

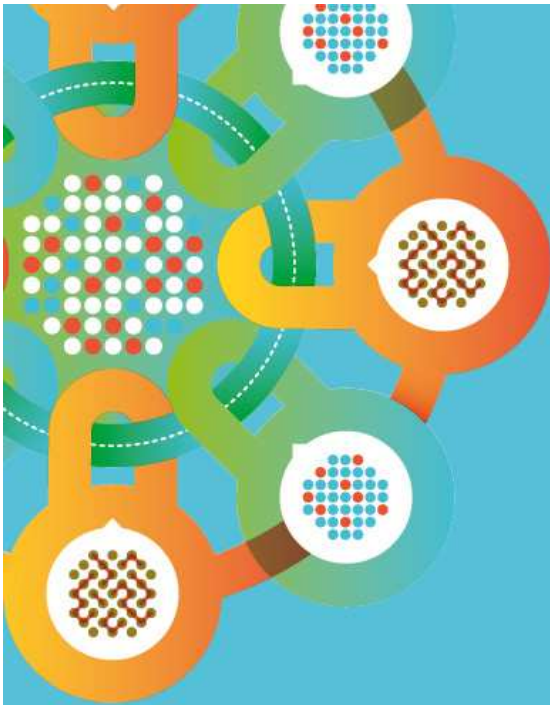
IBM Forum Segrate - Milano



18 settembre: Missione Sicurezza

Identifica e combatti i rischi con la Security Intelligence IBM

Tom Turner, VP Marketing
IBM Security Strategy and
Security Intelligence



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

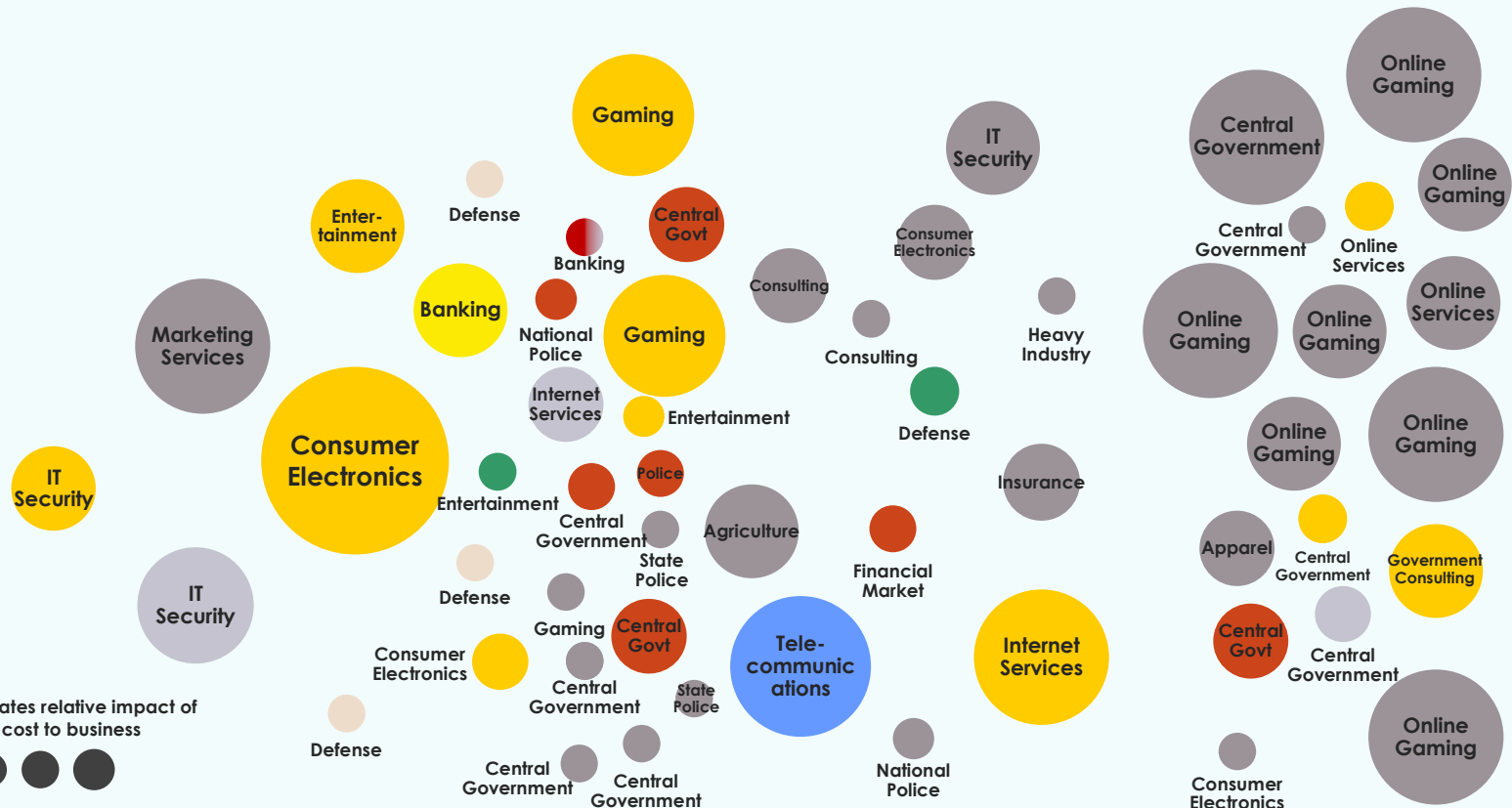
Attack Type

SQL Injection
URL Tampering
Spear Phishing
3rd Party Software
DDoS
SecureID
Trojan Software
Unknown

Size of circle estimates relative impact of breach in terms of cost to business

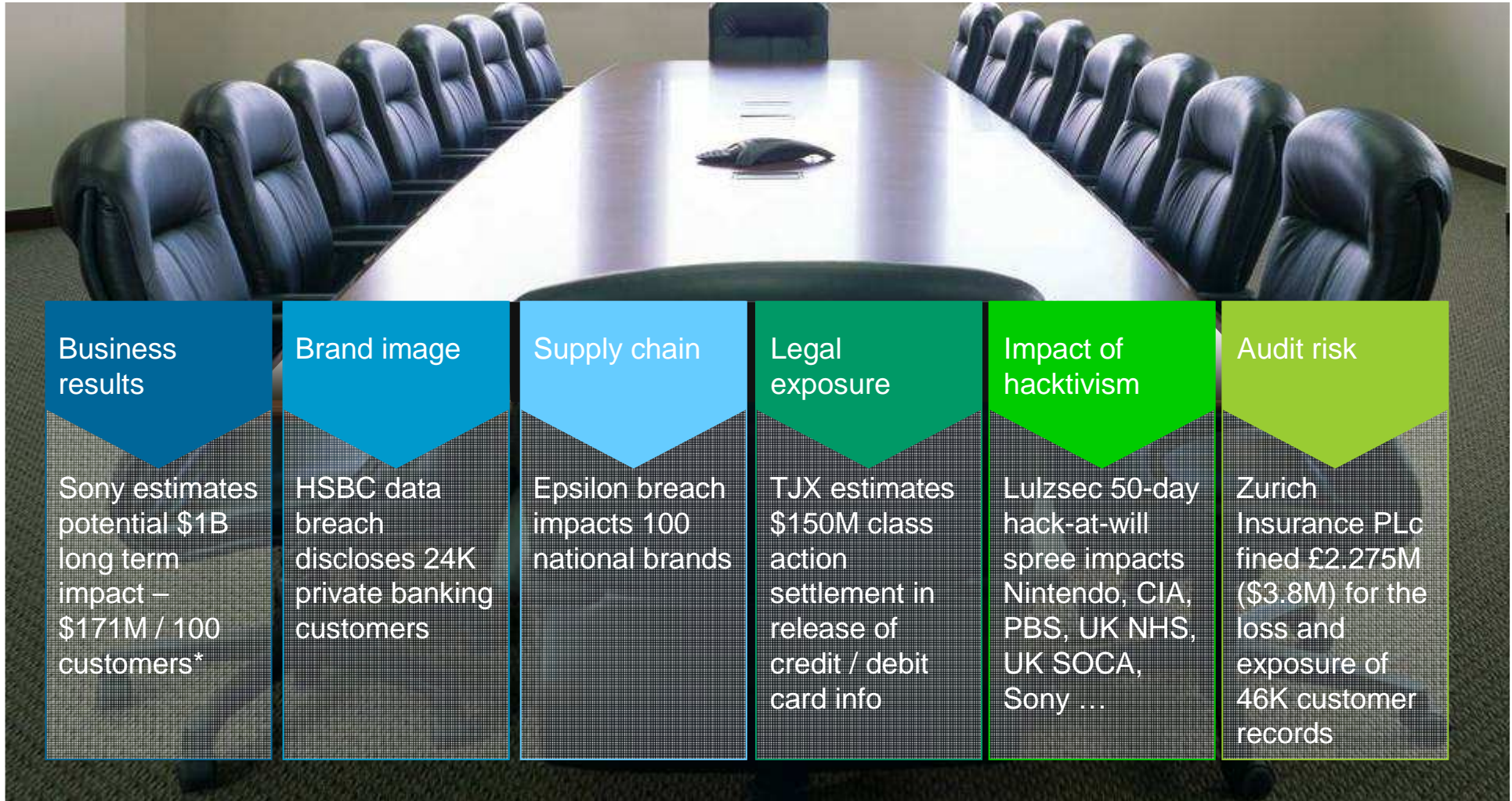


Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec



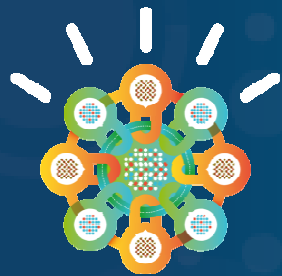
Source: IBM X-Force® Research 2011 Trend and Risk Report

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

*Sources for all breaches shown in speaker notes



What is IBM doing about it?



IBM is investing in security

IBM Security

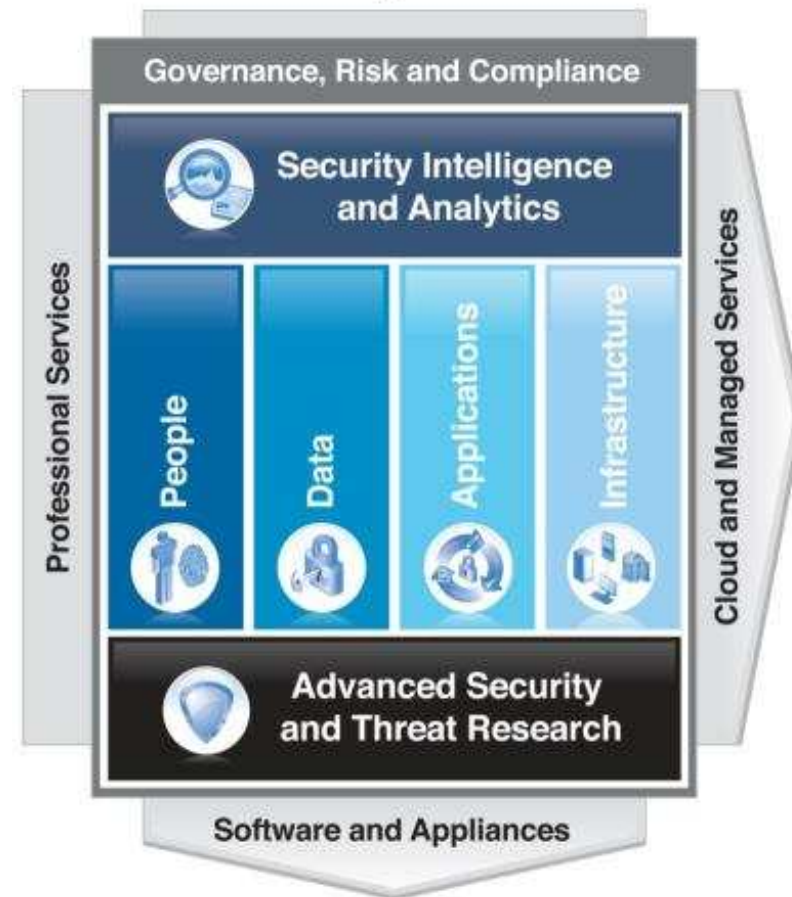


IBM Security Intelligence



- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Large vulnerability database

IBM Security Framework

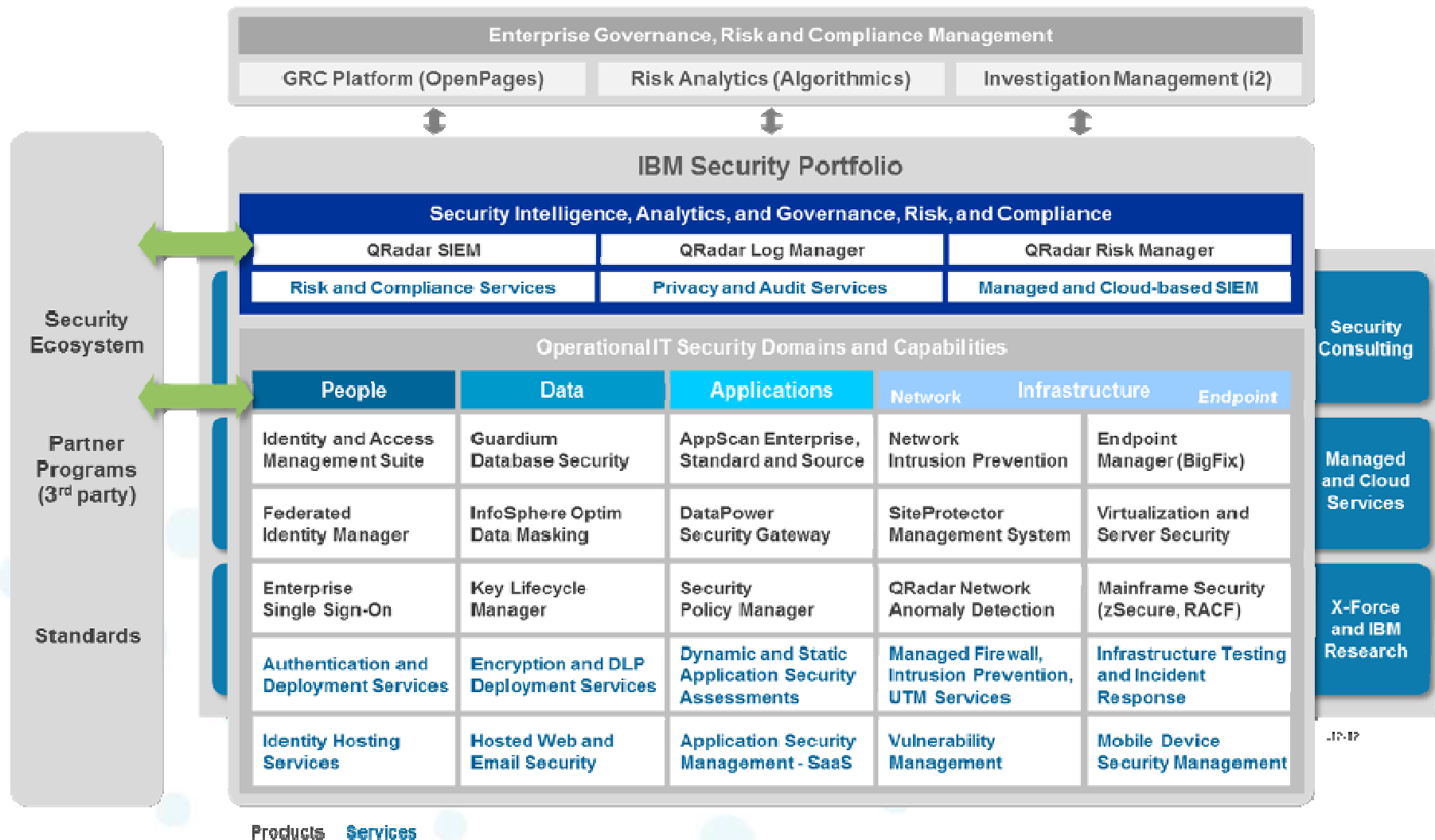


Intelligence

Integration

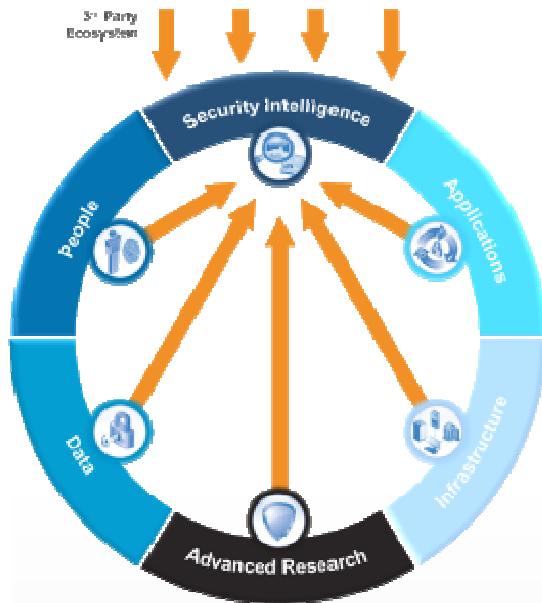
Expertise

Intelligence: A comprehensive portfolio of products and services across all domains



Integration: Help increase security, collapse silos, and reduce complexity

Integrated Intelligence.



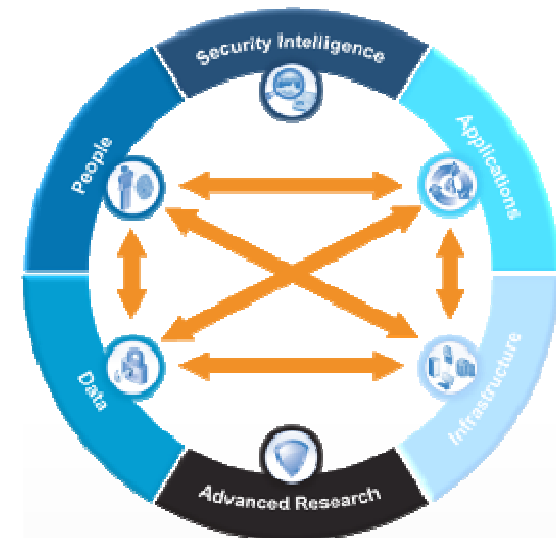
- Consolidate and correlate siloed information from hundreds of sources
- Designed to help detect, notify and respond to threats missed by other security solutions
- Automate compliance tasks and assess risks

Integrated Research.



- Stay ahead of the changing threat landscape
- Designed to help 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

Expertise: Global coverage and security awareness



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



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)

IBM Security Strategy

Buyers



CISO – CIO – Line-of-Business

Megatrends

Advanced Threats



Cloud



Mobile



Regulation and Compliance



Capabilities



Security Intelligence



People



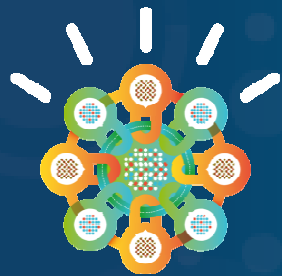
Data



Applications



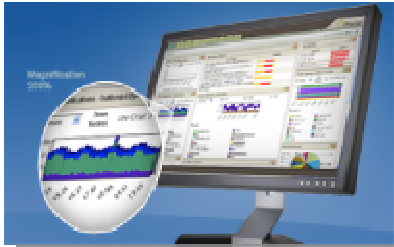
Infrastructure



How is IBM helping solve complex security challenges?

How do we help with today's security mega-trends?

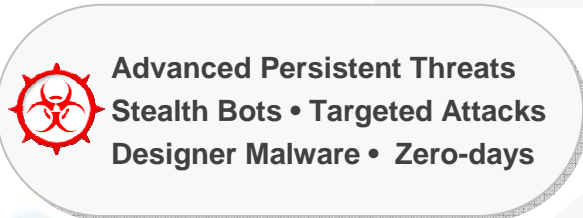
1 Security Intelligence



2 Cloud Computing



3 Advanced Threats



4 Mobile Computing



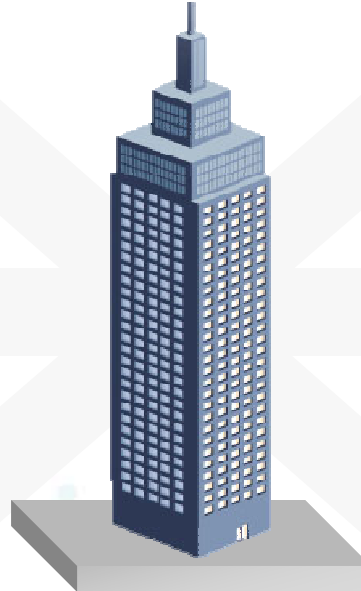
5 Identity



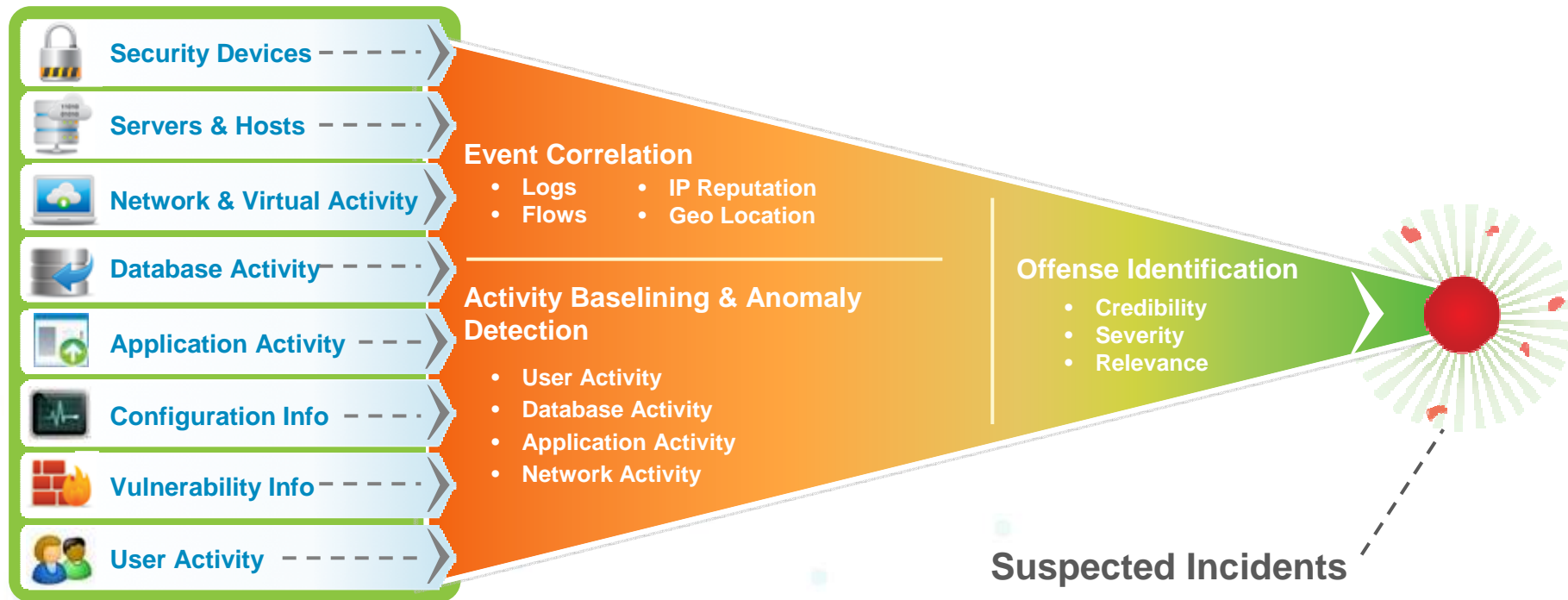
6 Regulation/Compliance



Enterprise Customers



1 **Security Intelligence: Integrating across IT silos with Security Intelligence solutions**



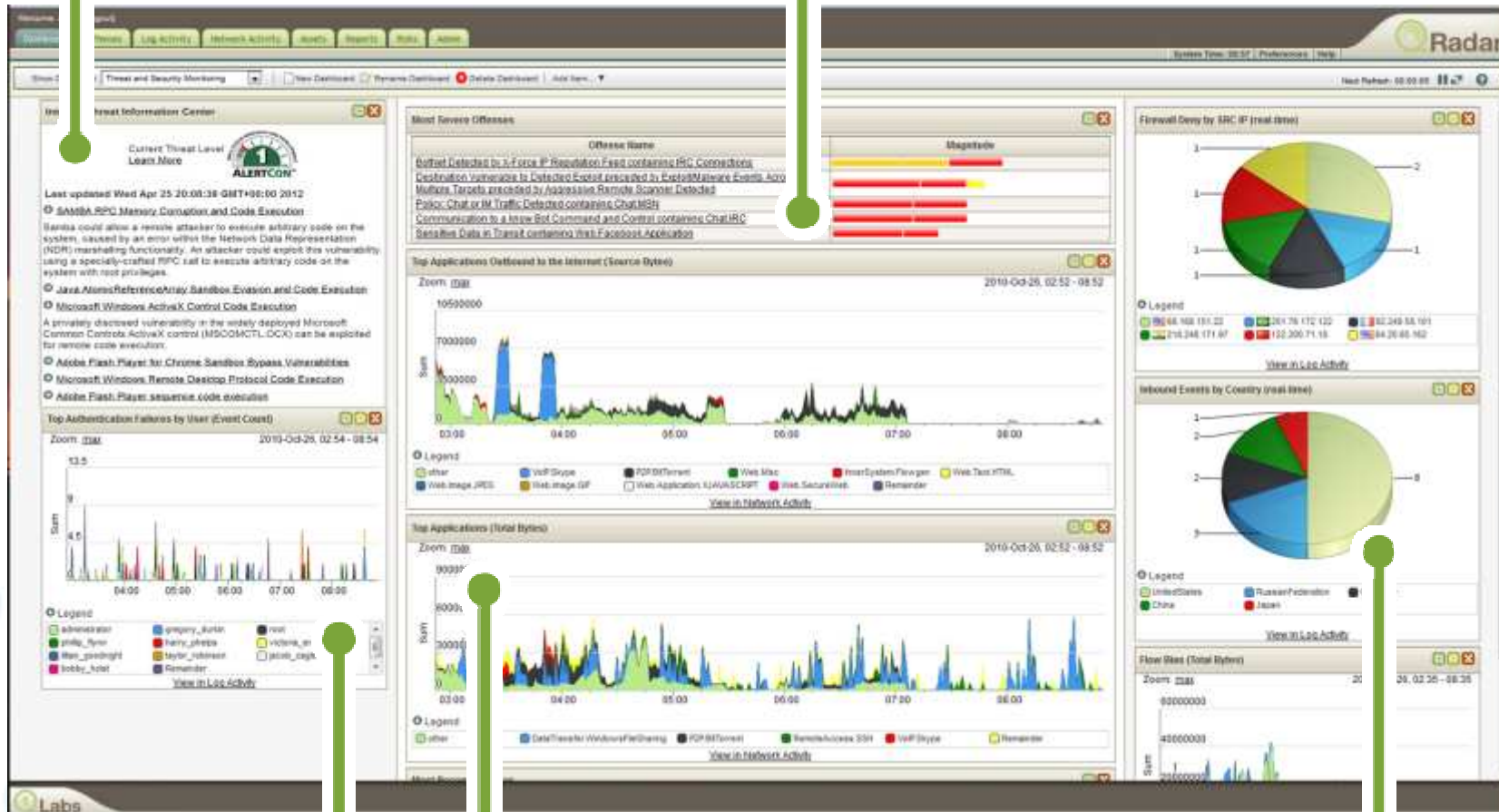
Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight



Security Intelligence: QRadar provides security visibility

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

Enterprise SIEM - SOC and Cloud Services Monitoring

Customer Facts

- One of the largest software companies in the world
- 110,000 employees
- OnDemand environment currently services 4.5 million customers including the Department of Defense and the IRS

- Customer since 2006
- 15,000 + devices monitored
 - 7150 Linux servers
 - 120+ Netscreen Firewalls
 - Strategic integration with McAfee ePO
 - Others: Oracle DB, Intrushield, Symark, IOS, Array, Tripwire, Apache
- Threat management use cases:
 - Internal IT & SOC (5 operators)
 - QFlow analysis for deep forensics
 - OnDemand Cloud Services environment
 - Custom application monitoring
 - 1M to 1 data reduction factor witnessed in the SOC
 - 30-50 Qradar offenses reviewed daily
- Compliance use cases:
 - Monitoring, reporting and logging that helps to sustain the following compliance requirements
 - ISO 27002, SAS 70, HIPPA, PCI DSS (level 1), NIST, 21 CFR 11 (life sciences)
 - Internal compliance and compliance for customers of the OnDemand environment



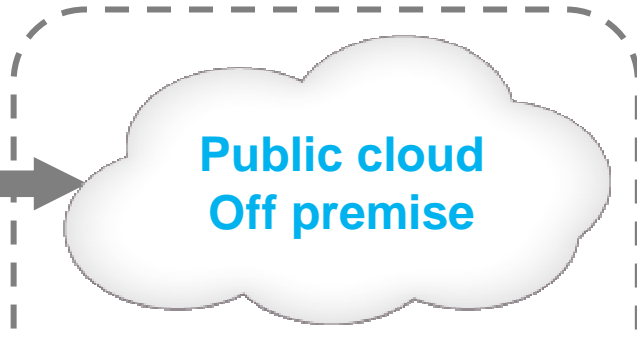
2 Cloud: Our focus is in two areas of cloud security

1 Security from the Cloud

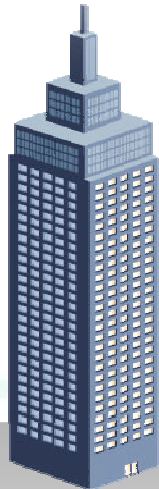


Use cloud to deliver security as-a-Service - focusing on services such as vulnerability scanning, web and email security, etc.

2 Security for the Cloud



Secure usage of Public Cloud applications – focusing on Audit, Access and Secure Connectivity



Securing the Private Cloud stack – focusing on building security into the cloud infrastructure and its workloads



2


Cloud: Leverage solutions in each area of cloud risk



IBM Identity and Access Management Suite
Identity integration, provision users to SaaS applications
Desktop single sign on supporting desktop virtualization



IBM QRadar Security Intelligence
Total visibility into virtual and cloud environments



IBM AppScan Suite
Scan cloud deployed web services and applications for vulnerabilities



Securing Cloud with IBM Security Systems


Security Intelligence • People • Data • Apps • Infrastructure



IBM InfoSphere Guardium Suite
Protect and monitor access to shared databases



IBM Network IPS
Protect and monitor access to shared databases



IBM Endpoint Manager
Patch and configuration management of VMs

IBM Virtual Server Protection for VMware
Protect VMs from advanced threats

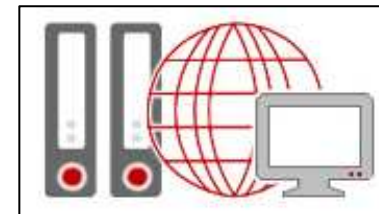
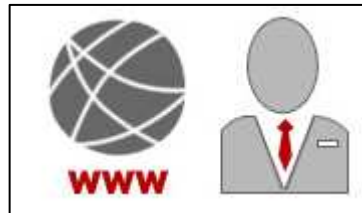


Securing Privileged Identities: An international telecommunications company increases privileged user security and mitigates insider threat

A growing international telecommunications firm plans to manage

250

privileged users
by end of 2012



Business challenge:

- Ensure privileged user accesses maintain the compliance posture required by regulatory bodies
- Automate manual lifecycle management of privileged IDs
- Insecure spreadsheet used for tracking privileged IDs inherently not secure

Solution: IBM Security Privileged Identity Manager

- Increased security by restricting visibility of sensitive login credentials to users
- Provided a central auditable control point of privileged IDs
- Reduced Help Desk costs with single sign-on and automated password resets

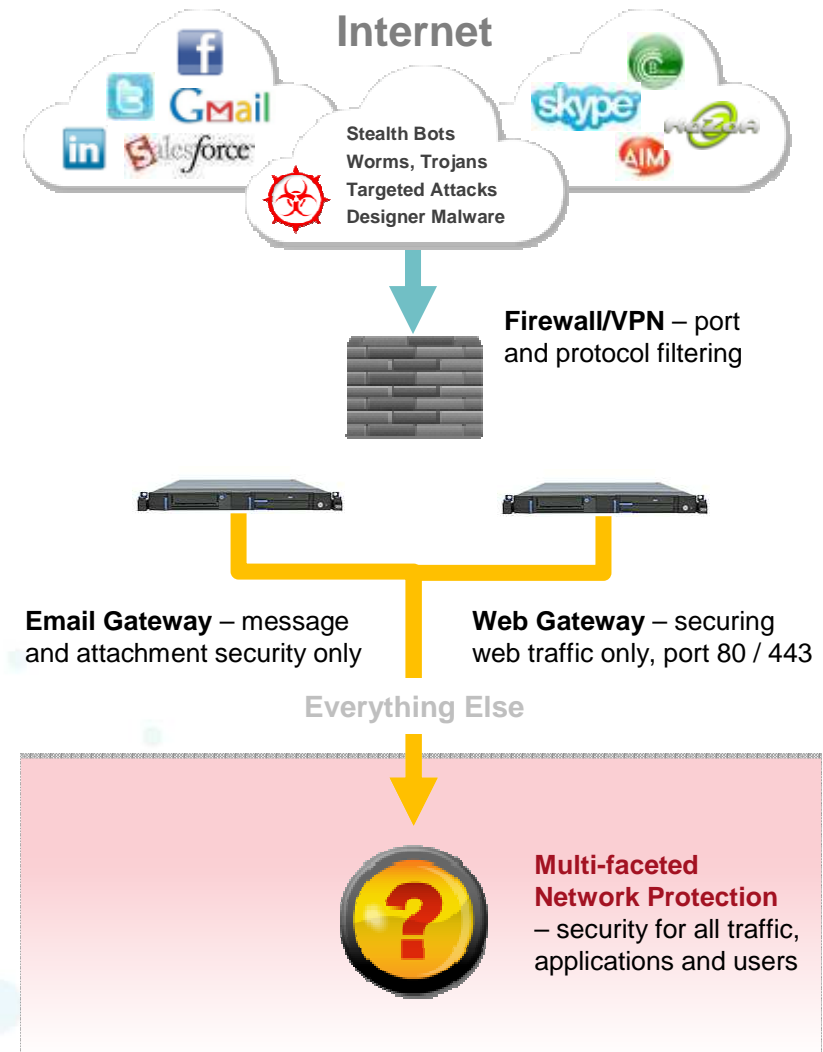
3 Advanced Threat: *Perimeter solutions not up to today's challenges*

Current Limitations

- Threats continue to evolve and standard methods of detection are not enough
- Streaming media sites and Web applications introduce new security challenges
- Basic "Block Only" mode limits innovative use of streaming and new Web apps
- Poorly integrated solutions create "security sprawl", lower overall levels of security, and raise cost and complexity

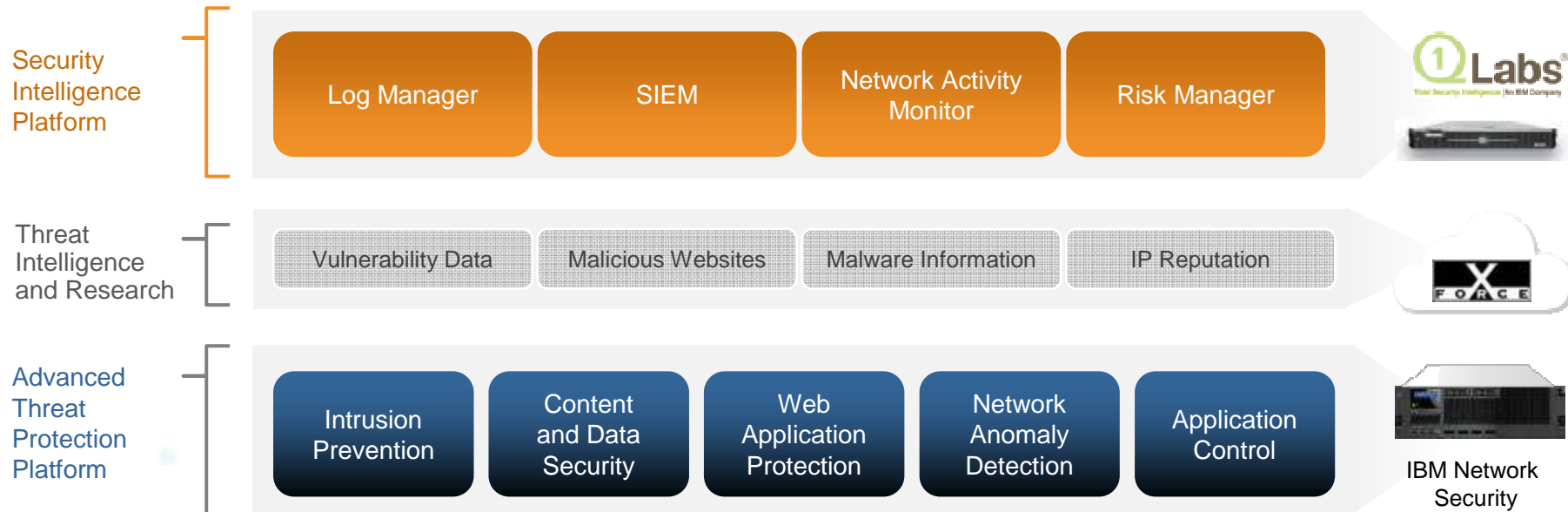
Requirement: Multi-faceted Protection

- 0-day threat protection tightly integrated with other technologies i.e. network anomaly detection
- Ability to reduce costs associated with non-business use of applications
- Controls to restrict access to social media sites by a user's role and business need
- Augment point solutions to reduce overall cost and complexity





3 Advanced Threats: *IBM's vision for Threat*



Advanced Threat Protection Platform

Help prevent sophisticated threats and detect abnormal network behavior by leveraging an extensible set of network security capabilities - in conjunction with real-time threat information, Security Intelligence, and granular application control

Expanded X-Force Threat Intelligence

Increased coverage of world-wide threat intelligence harvested by X-Force® and the consumption of this data to make smarter and more accurate security decisions across the IBM portfolio

Security Intelligence Integration

Tight integration between the Advanced Threat Protection Platform and QRadar Security Intelligence platform to provide unique and meaningful ways to help detect, investigate and remediate threats

Independent Validation for Threat Protection Vision

InformationWeek
:: reports

Reports.InformationWeek.com August 2012 \$99

IT Pro Ranking: IPS and IDS

IBM/ISS leads our vendor evaluation survey of network IPS/IDS vendors, earning an overall performance rating of **75%**. Cisco Systems and Check Point Software Technologies are just behind at **74%**. IT pros also evaluated HP, Intel, Juniper Networks and Snort. When it comes to IPD/IDS features, IBM topped the competition for attack blocking and centralized management—two categories where open source stalwart Snort fared the worst.

By Allen Glines

Report ID: RS190812

InformationWeek
:: reports

Reports.InformationWeek.com June 2012 \$99

IT Pro Ranking: SIEM

IBM's Q1 Labs leads our vendor evaluation survey of SIEM vendors, earning an overall performance rating of **76%**. Novell's SIEM (now owned by NetIQ) is a close second at **75%**. Other vendors evaluated by IT pros include HP/ArcSight, NetIQ, Quest Software, Splunk, Symantec and Tripwire. **58%** of respondents are satisfied or very satisfied with their SIEM products, but complexity tops IT's challenges with SIEM technology.

By Dean Francis

Report ID: RS030612

IBM Tops InformationWeek Customer Performance Surveys for IPS/IDS and SIEM

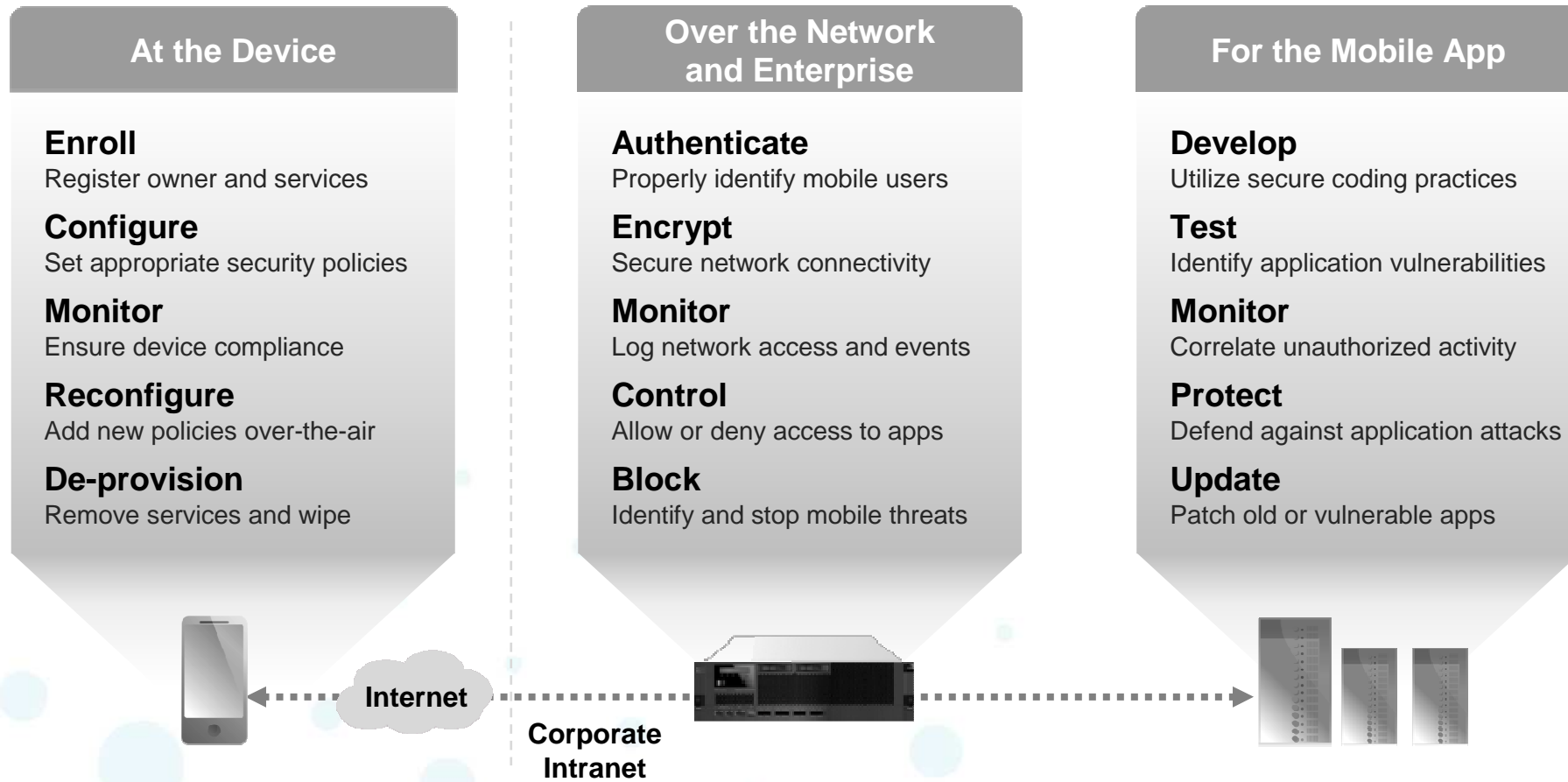
3 **NextGen IPS: Introducing IBM Security Network Protection XGS 5000**



IBM Security Network Protection XGS 5000
builds on the proven security of IBM intrusion prevention solutions by delivering the addition of next generation *visibility* and *control* to help balance security and business requirements



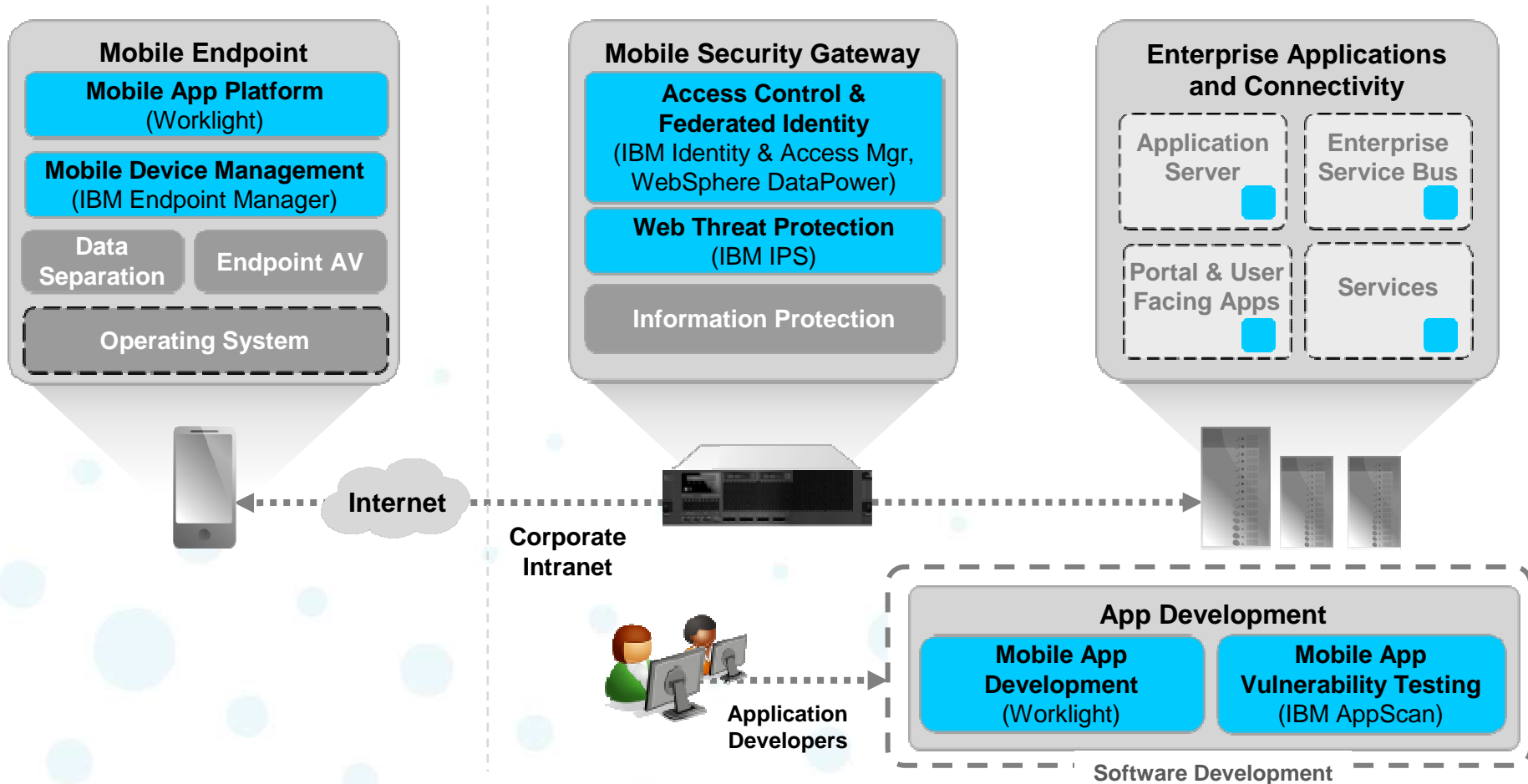
Mobility: Thinking through mobile security



IBM Mobile Security Strategy

- Safe usage of smartphones and tablets in the enterprise
- Secure access to corporate data and supporting privacy
- Visibility and security of enterprise mobile platform

4 **Mobility: IBM's mobility capabilities today**





Mobile Security In Action

European Bank to Deliver Secure Mobile Internet Banking



AimArs needed to reduce operational complexity and cost with a single, scalable infrastructure to secure access to various back-end services from multiple mobile apps.

A customized authentication mechanism empowered the bank to guarantee the security of its customers while safeguarding the trust relationship with a safe app platform that encrypts local data and delivers app updates immediately.

Customer Needs

- Extend secure access to banking apps to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices
- Support for iOS, Android, and Windows Mobile

Key Features & Outcomes

- Authenticates requests made via HTTPS from hybrid mobile apps running on WorkLight platform to back-end services
- A custom certificates-based authentication mechanism implemented to secure back-end banking application

Adding Mobile Devices Without Adding Infrastructure



Serving 4.5 million customers in the southwestern region of the United States, this electric company of 25,000 employees is a leader in clean energy while exceeding reliability standards and keeping consumer costs below average. They are experiencing a migration from traditional endpoints to mobile devices.

Customer Needs

- Support 20,000+ mobile devices
- Corporate and employee-owned, many platforms and OS versions
- High availability for certain devices used in the field
- Adherence to Internal security policies, external regulations

Key Features & Outcomes

- Scalability to 250,000 endpoints provides room to grow
- Added mobile devices to existing IEM deployment in days
- Ability to integrate with Maximo, Remedy
- Responsiveness and agility of product and product team



Identity: IBM's IAM governance strategy and vision



Integration with Threat and Security Intelligence

Expansion of IAM vertically through governance, analytics and reporting; Horizontal integration with additional security products and technologies

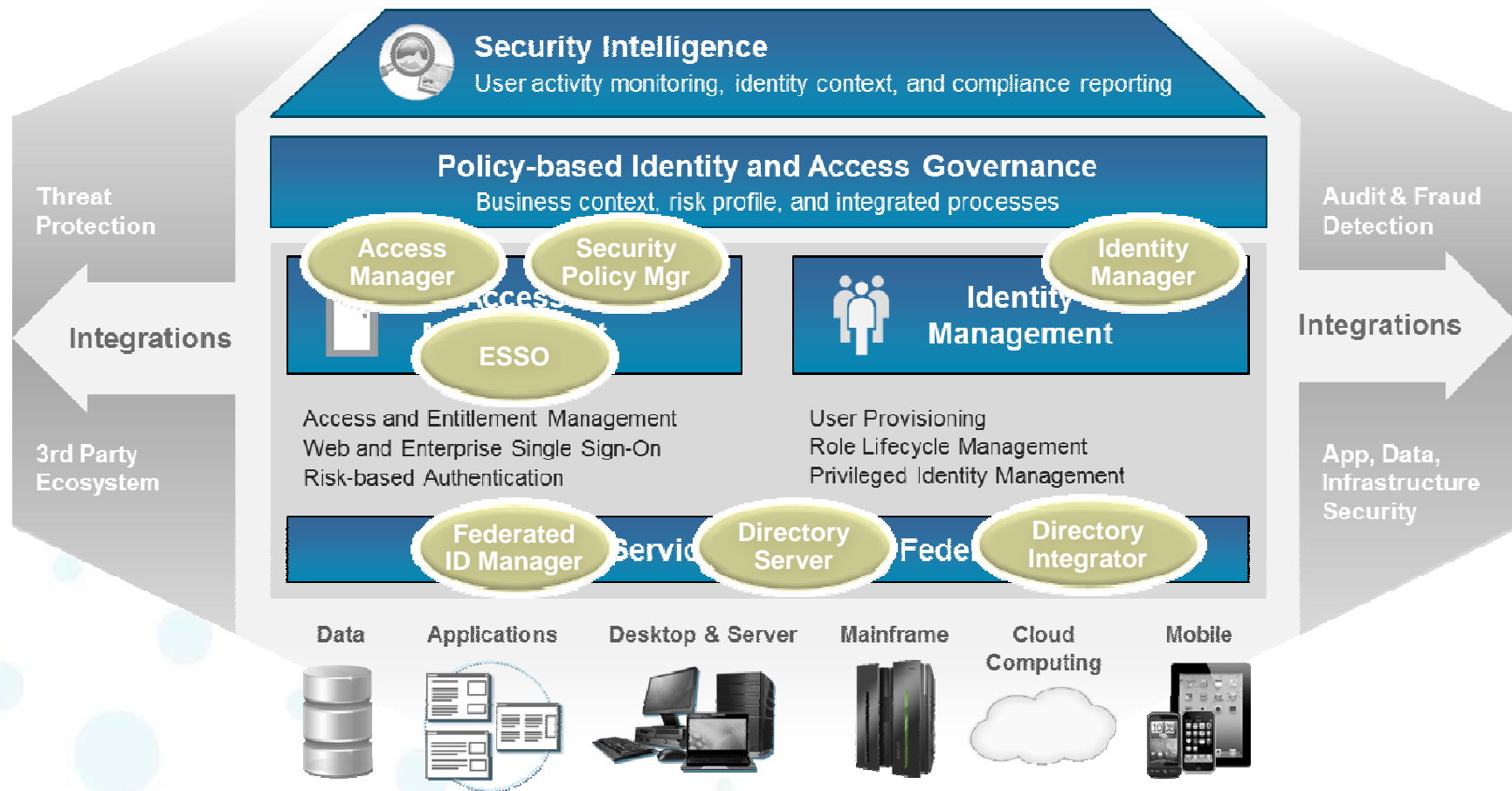
Enhanced Identity Assurance

Improved built-in risk-based access control for cloud, mobile and SaaS access, as well as integration with proofing and validation solutions

Insider Threat and IAM Governance

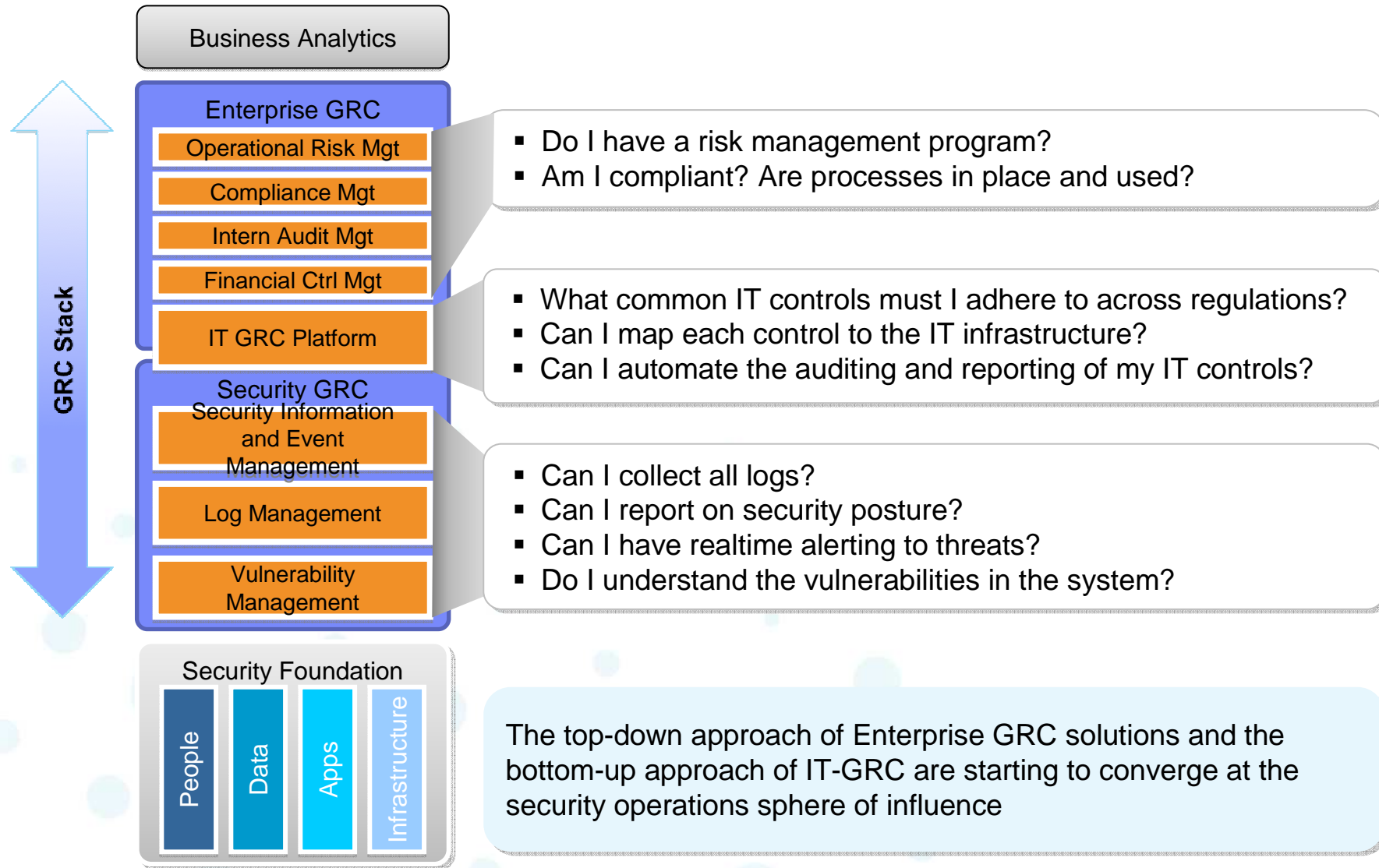
Further development of Privileged Identity Management (PIM) capabilities and enhanced Identity and Role Management

5 Identity: IBM's IAM vision – product mapping



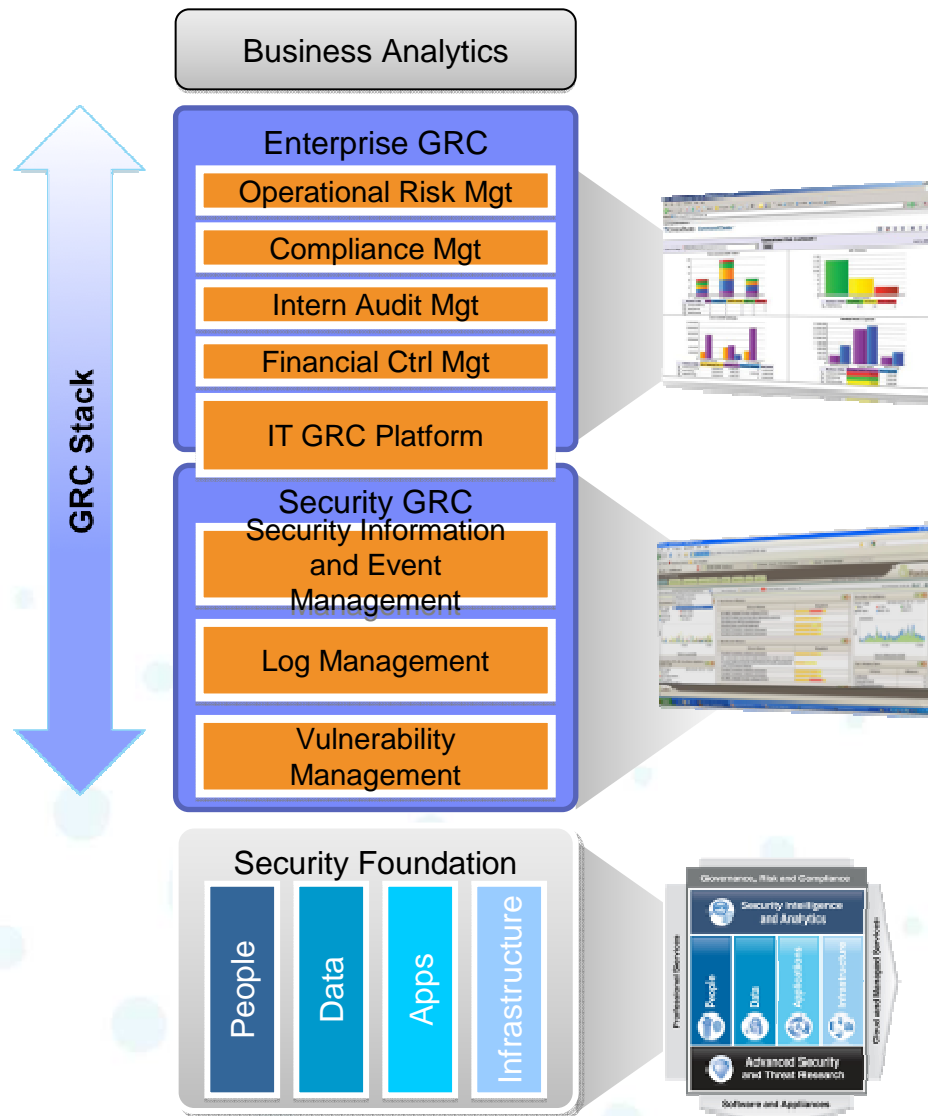
6

GRC: Customers are looking for a stack of GRC capabilities



6

GRC: The GRC stack and IBM



OpenPages – Enterprise GRC Platform

- Primarily driven by Enterprise Risk Management teams focusing on regulations such as SOX, HIPAA
- Focus is on Finance, Legal and Operational requirements (e.g. Finance controls, business continuity, vertical regulations)
- Top down approach to requirements

QRadar SIEM and Risk Manager

- Primarily driven by IT Security teams focusing on log collection, event analysis and compliance reporting
- Focus is on distilling vast amounts of data in an IT environment down to timely, relevant security information
- Bottom up approach to requirements

Security portfolio, leading assets in (or 3rd party integrations with!):

- Identity management
- Data security
- Application security
- Network and endpoint security

Major Global Bank reduces compliance costs by \$20M USD

Value

- Saved \$20M USD by using InfoSphere Guardium as compensating security control
- Saved \$1.5M/year in storage costs
- InfoSphere Guardium forms the foundation of the security infrastructure
- Culture change – new awareness of data security
- Real time processes to investigate insider threats

Business Challenge

1. Ensure privacy & integrity of: financial data; HR data; ERP data; credit card data; PII; strategic & intellectual property
2. Address PCI (Requirements 3, 6 & 10); SOX; international data privacy laws; internal standards
3. Protect diverse environment: Oracle, SQL Server, Sybase, DB2 UDB; DB2 on z & iSeries; Informix; MySQL; Teradata, Solaris, HP-UX, AIX, Windows, Linux, about 2000 database instances

Solution

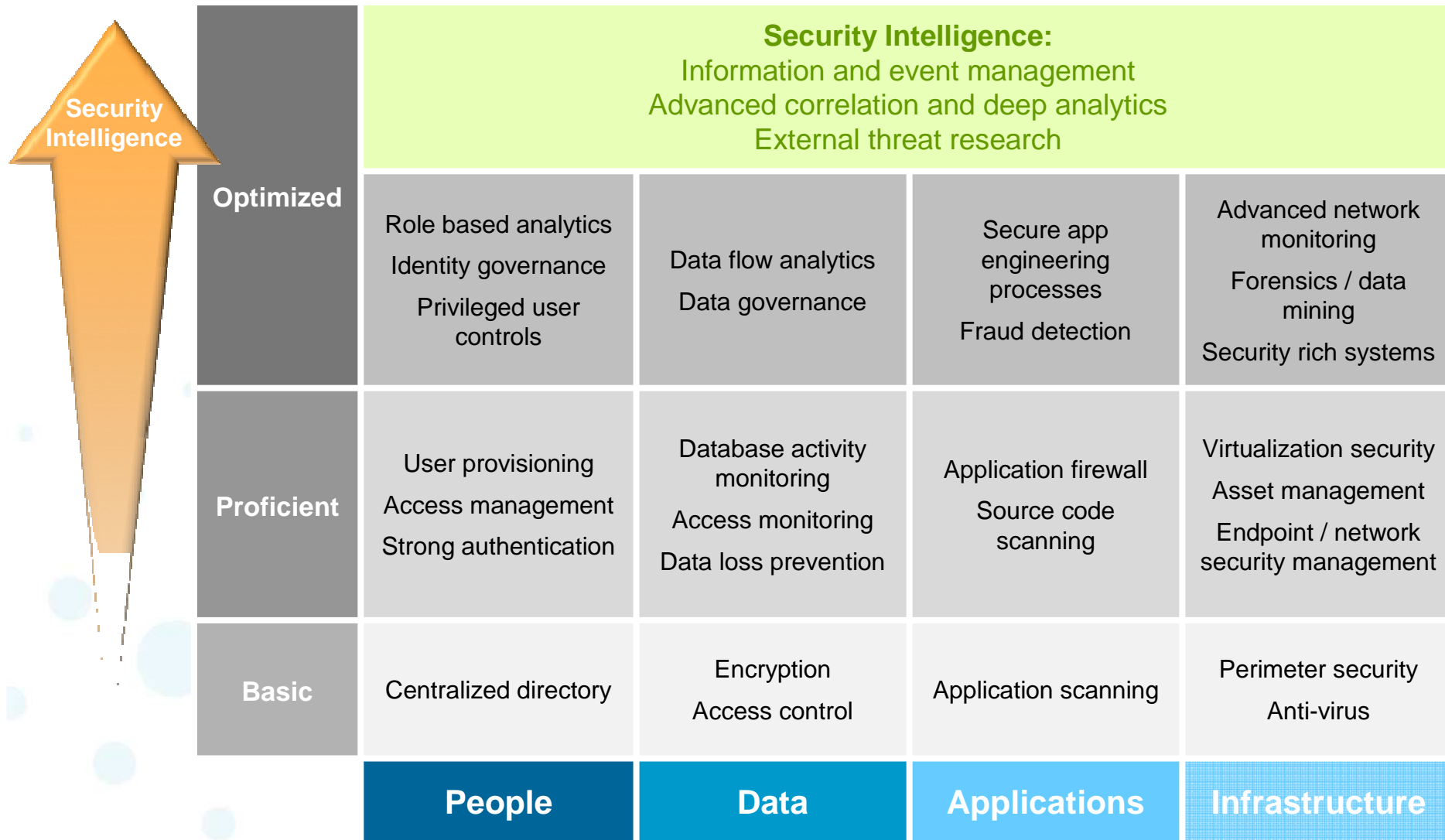
After considering native database logging, Symantec and other smaller vendors, this bank chose the InfoSphere Guardium solutions to monitor activity and protect privacy of mission critical data



Solution components:

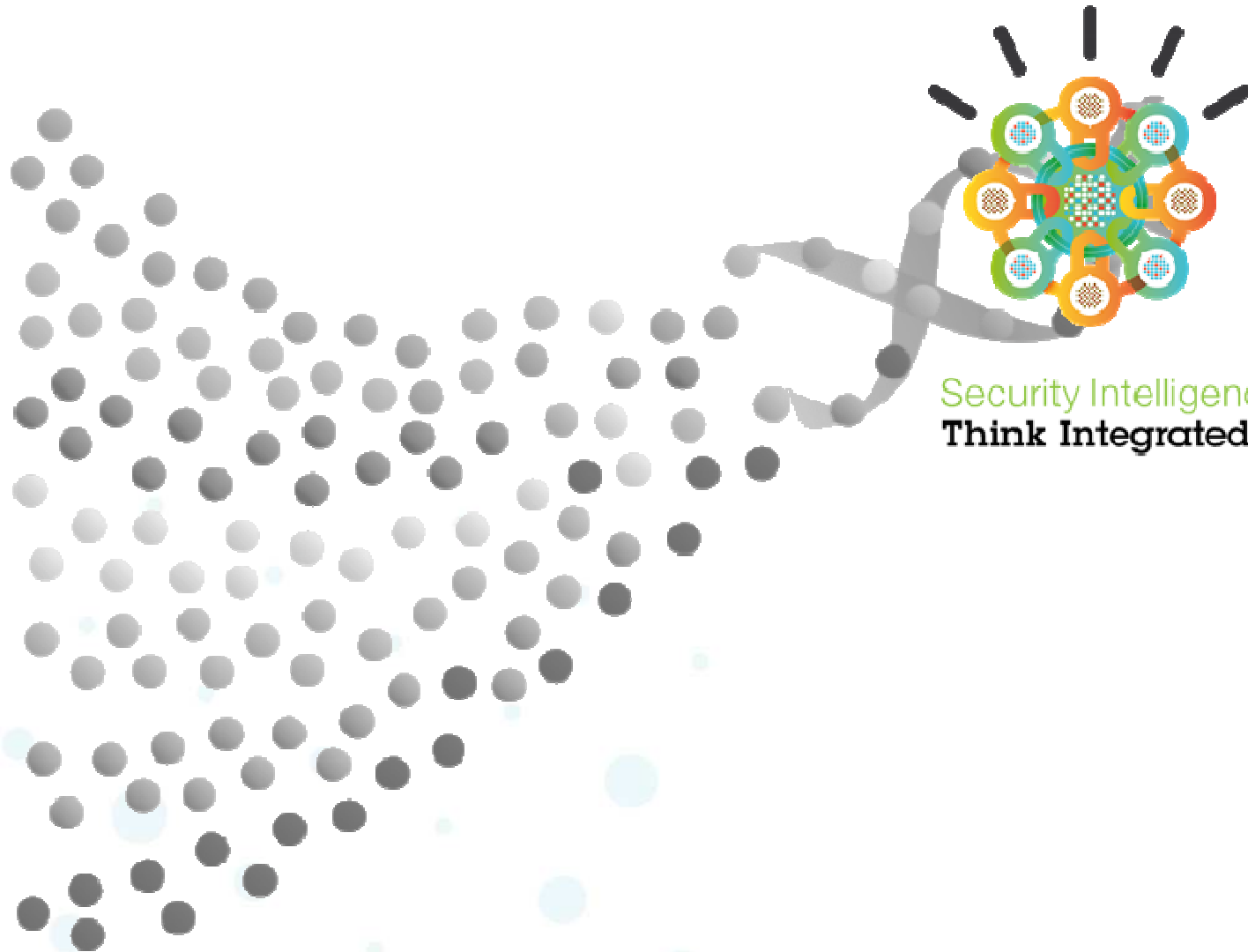
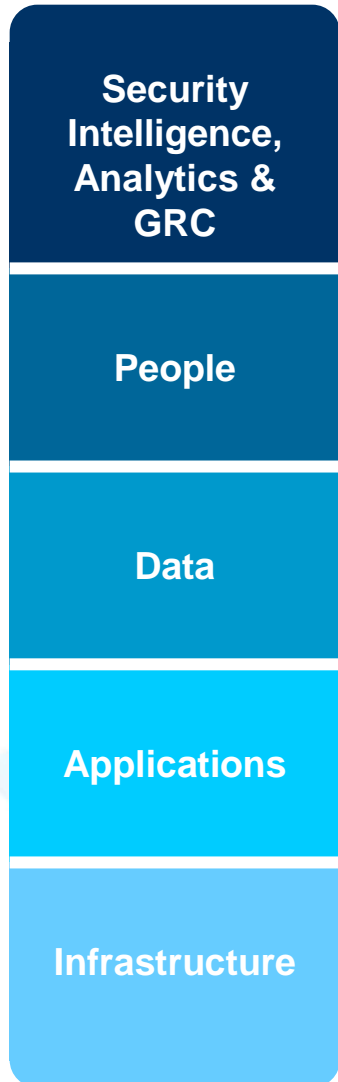
- IBM InfoSphere Guardium Database Activity Monitor

Security Intelligence is enabling progress to optimized security



JK 2012-04-26

Intelligent solutions provide the DNA to secure a Smarter Planet



Security Intelligence.
Think Integrated.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.



ibm.com/security

© **Copyright IBM Corporation 2012. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.