Big Data – Opportunité et risques

Security for a Smarter Planet
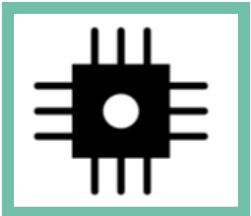
Michel Bobillier
Global Sales Leader, IBM Security Solutions
November 6th, 2012

Today's Discussion Topics

- **Big Data**
- **Smarter Planet**
- **Security impact**
- **The implications - Security "New Normal"**

IBM

Revenue 2011: $107B (+7%). Profit $15.8B +7%)
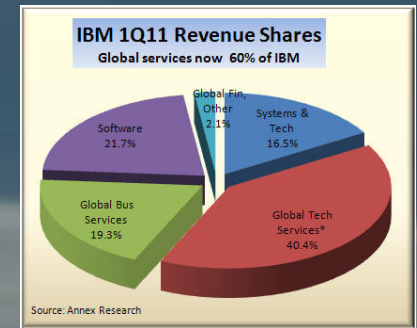
427'000 employees in 170 countries

M → S : Software, Services (>80%)

Acquisitions

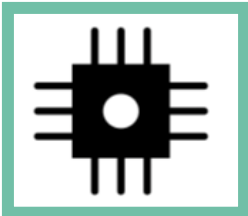Smarter Planet, Business Analytics, Cloud computing

IBM 1Q11 Revenue Shares
Global services now 60% of IBM

Global Fin, Other 2.1%
Systems & Tech 16.5%
Software 21.7%
Global Bus Services 19.3%
Global Tech Services* 40.4%

Source: Annex Research

"Big Data" Buzz Word or Revolution?

Memory cheaper than paper

5 EB created every 2 days (Google' CEO)

Equal to mankind created data till 2003

Machine generated, duplicate, unstructured

Augmented Reality to Duplicated Reality
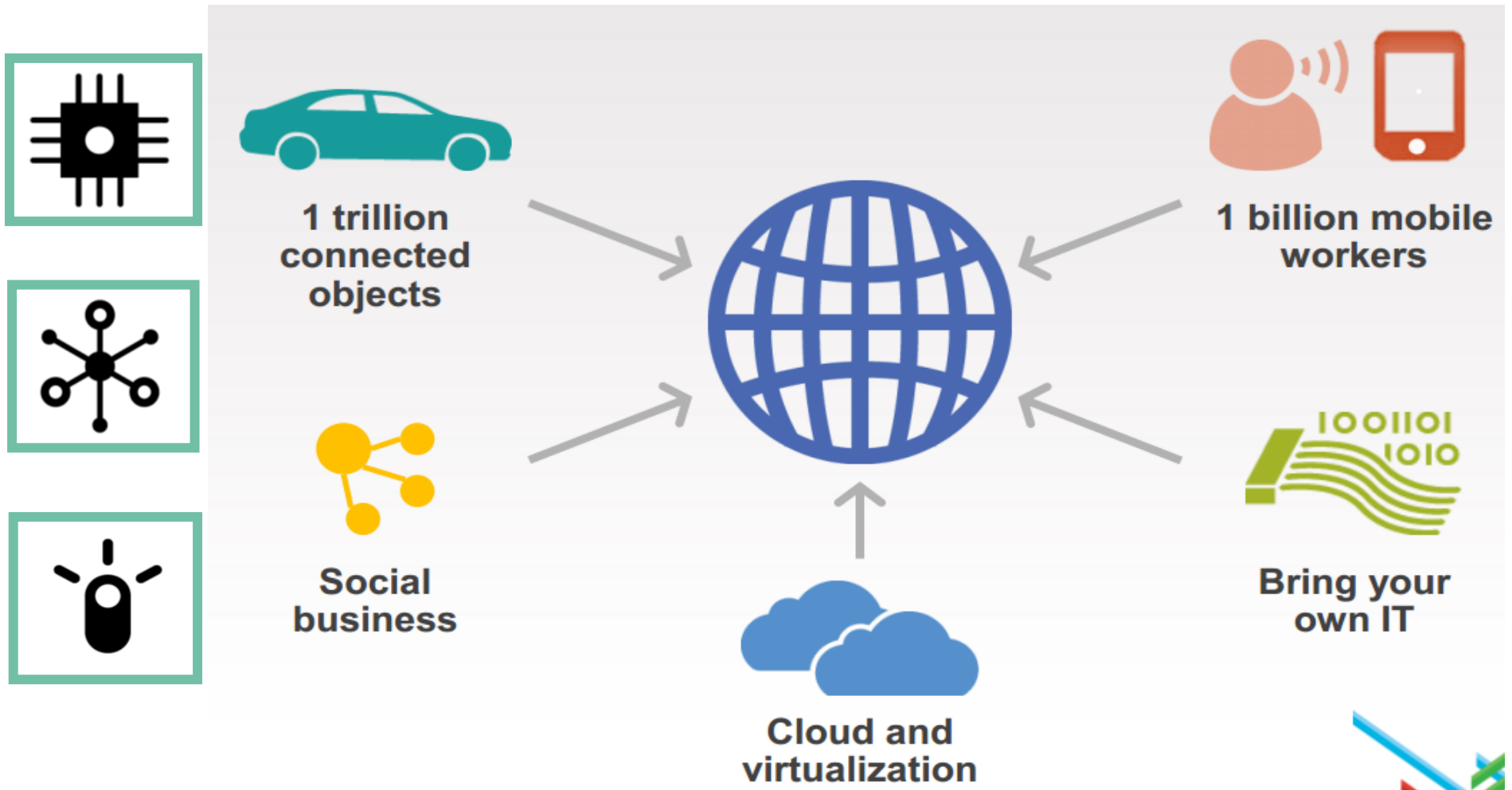
TB, PB, EB, ZB, YB …

Gold mine …

… and a security risk

Innovative technology changes everything
Better, Faster, Cheaper

1 trillion connected objects

Social business

Cloud and virtualization

1 billion mobile workers

Bring your own IT

The Smarter Planet
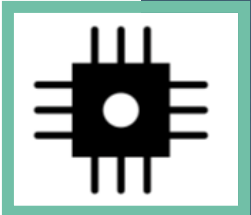
Our world is getting **Instrumented**

Our world is getting **Interconnected**

Our world is getting **Intelligent**

The Planet is getting more…

Smart Supply Chains

Smart Countries

Smart Retail

Smart Water Management
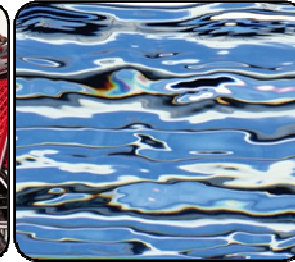
Smart Weather
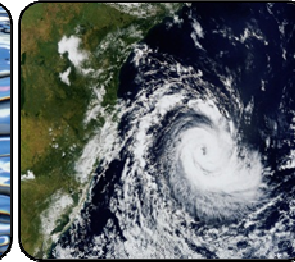
Smart Energy Grids
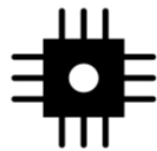
INSTRUMENTED   **INTERCONNECTED**   **INTELLIGENT**

Smart Oil Field Technologies

Smart Regions
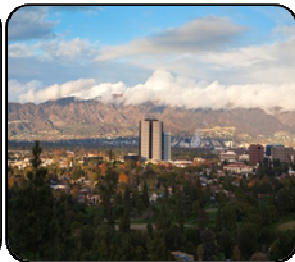
Smart Healthcare

Smart Traffic Systems
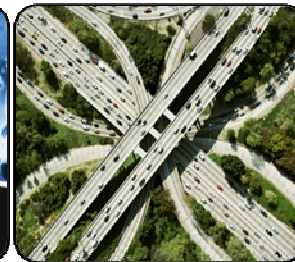
Smart Cities

Smart Food Systems
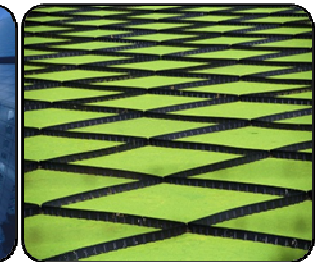
It isn't just because we can. It is because we must.

In a typical city, driving around for **parking in one year** generates the equivalent of **38 trips around the world**, burns 180,000 liters of gas, emitted 730 tons of carbon dioxide.

Congested roadways cost $160 billion real annually in the form of 4.2 billion lost hours and 11billion liters of wasted gas.

A typical **carrot has traveled 2,500 km,** a potato 1,900 km, a chuck roast 1,000 km…

…grocers and consumers throw away $74.4 billion real worth of food every year.

Just think about it …

Business moves to mobility

Turn information into insights

Drive enterprises' effectiveness and efficiency

Connect and empower people
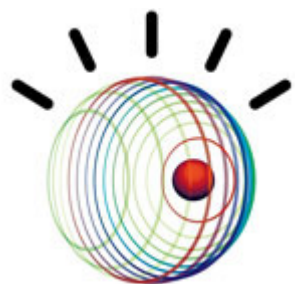
What is the risk?

DATA EXPLOSION

Protection of sensitive and large volumes of data, shared globally

ENDPOINTS

Protection of sensors & actuators in the wild

ATTACK SOPHISTICATION

Addressing the new cyber threat landscape

CLOUD

Adoption of virtualization and cloud computing

COMPLIANCE

Addressing compliance complexity

PRIVACY

Expectation of privacy

Motivations and sophistication are rapidly evolving

Flame

National Security	Nation-state actors **Stuxnet**
Espionage, Activism	Competitors and Hacktivists **Aurora**
Monetary Gain	Organized crime **Zeus**
Revenge, Curiosity	Insiders and Script-kiddies **Code Red**

Techniques, tools, and targets are also increasing

In 2011 there was an

80%

increase in phishing attacks, many of which impersonate social networking sites.

In 2011 there was a

19%

increase in the number of tools released publicly that can be used to attack mobile devices.

So far in 2012, IBM reports over

4,400

new security **vulnerabilities**.

2011: Year of the Targeted Attack

2011 Sampling of Security Incidents by Attack Type, Time and Impact
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses
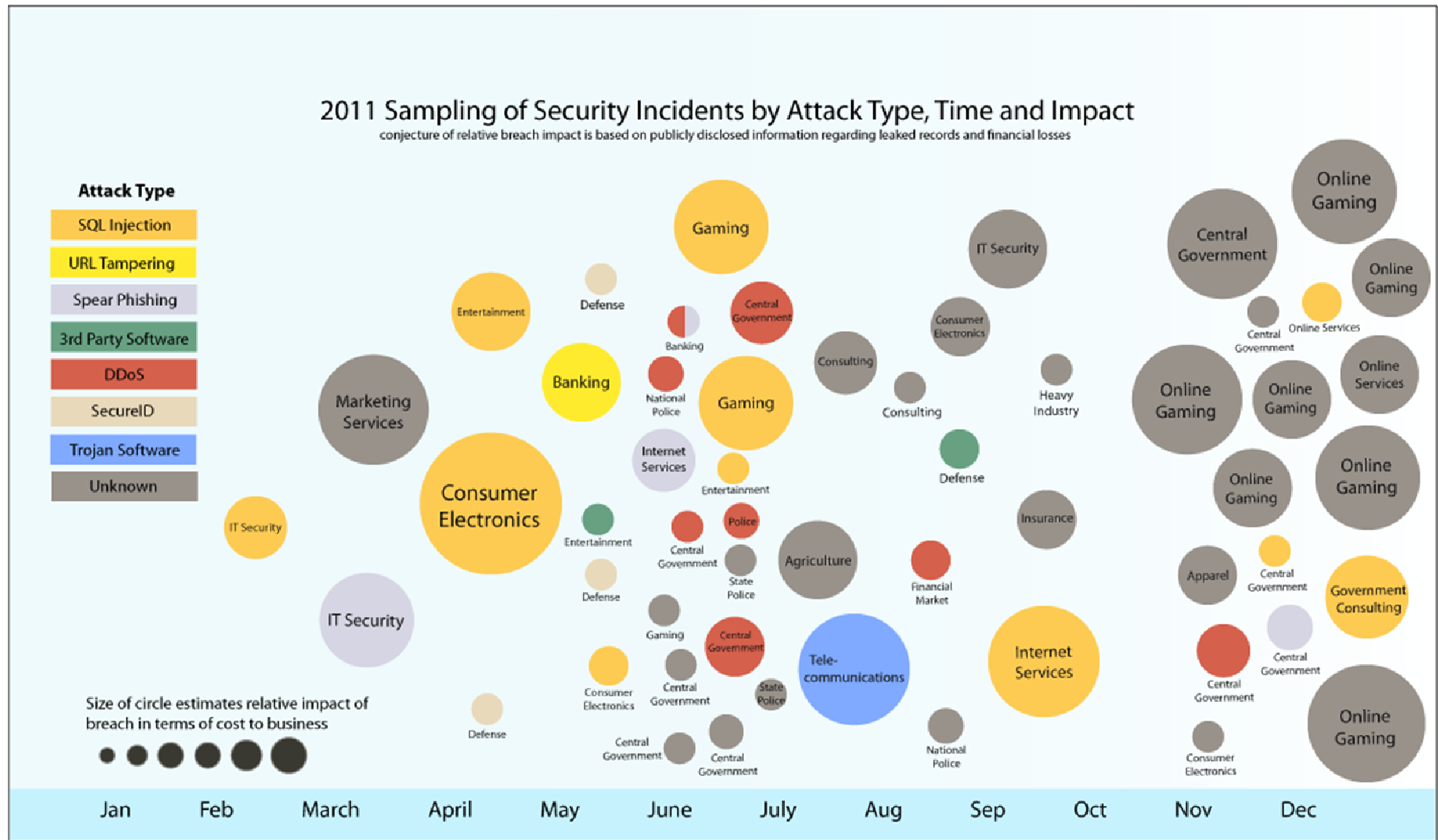
Source: IBM X-Force® Research 2011 Trend and Risk Report

IBM

Global coverage brings expertise and detailed security awareness

Zurich, CH

Waltham, US | Fredericton, CA | Delft, NL | Belfast, N IR

Ottawa, CA | Toronto, CA | Brussels, BE | IAS Europe | Herzliya, IL

Boulder, US | TJ Watson, US | Tokyo, JP

Almaden, US | Detroit, US | Tokyo, JP

IAS Americas

Costa Mesa, US | Haifa, IL | Bangalore, IN

Austin, US | Raleigh, US | Pune, IN | Taipei, TW

Atlanta, US | Bangalore, IN

Atlanta, US | Atlanta, US | Singapore, SG

New Delhi, IN | Brisbane, AU

Gold Coast, AU

Hortolândia, BR | Perth, AU | IAS Asia Pacific

- 🟨 **Security Operations Centers**
- 🟢 **Security Research Centers**
- ⬜ **Security Solution Development Centers**
- 🏛 **Institute for Advanced Security Branches**

IBM Research

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

X FORCE

World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

JK 2012-04-26

What are we seeing? Key Findings from the 2012 Trend Report

Progress in Internet Security

– Significant decrease of PDF vulnerabilities

– Fewer exploit releases

– Better patching

But…

New Attack Activity

– MAC APT and Java exploits surface

– Password leaks raise renewed awareness

– SQL injection most preferred attack type

– XSS tops at 51% of all web app vulnerabilities

The Challenge of Mobile BYOD

– Patching of mobile devices a real challenge

– CISOs say mobile security is greatest near-term technology concern

Download the report: http://www.ibm.com/security/xforce

IBM X-Force 2012
Mid-year Trend and Risk Report
September 2012

IBM

IBM.
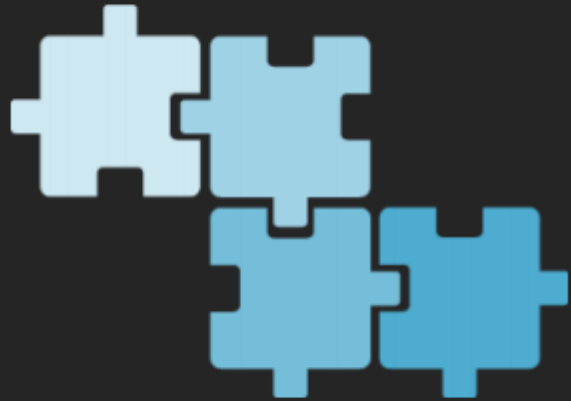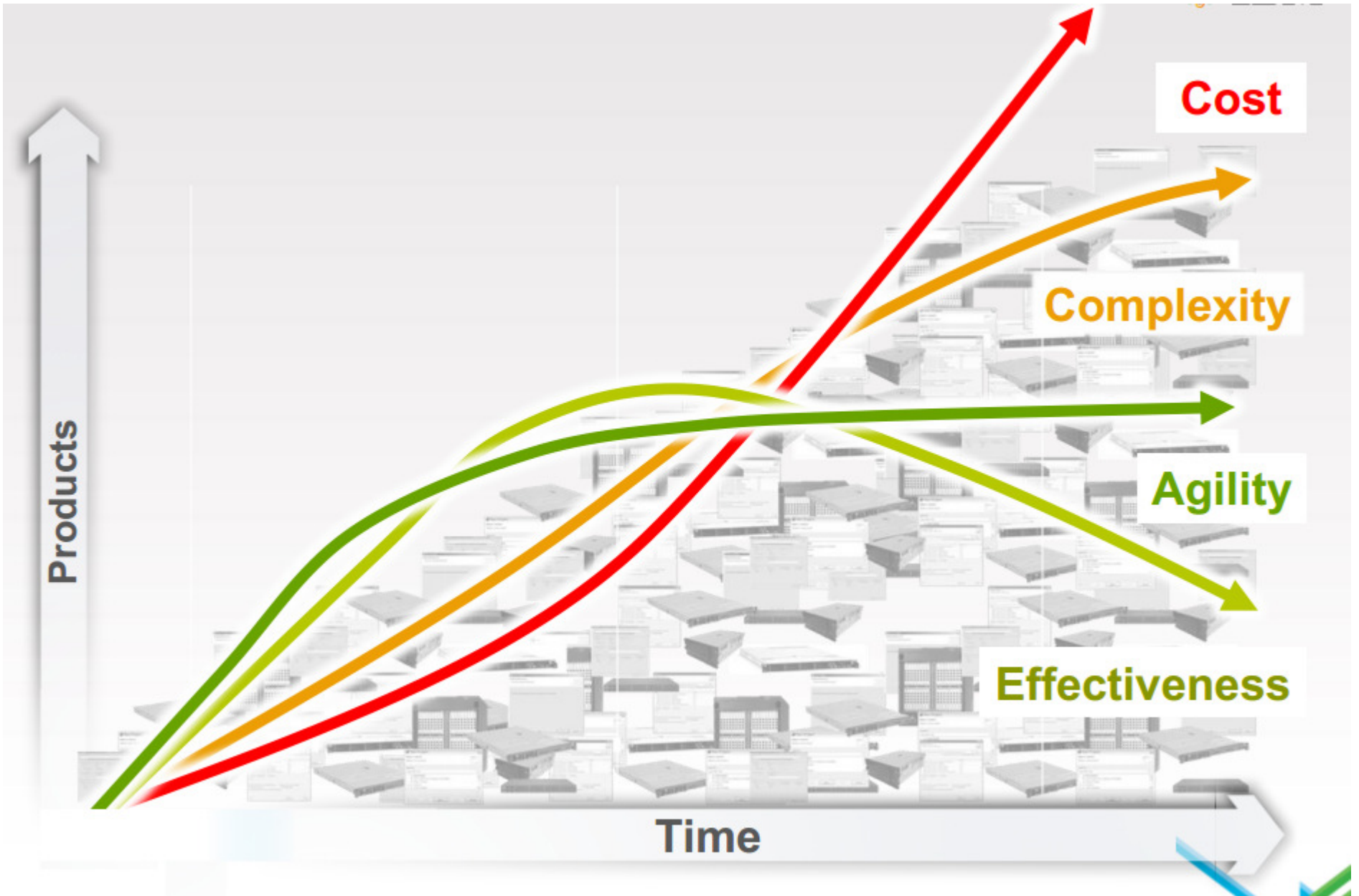
The attack surface is growing exponentially

People
- Employees
- Hackers
- Consultants
- Terrorists
- Outsourcers
- Suppliers
- Customers

Data
- Structured
- Unstructured
- At rest
- In motion

Applications
- Systems Applications
- Web Applications
- Web 2.0
- Mobile Applications

Infrastructure
- Datacenters
- PCs
- Laptops
- Mobile
- Cloud
- Non-traditional
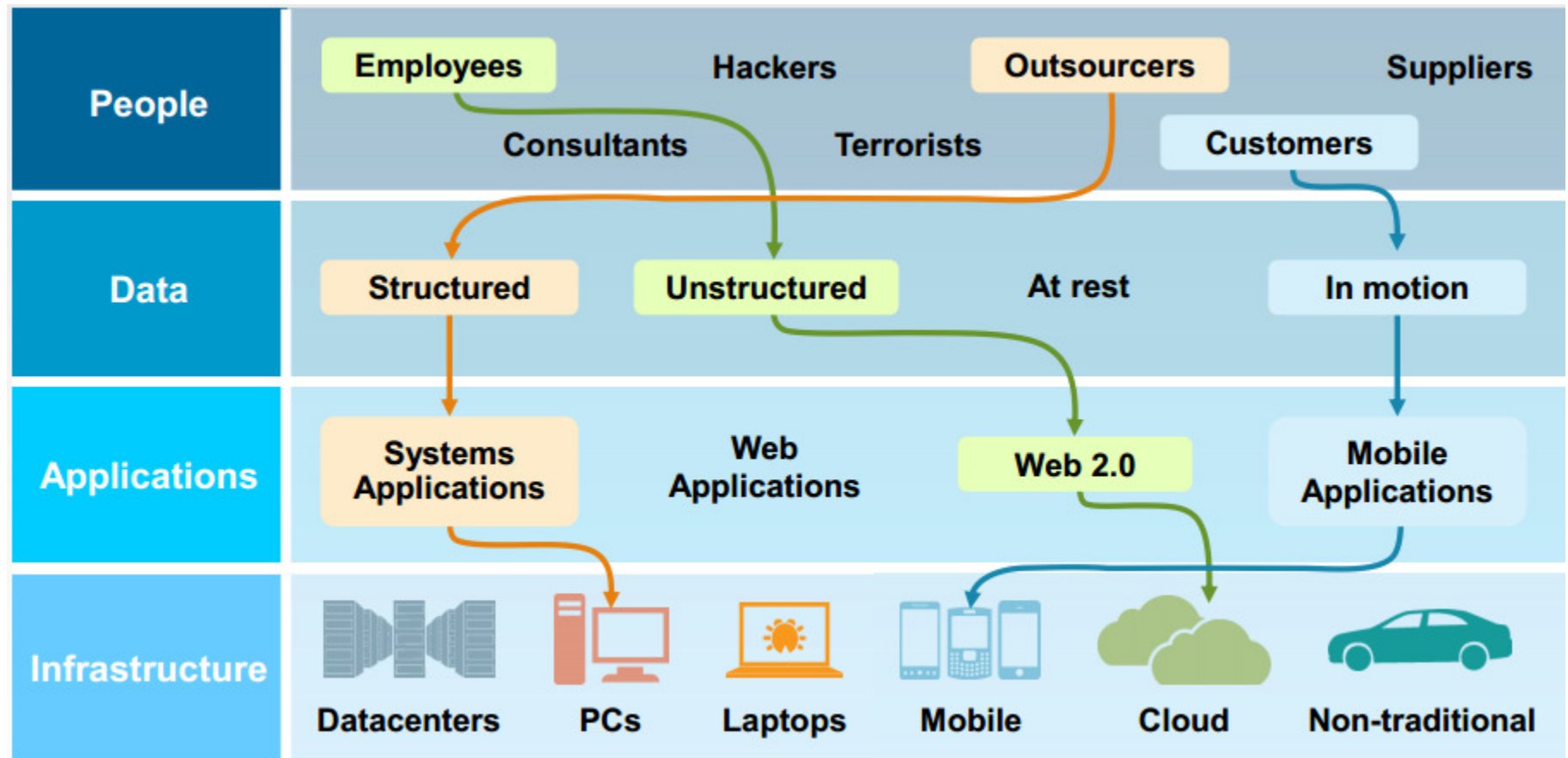
77% of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent

IBM Security Point Of View : shift from point product to integrated enterprise defense

Security will shift from a point product approach to an integrated enterprise approach, based on key foundational elements that allow for **active management, real time information, analytical correlation, and predictive threat management**

Security Domains	Today	Tomorrow	
People	Manage identities per application	Deploy role-based governance and privileged user management	Apply advanced correlation and deep analytics
Data	Deploy access control and encryption	Monitor usage and control leakage	
Applications	Scan for vulnerabilities	Build securely from day one	
Infrastructure	Block unwanted network access and viruses	Execute real time advanced threat detection and forensics	

Security Gap

Reactive ●- - - - - - - - - - - - - - -▶ **Proactive**

A "New Normal" led by Security Intelligence

Security Intelligence

Automated

Manual

Optimized

Proficient

Basic

Reactive   **Proactive**

Organizations employ *perimeter protection*, which regulates access and feeds manual reporting

Organizations use *predictive and automated* security analytics to drive toward *security intelligence*

Security is layered into the *IT fabric* and *business operations*

IBM
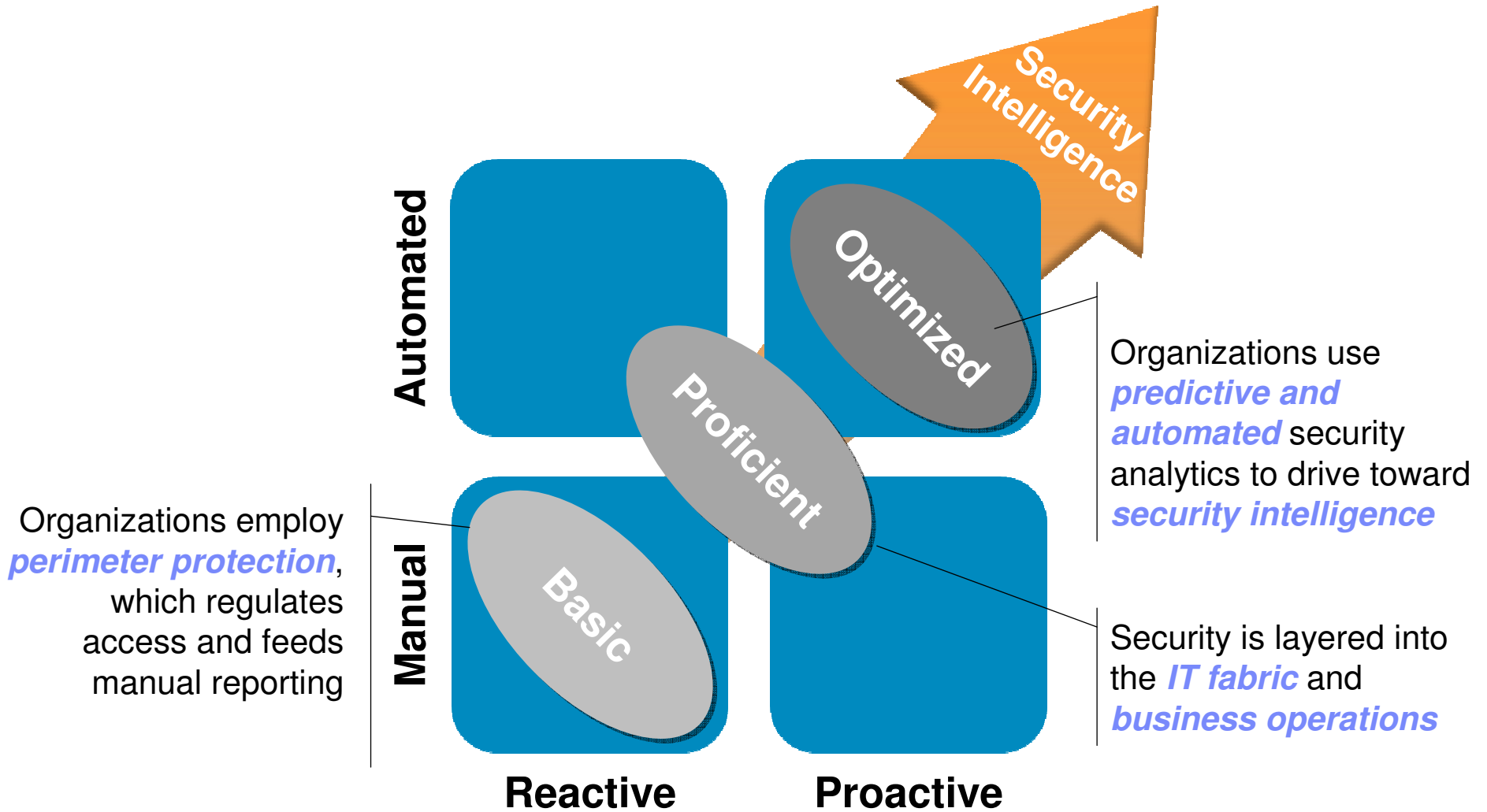
Full Visibility and Actionable Insight for Total Security Intelligence

Security Devices - - - - ->

Servers & Hosts - - - - ->

Network & Virtual Activity - - - ->

Database Activity - - - - ->

Application Activity - - - - ->

Configuration Info - - - - ->

Vulnerability Info - - - - ->

User Activity - - - - ->

Event Correlation
- Logs   • IP Reputation
- Flows   • Geo Location

Activity Baselining & Anomaly Detection
- User Activity
- Database Activity
- Application Activity
- Network Activity

Offense Identification
- Credibility
- Severity
- Relevance

Suspected Incidents

Extensive Data Sources	+	Deep Intelligence	=	Exceptionally Accurate and Actionable Insight

Security and Business Intelligence offer insightful parallels

IBM Security Intelligence

DASCOM
princeton softech an IBM®Company
Guardium SAFEGUARDING DATABASES™ AN IBM® COMPANY
NISC National Internet Security Company, An IBM Company

METAMERGE

access 360 A Better Way To Manage Access Rights
INTERNET SECURITY SYSTEMS™
watchfire
consul an IBM company

BIGFIX An IBM Company
1 Labs

ENCENTUATE An IBM Company
OUNCE LABS an IBM company
DATAPOWER

Market Changes

Security Intelligence

Security as a Service

Application Security

Database Monitoring

BI Convergence with Security

SOA Security

Managed Security Services

Decision Management

Network Intrusion Prevention

Simplified Delivery (i.e., Cloud)

Compliance Management

BI Convergence with Collaboration

Identity and Access Management

Mainframe and Server Security - RACF

Text & Social Media Analytics

Predictive Analytics

IBM Business Intelligence

IOD Business Optimization

Cognos software
OPENPAGES
i 2

Performance Management

SPSS AN IBM® COMPANY
Algorithmics KnowYourRisk.
N NETEZZA

Business Intelligence Suite

Enterprise Reporting

Time
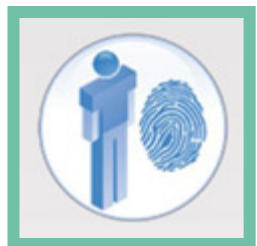
JK 2012-04-26

Security Intelligence

From

- Log collection and signature based detection

To

- Real Time Monitoring

- Context-aware anomaly detection

- Automated correlation and analytics

Integration of the IBM Security Framework provide incremental security value

Integrated Intelligence

Security Intelligence

People

Applications

Data

Infrastructure

Advanced Research

Monitor Everything

Integrated Research

Integrated Protection

Integration: Increase security, collapse silos, and reduce complexity

Integrated Intelligence.

3rd Party Ecosystem
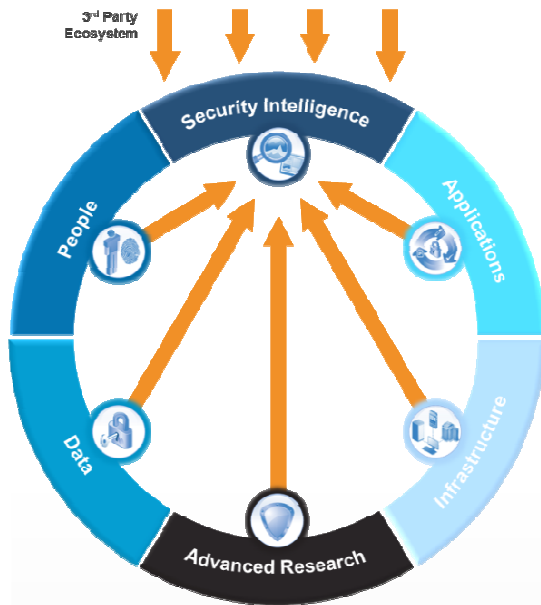
- Consolidate and correlate silo-ed information from hundreds of sources
- Designed to detect, notify and respond to threats missed by other security solutions
- Automate compliance tasks and assess risks

Integrated Research.
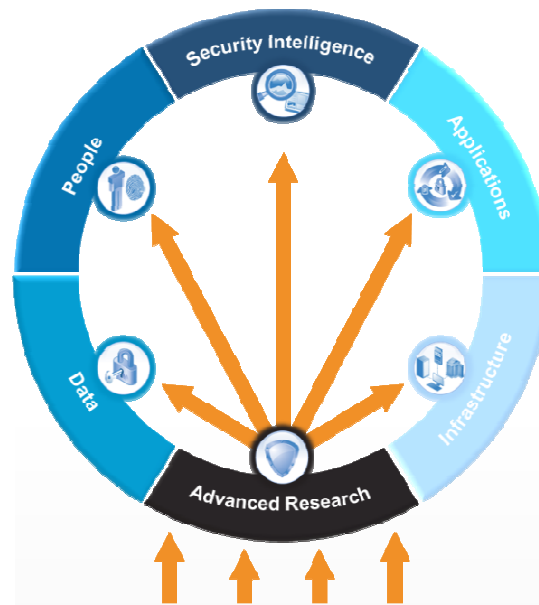
- Stay ahead of the changing threat landscape
- Designed to detect the latest vulnerabilities, exploits and malware
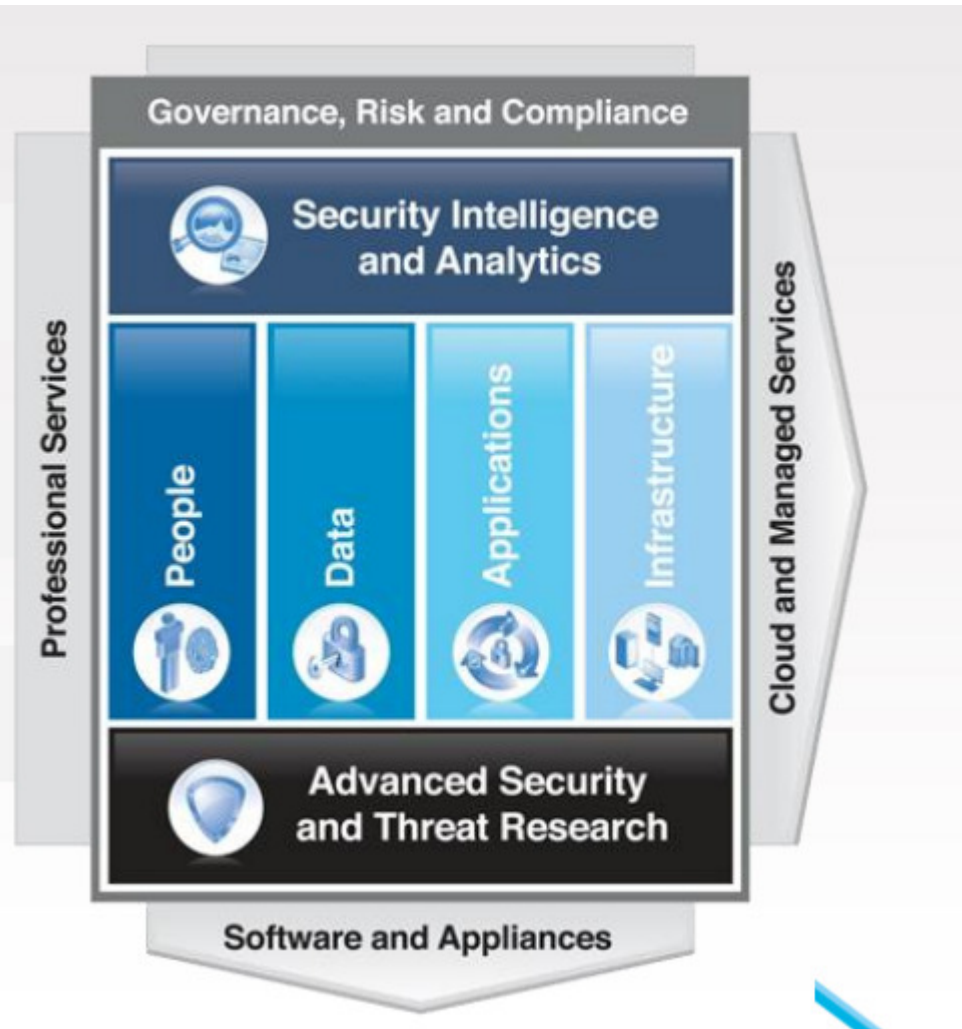- Add security intelligence to non-intelligent systems

Integrated Protection.
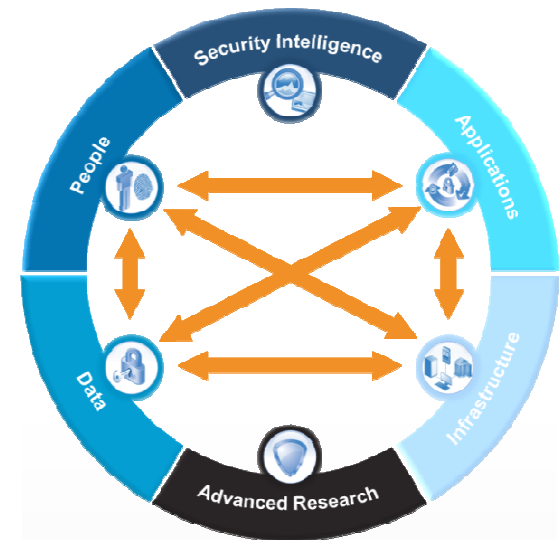
- Customize protection capabilities to block specific vulnerabilities using scan results
- Converge access management with web service gateways
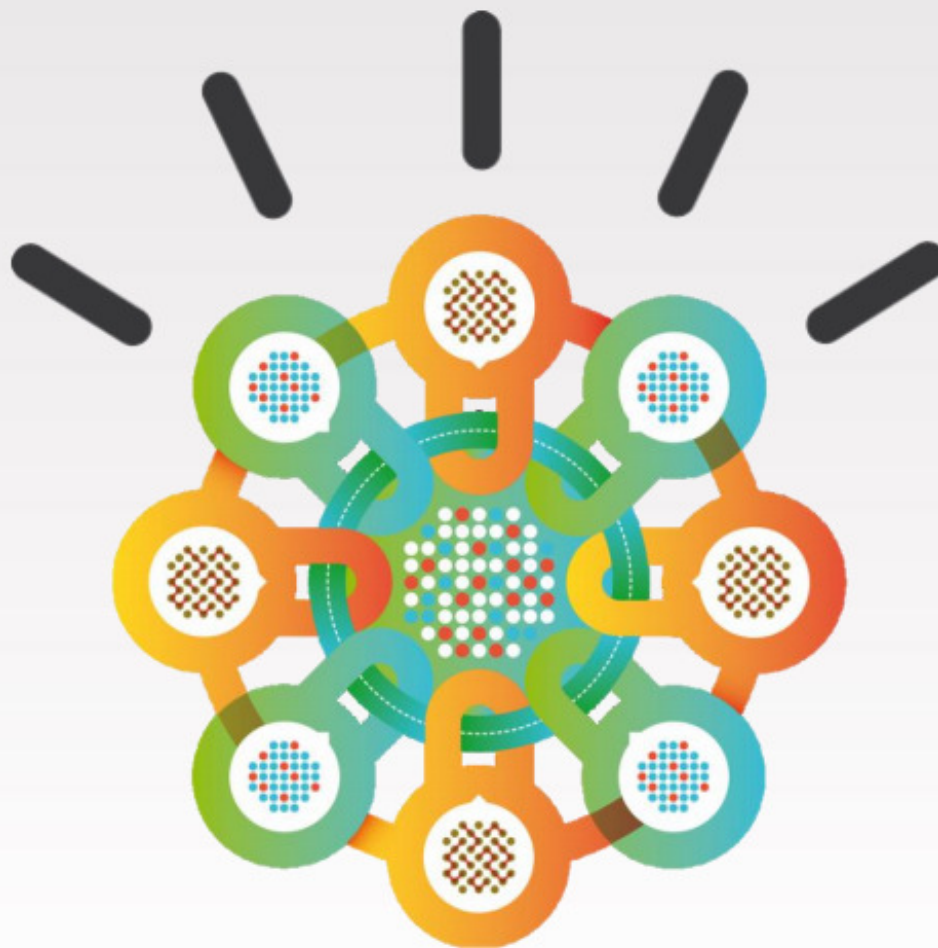- Link identity information with database security

Security Intelligence delivered through a comprehensive framework

Security Intelligence

Michel Bobillier
bobillier@ch.ibm.com
+41 58 333 4066