

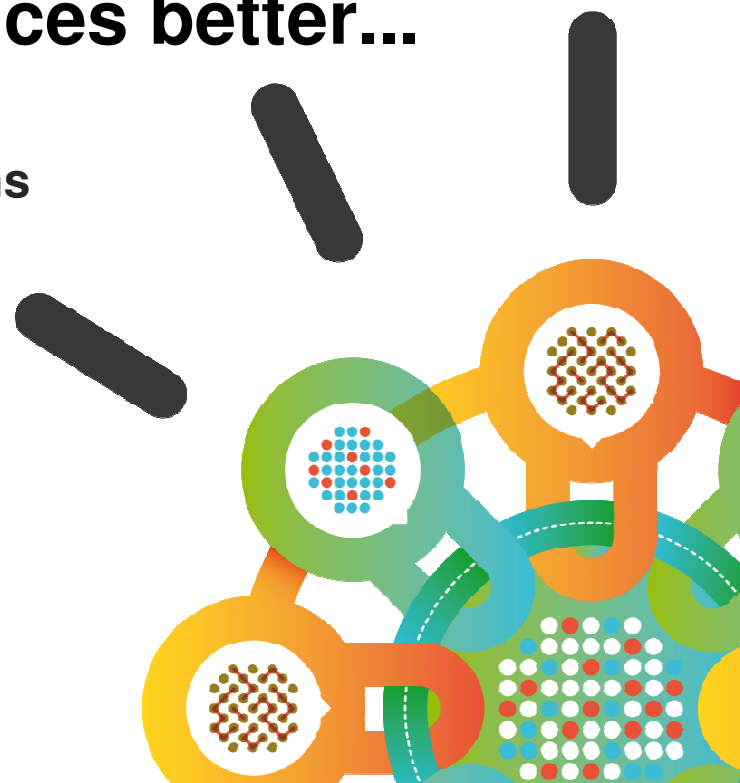
Security Intelligence.
Think Integrated.

Thinking Like an Attacker

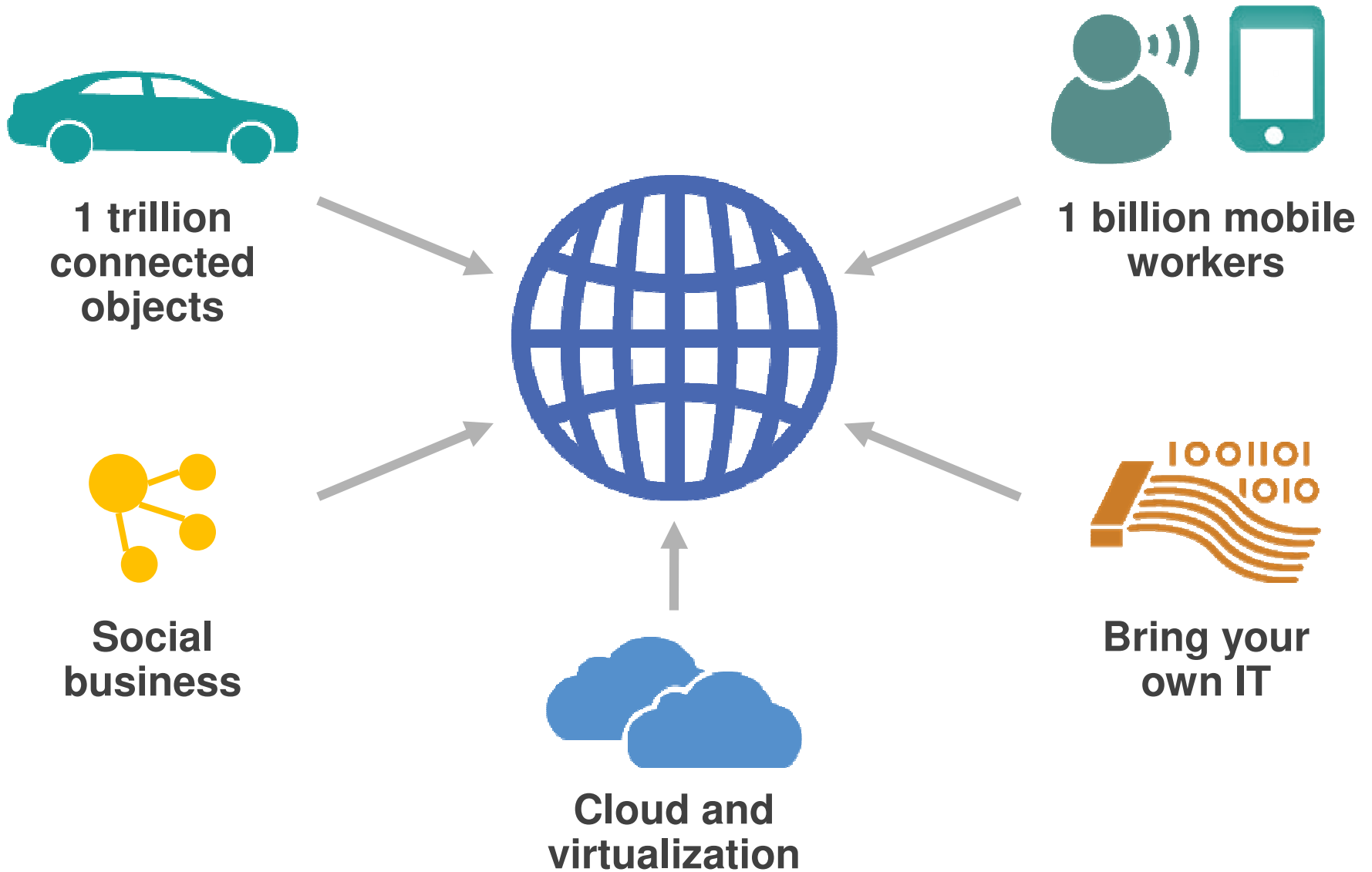
How to make your defences better...

IBM Security Systems

April 2013



Innovative technology changes everything



What is the scale of the problem?

2,641,350

Security Attacks

The Average Company Faces per Week

Who's most at risk?

- 1. Health & Social Services**
- 2. Transportation**
- 3. Hospitality**
- 4. Finance & Insurance**
- 5. Manufacturing**
- 6. Real Estate**
- 7. Mining, Oil & Gas**

Top 7 Most **Attacked** Industries

Recent **Increase** in Attacks on **Pharma**

What effect does this have?

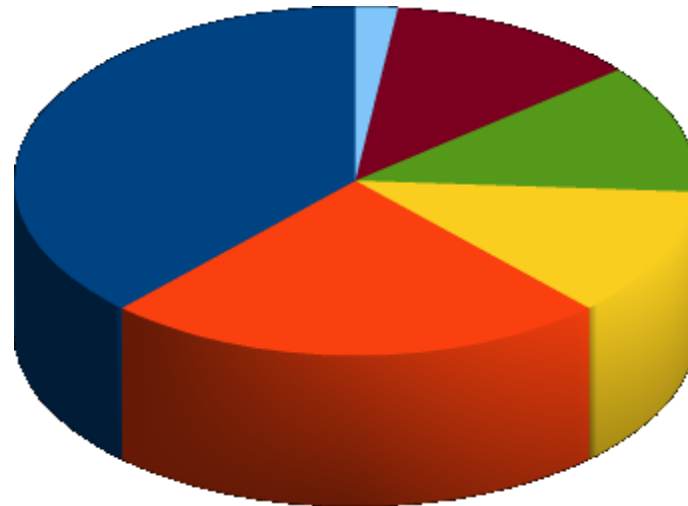
62

Security Incidents

The **Average Company** Faces per Week

How do attackers attack?

Categories of Attack



- Malicious Code
- Sustained Probe or Scan
- Unauthorised Access
- Low-and-Slow Attack
- Access Credentials Abuse
- Denial of Service

This is What **IBM** Sees

How do defenders fail?

- 1. End user didn't think before clicking**
- 2. Weak password / default password**
- 3. Insecure configuration**
- 4. Unpatched hardware / software**
- 5. Missing network protection / segmentation**

Top 5 Reasons **Why Attacks Were Possible**

What is good practice?

6

Security Incidents

The Average **Mature** Company Faces per Week

What type of organisation are you?

Most Mature

Real Estate
Transportation
Hospitality
Finance & Insurance
**Health & Social
Services**

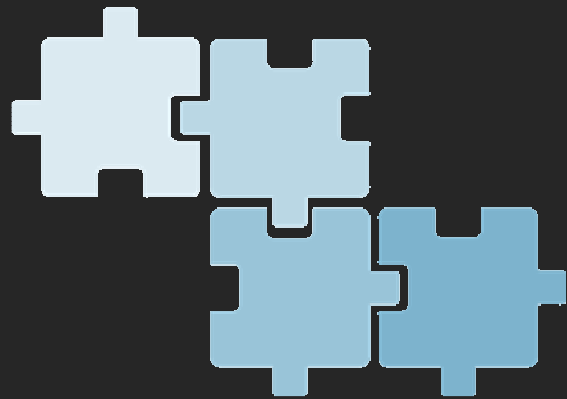
Least Mature

Construction
Education
Utilities
Mining, Oil & Gas
**“Extraterritorial”
Activities**

Industry Maturity Indicator based on Incidents / 1M Attacks

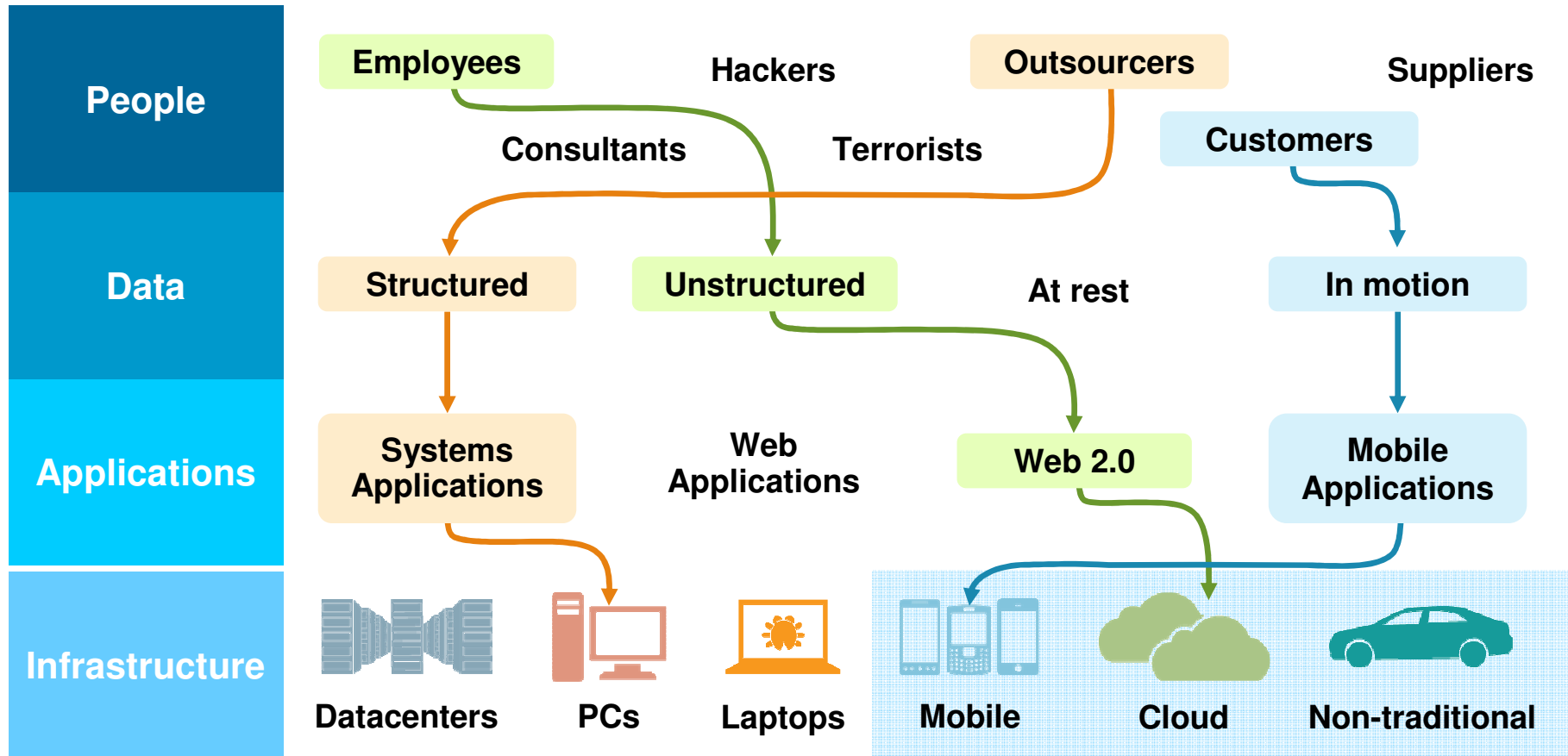
Motivations and sophistication are rapidly evolving





How Does an Attacker Exploit a Breach?

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

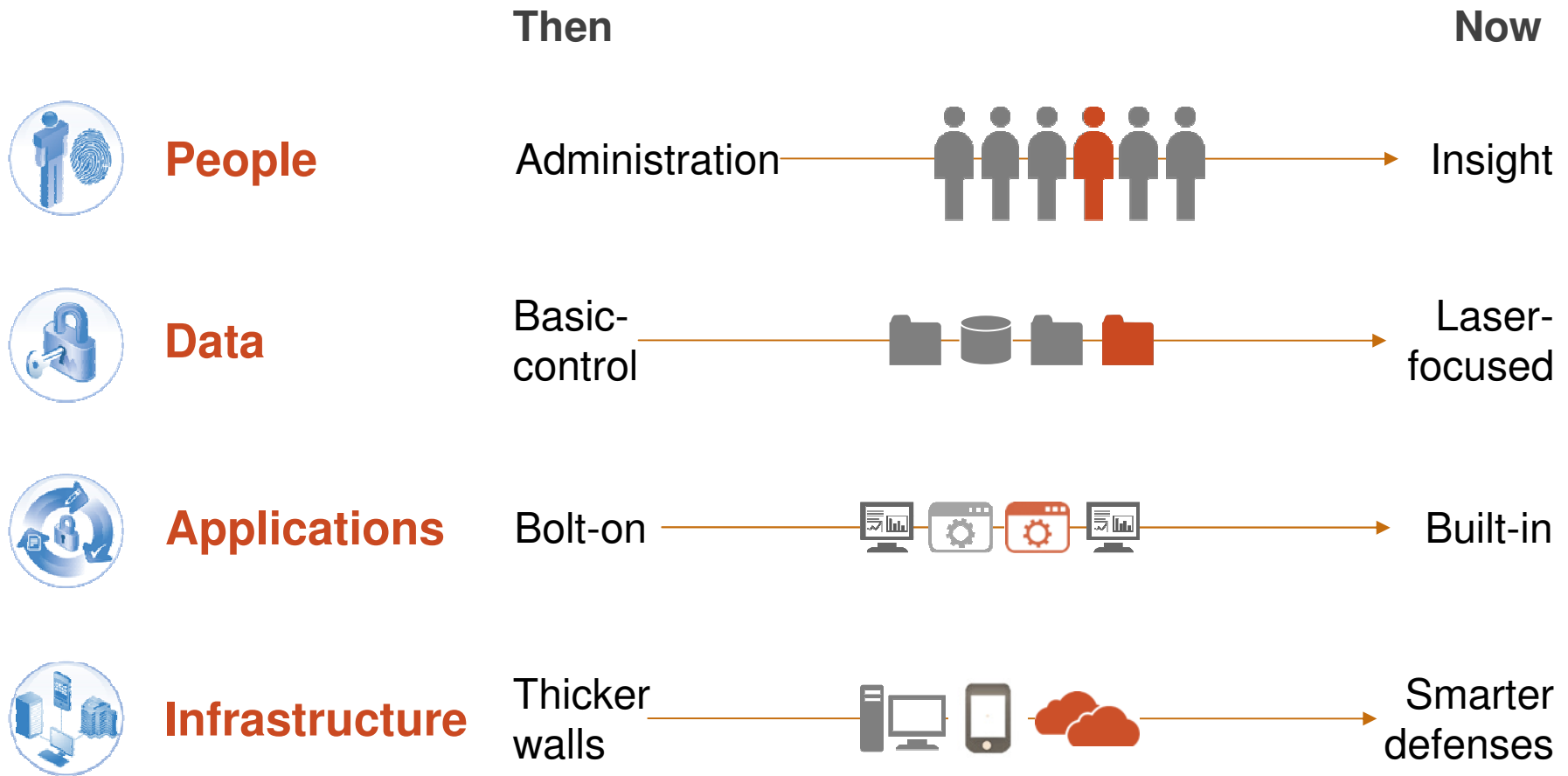


... that requires a new approach

The 5 Steps Used by Attackers

- 1. Break in**
- 2. Load Malware**
- 3. Expand**
- 4. Gather Data**
- 5. Exfiltrate**

Thinking differently about security



Collect and Analyze Everything



Advanced Research

Domain	IP Address	File Checksum
dogpile.com	117.0.178.252	c69d172078b439545dfff28f3d3aacc1
kewww.com.cn	83.14.12.218	51e65e6c798b03452ef7ae3d03343d8f
ynnsuue.com	94.23.71.55	6bb6b9ce713a00d3773cfcecef515e02

Monitor Everything

Then: Reaction

- Read about the latest threats from blogs and news
- Match against known signatures and bad actors

Now: Situational Awareness

- Consume real-time intelligence about the latest threats
- Correlate alerts against external behavior and reputation
- Proactively block bad domains, IP address and malware



Security Intelligence



Then: **Collection**

- Log collection
- Signature-based detection

Now: **Intelligence**

- Real-time monitoring
- Context-aware anomaly detection
- Automated correlation and analytics

Applying these
principles

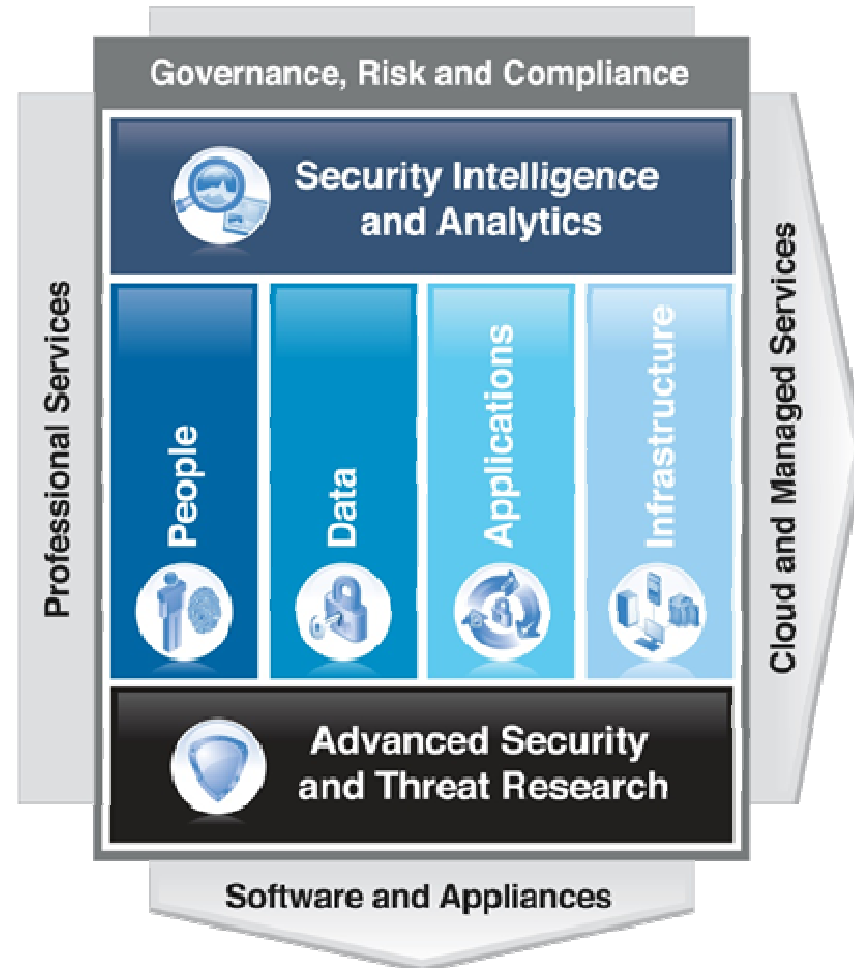


IBM delivers solutions across a security framework

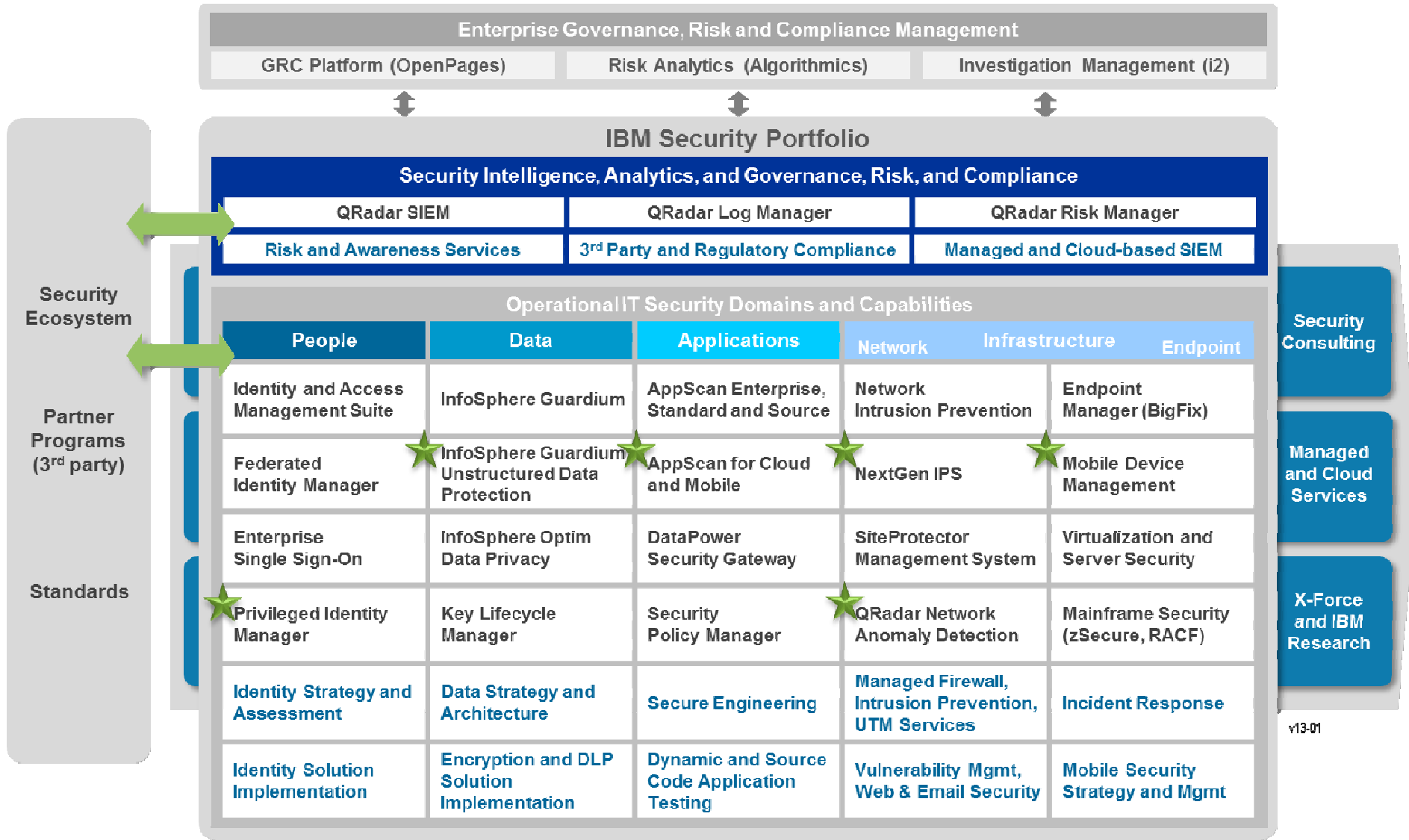
Intelligence

Integration

Expertise






















Intelligence: A comprehensive portfolio of products and services







★ New in 2012


Products Services

Analysts recognize IBM's superior products and performance

Domain	Segment / Report	Analyst Recognition	
Security Intelligence, Analytics and GRC	Security Information & Event Management (SIEM)	2012 	2010 
	Enterprise Governance Risk & Compliance Platforms	2011  2011	
People	Identity & Access Governance	2012 	
	User Provisioning / Administration	2012 	2012*** 
	Role Management & Access Recertification		2011 
	Enterprise Single Sign-on (ESSO)	2011* 	2010 
	Web Access Management (WAM)	2012** 	
Data	Database Auditing & Real-Time Protection		2011 
	Data Masking	2013 	
Applications	Static Application Security Testing (SAST)	2010 	2010 
	Dynamic Application Security Testing (DAST)	2011 	
Infrastructure	Network Intrusion Prevention Systems (NIPS)	2012 	2010 
	EndPoint Protection Platforms (EPP)	2013 	

Gartner  Leader  Visionary  Niche Player  Challenger

FORRESTER  Leader  Strong Performer  Contender

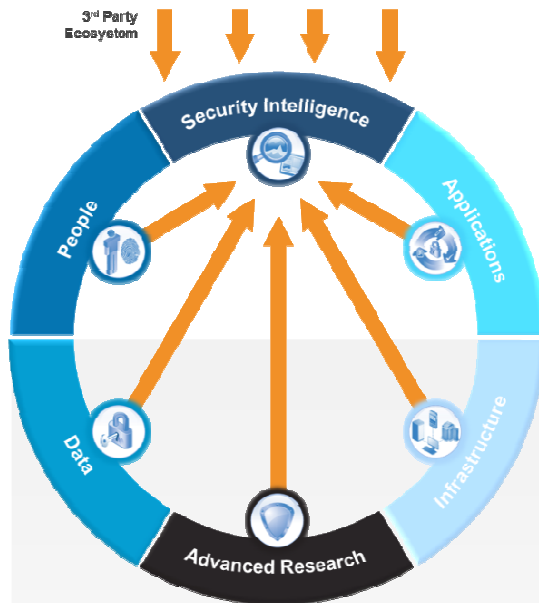
IDC  Leader (#1, 2, or 3 in segment)

* Gartner MarketScope (discontinued in 2012)
 ** Gartner MarketScope
 *** 2012 IDC MarketScape ranked IBM #1 in IAM

V13-05

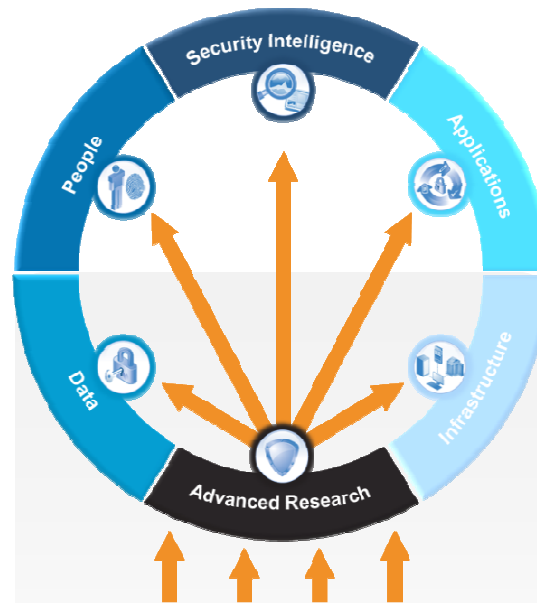
Integration: Increase security, collapse silos, and reduce complexity

Integrated Intelligence.



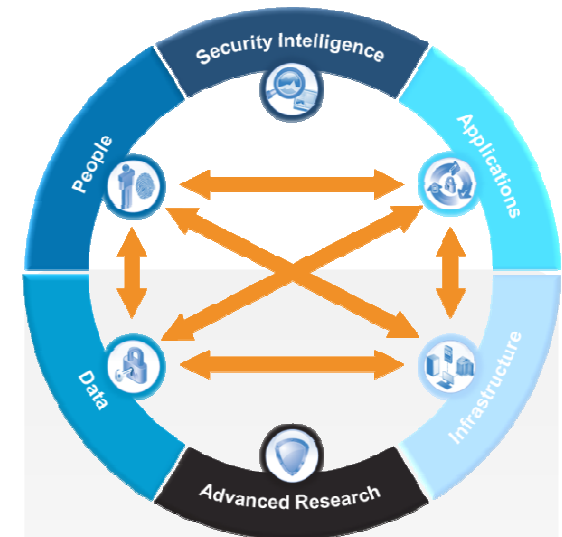
- Consolidate and correlate siloed information from hundreds of sources
- Designed to help detect, notify and respond to threats missed by other security solutions
- Automate compliance tasks and assess risks

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

IBM Security – A full range of security capabilities

Consulting Services

- 3700+ security consultants and architects
- Assess security risk and compliance, evolve security program
- **Why IBM?** Unique, practical approach based on our experience as an enterprise and service provider

Managed Services

- Globally available managed security services platform
- Manage security ops, detect and respond to emerging risk
- **Why IBM?** IBM's global coverage of security operations centers powered by unmatched cybersecurity analytics

Software Solutions

- Market leading solutions across the IBM Security Framework
- Help secure identities, data, applications, network and endpoints
- **Why IBM?** Integrated security portfolio, Cloud, mobile, threat security solutions, global threat research, and Security Intelligence

Intelligence

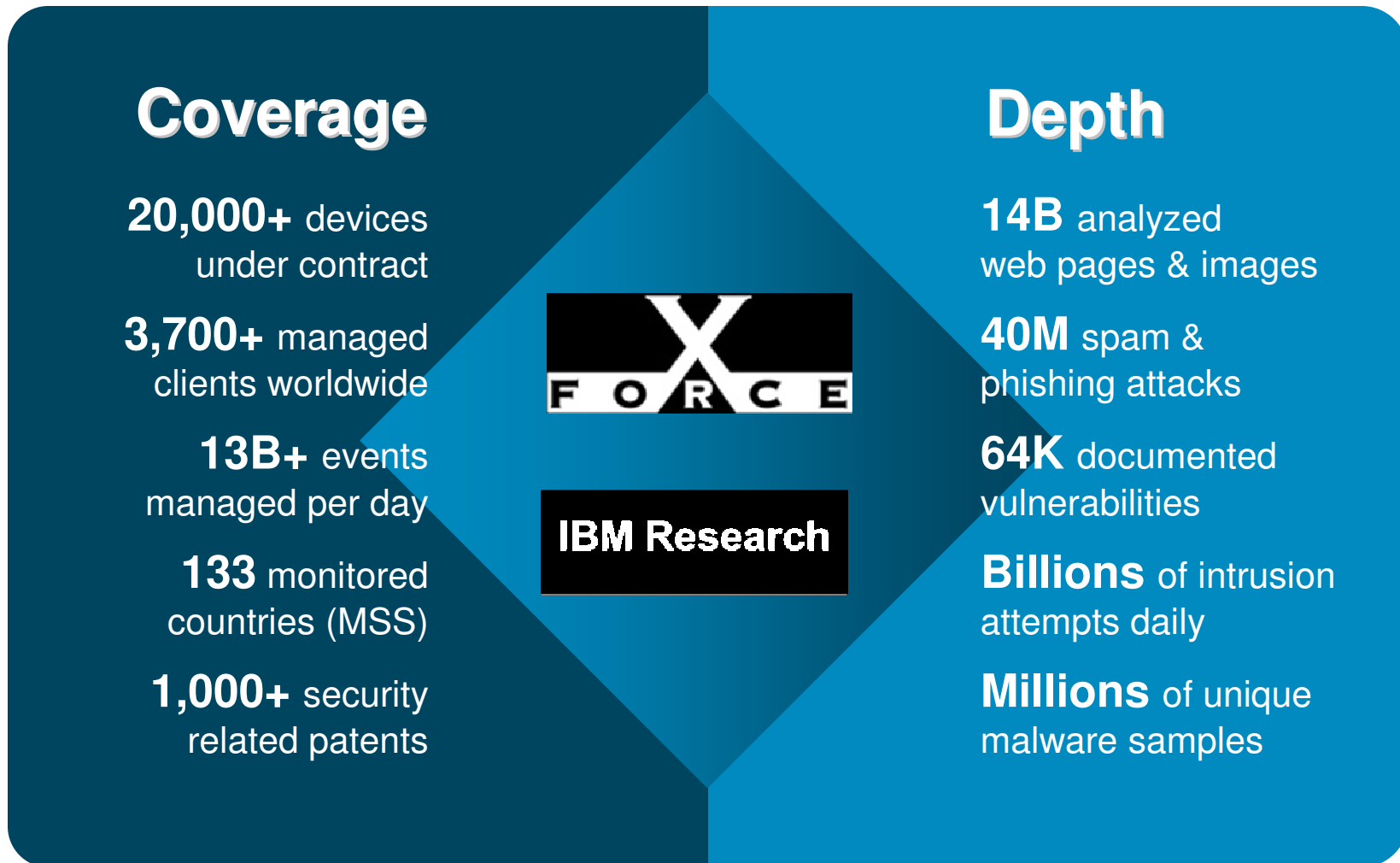


Integration

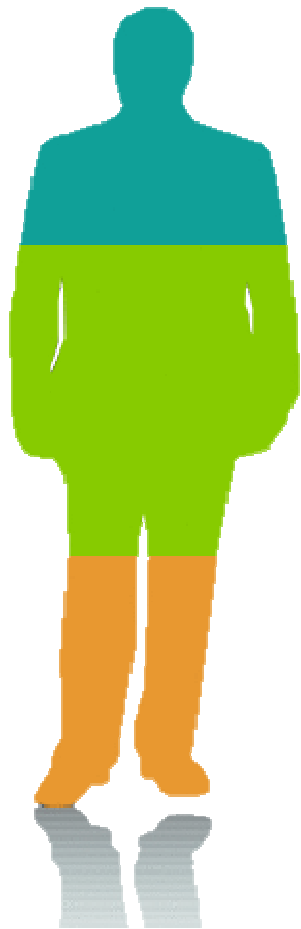


Expertise

Collaborative IBM teams monitor and analyze the latest threats



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
strategy



IBM Identity and Access Management Vision



Key Themes

Standardized IAM and Compliance Management

Expand IAM vertically to provide identity and access intelligence to the business; Integrate horizontally to enforce user access to data, app, and infrastructure

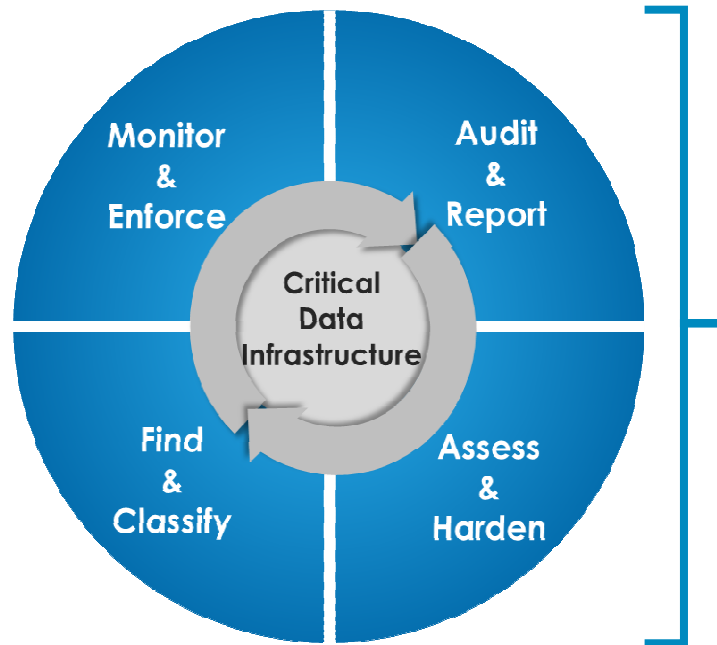
Secure Cloud, Mobile, Social Interaction

Enhance context-based access control for cloud, mobile and SaaS access, as well as integration with proofing, validation and authentication solutions

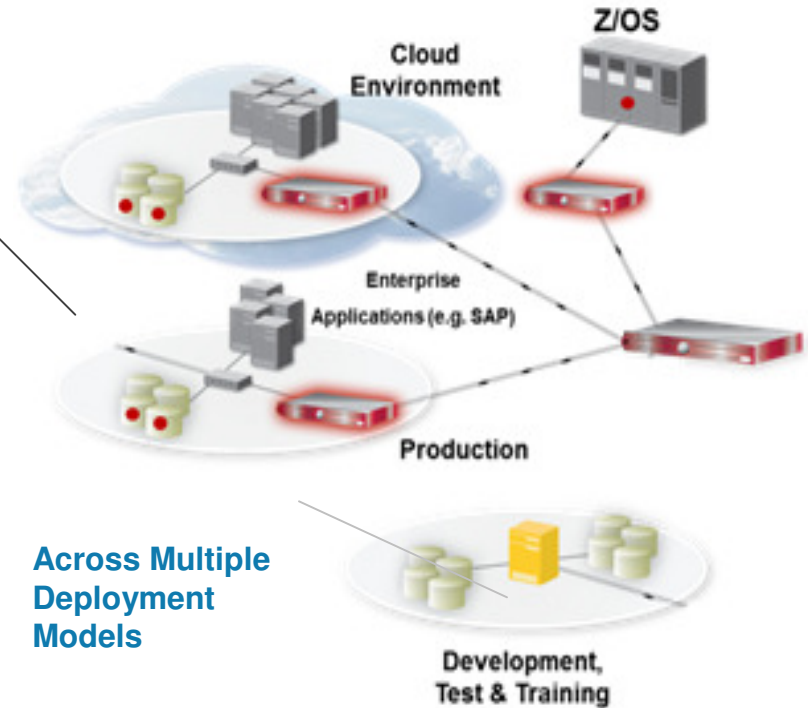
Insider Threat and IAM Governance

Continue to develop 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

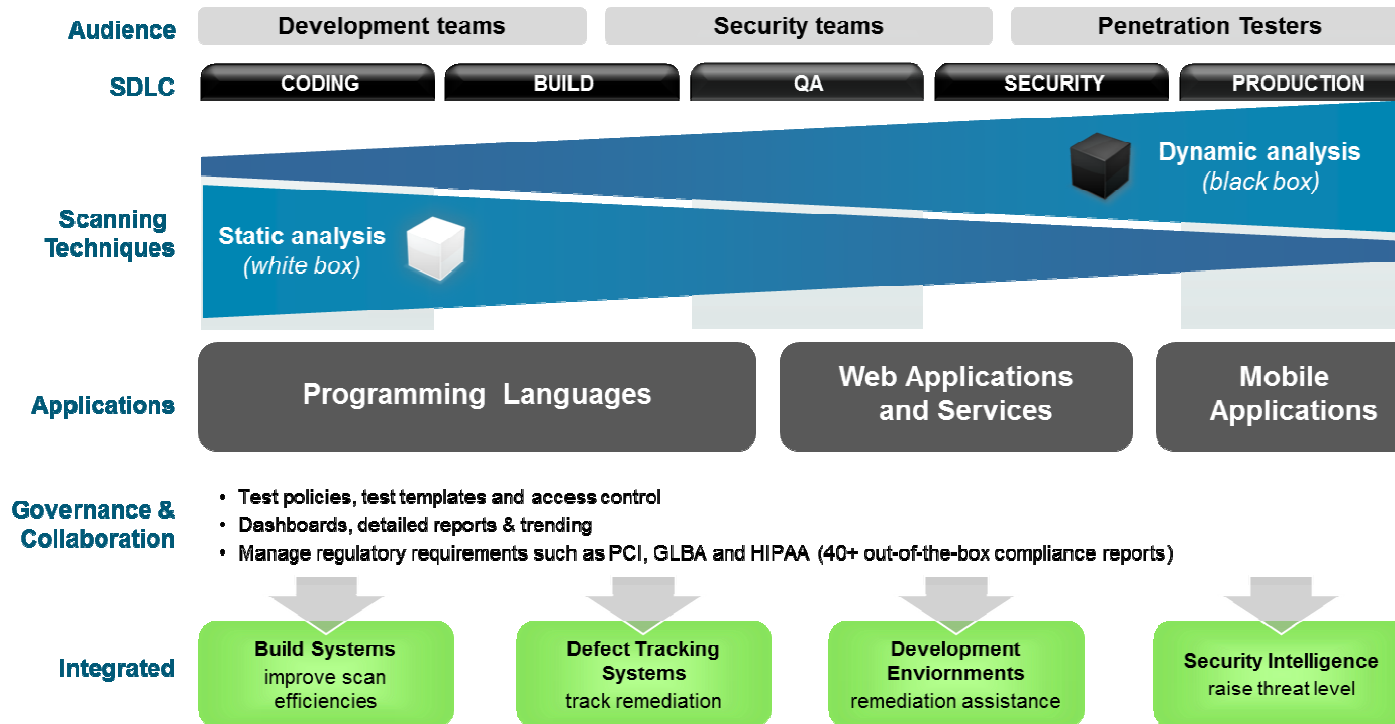
Enhanced Compliance Management

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

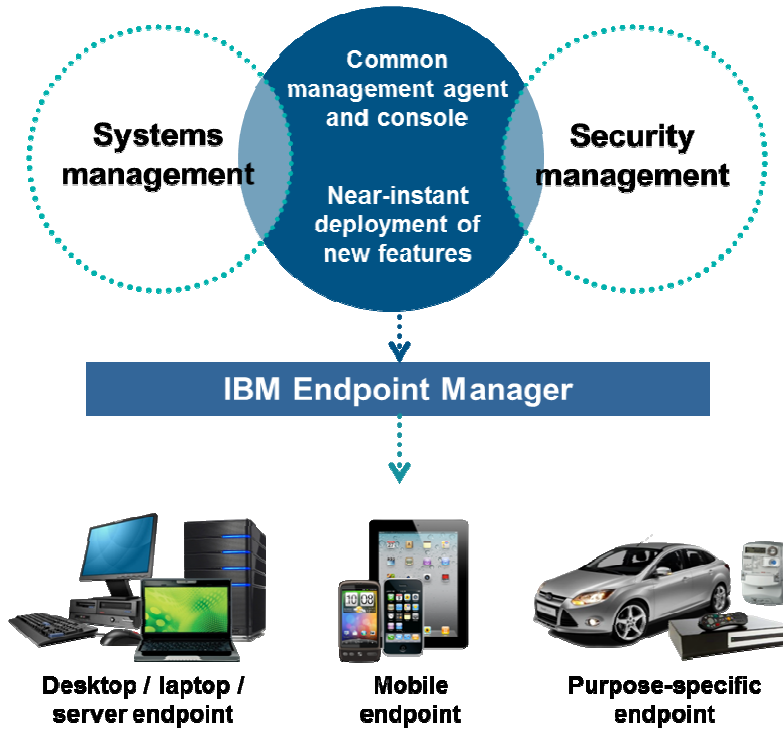
Simplified interface and accelerated ROI

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

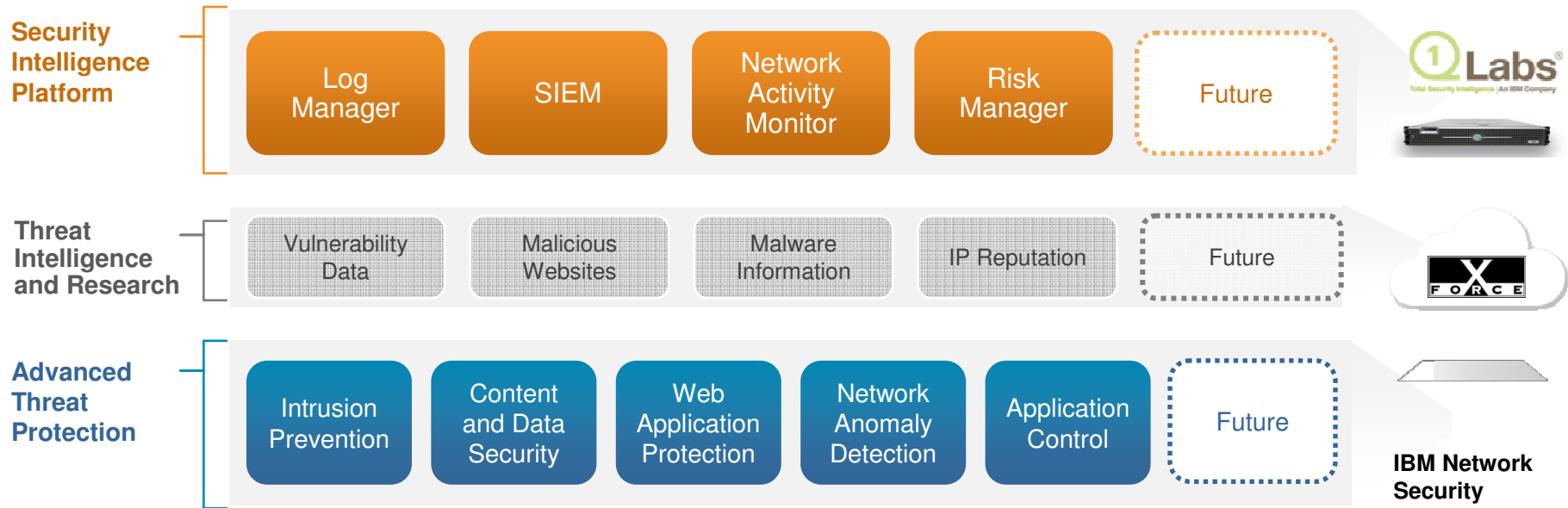
Expansion of Security Content

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

Infrastructure Protection – Advanced Threat



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

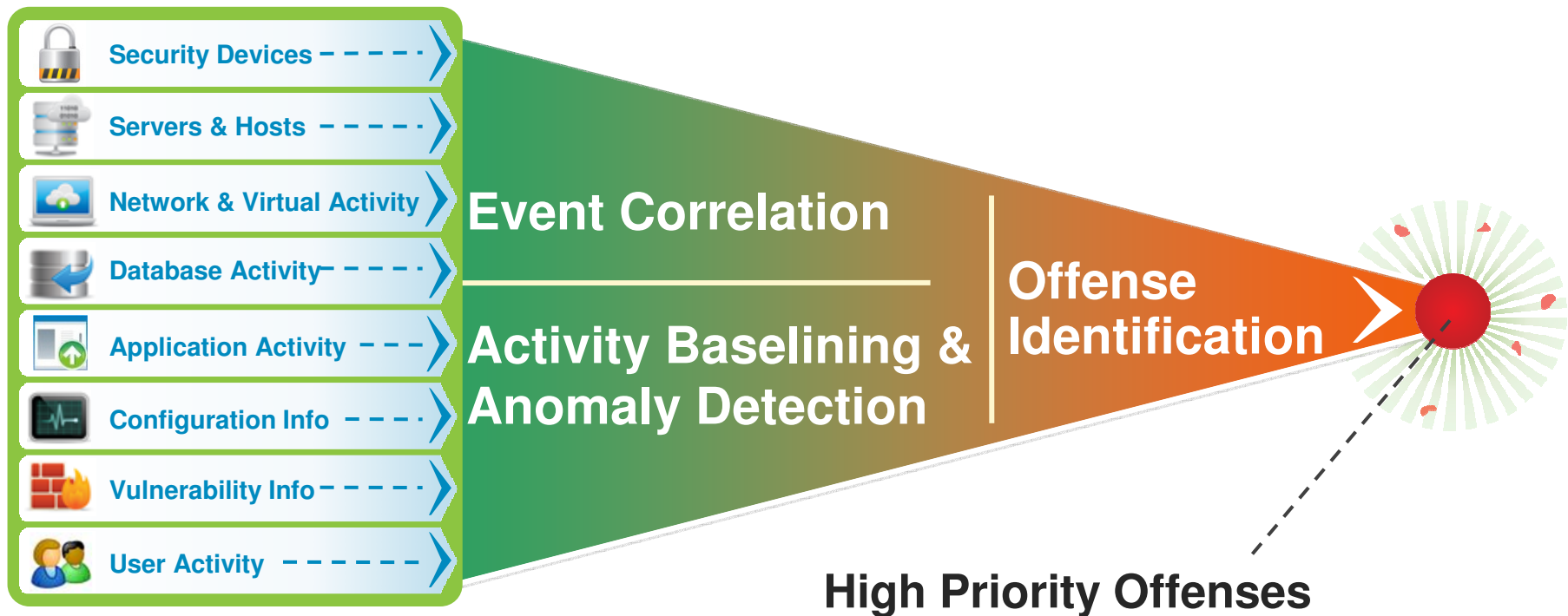
X-Force Threat Intelligence: The IBM Differentiator



- X-Force database** - extensive catalog of vulnerabilities
- Web filter database** – malicious or infected websites
- IP Reputation** – botnets, anonymous proxies, bad actors
- Application Identification** – web application information
- Vulnerability Research** – latest vulnerabilities and protections
- Security Services** – manage IPS for 3000+ Customers



Security Intelligence: Integrating across IT silos

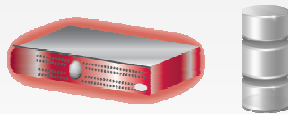


Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

All domains feed Security Intelligence



Correlate new threats based on X-Force IP reputation feeds



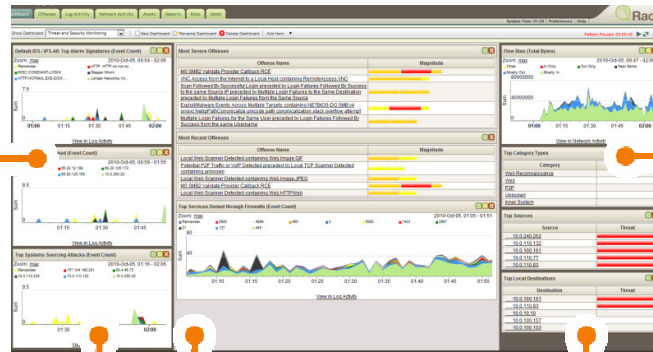
Guardium

Database assets, rule logic and database activity information

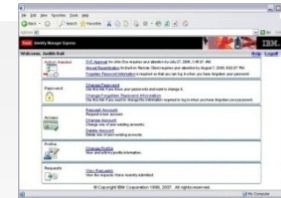


Tivoli Endpoint Manager

Endpoint Management vulnerabilities enrich QRadar's vulnerability database

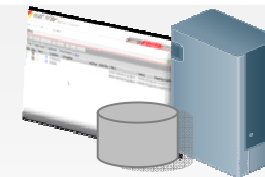


Hundreds of 3rd party information sources



Identity and Access Management

Identity context for all security domains w/ QRadar as the dashboard



AppScan Enterprise

AppScan vulnerability results feed QRadar SIEM for improved asset risk assessment

IBM Security Network Intrusion Prevention System

Flow data into QRadar turns NIPS devices into activity sensors

In 2013 we will continue to focus on solving the big problems

Advanced Threats

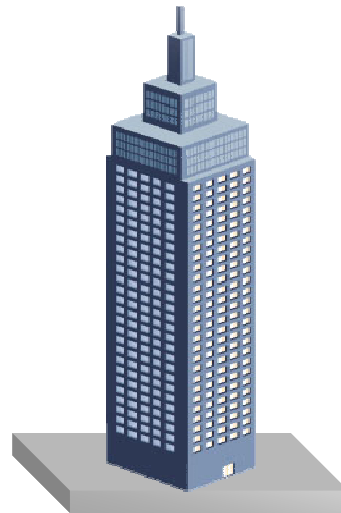
Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence



Advanced Persistent Threats
Stealth Bots Targeted Attacks
Designer Malware Zero-days

Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility



Enterprise Customers

Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed



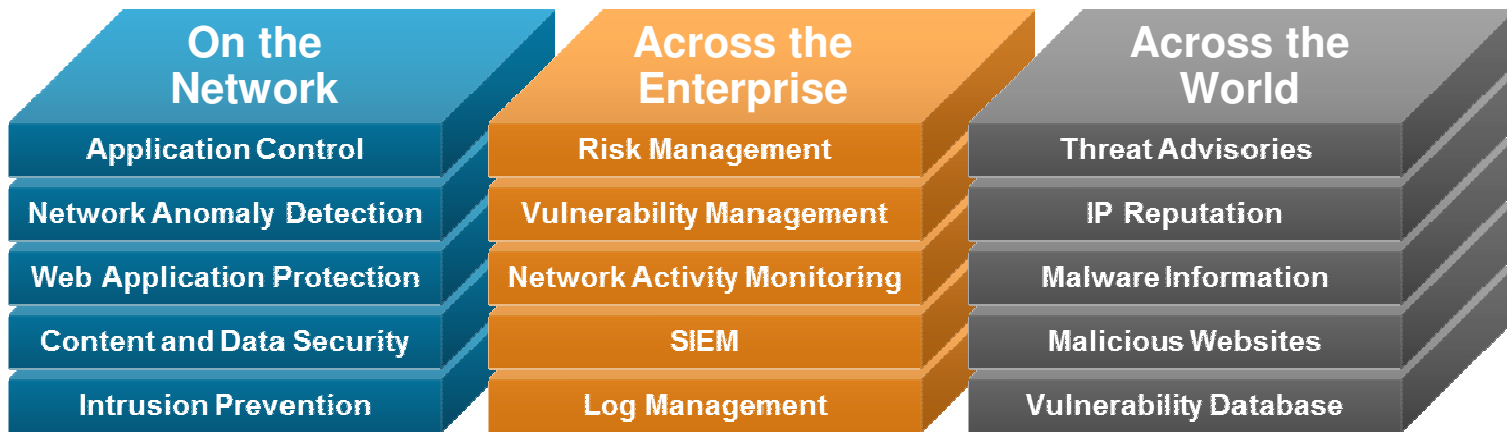
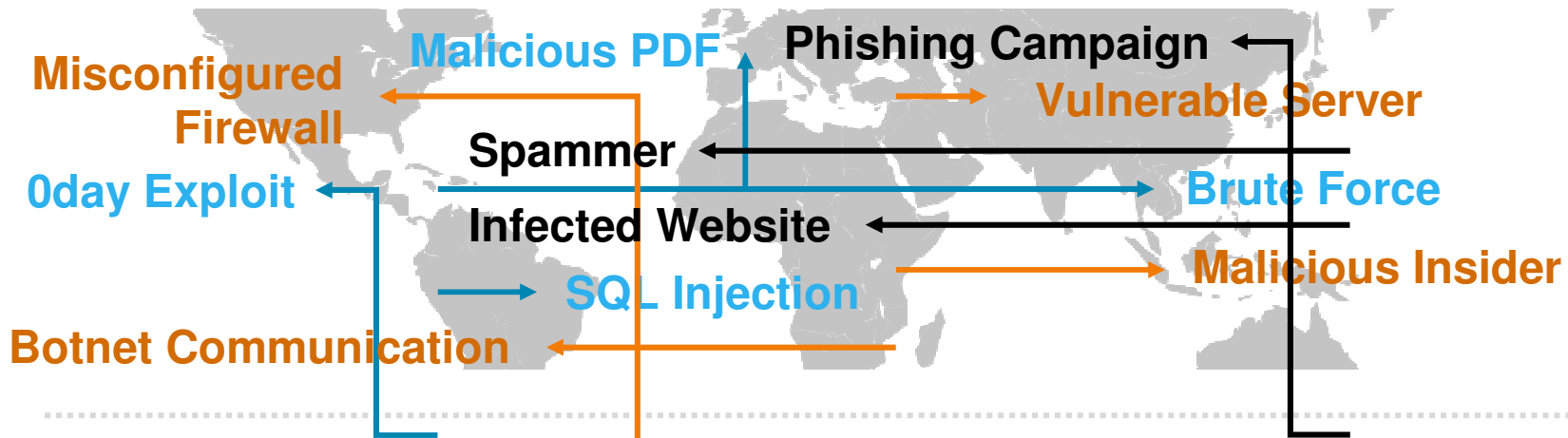
Regulation and Compliance

Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures



Better protection against sophisticated attacks

IBM Advanced Threat Protection Platform

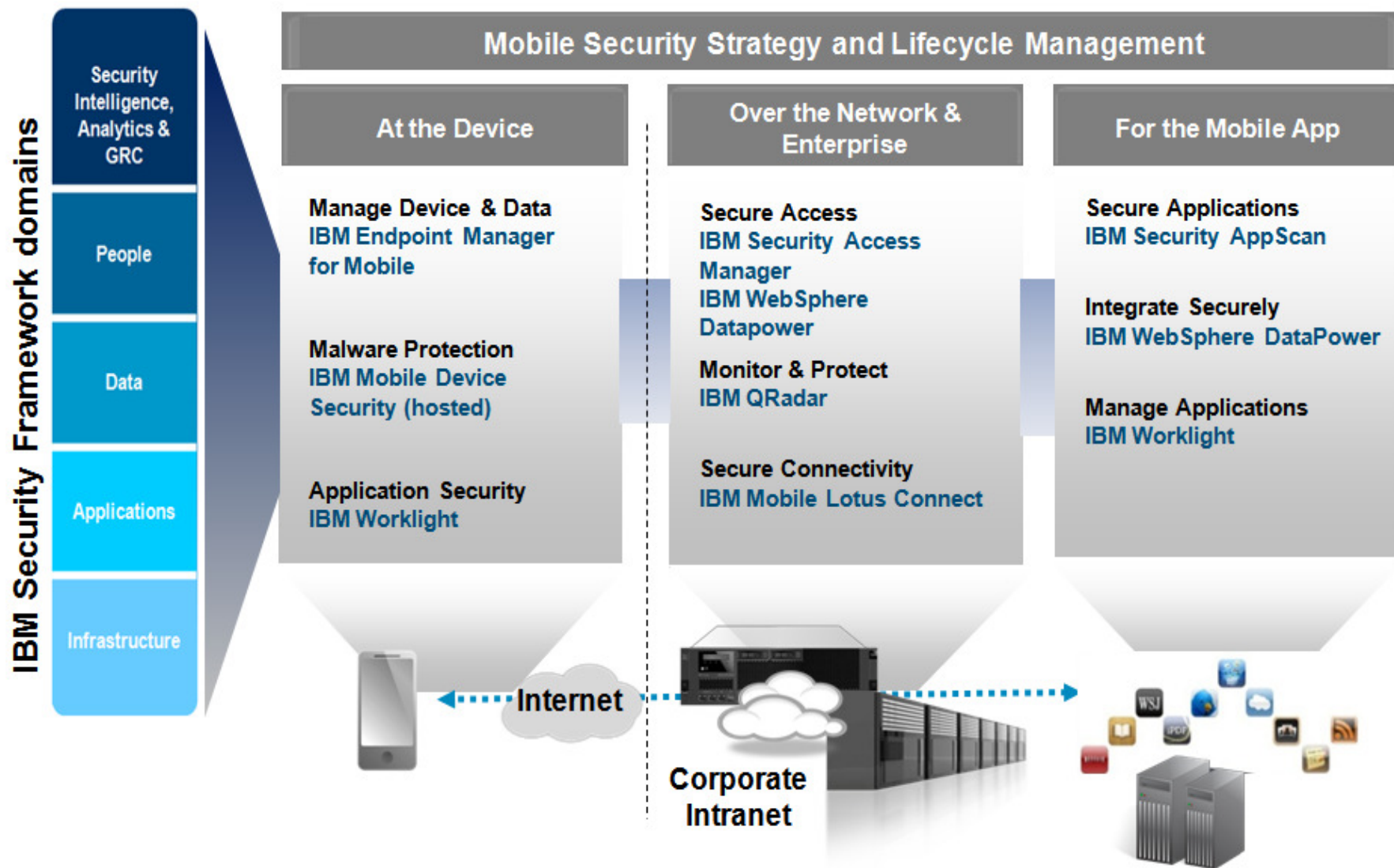


IBM Advanced Threat Protection

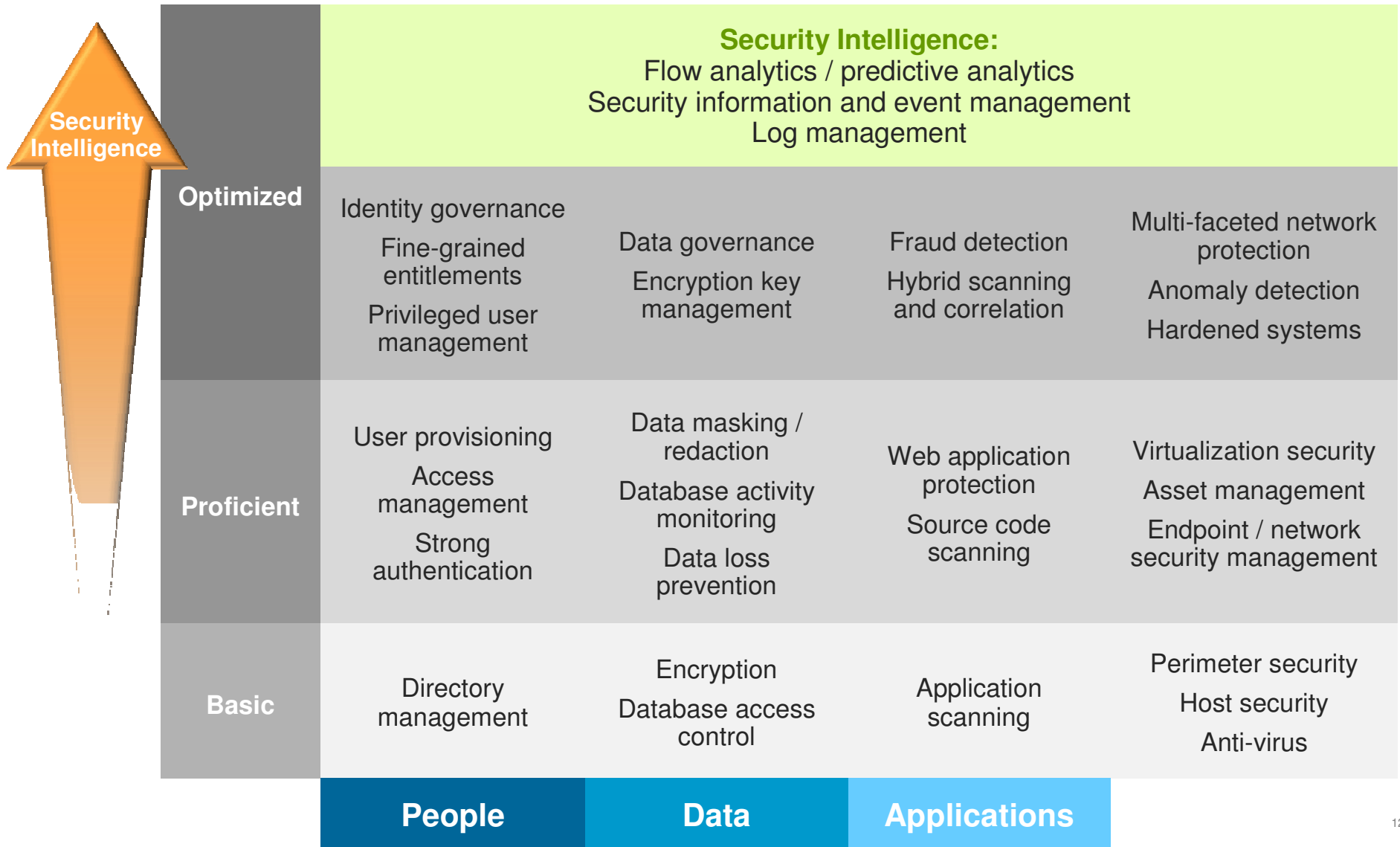
IBM QRadar Security Intelligence

IBM X-Force® Threat Intelligence

Securing the Mobile Enterprise with IBM Solutions



Security Intelligence is enabling progress to optimized security





ibm.com/security