

---

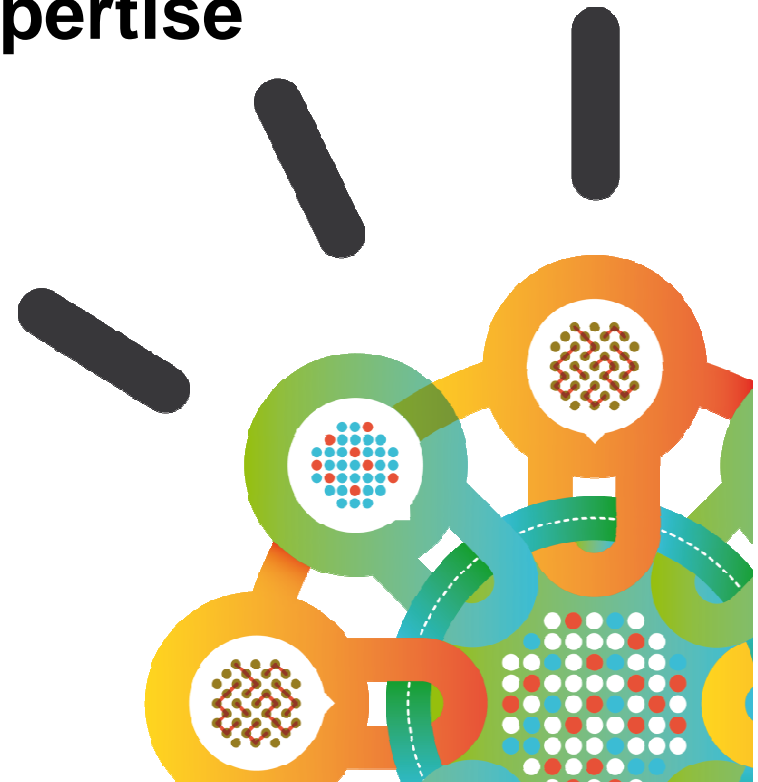
Security Intelligence.  
**Think Integrated.**

# IBM Security Strategy

## Intelligence, Integration and Expertise

Sandy Bird, Chief Technology Officer  
IBM Security Systems

August 2013



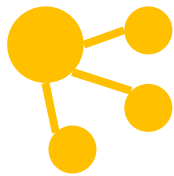
# Innovative technology changes everything



**1 trillion  
connected  
objects**



**1 billion mobile  
workers**



**Social  
business**



**Bring your  
own IT**



**Cloud and  
virtualization**

# Motivations and sophistication are rapidly evolving

National Security



Nation-state actors  
**Stuxnet**

Espionage, Activism



Competitors and Hacktivists  
**Aurora**

Monetary Gain

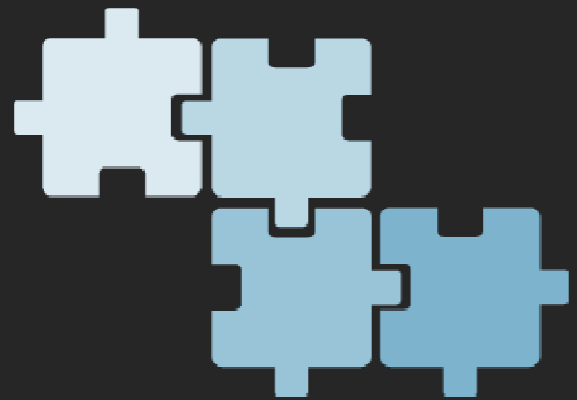


Organized crime  
**Zeus**

Revenge, Curiosity

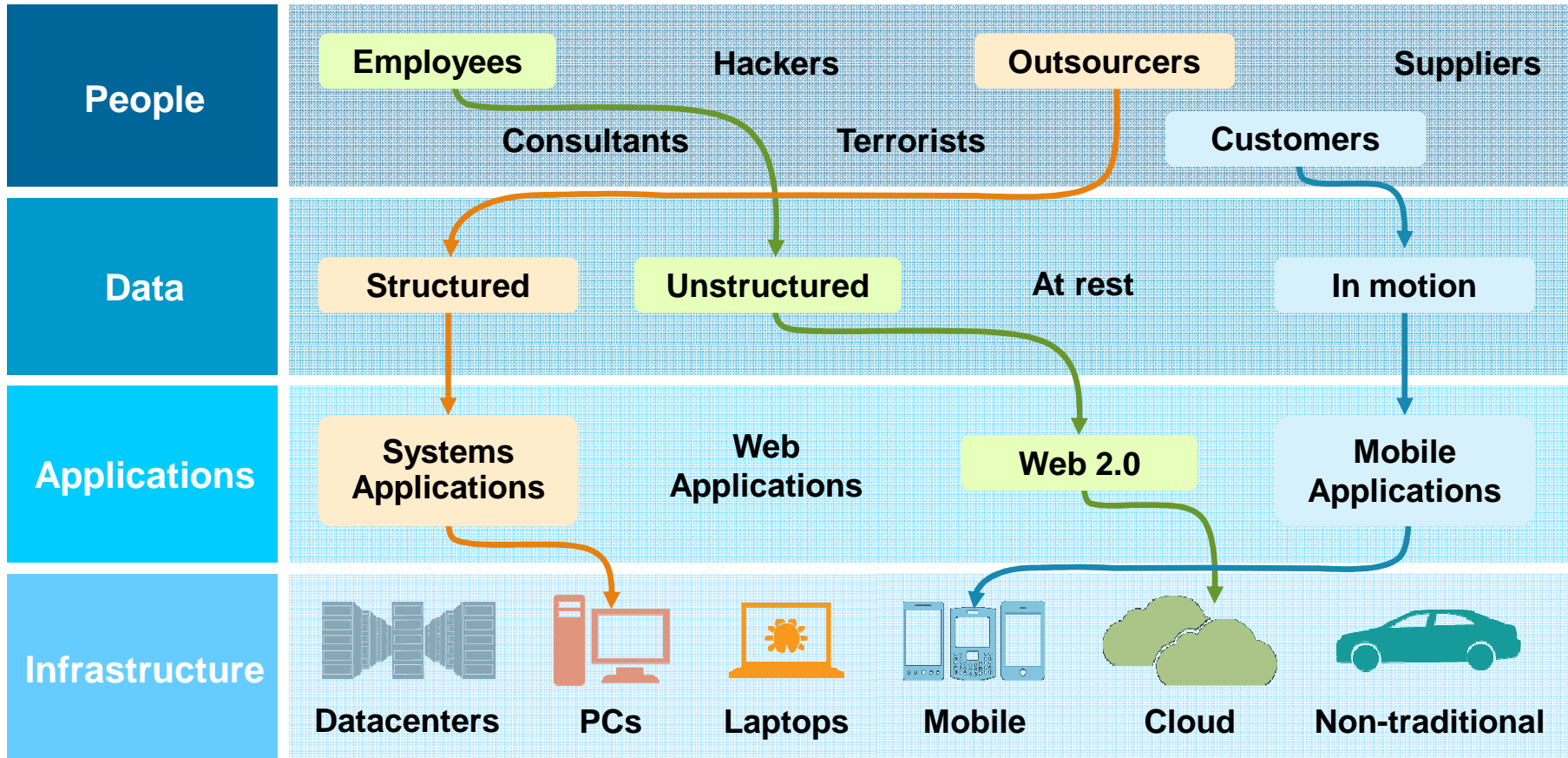


Insiders and Script-kiddies  
**Code Red**



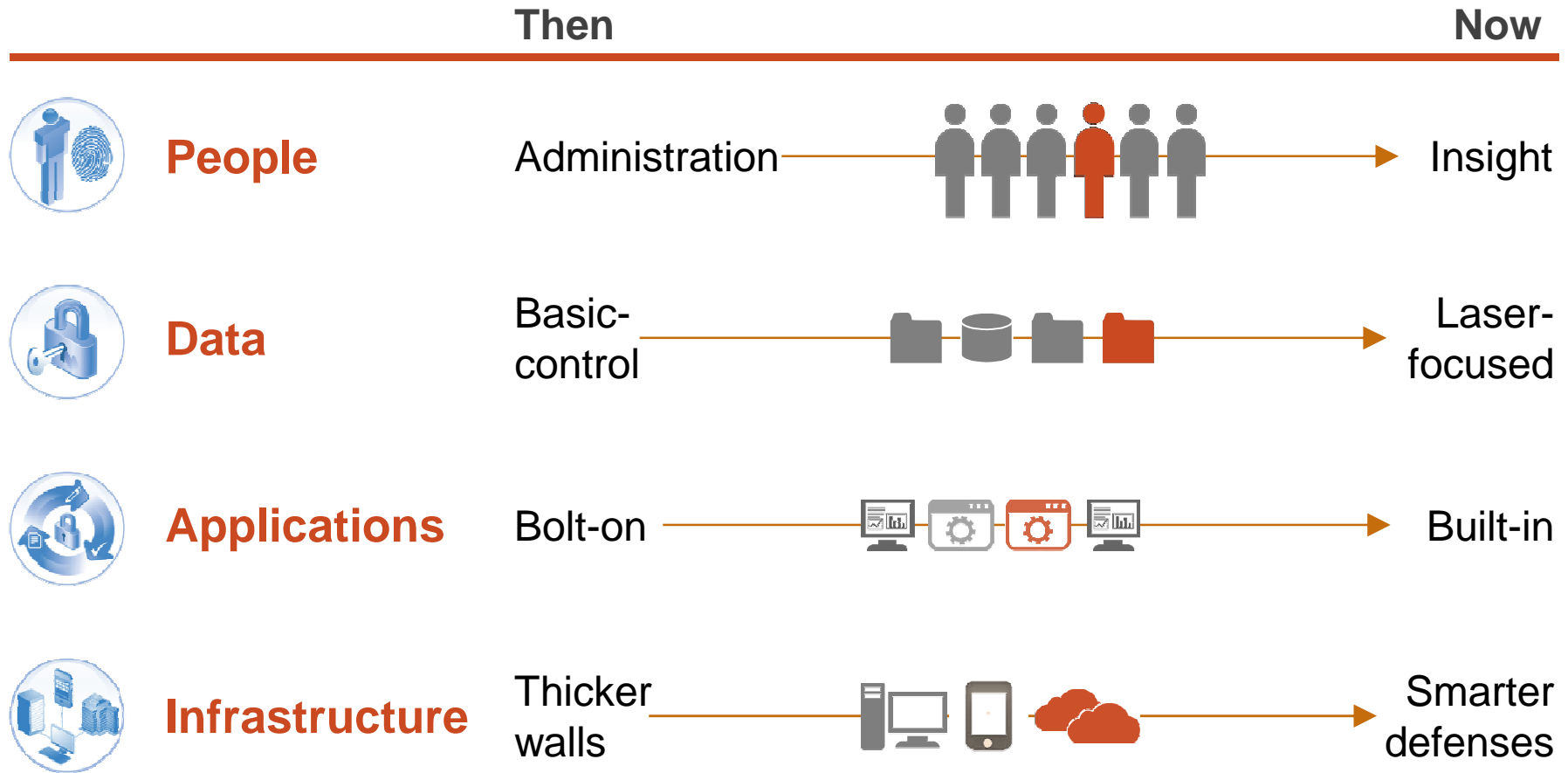
How do we  
solve this?

# Security challenges are a complex, four-dimensional puzzle ...



... that requires a new approach

# Thinking differently about security



**Monitor and Analyze Everything**

IBM Security  
strategy



IBM delivers solutions across a security framework

**Intelligence**

**Integration**

**Expertise**





# IBM security strategy


Generate higher value with continuous innovation across key security trends – leveraging our strengths in analytics, integration, and global skills to help secure our customers' most important assets



## IBM offers a comprehensive portfolio of security products

IBM Security Systems Portfolio					
Security Intelligence and Analytics					
QRadar SIEM	QRadar Log Manager	QRadar Risk Manager	QRadar Vulnerability Manager		
Advanced Fraud Protection					
Trusteer Rapport	Trusteer Pinpoint Malware Detection	Trusteer Pinpoint ATO Detection	Trusteer Mobile Risk Engine		
People	Data	Applications	Network	Infrastructure	Endpoint
Identity Management	Guardium Database Security	AppScan Source	Network Intrusion Prevention	Trusteer Apex	
Access Management	Guardium Vulnerability Assessment	AppScan Dynamic	Next Generation Network Protection	Mobile & Endpoint Management	
Privileged Identity Manager	Guardium / Optim Data Masking	DataPower Web Security Gateway	SiteProtector Threat Management	Virtualization and Server Security	
Federated Access and SSO	Key Lifecycle Manager	Security Policy Manager	Network Anomaly Detection	Mainframe Security	
IBM X-Force Research					

## Industry analysts rank IBM Security as leading the market

Domain	Market Segment / Report	Security Analyst Report Rankings		
		Gartner Magic Quadrant	Forrester Wave	IDC Market Share
Security Intelligence	Security Information and Event Management (SIEM)	Leader 2013		Leader 2011
Anti-Fraud	Web Fraud Detection	Leader 2013		
People	Identity and Access Governance	Challenger 2013		Leader 2013
	User Provisioning and Administration	Leader 2013		
	Role Management and Access Recertification		Contender 2011	
	Web Access Management (WAM)	Leader 2013 MarketScope		
Data	Database Auditing and Real-Time Protection		Leader 2011	
	Data Masking	Leader 2013		
Applications	Application Security Testing ( <i>dynamic and static</i> )	Leader 2013		Leader 2013
Infrastructure	Network Intrusion Prevention Systems (NIPS)	Challenger 2012		
	EndPoint Protection Platforms (EPP)	Visionary 2013	Strong Performer 2013	
Services	Managed Security Services (MSS)	Leader 2012	Leader 2012	
	Information Security Consulting Services		Leader 2013	

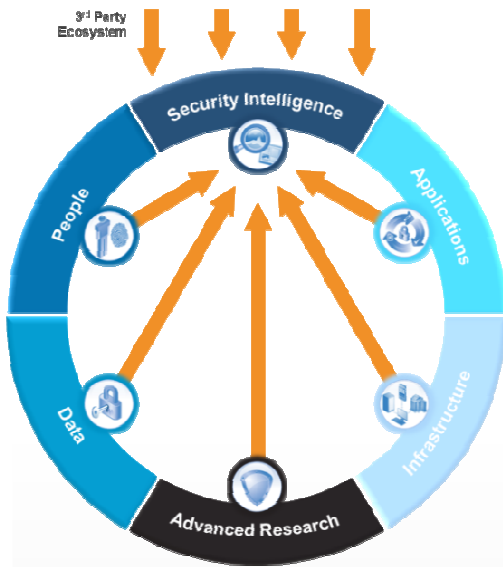
 Report not available

Note: Rankings compiled from latest available analyst reports as of July, 2013

© 2013 IBM Corporation

# Integration: Increase security, collapse silos, and reduce complexity

## Integrated Intelligence.



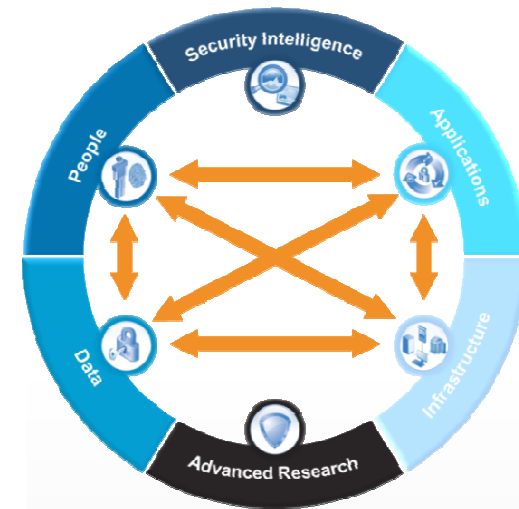
Consolidate and correlate siloed information from hundreds of sources

## Integrated Research.



Stay ahead of the changing threat landscape

## Integrated Protection.

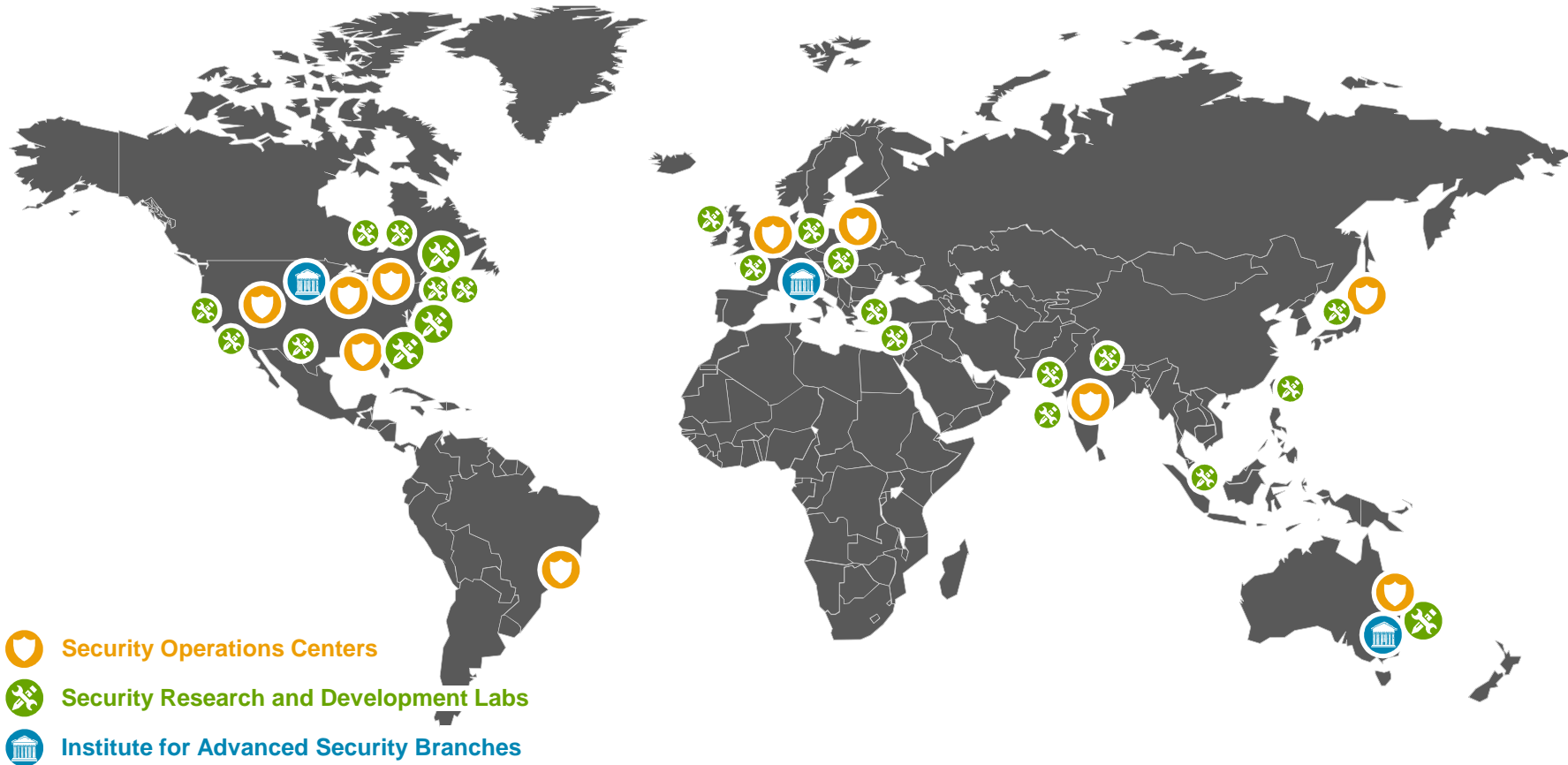


Link security / vulnerability information across domains

JK 2013-04-26

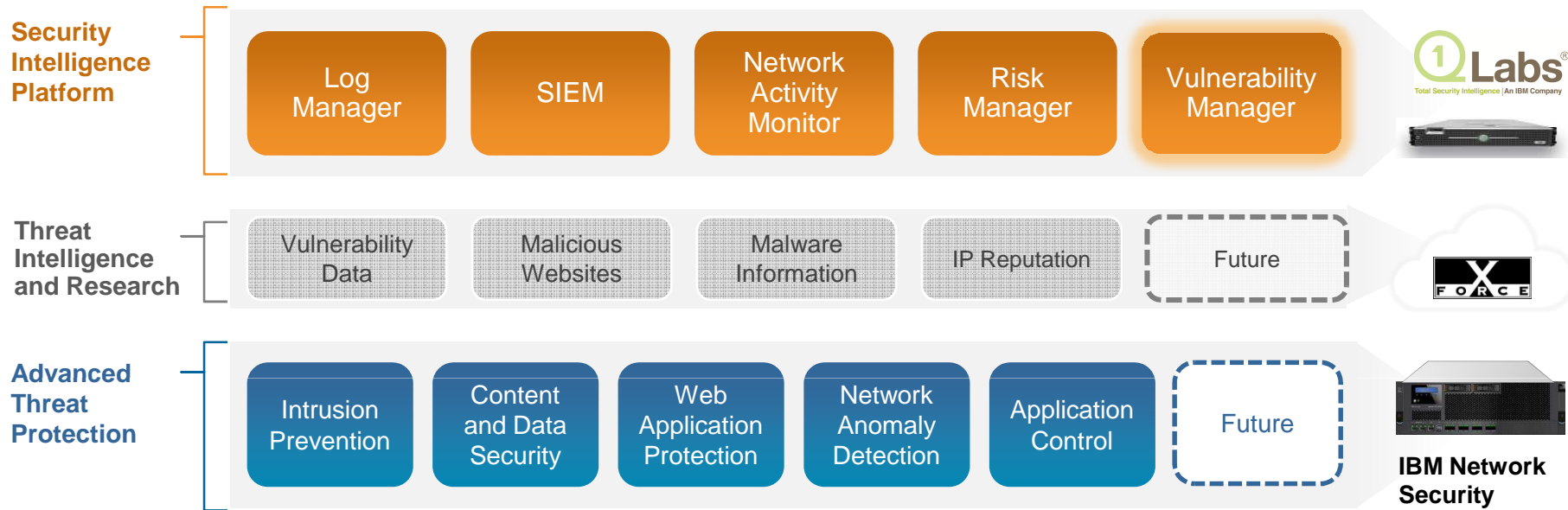


## At IBM, the world is our Security lab



- 6,000 researchers, developers and subject matter experts working security initiatives worldwide
- 3,000+ IBM security patents

# Advanced Threat Platform: Better protection against sophisticated attacks



## Key Themes

### Advanced Threat Protection Platform

Helps to prevent sophisticated threats and detect abnormal network behavior by using an extensible set of network security capabilities - in conjunction with real-time threat information and Security Intelligence

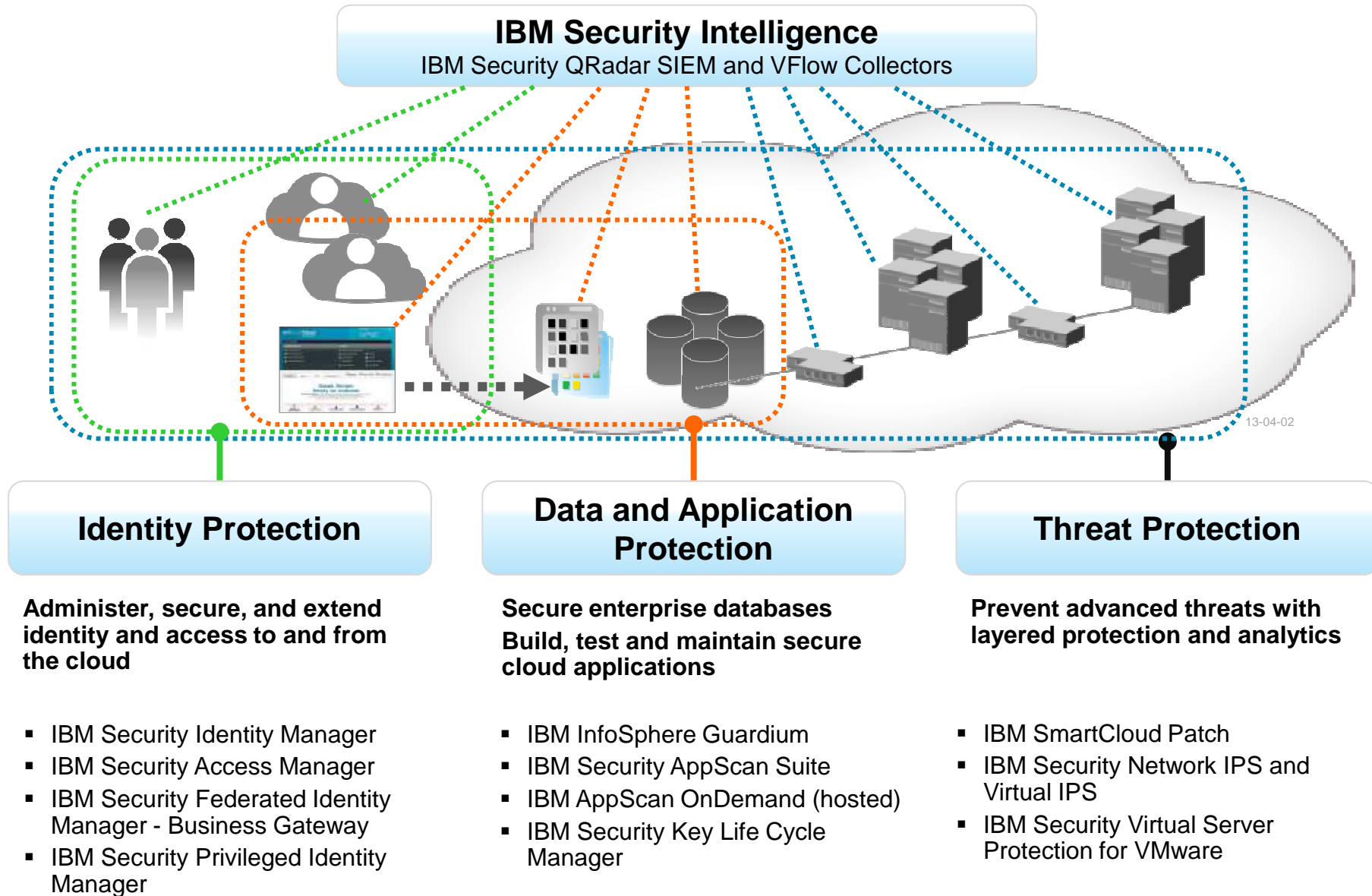
### Expanded X-Force Threat Intelligence

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

### Security Intelligence Integration

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

# IBM Cloud Security Capabilities



**Administer, secure, and extend identity and access to and from the cloud**

- IBM Security Identity Manager
- IBM Security Access Manager
- IBM Security Federated Identity Manager - Business Gateway
- IBM Security Privileged Identity Manager

**Secure enterprise databases  
Build, test and maintain secure cloud applications**

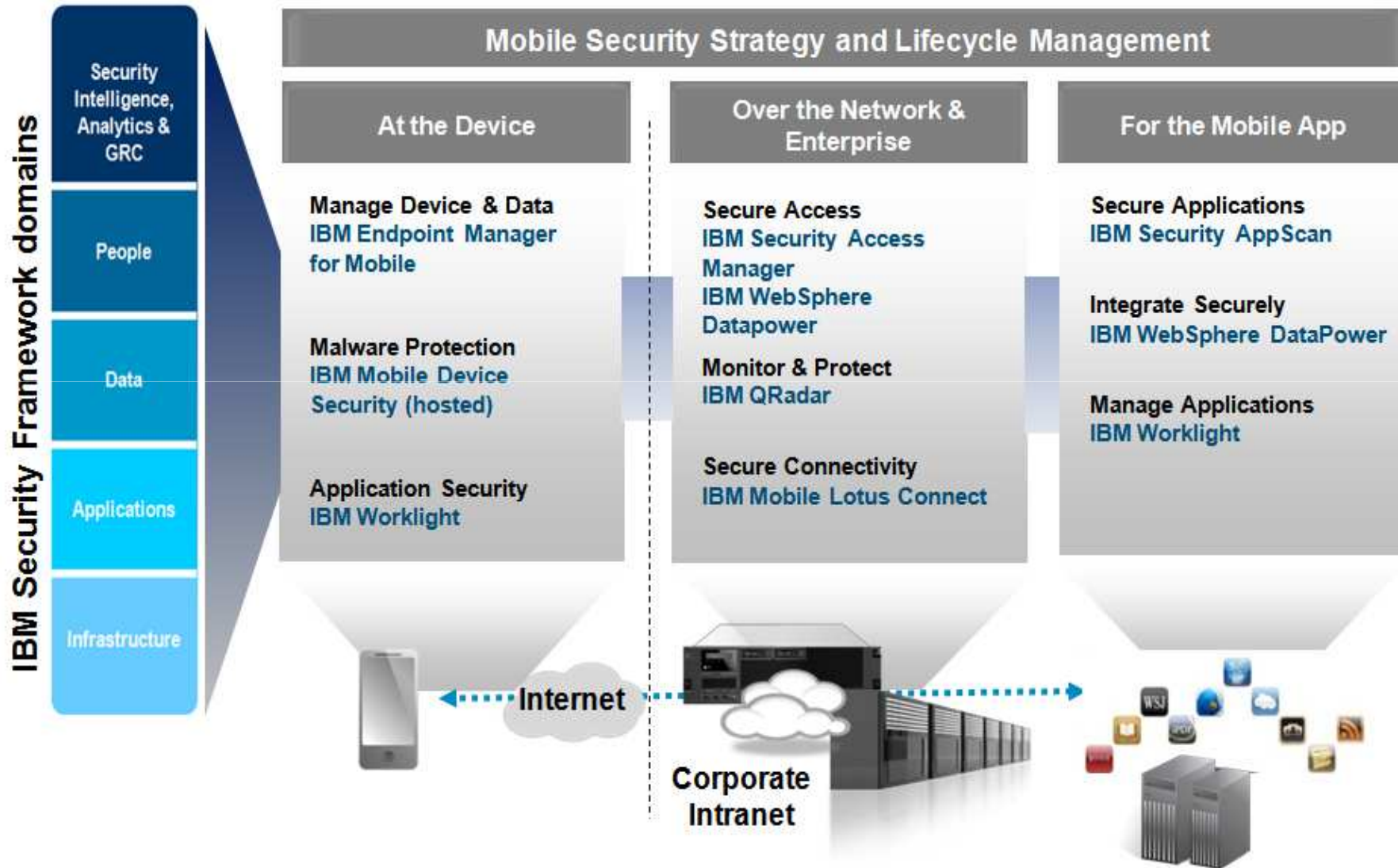
- IBM InfoSphere Guardium
- IBM Security AppScan Suite
- IBM AppScan OnDemand (hosted)
- IBM Security Key Life Cycle Manager

**Prevent advanced threats with layered protection and analytics**

- IBM SmartCloud Patch
- IBM Security Network IPS and Virtual IPS
- IBM Security Virtual Server Protection for VMware

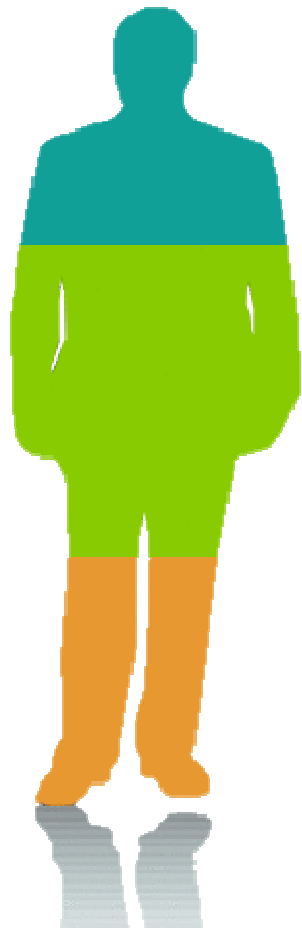


# Securing the Mobile Enterprise with IBM Solutions





# IBM's 2012 Chief Information Security Officer Study revealed the changing role of the CISO



## Influencers

- Confident / prepared
- Strategic focus

## Protectors

- Less confident
- Somewhat strategic
- Lack necessary structural elements

## Responders

- Least confident
- Focus on protection and compliance

## How they differ

have a dedicated CISO



have a security/risk committee



have information security as a board topic



use a standard set of security metrics to track their progress



focused on improving enterprise communication/collaboration



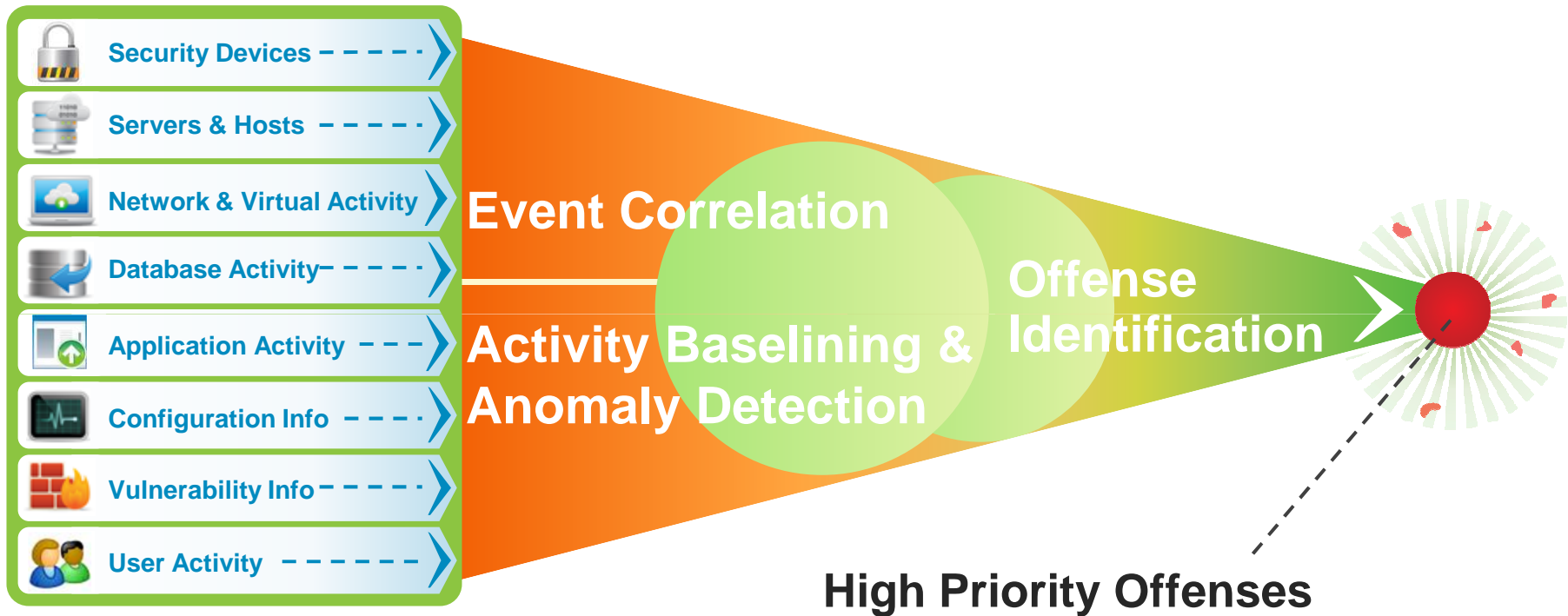
focused on providing education and awareness



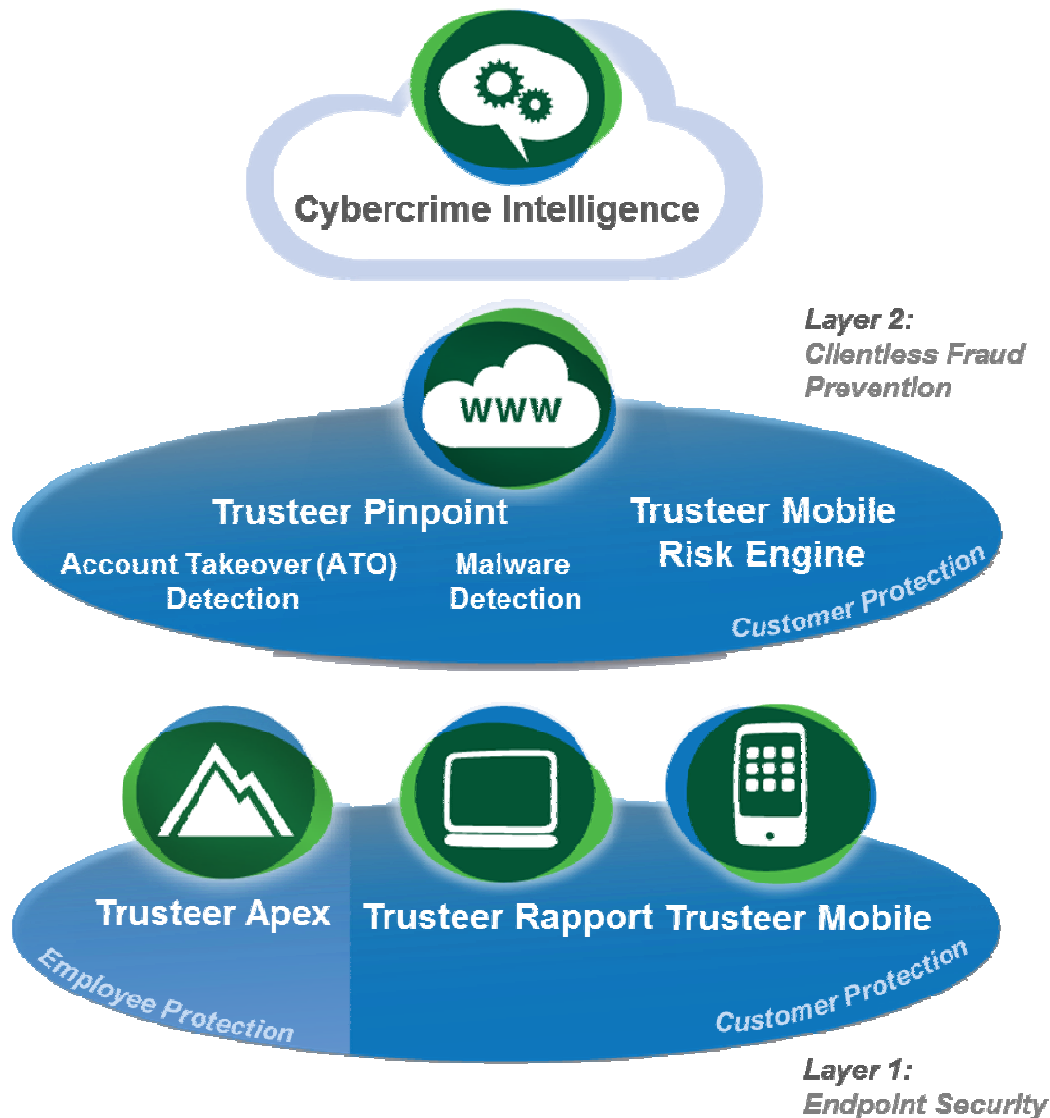
# IBM Security Capabilities



# Security Intelligence: Integrating across IT silos



# Key Trusteer software and cloud-based solutions



**Trusteer Cybercrime Intelligence**  
Global threat intelligence and fraudster database – including data from tens of millions of Trusteer-protected endpoints



**Trusteer Pinpoint Account Takeover (ATO) Detection**  
Correlation of multiple fraud risk indicators for conclusive account takeover and mobile risk detection

**Malware Detection**  
Clientless detection of Man-in-the-Browser malware infected endpoints

**Trusteer Mobile Risk Engine**  
Detect mobile and cross-channel fraud



**Trusteer Mobile**  
Embedded security library for native mobile apps , dedicated mobile browser, out-of-band authentication

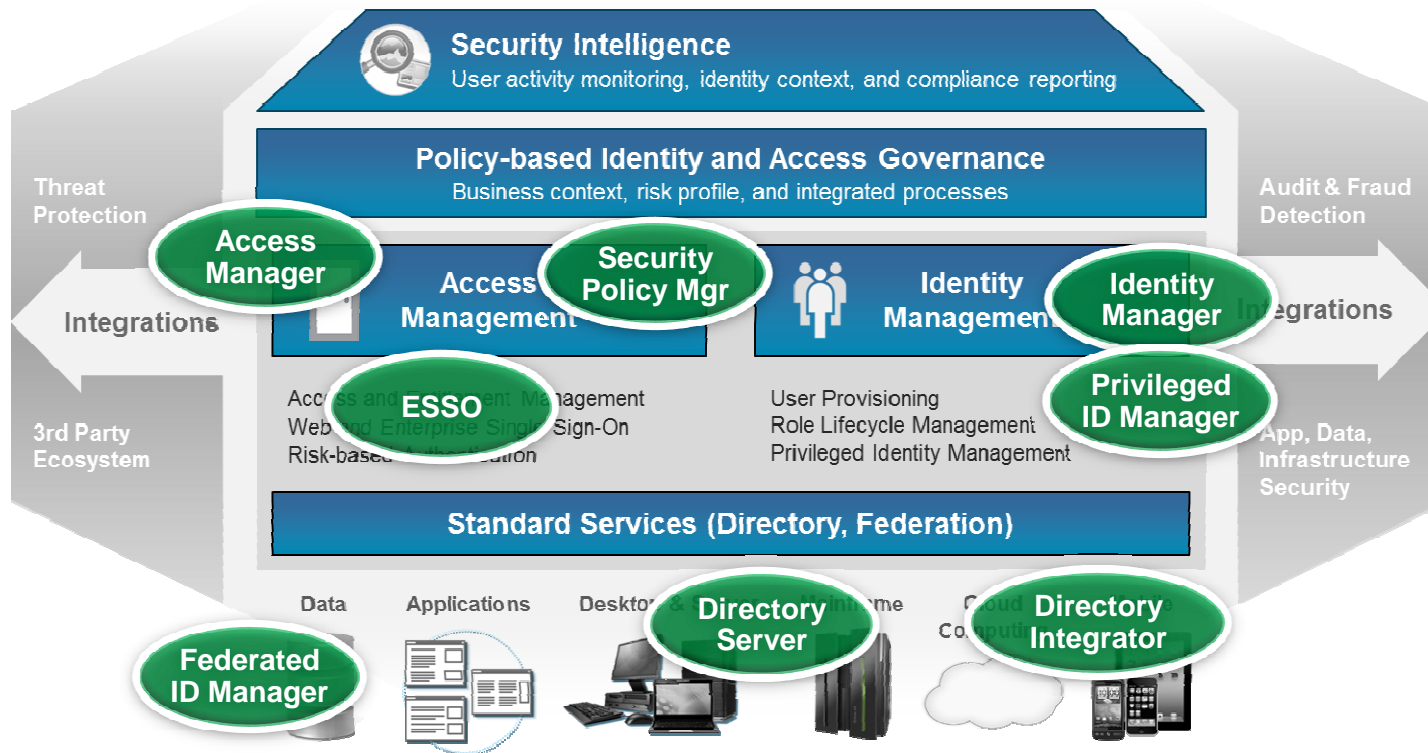


**Trusteer Rapport**  
Prevention and remediation of malware and phishing threats on PCs and Macs



**Trusteer Apex**  
Zero-day exploits and data exfiltration prevention for employees' endpoints

# 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

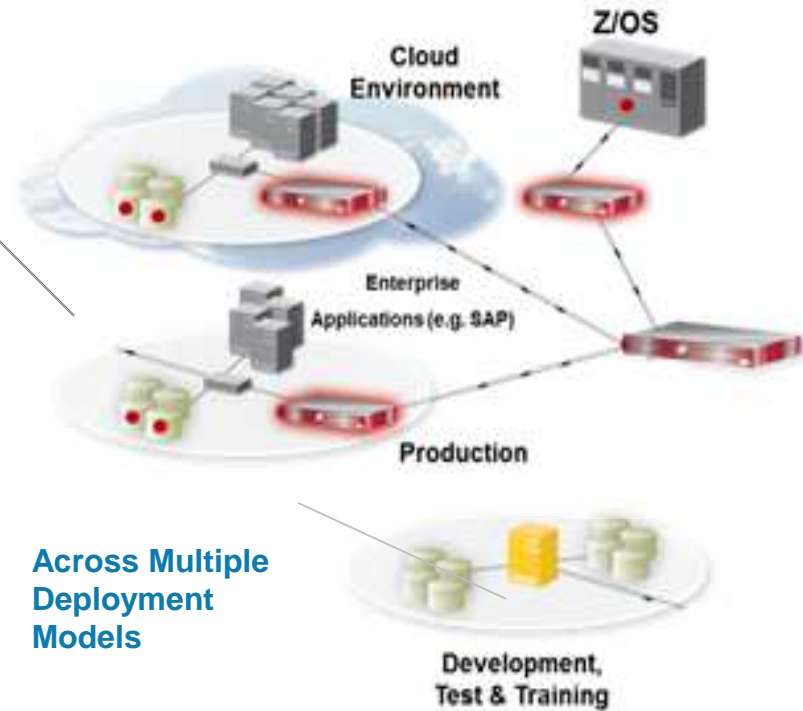
Further development of Privileged Identity Management (PIM) capabilities and enhanced Identity and Role Management



# Data Security Vision



QRadar Integration



Across Multiple Deployment Models

## Key Themes

### Reduced Total Cost of Ownership

Expanded support for databases and unstructured data, automation, handling and analysis of large volumes of audit records, and new preventive capabilities

### Enhanced Compliance Management

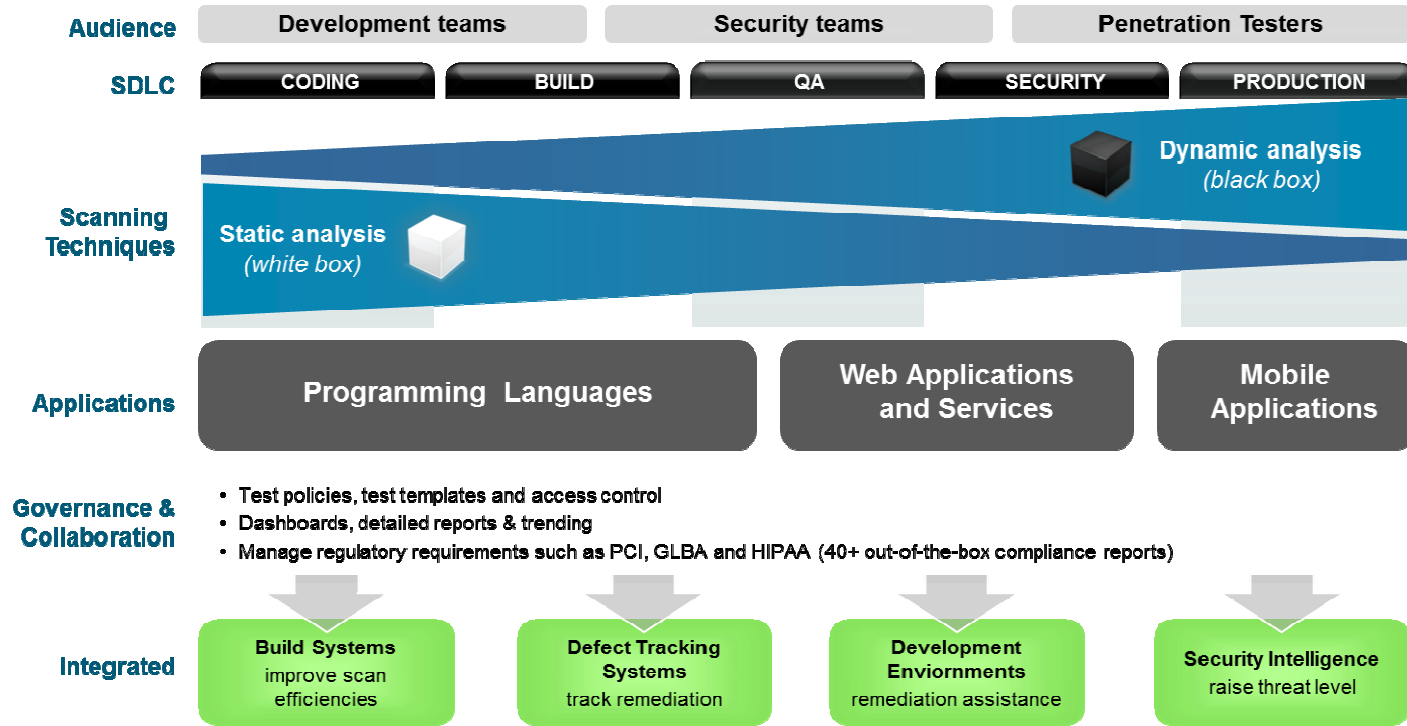
Enhanced Database Vulnerability Assessment (VA) and Database Protection Subscription Service (DPS) with improved update frequency, labels for specific regulations, and product integrations

### Dynamic Data Protection

Data masking capabilities for databases (row level, role level) and for applications (pattern based, form based) to safeguard sensitive and confidential data



# Application Security Vision



## Key Themes

### Coverage for Mobile applications and new threats

Continue to identify and reduce risk by expanding scanning capabilities to new platforms such as mobile, as well as introducing next generation dynamic analysis scanning and glass box testing

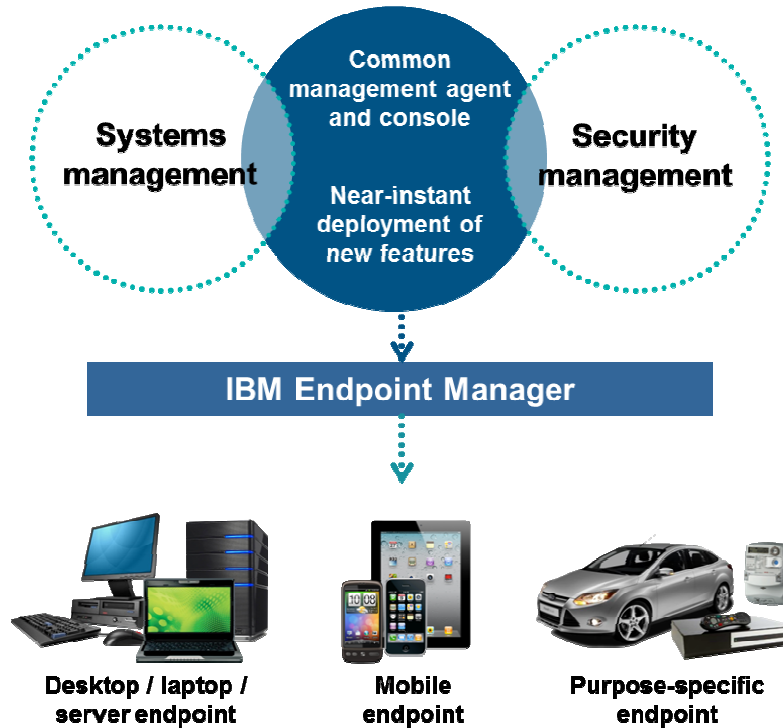
### Simplified interface and accelerated ROI

New capabilities to improve customer time to value and consumability with out-of-the-box scanning, static analysis templates and ease of use features

### Security Intelligence Integration

Automatically adjust threat levels based on knowledge of application vulnerabilities by integrating and analyzing scan results with SiteProtector and the QRadar Security Intelligence Platform

# Infrastructure Protection – Endpoint Vision



## Key Themes

**Security for Mobile Devices**

Provide security for and manage traditional endpoints alongside mobile devices such as Apple iOS, Google Android, Symbian, and Microsoft Windows Phone - using a single platform

**Expansion of Security Content**

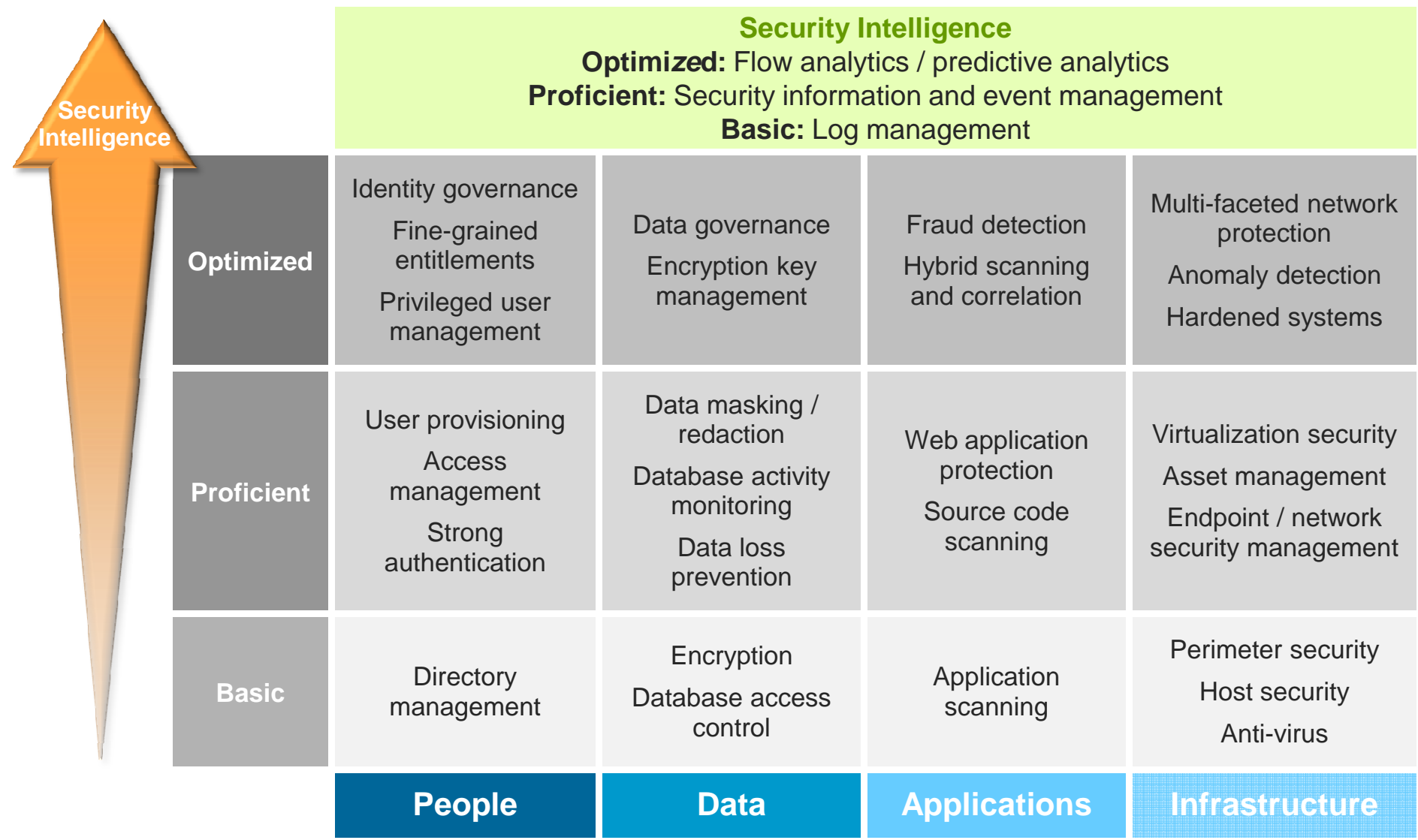
Continued expansion of security configuration and vulnerability content to increase coverage for applications, operating systems, and industry best practices

**Security Intelligence Integration**

Improved usage of analytics - providing valuable insights to meet compliance and IT security objectives, as well as further integration with SiteProtector and the QRadar Security Intelligence Platform

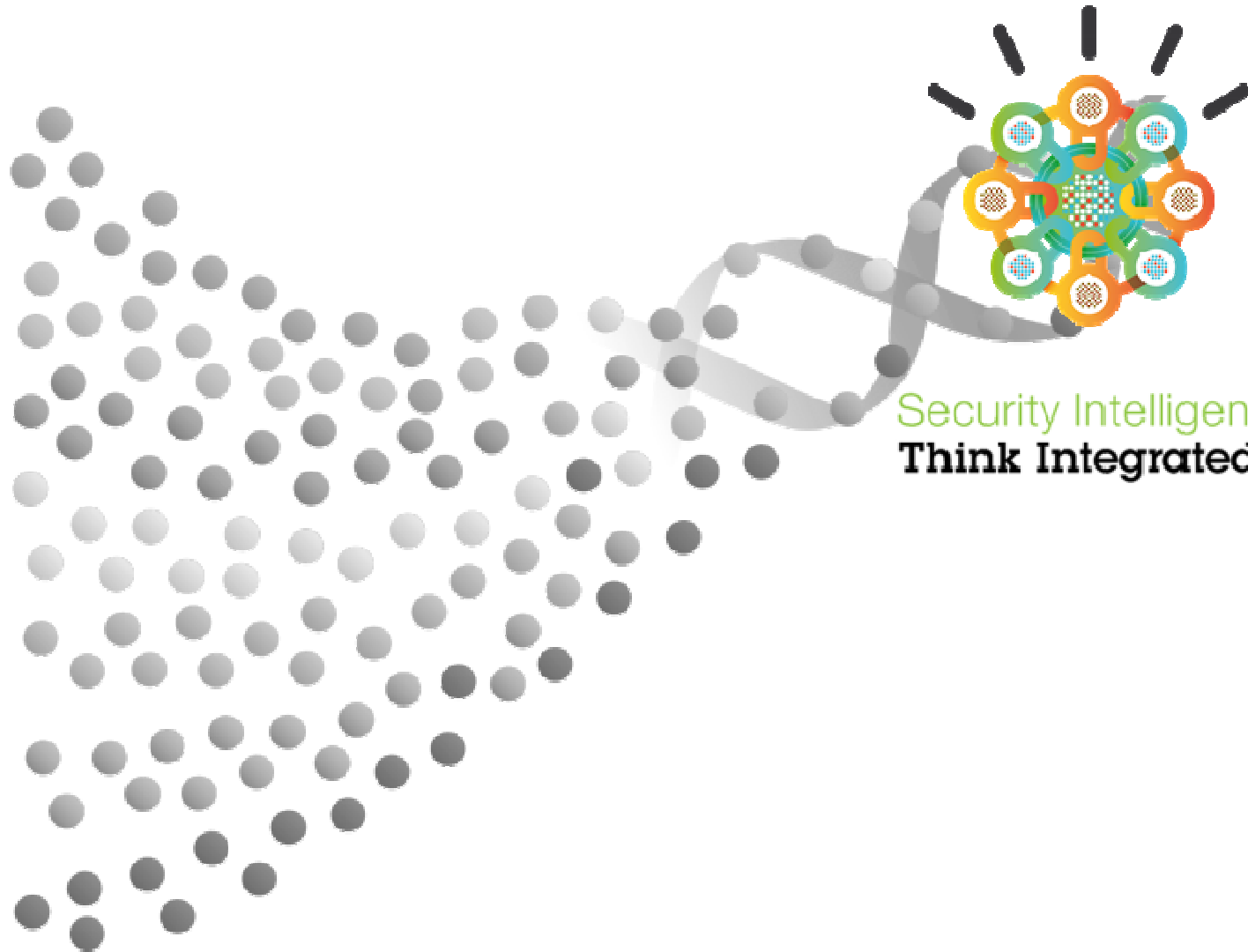
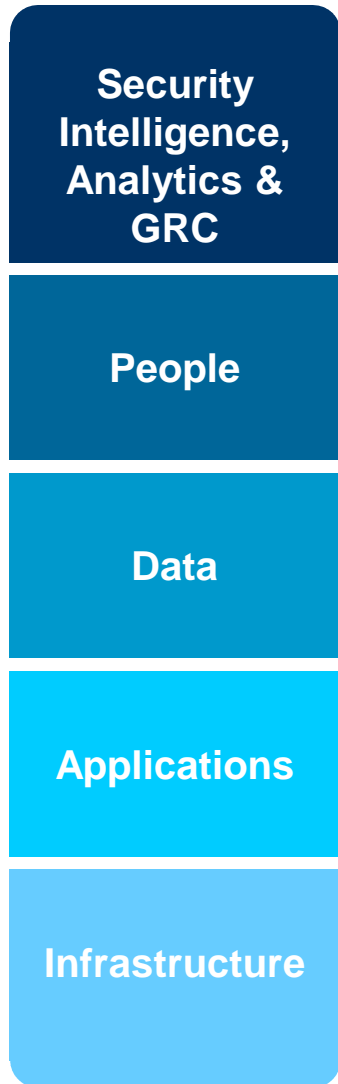


# Security Intelligence is enabling progress to optimized security



13-05-03

# Intelligent solutions provide the DNA to secure a Smarter Planet



Security Intelligence.  
**Think Integrated.**



## Disclaimer

### *Please Note:*

*IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.*

*Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.*

*The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.*

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](http://ibm.com/security)



© **Copyright IBM Corporation 2013. 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.