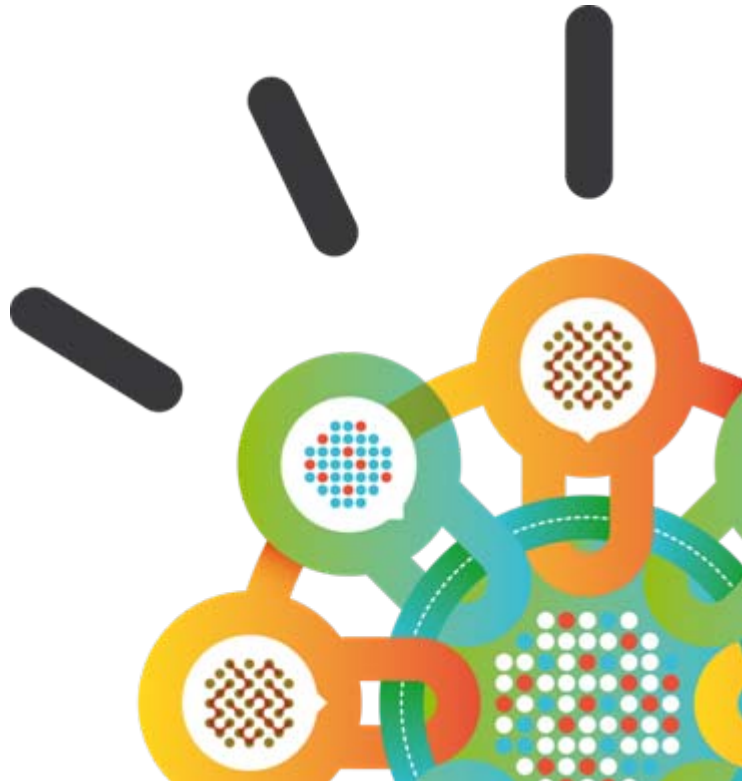
Security Intelligence.
Think Integrated.

# IBM Security

## Intelligence, Integration and Expertise

2Q 2012



# The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

**Data Explosion**

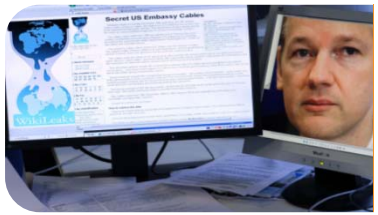
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

**Consumerization of IT**

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

**EVERYTHING IS EVERYWHERE**

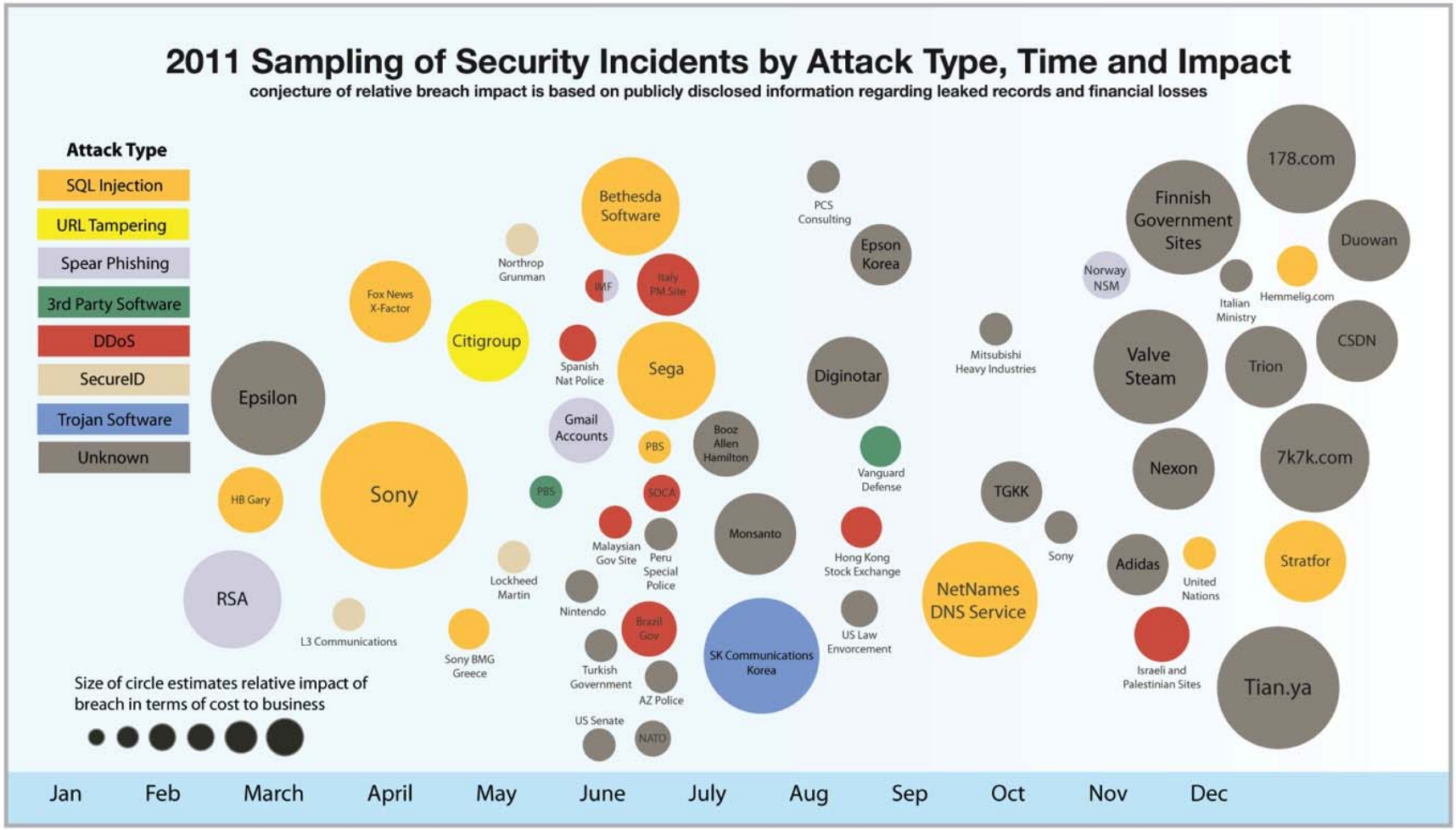
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more




**Attack Sophistication**

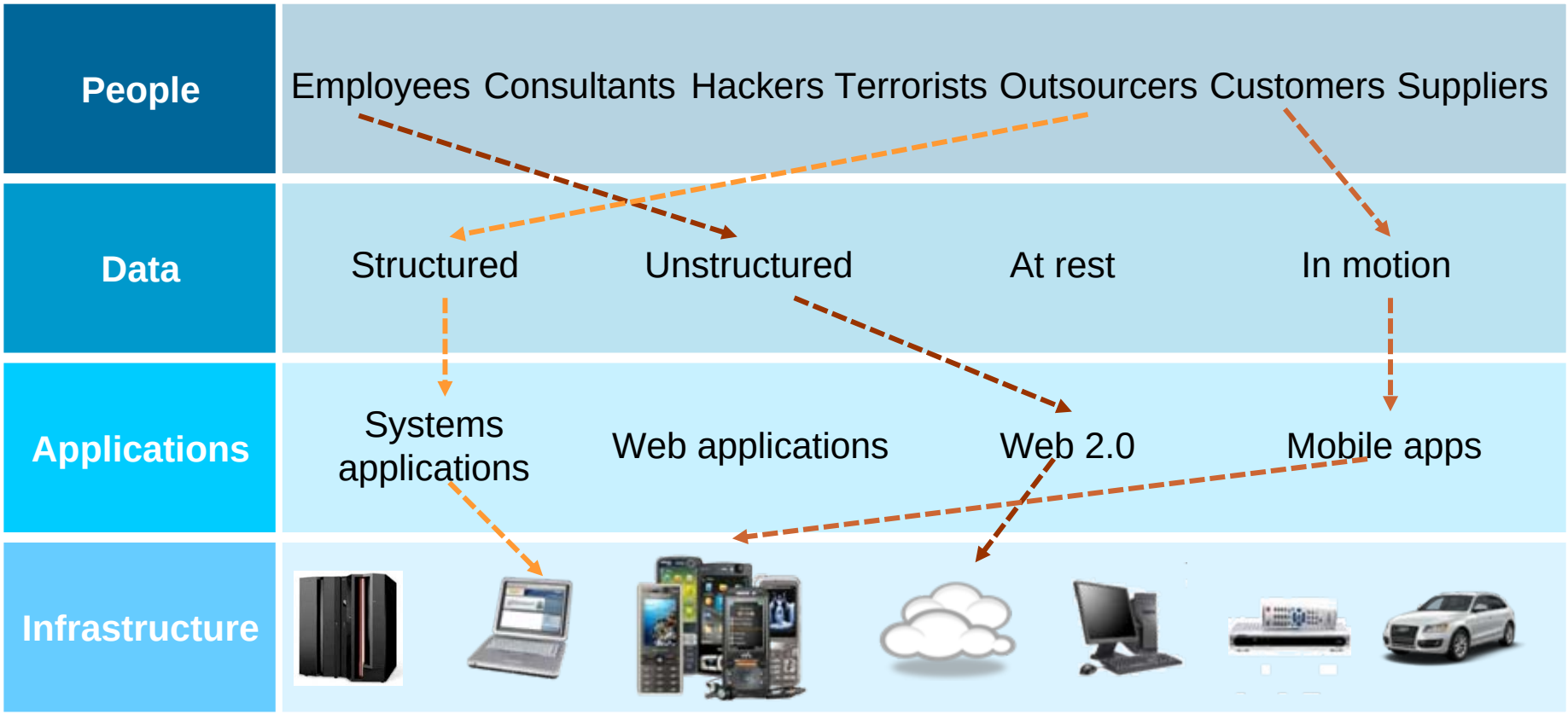
The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

# XFORCE: 2011: Year of the Breach



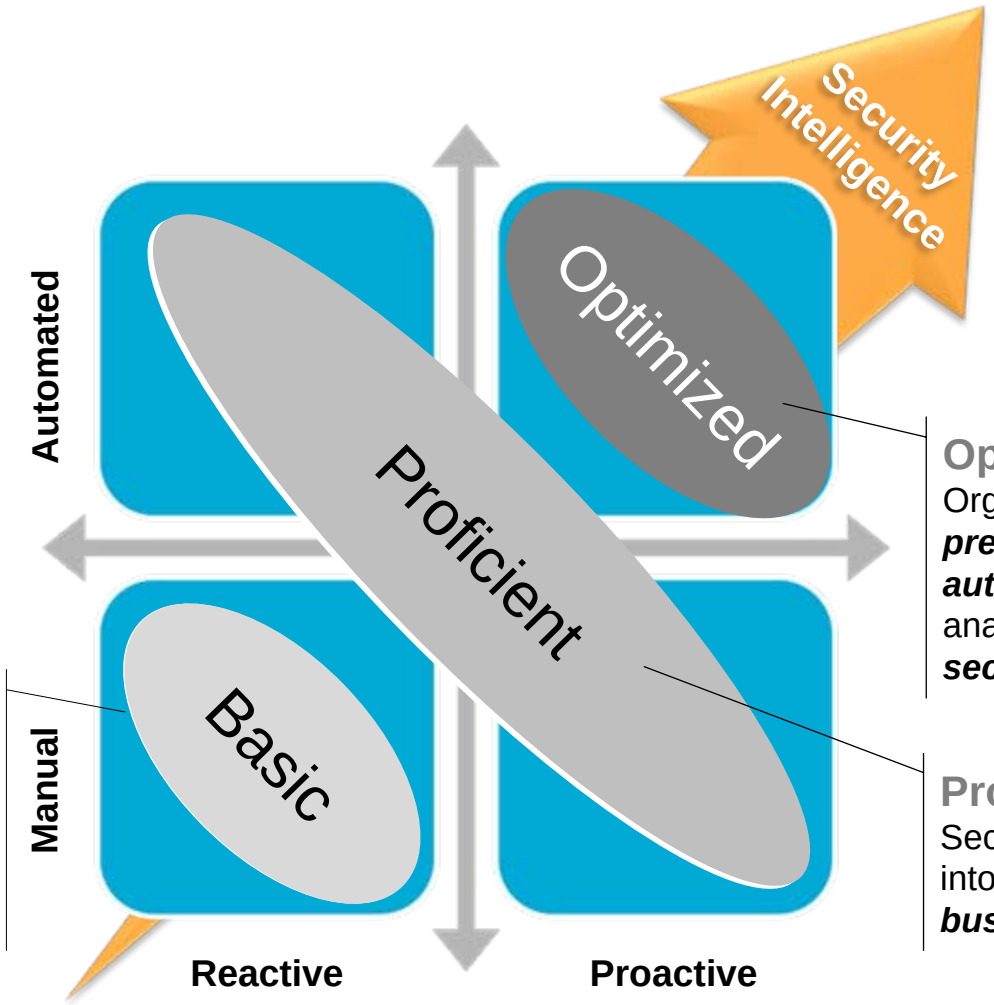

Source: IBM X-Force® Research and Development

# Solving a security issue is a complex, four-dimensional puzzle




It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

# In this “new normal”, organizations need an intelligent view of their security posture




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

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

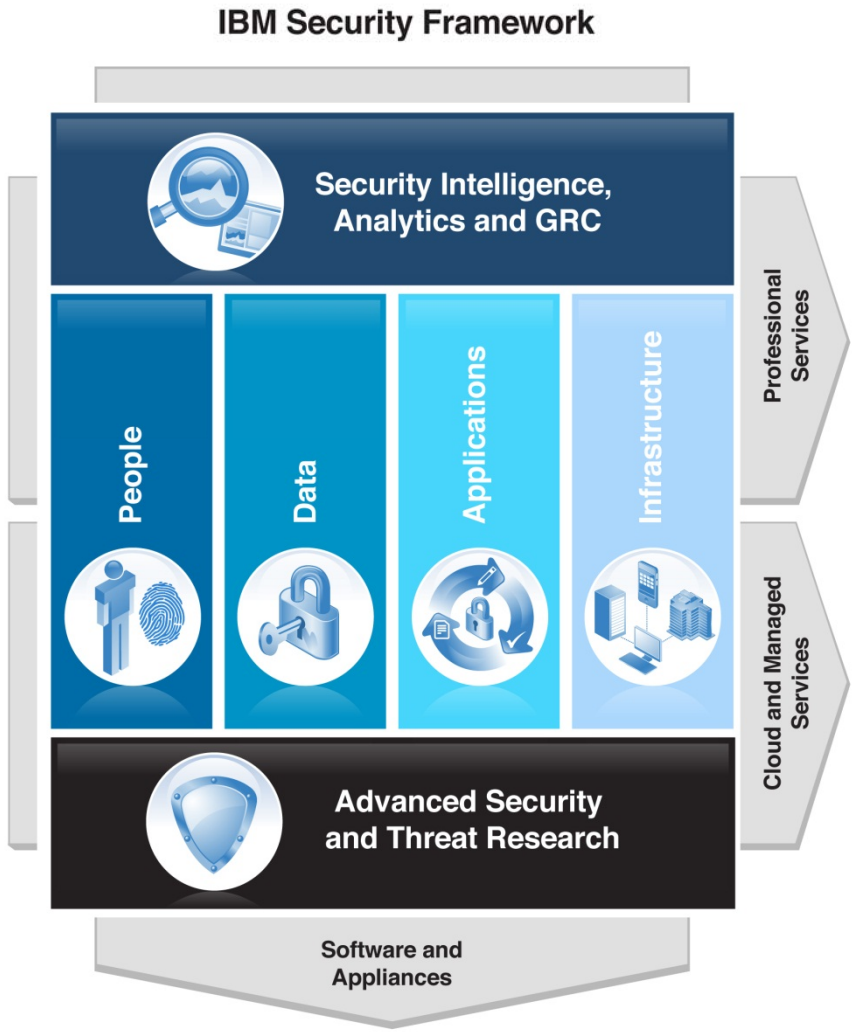
**Proficient**
Security is layered into the ***IT fabric*** and ***business operations***

# IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

## IBM Security Systems

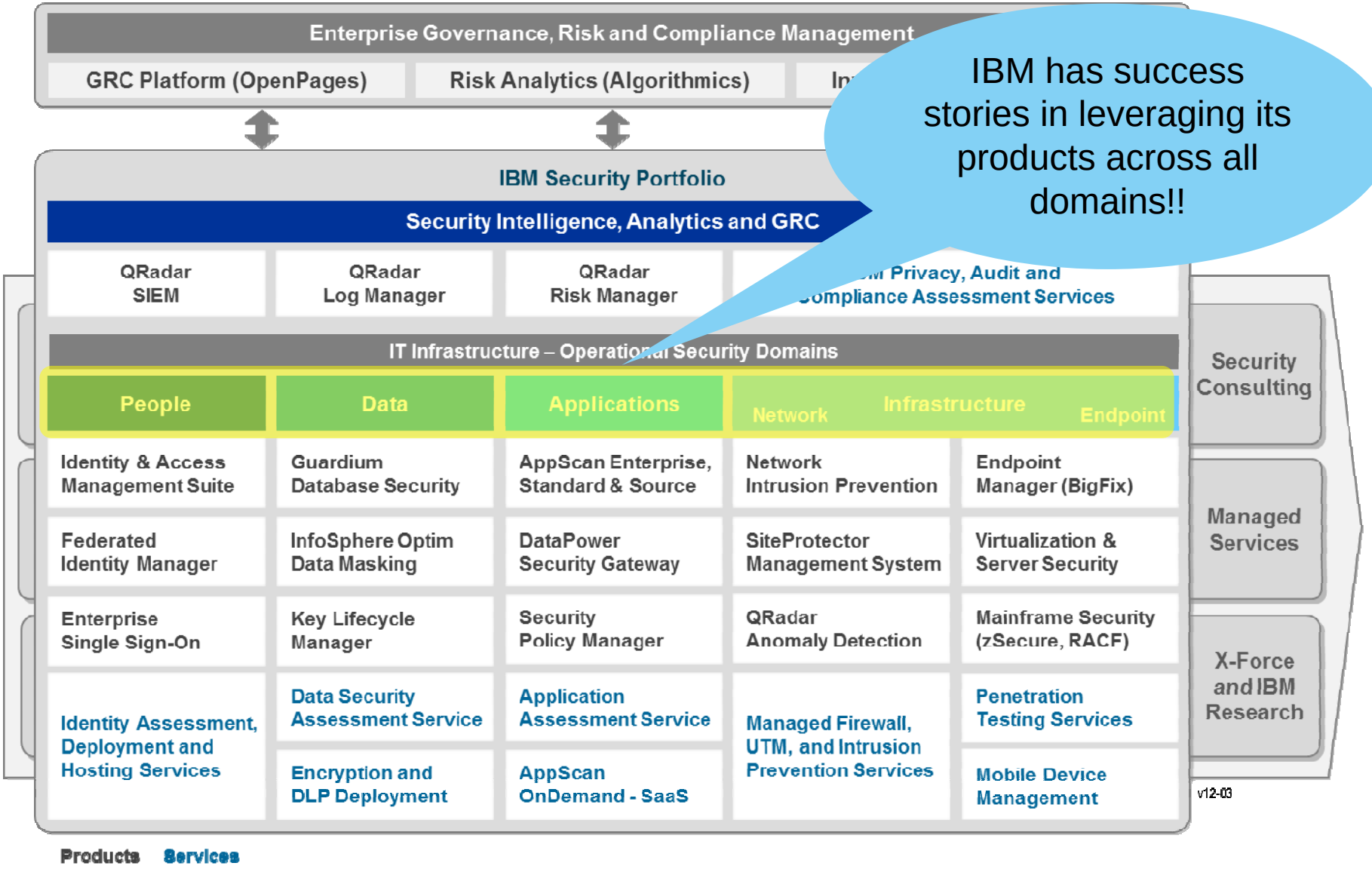
- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

**Intelligence • Integration • Expertise**



# How is IBM using it’s own products and services to solve it’s complex security challenges?

# IBM leverages many products across our portfolio to secure itself




IBM has success stories in leveraging its products across all domains!!

# Customer Story: IBM

## How IBM leverages Privileged Identity Management to improve security when accessing servers

### Business Problem Summary:

- IBM provides Server Outsource services to hundreds of customers globally
- Managing hundreds of servers across dozens of administrators quickly becomes millions of priv credentials (traditional approach)
- Alternately, sharing credentials decreases accountability
- More Priv credentials = More risk and potential for loss/theft

### Solution:

- Integration of ITIM, TAMeSSO and TSIEM
- Provides “reusable” IDs
- Provides accountability and auditability
- Originally developed as service to address IBM’s own challenge
- Currently available as a service
- Included in product roadmap

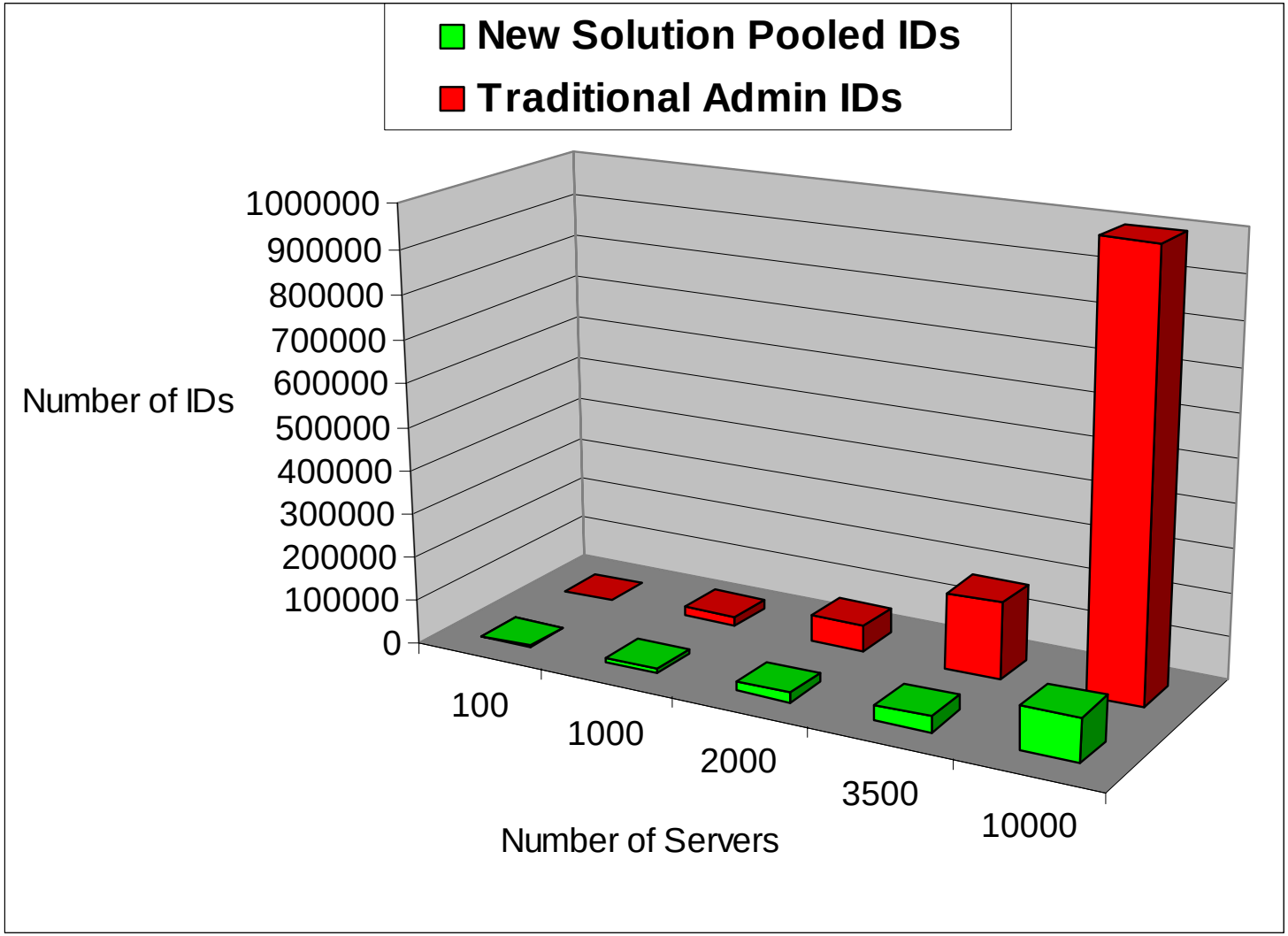
### Challenge:

- Rethink traditional approach:
  - “Everyone has a userid on every system, all the time, just in case” (Admins x Servers)
  - “Everyone shares access to a single userid for ease of administration”
- Desired approach:
  - “A user gets an individual userid on a system – but only…
    - If they need it
    - When they need it
    - For only as long as they need it

### Benefits:

- Centralized Privileged ID management improves IT control and **reduces risk**
- Automated sign on and check-in/out simplifies usage and **reduces cost**
- Comprehensive tracking and reporting **enhances accountability and compliance**

# PIM is currently being deployed as an IBM Global Strategic Solution



# Customer Story: IBM

## How IBM leverages Rational Appscan products to deliver secure products and applications

### Business Problem Summary:

- IBM's software development business consists of tens of thousands of developers across nearly every computing platform in existence
- Includes our own Software Group products across brands such as Lotus, Tivoli, Websphere, DB2 and many many others
- Also includes development of web-based applications for itself and many of it's customers
- Prior to acquisition of Rational, lacked cohesive secure software engineering development and test approach

### Solution:

- Adoption of Rational AppScan Source edition for use within the software engineering practices across IBM
- Corresponding education program that includes tooling and coding practices
- Policy tester being used for privacy and usability perspective
- Adoption of Rational AppScan Enterprise edition as requirement for web applications
  - Baseline policy for all CIO applications
  - Used in development/pre-production cycle
  - Provided as a service

### Challenge:

- Implement a comprehensive secure software engineering process that included:
  - Governance and compliance process to manage overall secure engineering practice
  - Secure SW engineering practices across all programmers (White box testing)
  - Process improvements that required development and pre-production testing for application-based vulnerabilities (Black box testing)

### Benefits:

- Acquisition of Rational has fundamentally changed IBM
- Widespread use of it's products to improve our own security as well as improve the security of our products for our customers

# Customer Story: IBM

## How IBM leverages Guardium to improve security in it's use of DB2

### Business Problem Summary:

- Risk appetite and increased regulation have lead IBM to desire that ability to monitor the actions of database administrators of select databases
- Difficulty in patching vulnerabilities in database middleware due to the significant changes in functionality included in current patching (i.e. makes significant changes to middleware, potentially breaking applications)

### Solution:

- Use of Guardium to address problem began as CIO-Sponsored POC in 2011
- Expanded to cover single strategic datacenter in 2012
  - Development of common architecture as deliverable
- Expansion to multiple global datacenters based on 2012 architecture planned

### Challenge:

- Seek alternate methods of monitoring database access that could result from exploitation of database vulnerabilities
- Provide administrator activity monitoring across a very large, globally dispersed enterprise in a concise, cost effective manner
- Develop skills inside IBM needed to support
- Specifically focused on high value applications
- Increase frequency of vulnerability-related alerts in pace with vulnerability discovery (Qtrly moving to Monthly)
- Development of global architecture that can be applied enterprise-wide

### Benefits:

- Provides user oversight needed for high value applications
- Assisted in allowing IBM to manage risk associated with extended patch/testing cycle needed for database middleware

# Customer Story: IBM

## How IBM leverages it's own Intrusion Prevention technology and XFORCE Intelligence to protect itself

### Business Problem Summary:

- IBM required automated 24X7 response to identified security issues globally
  - Across nearly 200 countries
  - Limited/no real time reliance on manual analysis
- Develop a service-based approach that ensured IBM continually identified security issues not addressed by traditional endpoint solutions
- Provide anomaly detection that extended to identification of potential participation in external Botnets

### Solution:

- Integration of IBM's Network IPS globally at multiple layers of IBM (200+ devices)
  - User egress
  - Critical locations
  - Development area
- Automated application of security intelligence against FW logs in continually updated, near-real time manner
- Anomaly detection at all user egress points
- Leverages other IBM components like Websphere and DB2 in "rules engine" that provides notification, etc

### Challenge:

- Capture analyst knowledge for use in automated approach that allows for reaction to potential security issues within 15 minutes
- Develop an approach that expands to IBM globally – across one+ Class A network
  - Engage proper support personnel for network removal and remediation wherever the machine exists
- Real time reactivity to constantly changing anomaly detection indicators
- Harness XFORCE research knowledge of emerging threats into action

### Benefits:

- Automated additional layers of protection that have identified significant volumes of issues not identified by AV, etc
- Security metrics that provide constant operational view of issues with enterprise
  - Allows tactical focus on problem areas
  - Allows direct input into effectiveness of endpoint protection technologies
- Extremely small overhead for continual 24X7 service

# Customer Story: IBM

## How IBM is developing an advanced threat analysis and detection system around Q1 Labs technology

### Business Problem Summary:

- Targeted attacks have become far more common but most currently implemented solutions will not provide appropriate analysis and detection capabilities
- Truly security-related "Big Data" problem
  - Requires huge amounts of continual data across network, endpoint, application sources
  - "Grain of sand at the bottom of the ocean"

### Solution:

- Define solution approach based on identified use cases. They fall into two categories
  - **Investigation, reporting and analysis –** Historic (data at rest) analysis. Prototype implementation using Infosphere BigInsights on sample information.
  - **Real time insight to detect potential targeted threats** – To explore Q1 capabilities, on how it could help address the real time use cases.
- Implementing **Q1 capabilities**, along with **Infosphere BigData** to be explored in the context of use cases.

### Challenge:

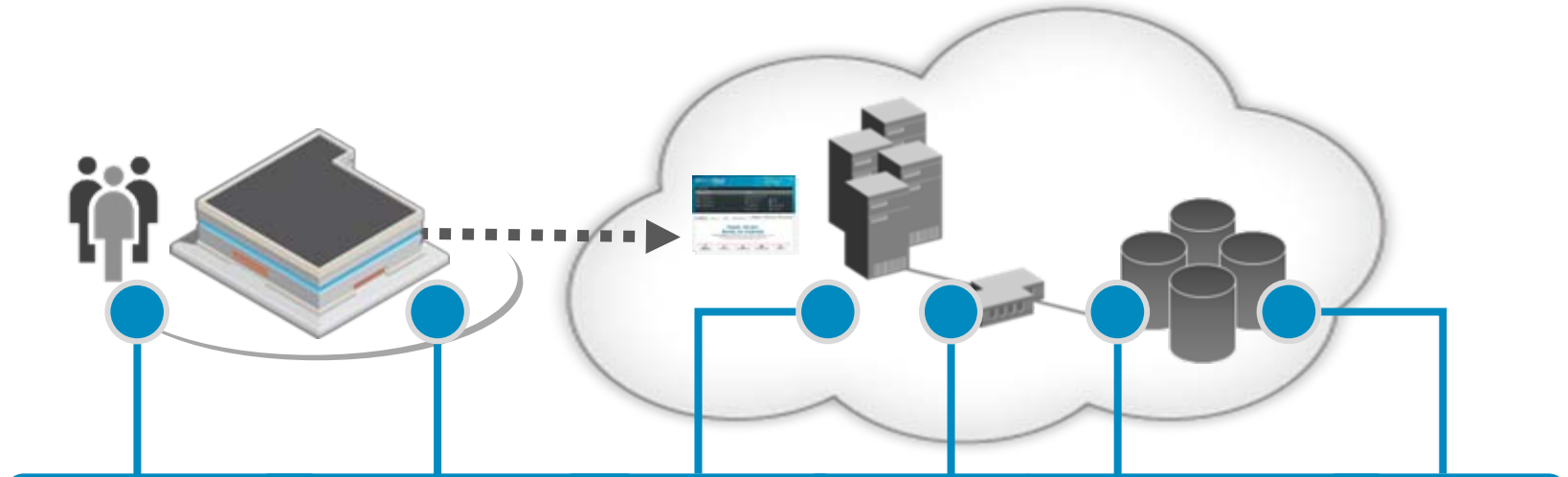
- **Targeted malware attacks are very difficult to detect and analyze**, reliant on external intelligence, lacking proactive identification. Current operational approaches to targeted attacks highly manual, reactive, and will not scale.
- Potential detection (versus reaction) requires the ability to draw relationships between events difficult/impossible by humans
- Requires significant amounts of data storage if desired window extends to multiple years historically

### Benefits:

- Innovation and use of IBM technologies will provide blueprint that potentially assists IBM customers with how to leverage in similar fashion
- Clearly still in development, innovation and integration but ultimately, most difficult problem we've had to solve in security space

# Everything is Everywhere

*IBM is helping clients adopt cloud with flexible, layered security solutions*




**IBM Security Intelligence**

# Customer Story: IBM

## How IBM leverages it's secure endpoint solution to decrease security issues and better protect it's endpoint devices (including Mobile)

### Business Problem Summary:

- IBM desired to decrease security issues that were result of business transformation
  - Significant growth
  - Joint development/Partnerships/Outsourcing
  - Improve employee efficiency by increasing compliance mgmt via automation
- Implement technology that easily supported flexible roles-based profiles across heterogeneous client platforms and devices (that included mobile platforms)

### Solution:

- Tivoli Endpoint Manager (IBM Endpoint Manager) implemented globally across IBM
- Fastest client deployment in IBM history - deployed to all Windows clients within 6 months
- Supports multiple profiles and operating systems (including Windows XP/7, Mac, Linux)
- Flexible solution allowed use of shared servers as well as desktops in relay infrastructure (managed dynamically)
- Mobile deployment underway
- Has become fundamental security framework across all devices

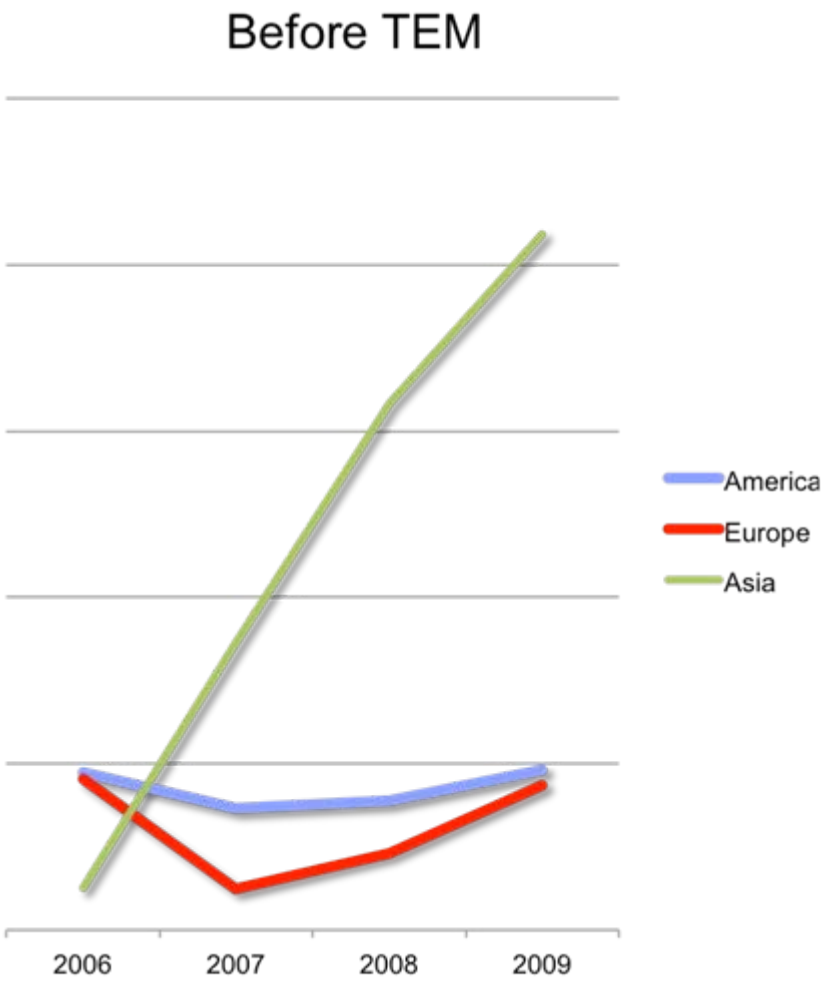
### Challenge:

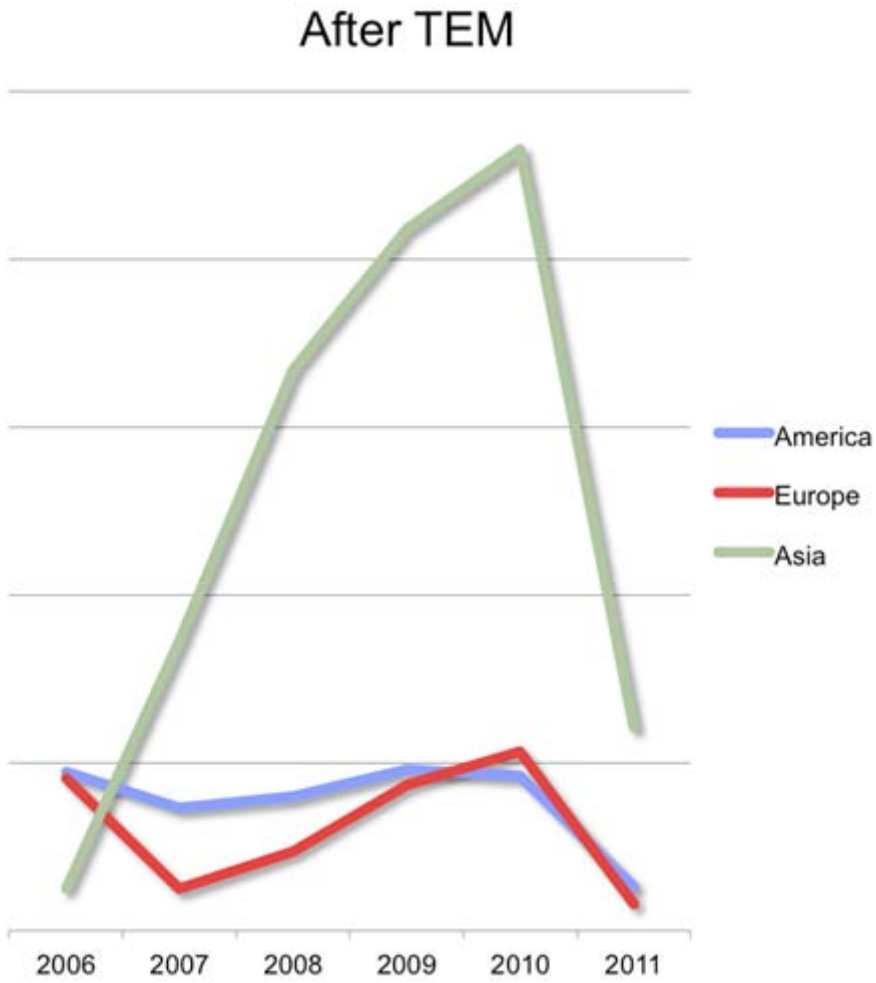
- Displace home-grown legacy technology
- Support Windows, Mac, Linux, iOS, Android
- Support definition of role and data-focused security profiles encompassed in migration from "one size fits all" security to new model
- Highly scalable – 500K-1M devices
- "Client light"
- Easily deployable

### Benefits:

- 78% decrease in security-related problems since deployment
- >$10M savings in associated cost avoidance
- Extremely efficient – 3 FTEs managing >500K workstations
- Migration to persistent compliance model from employee reliant model

# Endpoint security issues by GEO



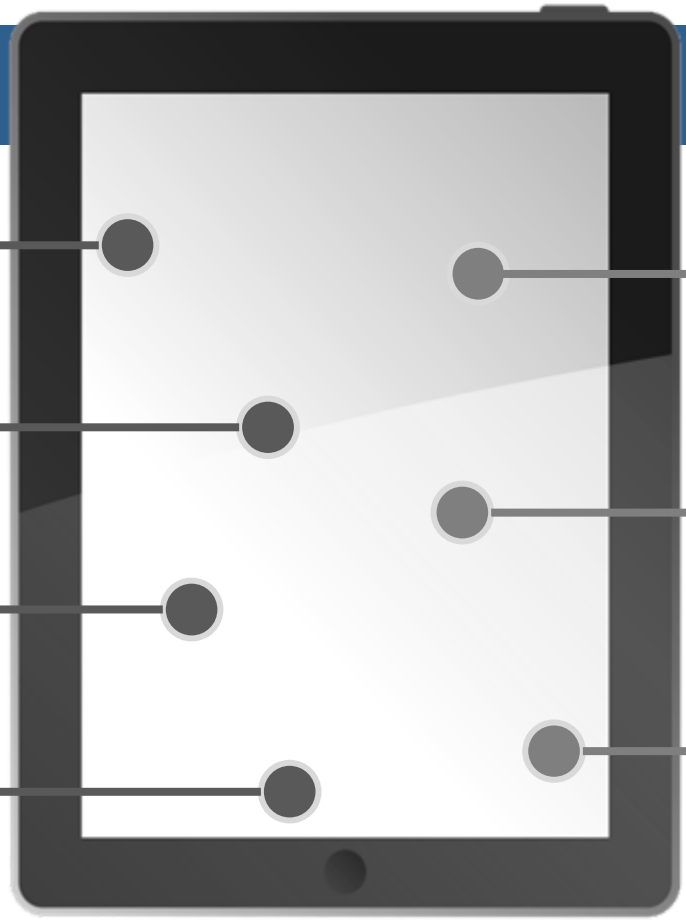



# Consumerization of IT

*IBM is converging traditional endpoint and mobile security management into a single solution with complementary services*

## IBM Mobile Security Software

- Device Inventory
- Security Policy Management
- Device and Data Wipe
- Anti-Jailbreak and Anti-Root

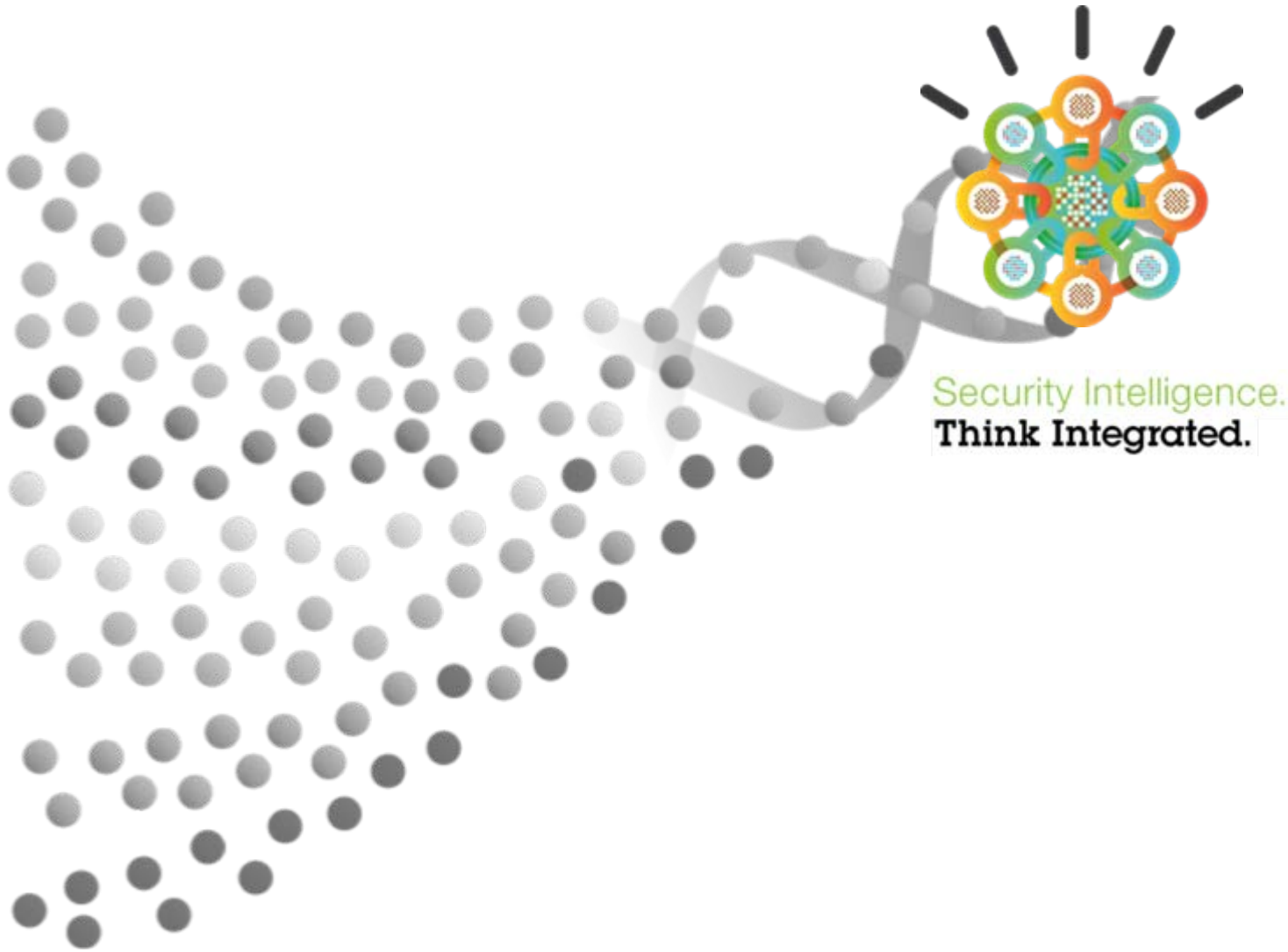


## IBM Mobile Security Services

- **Lifecycle Management** Mobile Enterprise Services (MES)
- **Endpoint Management** Hosted Mobile Device Security Management
- **Secure Connectivity** Secure Enterprise Smartphone and Tablets

# Intelligent solutions provide the DNA to secure a Smarter Planet

- Security Intelligence, Analytics & GRC
- People
- Data
- Applications
- Infrastructure



ibm.com/security