# IBM SECURITY FRAMEWORK

Hakan TURGUT
IBM Security Systems Bölge Yöneticisi
Türkiye, Doğu Avrupa, Rusya ve CIS Ülkeleri

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

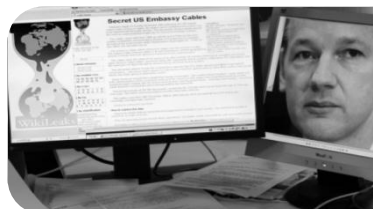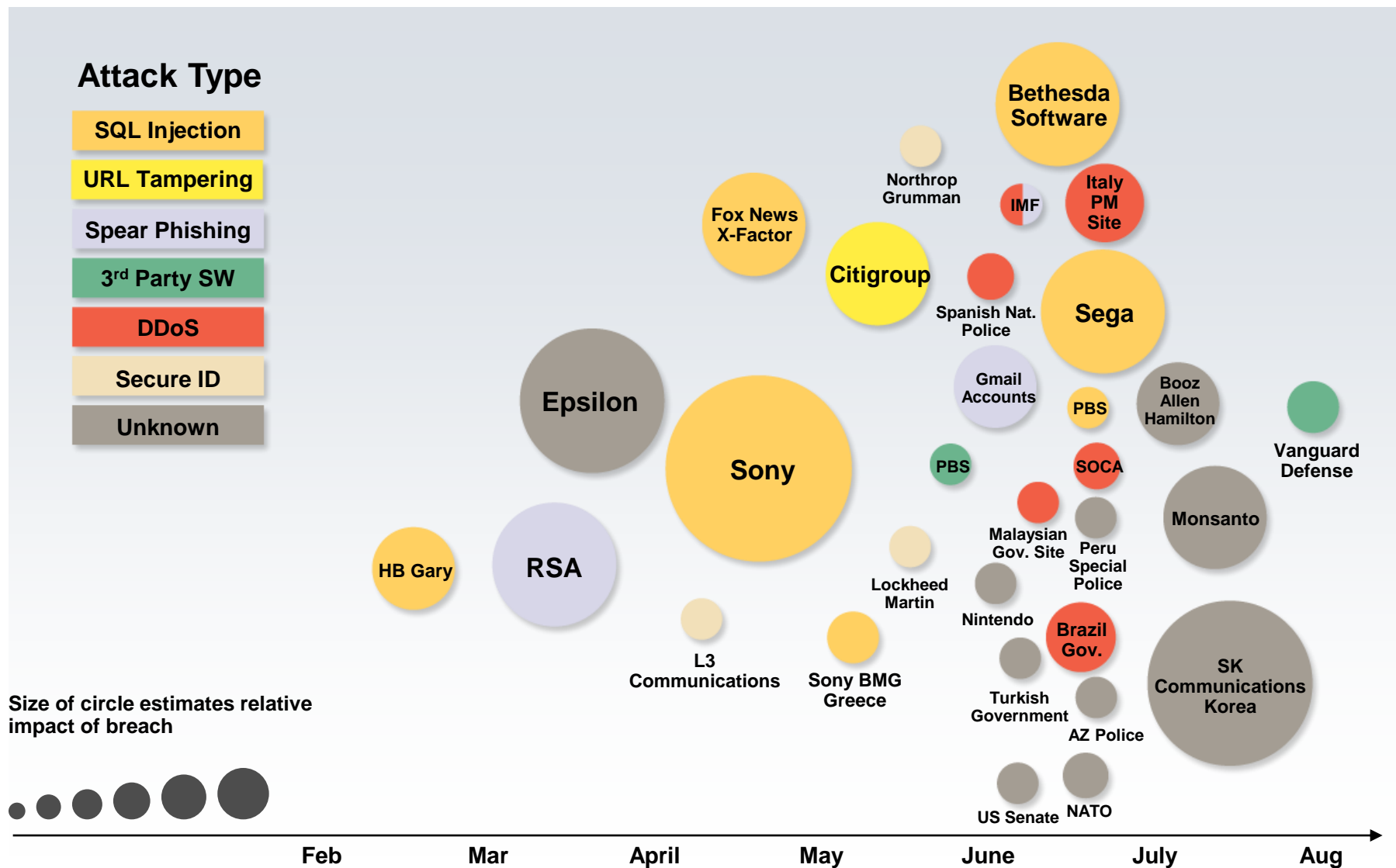| | **DATA EXPLOSION** | The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere |
| --- | --- | --- |
| | **CONSUMERIZATION OF IT** | With the advent of Enterprise 2.0 and social business, the line between 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 |

# Targeted Attacks Shake Businesses and Governments

## Attack Type

- SQL Injection
- URL Tampering
- Spear Phishing
- 3rd Party SW
- DDoS
- Secure ID
- Unknown

Bethesda Software

Northrop Grumman

IMF

Italy PM Site

Fox News X-Factor

Citigroup

Spanish Nat. Police

Sega

Epsilon

Gmail Accounts

PBS

Booz Allen Hamilton

Sony

PBS

SOCA

Vanguard Defense

HB Gary

RSA

Malaysian Gov. Site

Peru Special Police

Monsanto

Lockheed Martin

Nintendo

Brazil Gov.

L3 Communications

Sony BMG Greece

Turkish Government

SK Communications Korea

AZ Police

**Size of circle estimates relative impact of breach**

US Senate    NATO

Feb        Mar        April        May        June        July        Aug
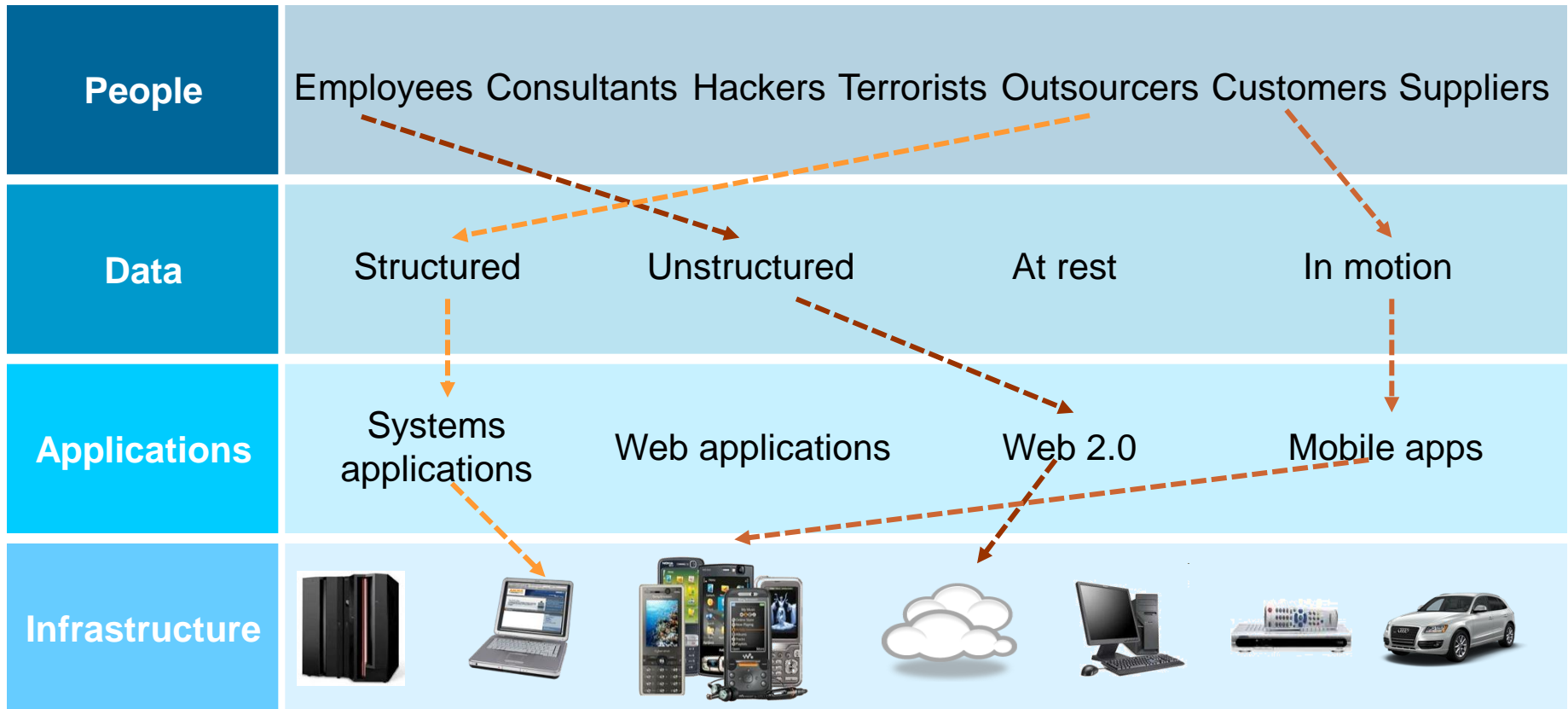
# IT Security is a board room discussion

| Business results | Brand image | Supply chain | Legal exposure | Impact of hacktivism | Audit risk |
|---|---|---|---|---|---|
| Sony estimates potential $1B long term impact – $171M / 100 customers* | HSBC data breach discloses 24K private banking customers | Epsilon breach impacts 100 national brands | TJX estimates $150M class action settlement in release of credit / debit card info | Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony … | Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records |

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

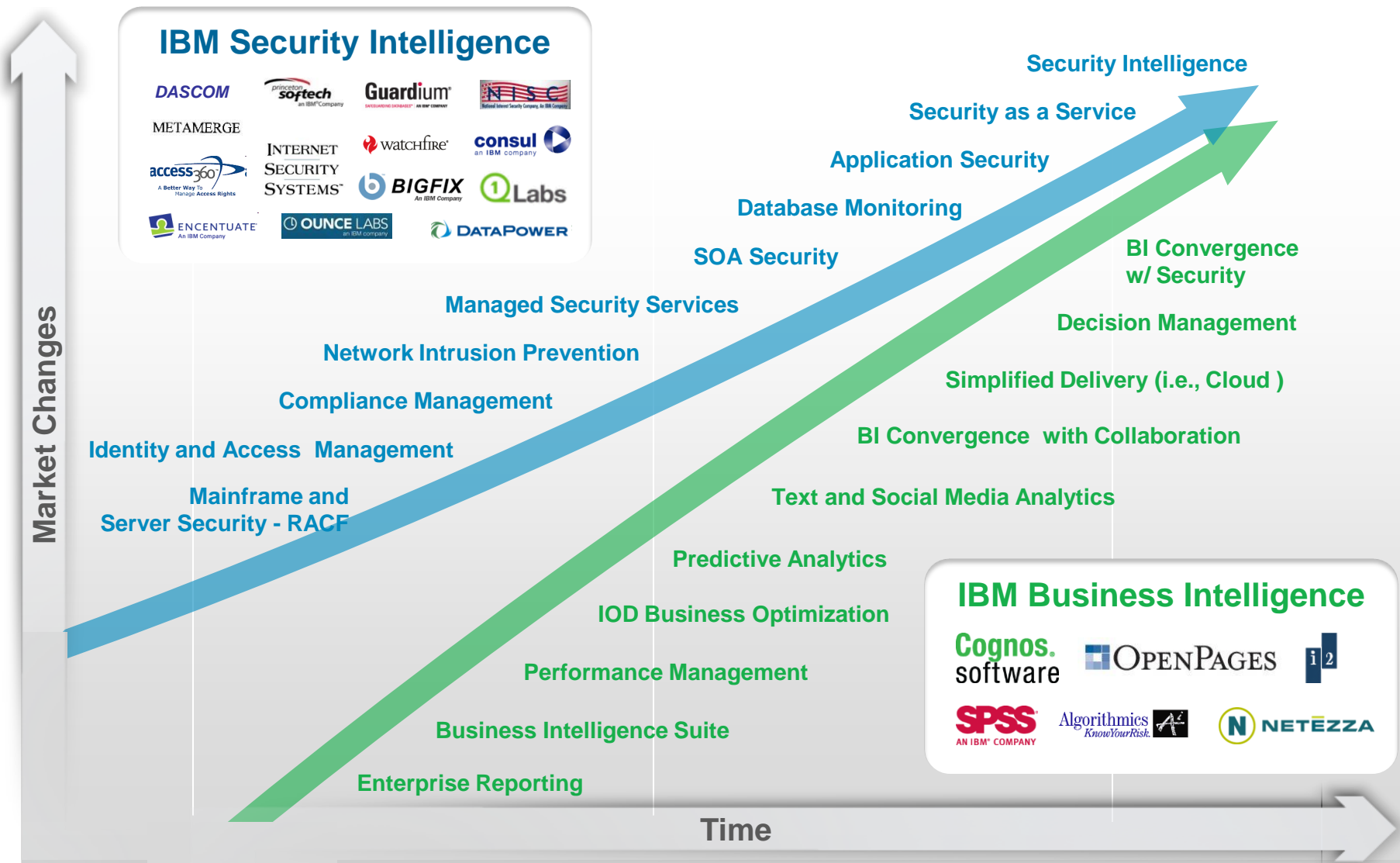| | |
|---|---|
| **People** | Employees Consultants Hackers Terrorists Outsourcers Customers Suppliers |
| **Data** | Structured          Unstructured          At rest          In motion |
| **Applications** | Systems applications          Web applications          Web 2.0          Mobile apps |
| **Infrastructure** |  |

**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*
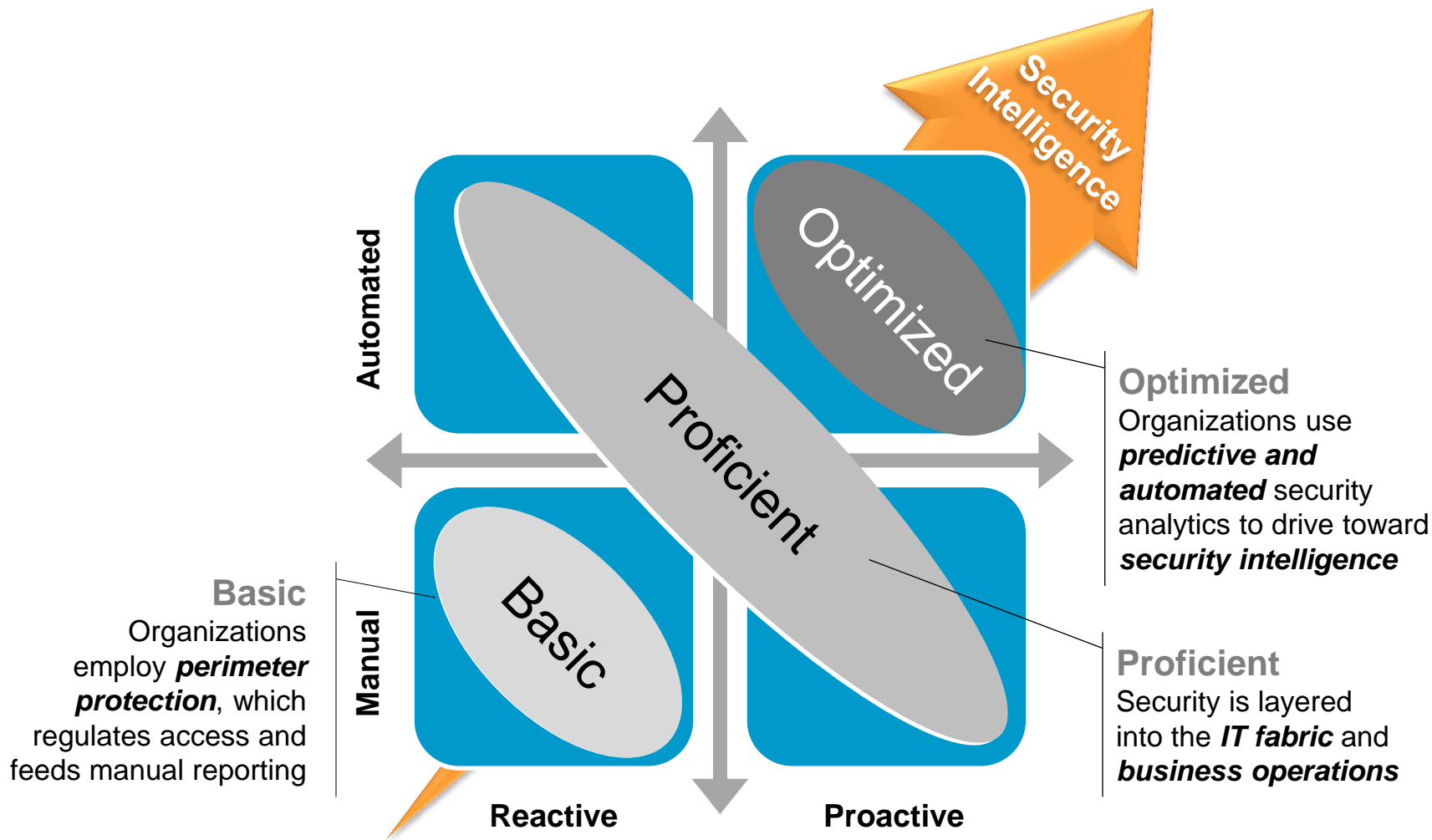
# For IBM, Security and Business Intelligence offer insightful parallels



**IBM Security Intelligence**

DASCOM · princeton softech an IBM Company · **Guardium** SAFEGUARDING DATABASES · AN IBM COMPANY · NISC National Internet Security Company an IBM Company

METAMERGE

access360 A Better Way To Manage Access Rights · INTERNET SECURITY SYSTEMS · watchfire · consul an IBM company

ENCENTUATE An IBM Company · OUNCE LABS an IBM company · BIGFIX An IBM Company · Labs · DATAPOWER

**Market Changes** (vertical axis)

**Time** (horizontal axis)

Blue track (Security Intelligence):
- Mainframe and Server Security - RACF
- Identity and Access Management
- Compliance Management
- Network Intrusion Prevention
- Managed Security Services
- SOA Security
- Database Monitoring
- Application Security
- Security as a Service
- Security Intelligence

Green track (Business Intelligence):
- Enterprise Reporting
- Business Intelligence Suite
- Performance Management
- IOD Business Optimization
- Predictive Analytics
- Text and Social Media Analytics
- BI Convergence with Collaboration
- Simplified Delivery (i.e., Cloud )
- Decision Management
- BI Convergence w/ Security

**IBM Business Intelligence**

Cognos. software · OPENPAGES · i2

SPSS AN IBM COMPANY · Algorithmics KnowYourRisk · NETEZZA

JK 2012-04-26

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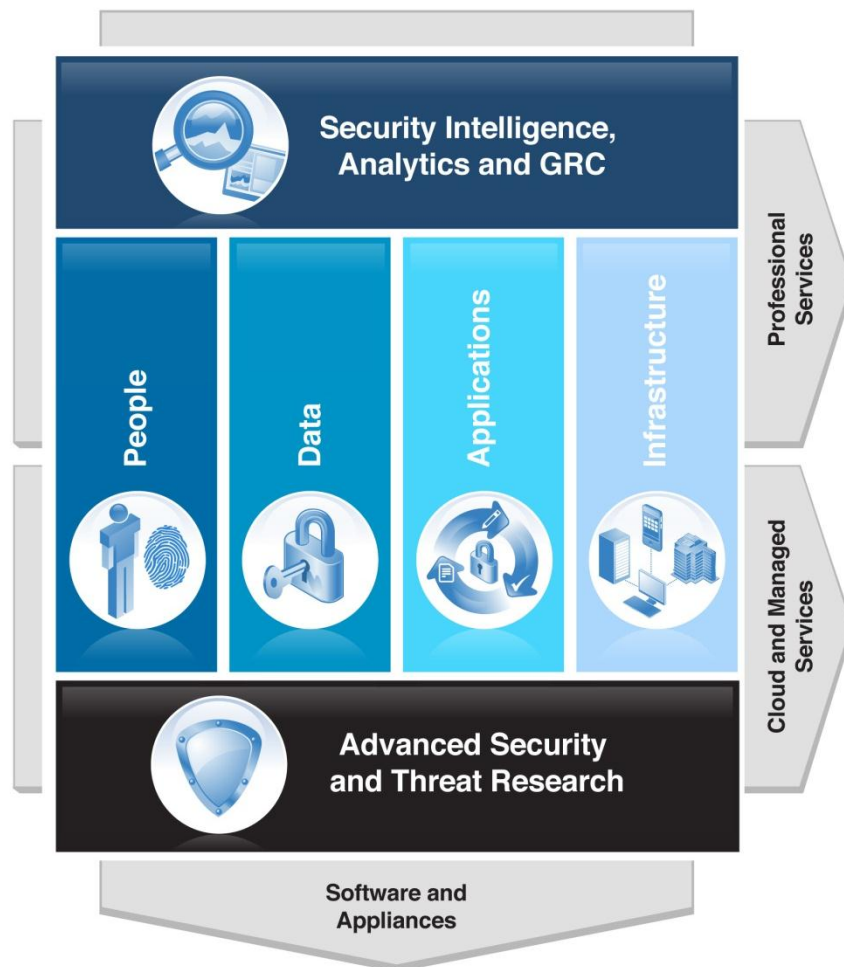
## IBM Security Systems

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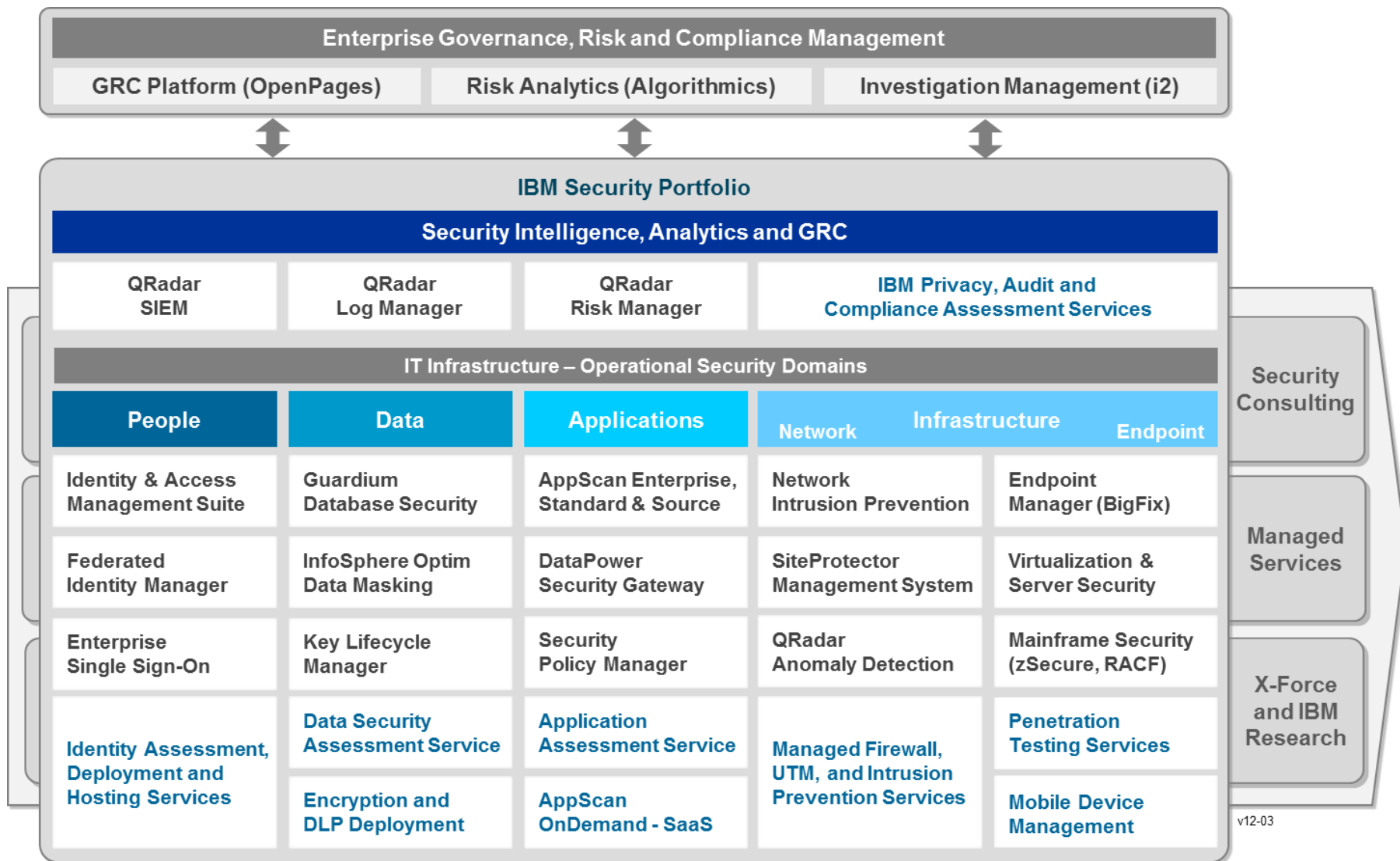- Largest vulnerability database in the industry

**Intelligence** • **Integration** • **Expertise**

**IBM Security Framework**

Security Intelligence, Analytics and GRC

People

Data

Applications

Infrastructure

Advanced Security and Threat Research

Professional Services

Cloud and Managed Services

Software and Appliances

# Intelligence: Leading products and services in every segment



| Enterprise Governance, Risk and Compliance Management | | |
|---|---|---|
| GRC Platform (OpenPages) | Risk Analytics (Algorithmics) | Investigation Management (i2) |

## IBM Security Portfolio

### Security Intelligence, Analytics and GRC

| QRadar SIEM | QRadar Log Manager | QRadar Risk Manager | IBM Privacy, Audit and Compliance Assessment Services |
|---|---|---|---|

### IT Infrastructure – Operational Security Domains

| People | Data | Applications | Infrastructure | |
|---|---|---|---|---|
| | | | **Network** | **Endpoint** |
| Identity & Access Management Suite | Guardium Database Security | AppScan Enterprise, Standard & Source | Network Intrusion Prevention | Endpoint Manager (BigFix) |
| Federated Identity Manager | InfoSphere Optim Data Masking | DataPower Security Gateway | SiteProtector Management System | Virtualization & Server Security |
| Enterprise Single Sign-On | Key Lifecycle Manager | Security Policy Manager | QRadar Anomaly Detection | Mainframe Security (zSecure, RACF) |
| Identity Assessment, Deployment and Hosting Services | Data Security Assessment Service | Application Assessment Service | Managed Firewall, UTM, and Intrusion Prevention Services | Penetration Testing Services |
| | Encryption and DLP Deployment | AppScan OnDemand - SaaS | | Mobile Device Management |

Security Consulting

Managed Services

X-Force and IBM Research

v12-03

Products    Services

# Analysts recognize IBM's superior products and performance

| Domain | Report | Analyst Recognition | | | |
|---|---|---|---|---|---|
| **Security Intelligence, Analytics and GRC** | Security Information & Event Management (SIEM) | 2011 | | | 2010 ⭐ |
| | Enterprise Governance Risk & Compliance Platforms | 2011 | 2011 | | |
| **People** | User Provisioning / Administration | 2011 | | | |
| | Role Management & Access Recertification | | 2011 | | 2010 ⭐ |
| | Enterprise Single Sign-on (ESSO) | 2011* | | | |
| | Web Access Management (WAM) | 2011* | | | |
| **Data** | Database Auditing & Real-Time Protection | | 2011 | | |
| **Applications** | Static Application Security Testing (SAST) | 2010 | | | 2010 ⭐ |
| | Dynamic Application Security Testing (DAST) | 2011 | | | |
| **Infrastructure** (Network / Endpoint) | Network Intrusion Prevention Systems (NIPS) | 2010 | | | 2010 ⭐ |
| | EndPoint Protection Platforms (EPP) | 2010 | | | |

**Gartner**   Challenger   Leader   Visionary   Niche Player

**FORRESTER**   Leader   Strong Performer   Contender

**IDC** Analyze the Future   Leader (#1, 2, or 3 in segment)

\* Gartner MarketScope

# **Integration**: Increasing security, collapsing silos, and reducing complexity

## **Increased Awareness and Accuracy**

- Detect advanced threats with real-time intelligence correlation across security domains
- Increase situational awareness by leveraging real-time feeds of X-Force® Research and global threat intelligence across IBM security products, such as QRadar SIEM and Network Security appliances
- Conduct comprehensive incident investigations with unified identity, database, network and endpoint activity monitoring and log management

## **Ease of Management**

- Simplify risk management and decision-making with automated reporting though a unified console
- Enhance auditing and access capabilities by sharing Identity context across multiple IBM security products
- Build automated, customized application protection policies by feeding AppScan results into IBM Network Intrusion Prevention Systems

## **Reduced Cost and Complexity**

- Deliver fast deployment, increased value and lower TCO by working with a single strategic partner



Think Integrated.

People · Data · Applications · Network · Endpoint · Security Intelligence
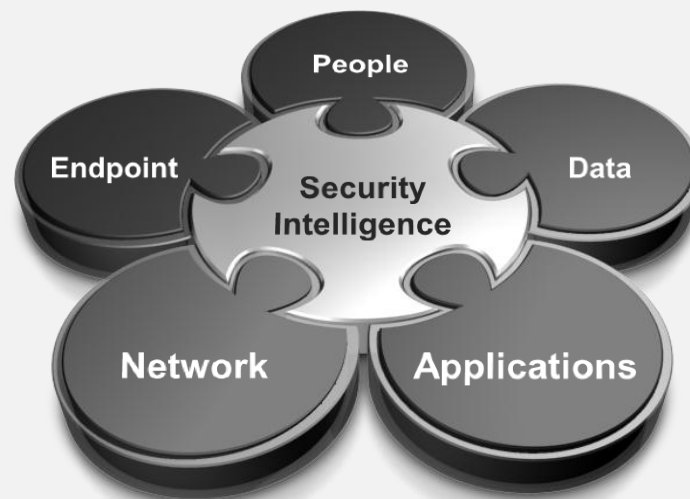
# **Expertise**: Unmatched global coverage and security awareness



**Security Operations Centers**
**Security Research Centers**
**Security Solution Development Centers**
**Institute for Advanced Security Branches**

Map locations: Zurich, CH; Waltham, US; Fredericton, CA; Delft, NL; Belfast, N IR; Ottawa, CA; Toronto, CA; Brussels, BE; IAS Europe; Herzliya, IL; Almaden, US; Boulder, US; TJ Watson, US; Tokyo, JP; Tokyo, JP; Costa Mesa, US; IAS Americas; Detroit, US; Bangalore, IN; Austin, US; Raleigh, US; Haifa, IL; Atlanta, US; Atlanta, US; Atlanta, US; Pune, IN; Taipei, TW; Bangalore, IN; Singapore, SG; Brisbane, AU; New Delhi, IN; Gold Coast, AU; Hortolândia, BR; Perth, AU; IAS Asia Pacific

## IBM Research

**IBM Institute for Advanced Security**
Enabling cybersecurity innovation and collaboration

**10B** analyzed Web pages & images
**150M** intrusion attempts daily
**40M** spam & phishing attacks
**46K** documented vulnerabilities
Millions of unique malware samples

F O R C E

### **World Wide Managed Security Services Coverage**

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

# How is IBM solving complex security challenges?

# Data Explosion
## IBM is integrating across IT silos with Security Intelligence solutions



| Network Activity |
| Virtual Activity |
| Config/Change Info |
| Application Activity |
| Servers & Hosts |
| Security Systems |
| User Activity |

Category

Credibility

Severity

Asset Discovery

Active Vulnerability Assessment

Passive Vulnerability Assessment

Statistical

Correlation

Rules Corelation

Attacker Profile

IP Location

Geo Location

User Logs

Network User

Application

Behavior

Activity Context

**Offense ›**

SUSPECTED INCIDENTS

Sources **+** Intelligence **=** Most Accurate & Actionable Insight

# Solving complex problems that point solutions cannot

| | **Improving threat detection** | Discovered 500 hosts with "Here You Have" virus, which all other security products missed |
|---|---|---|
| | **Consolidating data silos** | 2 billion log and events per day reduced to 25 high priority offenses |
| | **Predicting risks against your business** | Automating the policy monitoring and evaluation process for configuration changes in the infrastructure |
| | **Addressing regulatory mandates** | Real-time monitoring of all network activity, in addition to PCI mandates |

# 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
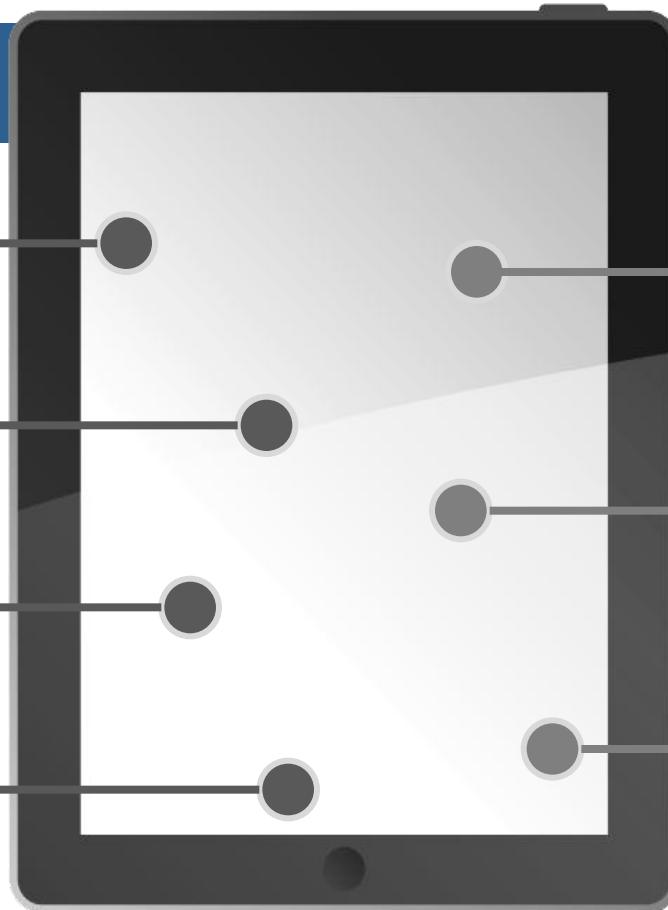
**IBM Mobile Security Services**

**Lifecycle Management** Mobile Enterprise Services (MES)

**Endpoint Management** Hosted Mobile Device Security Management

**Secure Connectivity** Secure Enterprise Smartphone and Tablets

# Allowing organizations to innovate with confidence

**Significantly Reducing Costs**

Saved on deployment time (400K users in <6 months) and management costs while helping to achieve compliance with IBM's end user device IT security policies (95% of patches applied within 24 hours)

**Time-to-Value & Performance Improvements**

Deployed Tivoli Endpoint Manager to 1K endpoints in days, reduced the software update and patching process from 20 to 1 person, remediation time from weeks to hours, and call volumes from 100 to less than 20 calls per day

**Ecosystem Value Creation**

Combining power, patch and lifecycle management along with security and compliance, Fiberlink was able to grow its cloud-based, mobile device management business by 25% annually over the last 5 years

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



| Identity Federation | Web Application Scanning | Virtualization Security | Network Security | Image & Patch Management | Database Monitoring |
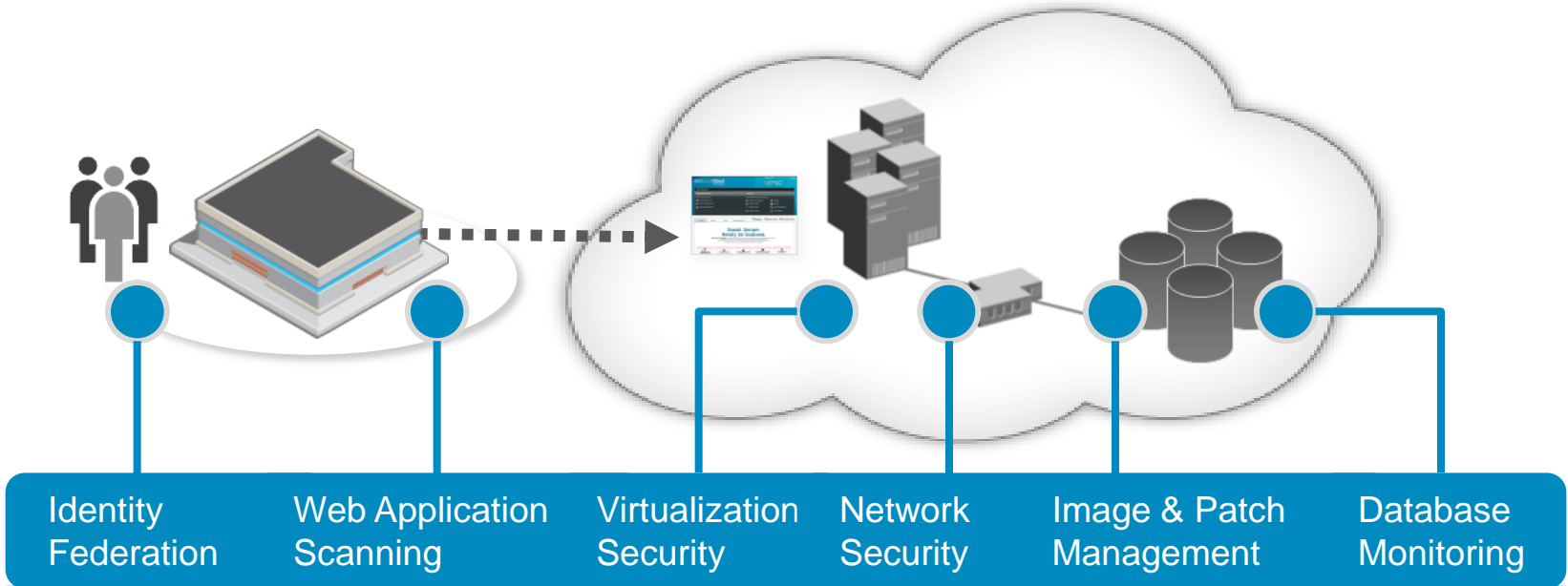
**IBM Security Intelligence**

# Enabling security for new business models and delivery methods

| | | |
|---|---|---|
| **European Energy Company** | **Worldwide access to SaaS applications** | Enabled security for access to public SaaS applications – including Google Apps and Salesforce.com – using cloud-enabled federation |
| bluelock | **Best-in-class security for a cloud provider** | Integrated security in a multi-tenant Infrastructure-as-a-Service environment using flexible, virtualized security managed from the cloud |
| MOLSON Coors | **Rapid Identity solution deployment** | Delivered identity and access management capabilities quickly and easily using a SaaS-deployed Tivoli solution |

# Attack Sophistication

*IBM is helping clients combat advanced threats with pre- and post-exploit intelligence and action*

| | | | |
|---|---|---|---|
| **What are the external and internal threats?** | **Are we configured to protect against these threats?** | **What is happening right now?** | **What was the impact?** |

Vulnerability    PREDICTION / PREVENTION PHASE    Exploit    REACTION / REMEDIATION PHASE    Remediation
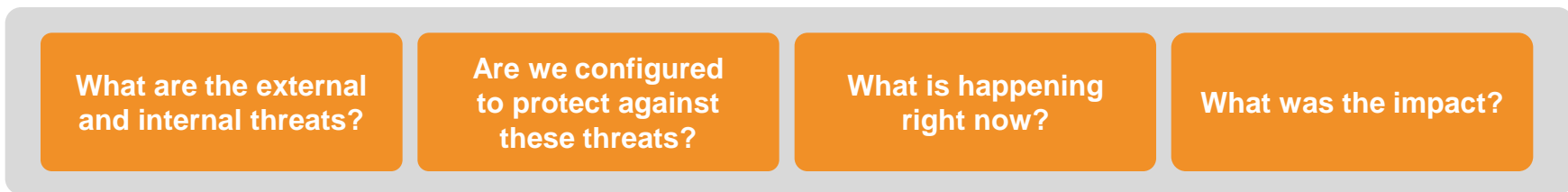
**Pre-Exploit**      **Post-Exploit**

**Prediction & Prevention**

Risk Management. Vulnerability Management.
Configuration and Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

**Reaction & Remediation**

Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Leak Prevention.
SIEM. Log Management. Incident Response.

**IBM Security Intelligence**

# Identifying and protecting against sophisticated attacks

| | Gruppo Intergea | **Securing across the enterprise ecosystem** | Deployed solutions to identify threats and vulnerabilities with protection across the entire infrastructure – from network to desktops in the customers' showrooms and remote offices |
| --- | --- | --- | --- |
| | **Luxury Brand Retailer** | **Detecting insider fraud** | Cross-correlated identity, access, and application data to identify trusted insider stealing and destroying key data |
| | HUDSON'S BAY CO. | **End-to-end monitoring and managed protection services** | Outsourced security management for critical credit card holding systems (318 network devices and servers), security-event log monitoring and reporting through a SaaS-based customer portal to detect and prevent attacks |

# Security Intelligence is enabling progress to optimized security

**Security Intelligence**

| | | **Security Intelligence:** Information and event management / Advanced correlation and deep analytics / External threat research | | |
|---|---|---|---|---|
| **Optimized** | Role based analytics / Identity governance / Privileged user controls | Data flow analytics / Data governance | Secure app engineering processes / Fraud detection | Advanced network monitoring / Forensics / data mining / Secure systems |
| **Proficient** | User provisioning / Access mgmt / Strong authentication | Access monitoring / Data loss prevention | Application firewall / Source code scanning | Virtualization security / Asset mgmt / Endpoint / network security management |
| **Basic** | Centralized directory | Encryption / Access control | Application scanning | Perimeter security / Anti-virus |
| | **People** | **Data** | **Applications** | **Infrastructure** |

# Intelligent solutions provide the DNA to secure a Smarter Planet

**Security Intelligence, Analytics & GRC**

**People**

**Data**

**Applications**

**Infrastructure**
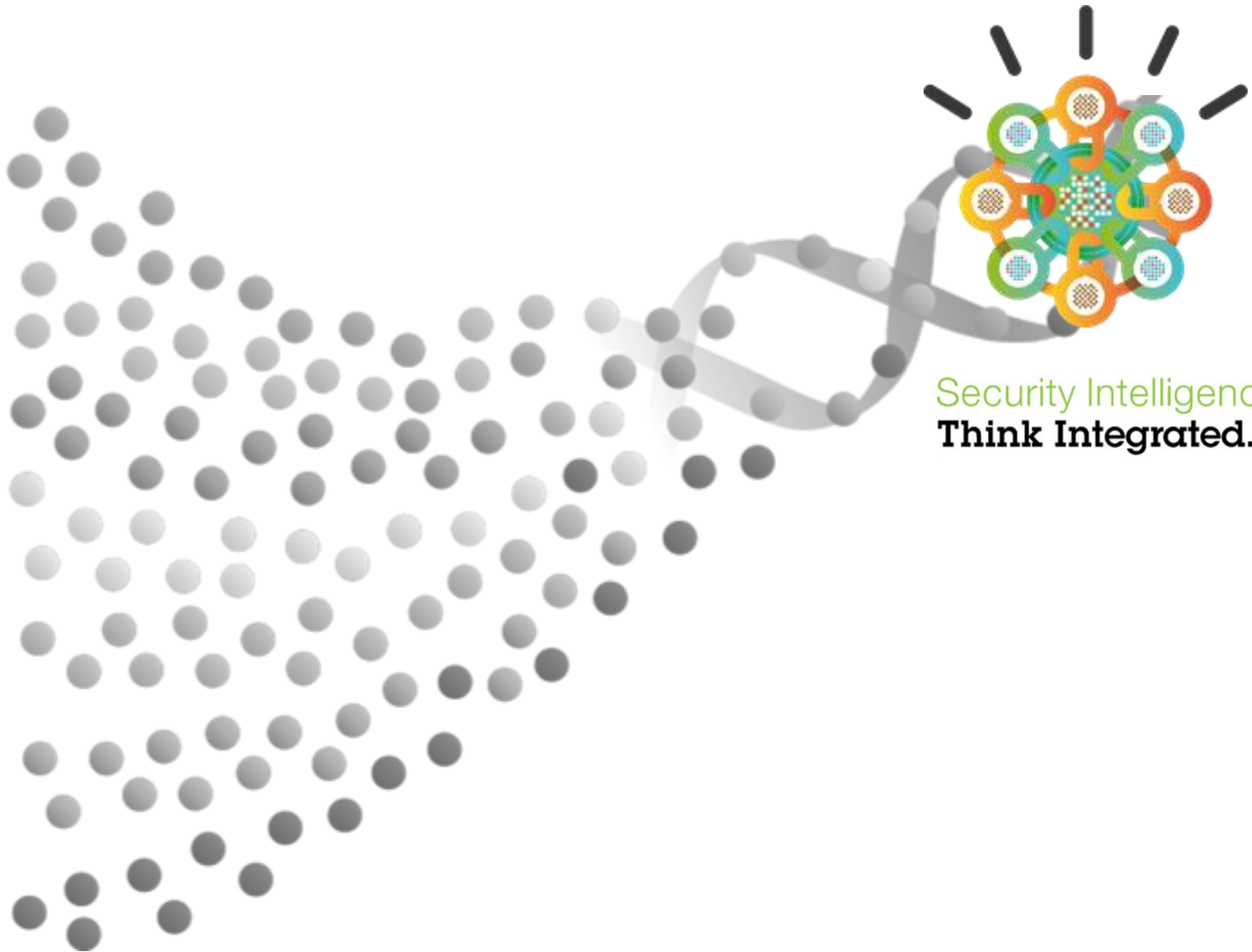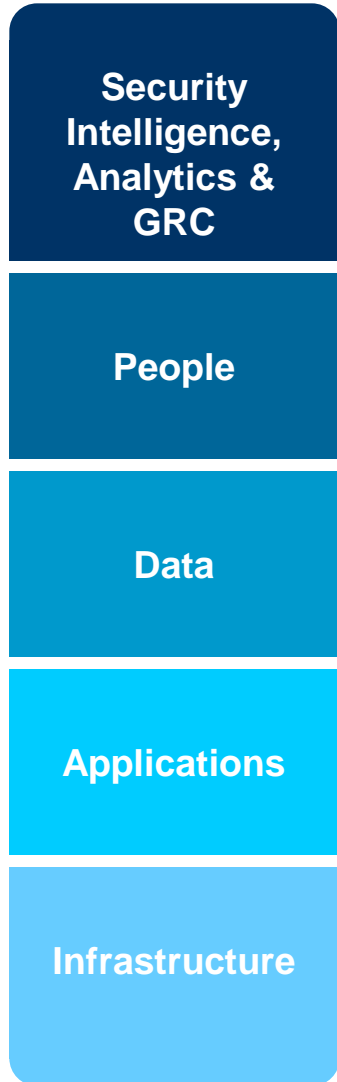


Security Intelligence.
**Think Integrated.**

ibm.com/security