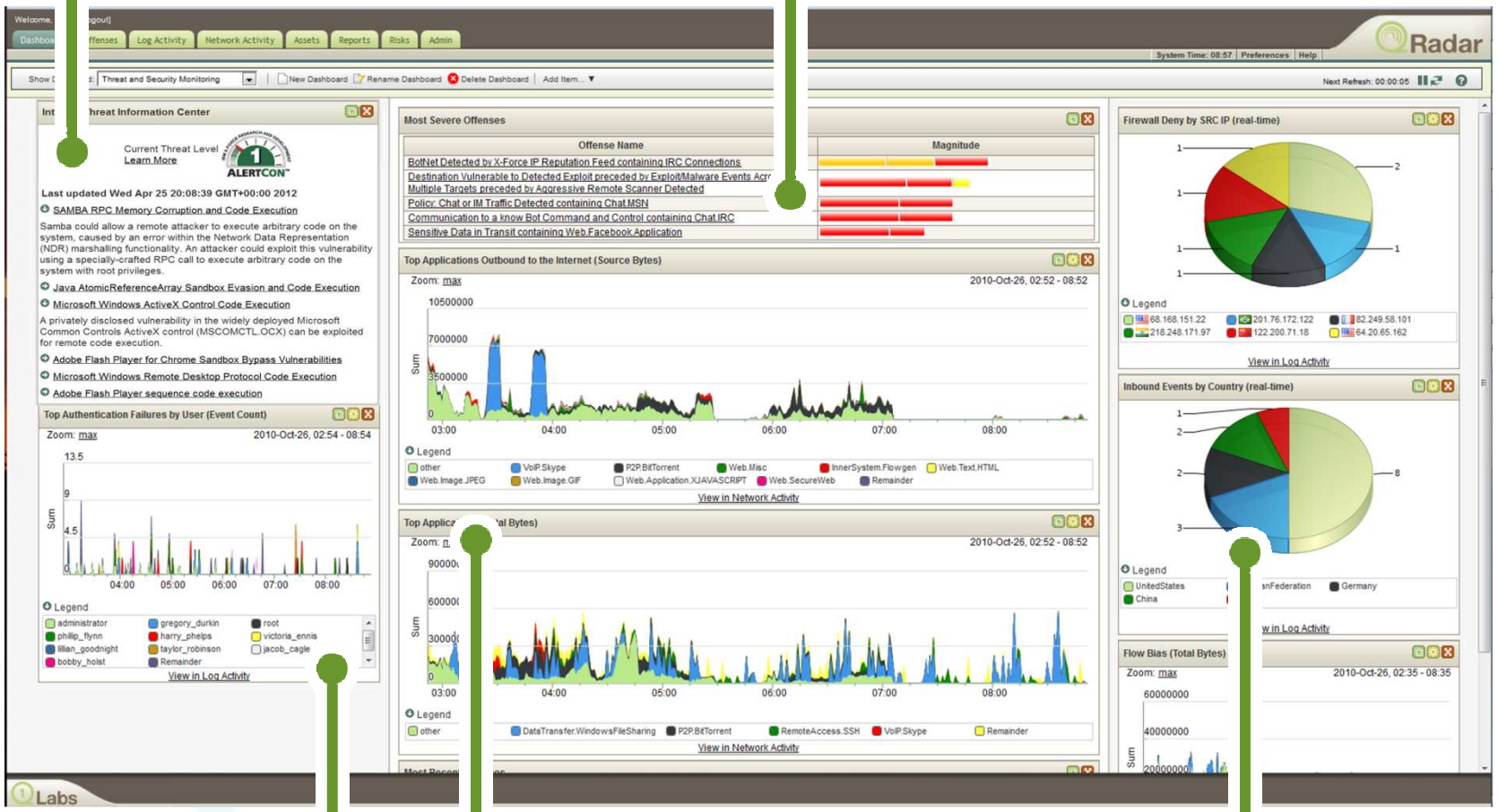
Leading solutions in every segment



18 settembre: Missione Sicurezza

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation

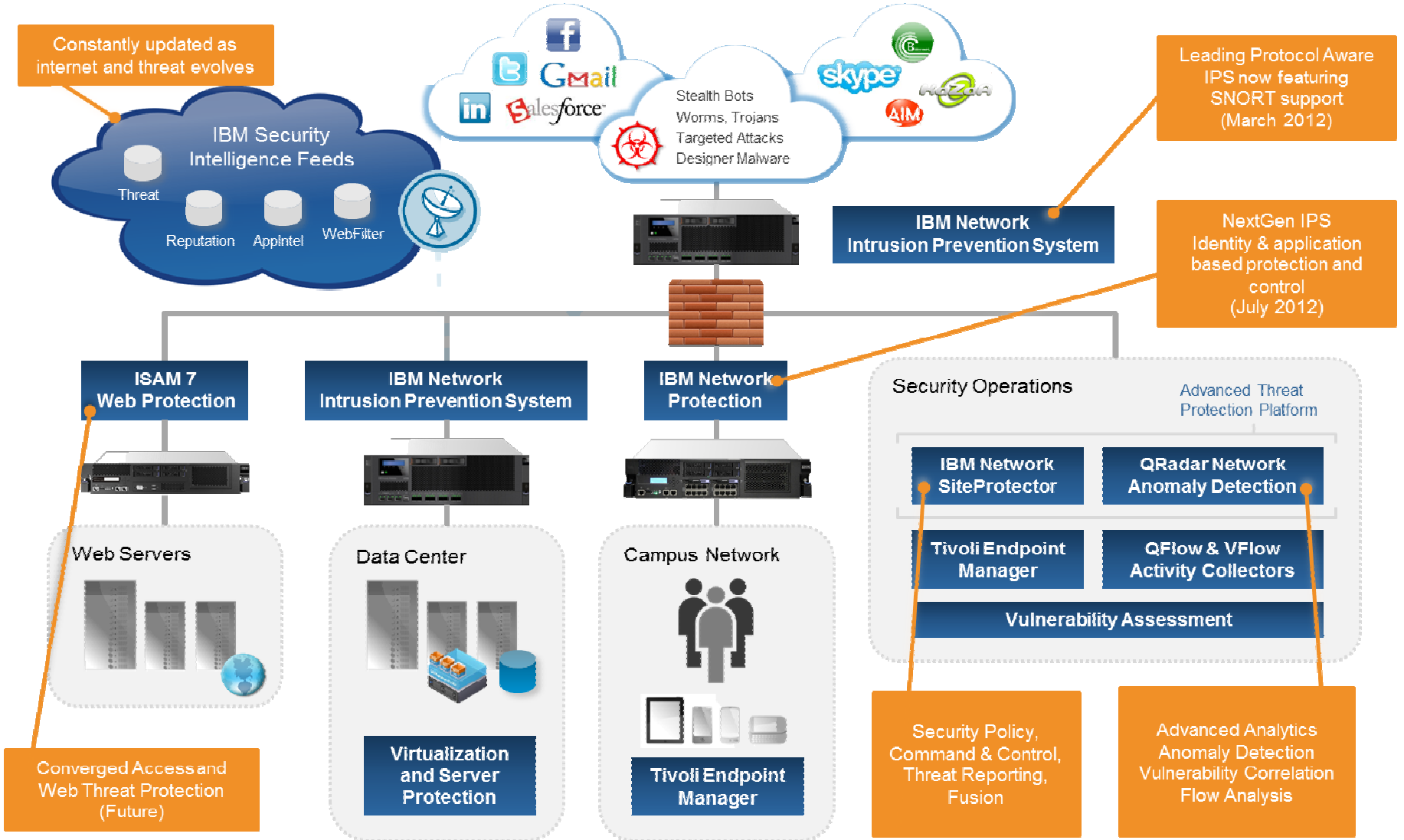


Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

Advanced Threat Protection Platform



Introducing Advanced Controls

- Server
- Network
- Geography
- Reputation
- User or Group

Web Applications

Non-web Applications

- Web Category Protection — Allow marketing and sales teams to access social networking sites
- Access Control — Block attachments on all outgoing emails and chats
- Protocol Aware Intrusion Protection — A more strict security policy is applied to traffic from countries where I do not do business
- Client-Side Protection — Advanced inspection of web application traffic destined to my web servers
- Botnet Protection — Block known botnet servers and phishing sites
- Network Awareness — Allow, but don't inspect, traffic to financial and medial sites
- Web Protection
- Reputation

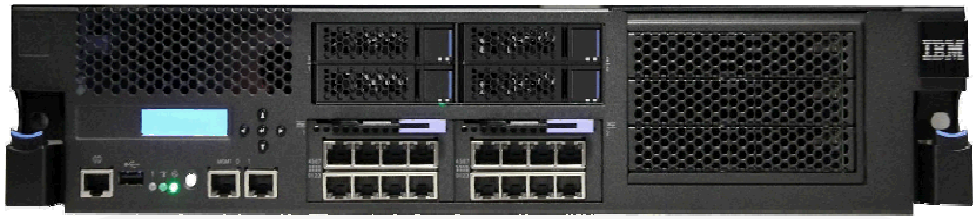
Who	What	Controls	Security
172.29.230.15, 192.168.0.0 /16	80, 443,25, 21, 2048-65535	?	

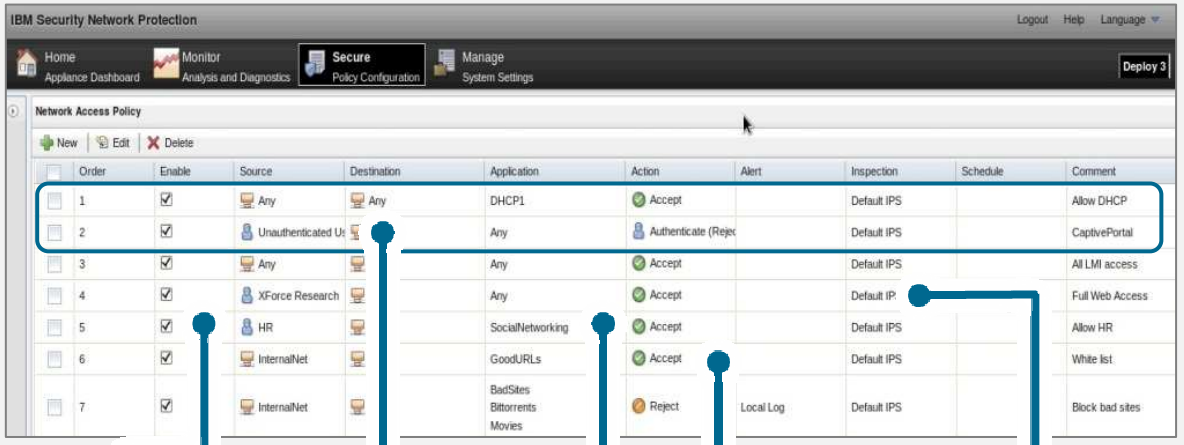
Complete Control: Overcoming a Simple Block-Only Approach

- **Network Control** by users, groups, systems, protocols, applications & application actions
- **Block evolving, high-risk sites** such as Phishing and Malware with constantly updated categories
- **Comprehensive up-to-date web site coverage** with industry-leading 15 Billion+ URLs *(50-100x the coverage comparatively)*
- **Rich application support** with 1000+ applications and individual actions

"We had a case in Europe where workers went on strike for 3 days after Facebook was completely blocked…so granularity is key."

– SecureDevice





Limit the use of social networking, file sharing, and web mail for common users

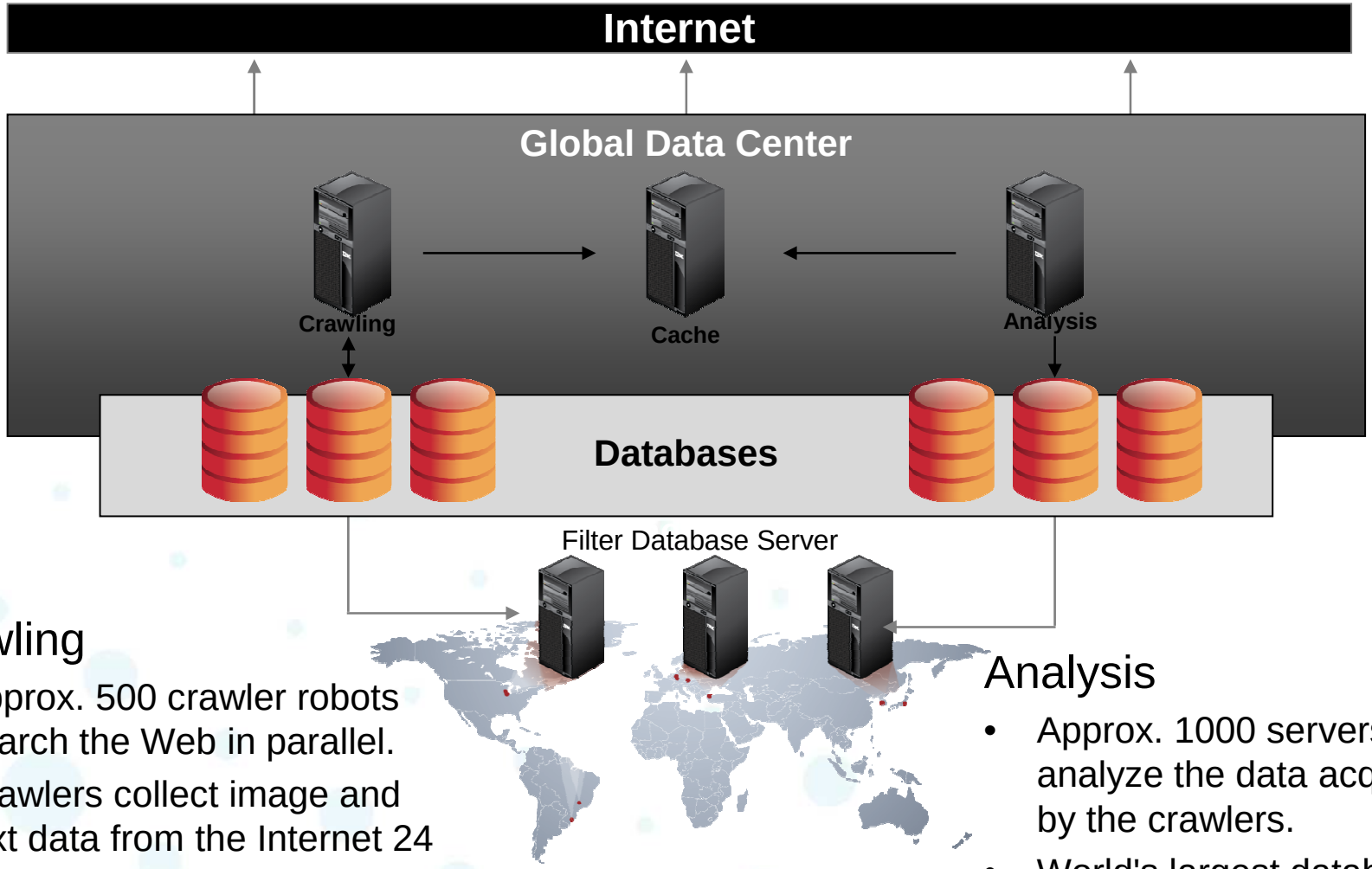
Flexible network access policies controls access to systems and applicable security policy by IP, Port, Protocol and vlan.

Allow full access to social networking sites for marketing and HR teams`

Stop broad misuse of the corporate network by blocking sites that introduce undue risk and cost

Tailored Security Policies for individual uses, groups or networks

IBM X-Force Global Datacenter - Content Analysis



Crawling

- Approx. 500 crawler robots search the Web in parallel.
- Crawlers collect image and text data from the Internet 24 hours a day on 365 days, which adds up to 200 million pages each month

Analysis

- Approx. 1000 servers analyze the data acquired by the crawlers.
- World's largest database with 15 billion evaluated web pages and images

Security is Everywhere

Tech Center: Database Security

Tweet 36 Mi piace Share Permalink BOOKMARK

Healthcare Industry Now Sharing Attack Intelligence

New HITRUST Cybersecurity Incident Response and Coordination Center lets healthcare organizations, U.S. Department of Health and Human Services swap information, forensics from firsthand attack experiences, other threats

Apr 24, 2012 | 04:00 PM |

By Kelly Jackson Higgins
Dark Reading

Large healthcare organizations and the U.S. Department of Health and Human Services (HHS) have banded together to share attack and threat intelligence in

Wearable firewall stops pacemaker hacking

Millions of people use insulin pumps, pacemakers and other personal medical devices that rely on wireless communication to function. But what happens if someone was to tamper with that vital communication line between the health care provider and the patient?

Researchers from Purdue and Princeton universities have developed a solution to what could be catastrophic problem: a signal-jamming personal firewall for medical devices.

TV-based botnets? DoS attacks on your fridge? More plausible than you think

By Dan Goodin | Published 16 days ago

It's still premature to say you need firewall or antivirus protection for your television set, but a duo of recently diagnosed firmware vulnerabilities in widely used TV models made by two leading manufacturers suggests the notion isn't as far-fetched as many may think.

Rise of "forever day" bugs in industrial systems threatens critical infrastructure

By Dan Goodin | Published 29 days ago

The future of security –

The Darwinian challenge: Evolve or lose

"It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is the most adaptable to change."

Charles Darwin

The **business environment** is evolving

- The **IT environment** is evolving
- The cyber **threat environment** is evolving

- The challenge every function is facing is how to **evolve** with them to deliver **New Security Solutions**

- If the information security function does not change, the result will be losing **influence, control** and in this environment a real **opportunity** for **impact** with the business

2010

Today

ibm.com/security