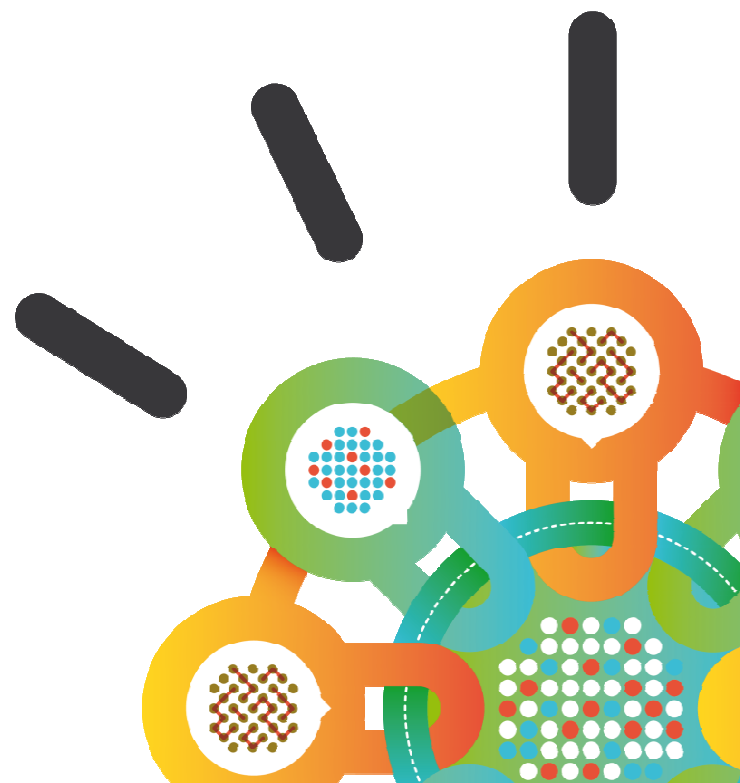Security Intelligence.
Think Integrated.

IBM Security Strategy
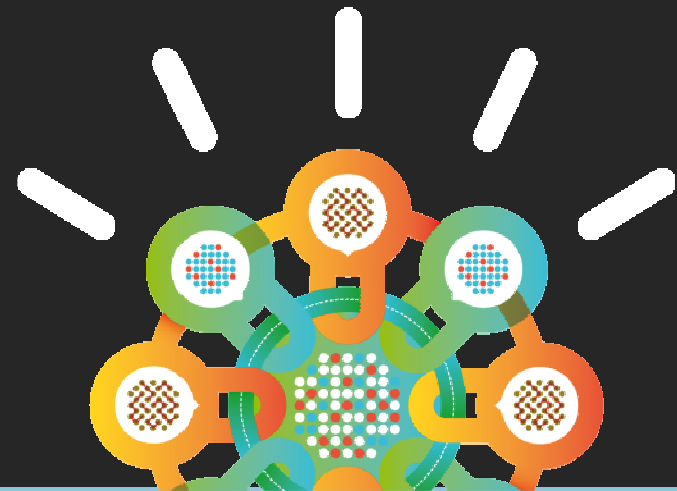
Intelligence, Integration and Expertise

September 2, 2014

Arnaud Delande

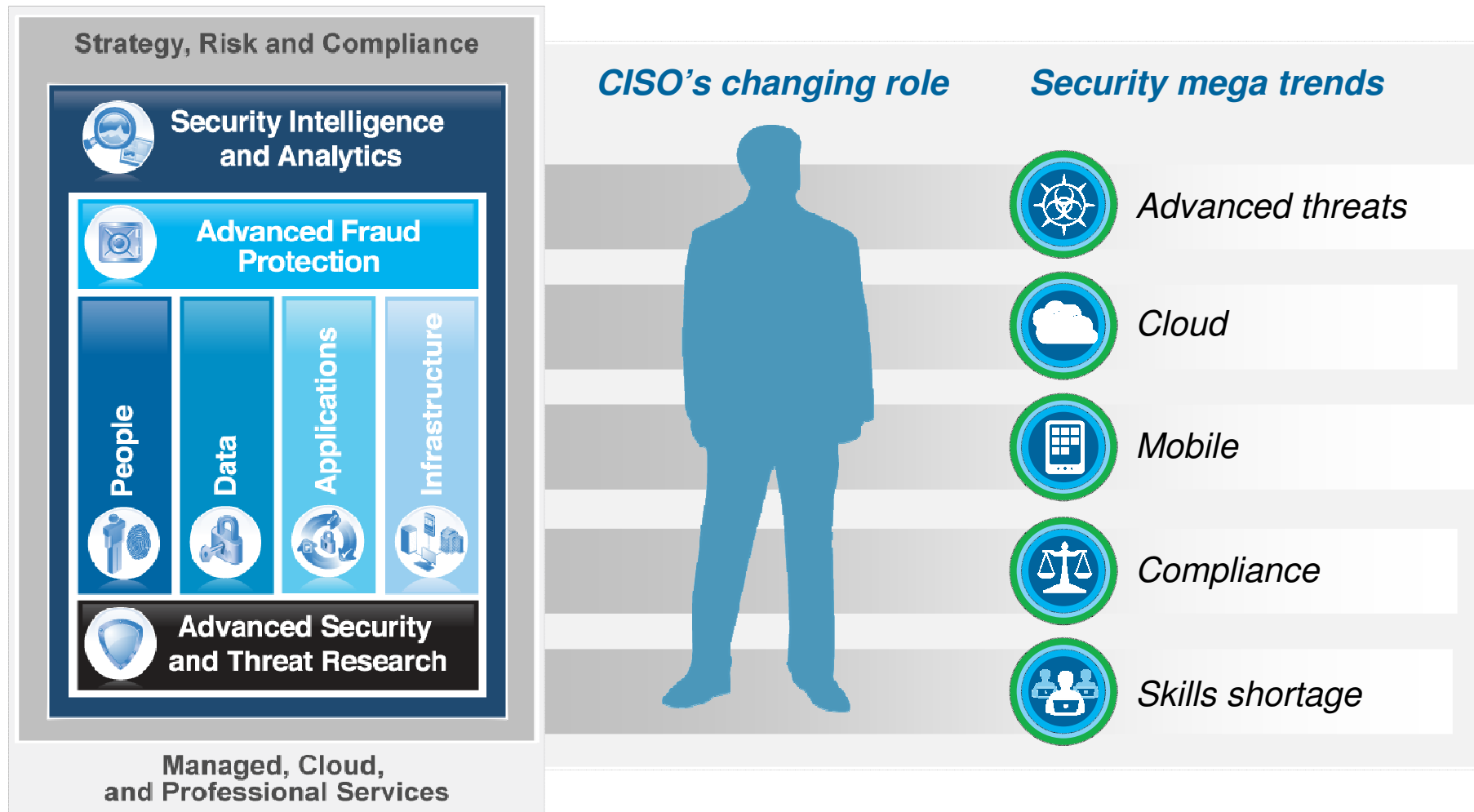France Security TechSales Manager

IBM is positioned to help

IBM Security strategy

Delivering intelligence, integration and expertise across a comprehensive framework

The IBM Security Framework

Strategy, Risk and Compliance

- Security Intelligence and Analytics
- Advanced Fraud Protection
- People
- Data
- Applications
- Infrastructure
- Advanced Security and Threat Research

Managed, Cloud, and Professional Services

CISO's changing role

Security mega trends

- Advanced threats
- Cloud
- Mobile
- Compliance
- Skills shortage

IBM Security market-changing milestones

Mainframe and server security
1976

Access management
1999

Identity management
Directory integration
2002
access360
METAMERGE
DASCOM

SOA management and security
2005
DATAPOWER

Network intrusion prevention
2006
INTERNET SECURITY SYSTEMS

Application security
Risk management
Data management
2007
watchfire
consul an IBM company
princeton softech an IBM Company

Enterprise single-sign-on
2008
ENCENTUATE An IBM Company

Application security
2009
OUNCE LABS an IBM company
Guardium

Database monitoring and protection
2010
NISC
BIGFIX An IBM Company

Information and analytics management
2011
Q1Labs

Endpoint management and security

Security intelligence
2012
IBM Security is created

Secure mobile management
Advanced fraud protection
2013
Trusteer
MaaS360 by Fiberlink

IBM Security Investment

- 6,000+ IBM Security experts worldwide
- 3,000+ IBM security patents
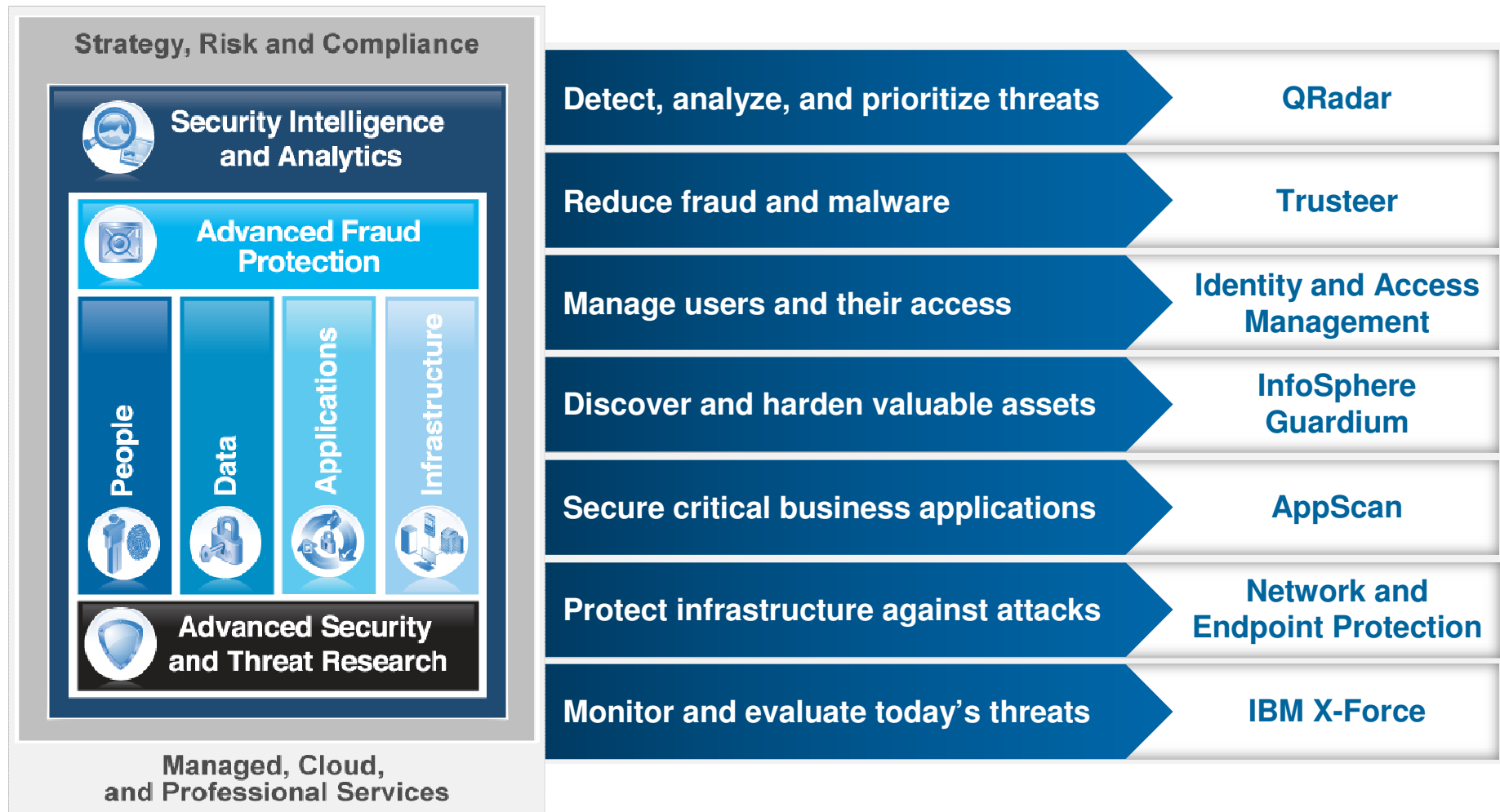- 4,000+ IBM managed security services clients worldwide
- 25 IBM Security labs worldwide

IBM Security

Integrated capabilities delivered across a comprehensive security framework

The IBM Security Framework

Strategy, Risk and Compliance

Security Intelligence and Analytics

Advanced Fraud Protection

People | Data | Applications | Infrastructure

Advanced Security and Threat Research

Managed, Cloud, and Professional Services

Detect, analyze, and prioritize threats	**QRadar**
Reduce fraud and malware	**Trusteer**
Manage users and their access	**Identity and Access Management**
Discover and harden valuable assets	**InfoSphere Guardium**
Secure critical business applications	**AppScan**
Protect infrastructure against attacks	**Network and Endpoint Protection**
Monitor and evaluate today's threats	**IBM X-Force**

IBM Security offers a comprehensive product portfolio

Security Intelligence and Analytics				
QRadar Log Manager	QRadar SIEM	QRadar Risk Manager	QRadar Vulnerability Manager	QRadar Incident Forensics

Advanced Fraud Protection			
Trusteer Rapport	Trusteer Pinpoint Malware Detection	Trusteer Pinpoint ATO Detection	Trusteer Mobile Risk Engine

People	Data	Applications	Network — Infrastructure — Endpoint	
Identity Manager	Guardium Database Activity Monitoring	AppScan Source	Network Intrusion Prevention (GX)	Trusteer Apex
Access Manager Family	Guardium Encryption Expert	AppScan Enterprise / Standard	Next Generation Network Protection (XGS)	FiberLink MaaS360
Privileged Identity Manager	Guardium / Optim Data Masking	DataPower Web Security Gateway	SiteProtector Threat Management	Endpoint Manager
Federated Identity Management				Host Protection
Directory Integrator / Directory Server	Key Lifecycle Manager	Security Policy Manager	QRadar Network Anomaly Detection	zSecure

IBM X-Force Research

IBM Security latest industry rankings

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 2013
Anti-Fraud	Web Fraud Detection (Trusteer ranking)	Leader 2013		
People	Federated Identity Management and Single Sign-On			Leader 2013
	Identity and Access Governance		Strong Contender 2013	
	Identity and Governance Administration	Visionary 2014		
	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 (dynamic and static)	Leader 2013		Leader 2013
Infrastructure	Network Intrusion Prevention Systems (NIPS)	Challenger 2013		
	EndPoint Protection Platforms (EPP)	Visionary 2014	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 January, 2014

At IBM, the world is our security lab

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

6,000+ IBM researchers, developers, and subject matter experts focused on security

3,000+ IBM security patents

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape

IP Reputation

Zero-day Research

URL / Web Filtering

Malware Analysis

Web Application Control

Vulnerability Protection

Anti-Spam

X FORCE

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape

- **Research** new attack techniques and develop protection for tomorrow's security challenges

- **Educate** our customers and the general public

- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

Integrated intelligence, protection, and research

Integrated Research
Stay ahead of the changing threat landscape

Integrated Intelligence
Consolidate and correlate information from hundreds of sources to detect threats missed by point solutions

Integrated Protection
Link security and vulnerability information across domains

Third-party Ecosystem

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

Strategy, Risk and Compliance

Security Intelligence and Analytics

Advanced Fraud Protection

People

Data

Applications

Infrastructure

Advanced Security and Threat Research

Managed, Cloud, and Professional Services

Intelligence

Integration

Expertise
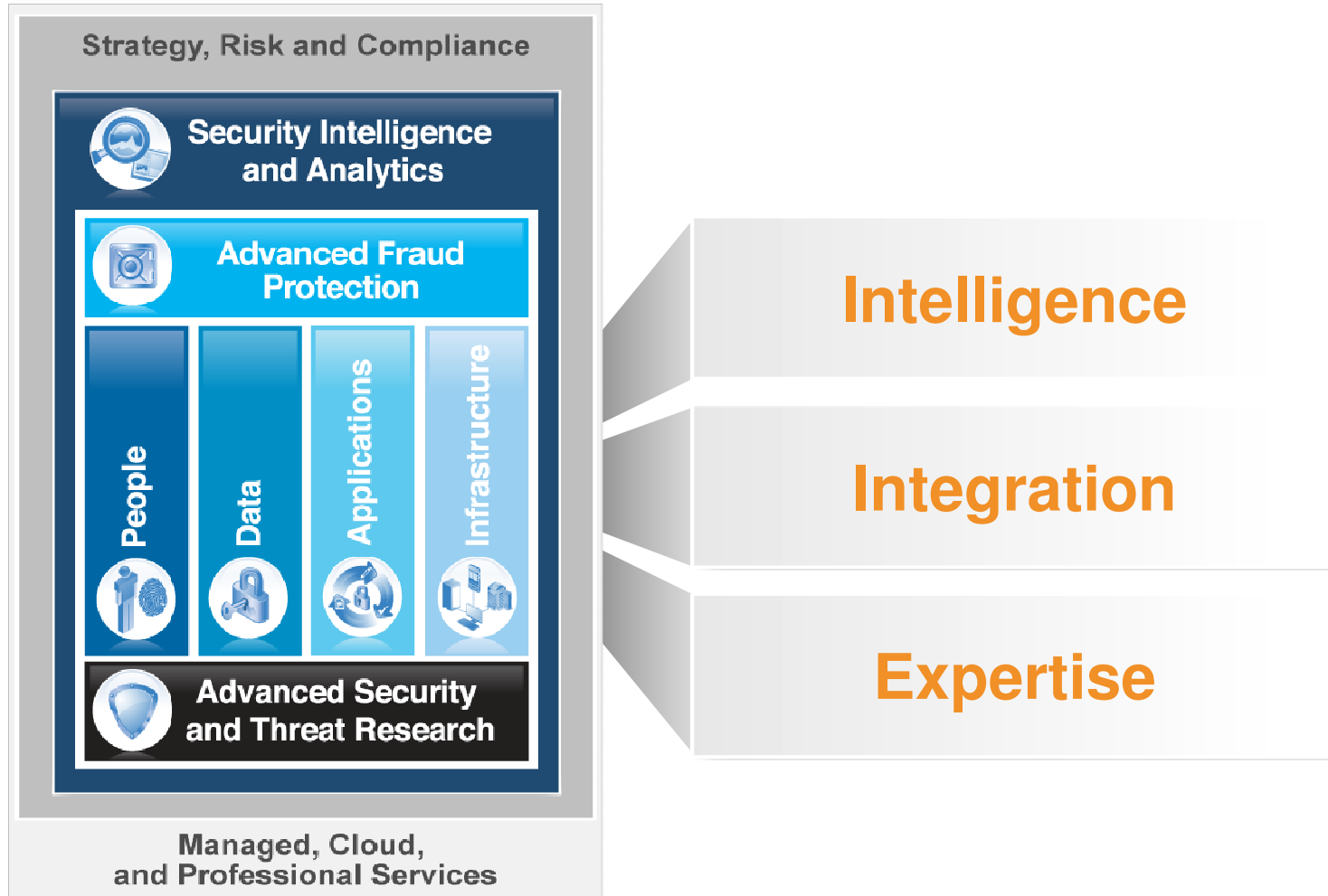
Solving complex
security problems

Security Intelligence and Analytics

Visibility into security posture and clarity around incident investigation

Extensive Data Sources

Integrated Dashboard

Embedded Intelligence

Log Management & Compliance Reporting

Real-time Analytics & Anomaly Detection

Prioritized Incidents

Vulnerability & Risk Management

Incident Evidence & Forensics
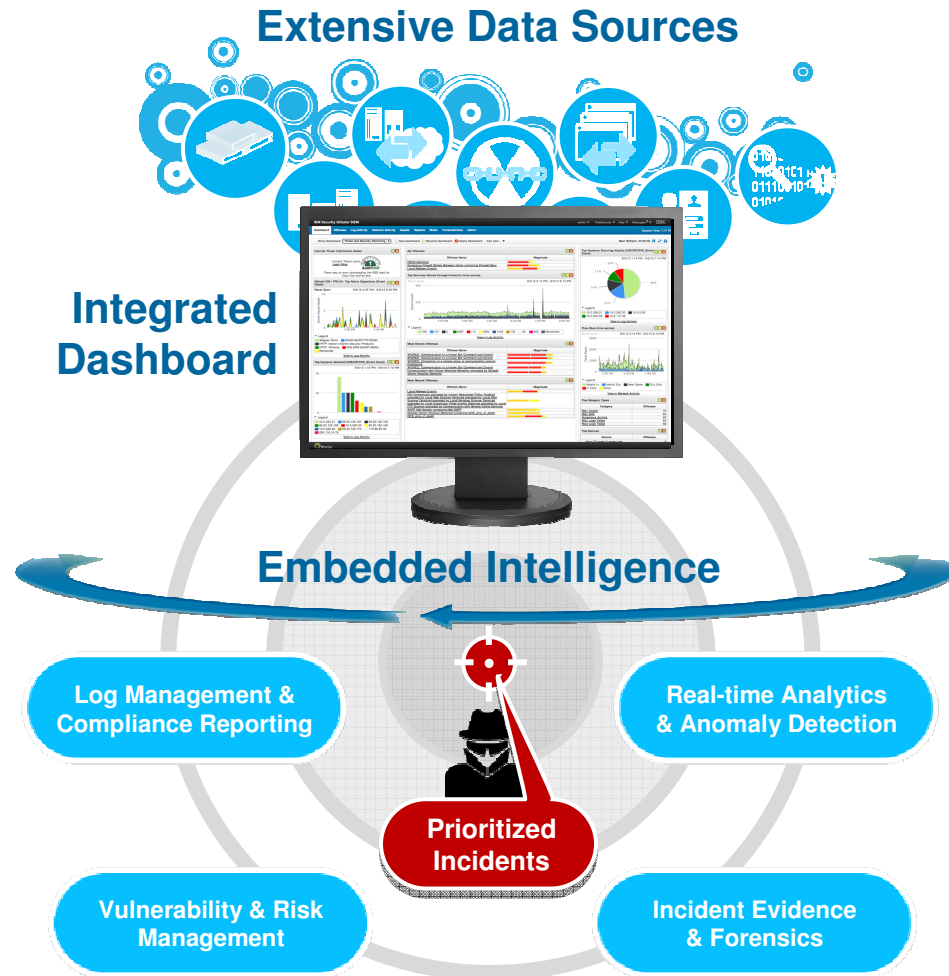
CLIENT SUCCESS

A Canadian financial services firm **analyzes**

30,000,000

security events per day to find

30

prioritized security offenses

IBM Security Solutions

- QRadar Log Manager
- QRadar SIEM
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Incident Forensics

Advanced Fraud Protection

Helping protect against financial fraud and advanced security threats

Trusteer
an IBM Company

Cybercrime Intelligence

Real-time threat data from millions of endpoints

Customer Protection

Account Takeover Detection

Malware Detection

Mobile Risk Engine

Clientless Fraud Prevention

Employee Protection

Customer Protection

Endpoint Security
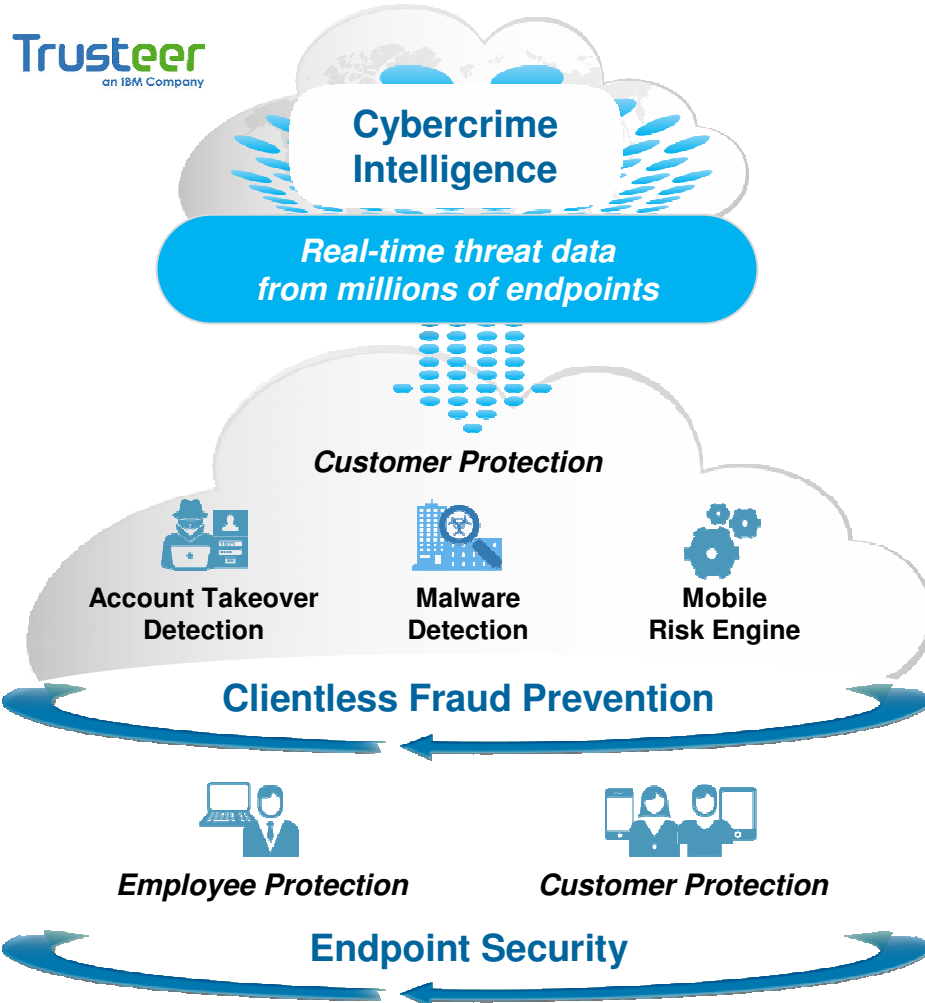
CLIENT SUCCESS

A large North American bank **reduced financial malware fraud incidents from**

500

to

0

in less than 3 months, moving the security border out to the customer

IBM Security Solutions

- Trusteer Apex
- Trusteer Rapport
- Trusteer Mobile
- Trusteer Pinpoint
- Trusteer Mobile Risk Engine

Identity and Access Management

Capabilities to help organizations secure the enterprise identity as a new perimeter

Safeguard mobile, cloud and social access

Prevent advanced insider threats

Deliver actionable identity intelligence

Simplify cloud integrations and identity silos

CLIENT SUCCESS

A large Asian paint company **governed user access and compliance in 17 countries for**

8,500 Employees, interns, contractors, and privileged administrators

25,000 Business partners and service providers

IBM Security Solutions

- Access Manager for Web
- Access Manager for Mobile
- Federated Identity Manager
- Identity Manager
- Privileged Identity Manager
- zSecure Suite

15

Data Security

Discover and harden your most valuable assets while enabling access

**Protect data at rest,
in motion, and in use**

Identify and Classify Data

Assess Vulnerabilities

Record Events

Protect Sensitive Data

Monitor Privileged Users
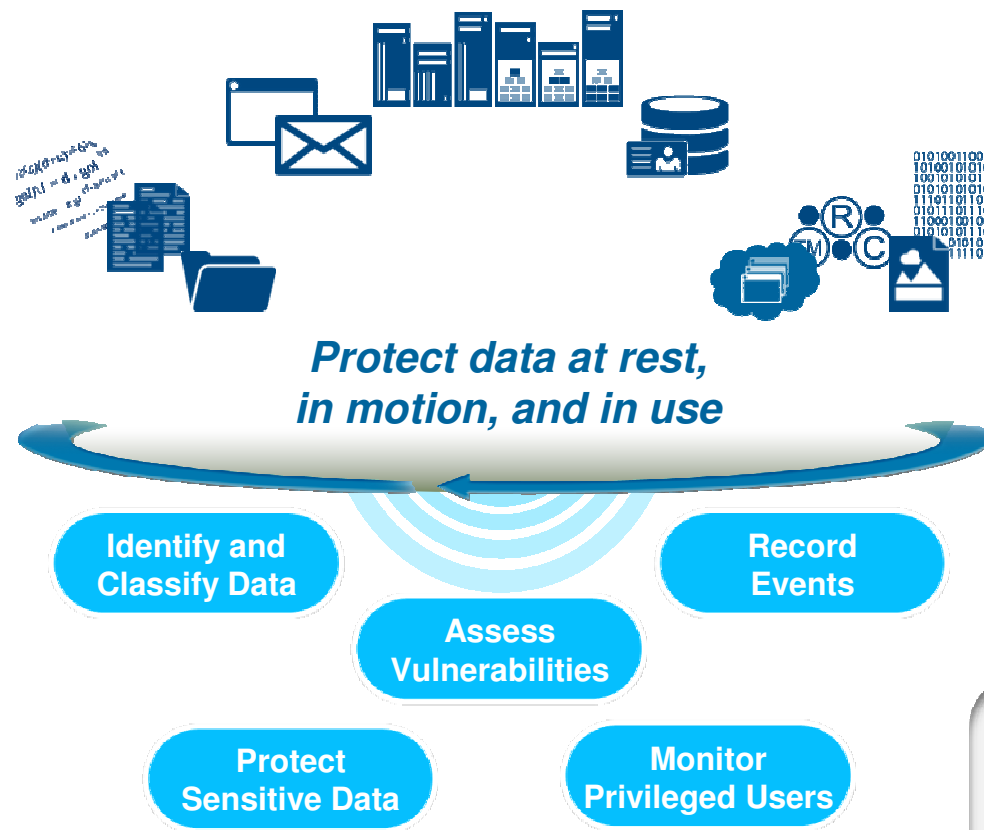
CLIENT SUCCESS

A global financial services company **secured 2,000 critical databases**

and saved

$21M

in compliance costs

IBM Security Solutions

- Guardium Database Activity Monitoring
- Guardium Encryption Expert
- Guardium / Optim Data Masking
- Key Lifecycle Manager

Application intelligence, policy and governance

Comprehensive, integrated, flexible solutions to help protect applications

Application Security Management

Test *Applications*

Protect *Deployed Applications*

Identify and mitigate risk

Dynamic Analysis

Static Analysis

Interactive Analysis

Mobile Analysis

Vulnerability Prioritization

Compliance Reporting

CLIENT SUCCESS

A computer services company with a small security team manages

2,500 applications

and drove a

33%

decrease in number of security issues found

IBM Security Solutions

- AppScan Source
- AppScan Enterprise / Standard
- DataPower Web Security Gateway
- Security Policy Manager

Infrastructure

In-depth security across network, servers, virtual servers, mainframes, endpoints, and mobile devices

Threat Management

Network Protection

Anomaly Detection

Host Protection

Endpoint Protection
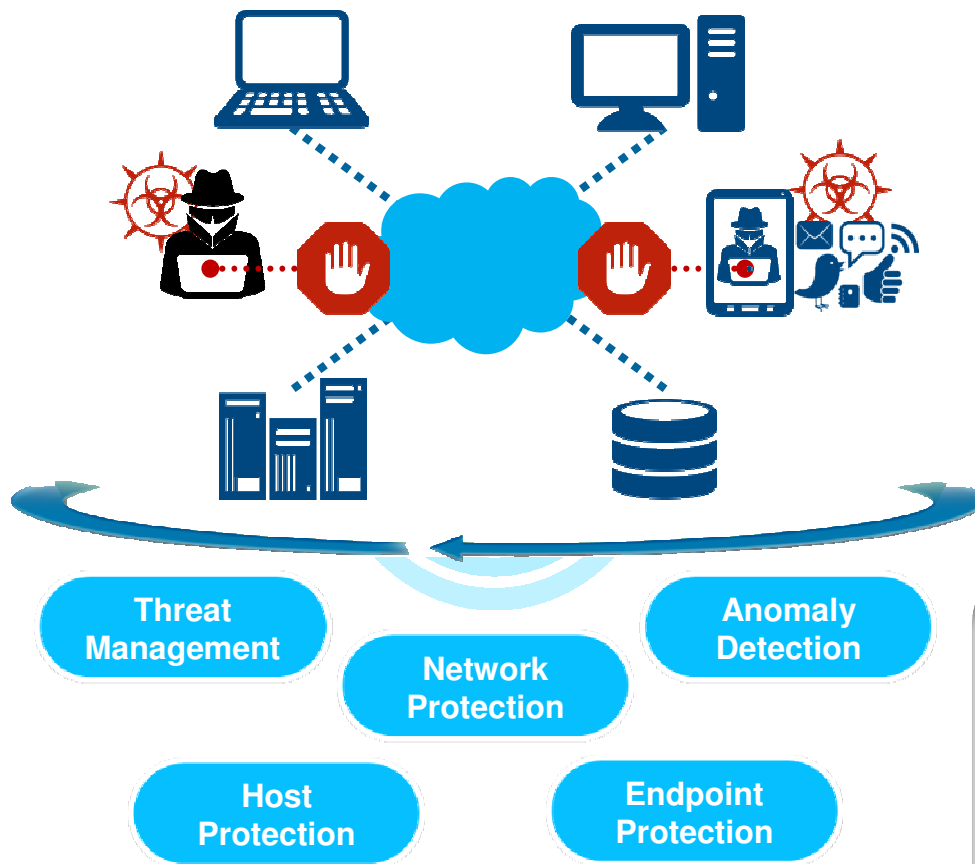
CLIENT SUCCESS

An international commodities exchange maintains system uptimes of over

99.9%

with

0

reported breaches in 3 years

IBM Security Solutions

- Next Generation Network Protection (XGS)
- Network Intrusion Prevention (GX)
- SiteProtector Threat Mgmt
- QRadar Network Anomaly Detection

- Trusteer Apex
- Fiberlink MaaS360
- Endpoint Manager
- Host Protection
- zSecure

IBM Intelligent Threat Protection

A dynamic, integrated system to disrupt the lifecycle of advanced attacks and prevent loss

Smarter Prevention

Trusteer Apex Endpoint Malware Protection

- Prevent malware installation
- Disrupt malware communications
- Limit the theft of user credentials

IBM Security Network Protection XGS

- Prevent remote network exploits
- Disrupt malware communications
- Limit the use of risky web applications

Security Intelligence

IBM Security QRadar Security Intelligence

- Discover and prioritize vulnerabilities
- Correlate enterprise-wide threats
- Detect suspicious behavior

Continuous Response

IBM Security QRadar Incident Forensics

- Retrace full attack activity
- Search for breach indicators
- Respond and harden defenses

IBM Emergency Response Services

- Get help to contain threats
- Leverage experts to analyze data
- Assess impact and plan strategically

Open Integrations

Ready for IBM Security Intelligence Ecosystem

- Share security context across multiple products
- 90+ vendors, 400+ products

Detect

Prevent

Respond

Threat Intelligence Network

DYNAMIC PROTECTION AND ANALYTICS PLATFORM
NETWORK | ENDPOINT   PHYSICAL | VIRTUAL | CLOUD

SECURITY PARTNER ECOSYSTEM

Global Threat Intelligence

IBM X-Force Threat Intelligence

- Leverage threat intelligence from multiple expert sources

Integrated security for public and private clouds

Protecting the cloud data center, and next-gen business and application platforms
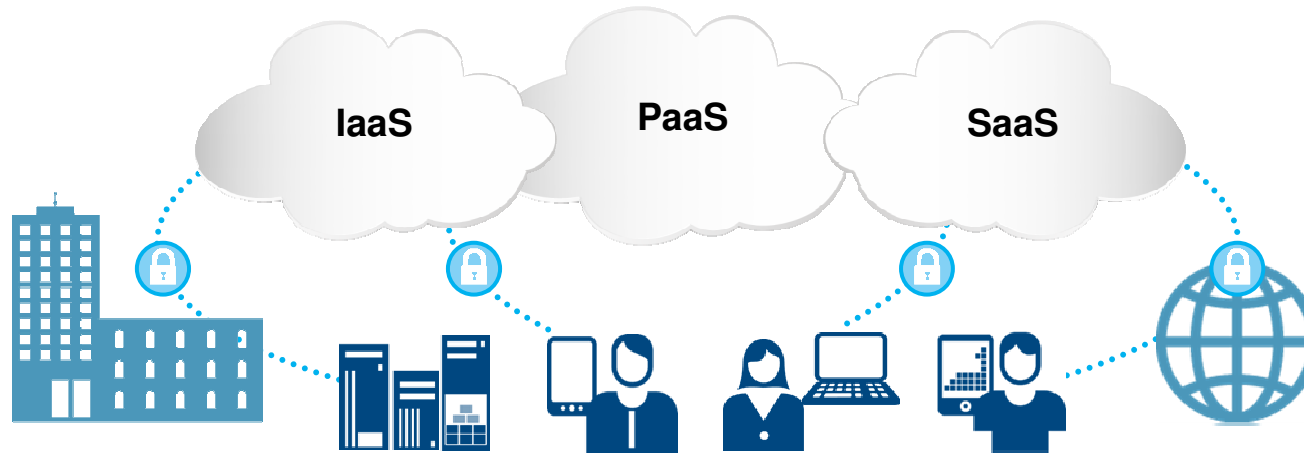
Manage Identities and Protect User Access	Monitor and Audit Applications and Data	Scan and Protect the Network from Threats	Establish Intelligence Across the Cloud

IBM Security Solutions

- Federated Identity Manager
- Directory Integrator
- Access Manager Virtual Appliance
- Privileged Identity Manager

- InfoSphere Guardium
- AppScan
- Key Life Cycle Manager

- Network Protection (XGS)
- Intrusion Prevention System (GX)

- QRadar SIEM
- QRadar Log Manager
- QRadar QFlow

IBM Security enterprise mobile protection

Personal and Consumer
Enterprise
DATA

Enterprise Applications and Cloud Services

Security Intelligence

Transaction Security
Application Security
Content Security
Device Security

Identity, Fraud, and Data Protection

Device Security	Content Security	Application Security	Transaction Security
Solutions to easily manage – from the cloud – a diverse set of mobile devices (corporate owned to BYOD)	Solutions to help secure file and document sharing across devices and SharePoint	Solutions to develop applications with security by design and protect enterprise data in both the applications you build and the applications you buy	Solutions to help protect mobile transactions with customers, business partners, and temporary workers that are not part of your enterprise mobile management framework

MaaS360

IBM Mobile Security Solutions

Trusteer
an IBM Company

IBM Mobile Security Services

Worklight

IBM Security AppScan

IBM Security Access Manager

Security Intelligence

A unified architecture for integrating mobile security information and event management (SIEM), anomaly detection, and log, configuration, and vulnerability management

IBM QRadar Security Intelligence Platform

Client success across advanced threats, cloud, and mobile

Advanced Threats

A financial services firm monitors threats to

600M+

customer accounts

with real-time alerts and proactive intelligence with

Zero

false positives

- IBM Network Protection
- IBM QRadar SIEM

Cloud

A global electronics firm moves its datacenter to the cloud and helps protect access to cloud-based applications for

10,000

employees

in North America while providing visibility to security events

- IBM Security Access Manager Virtual Appliance
- IBM Security QRadar SIEM

Mobile

A large U.S. children's hospital protects

3,000+

mobile devices

ensuring HIPAA compliance Installed and integrated with existing servers in just

90

minutes

- Fiberlink MaaS360

IBM Security: Helping clients optimize IT security

Strategy, Risk and Compliance

- Security Intelligence and Analytics
- Advanced Fraud Protection
- People
- Data
- Applications
- Infrastructure
- Advanced Security and Threat Research

Managed, Cloud, and Professional Services

- *Integrated Portfolio*
- *Managed and Professional Services*
- *Extensive Partner Ecosystem*
- *IBM Research*
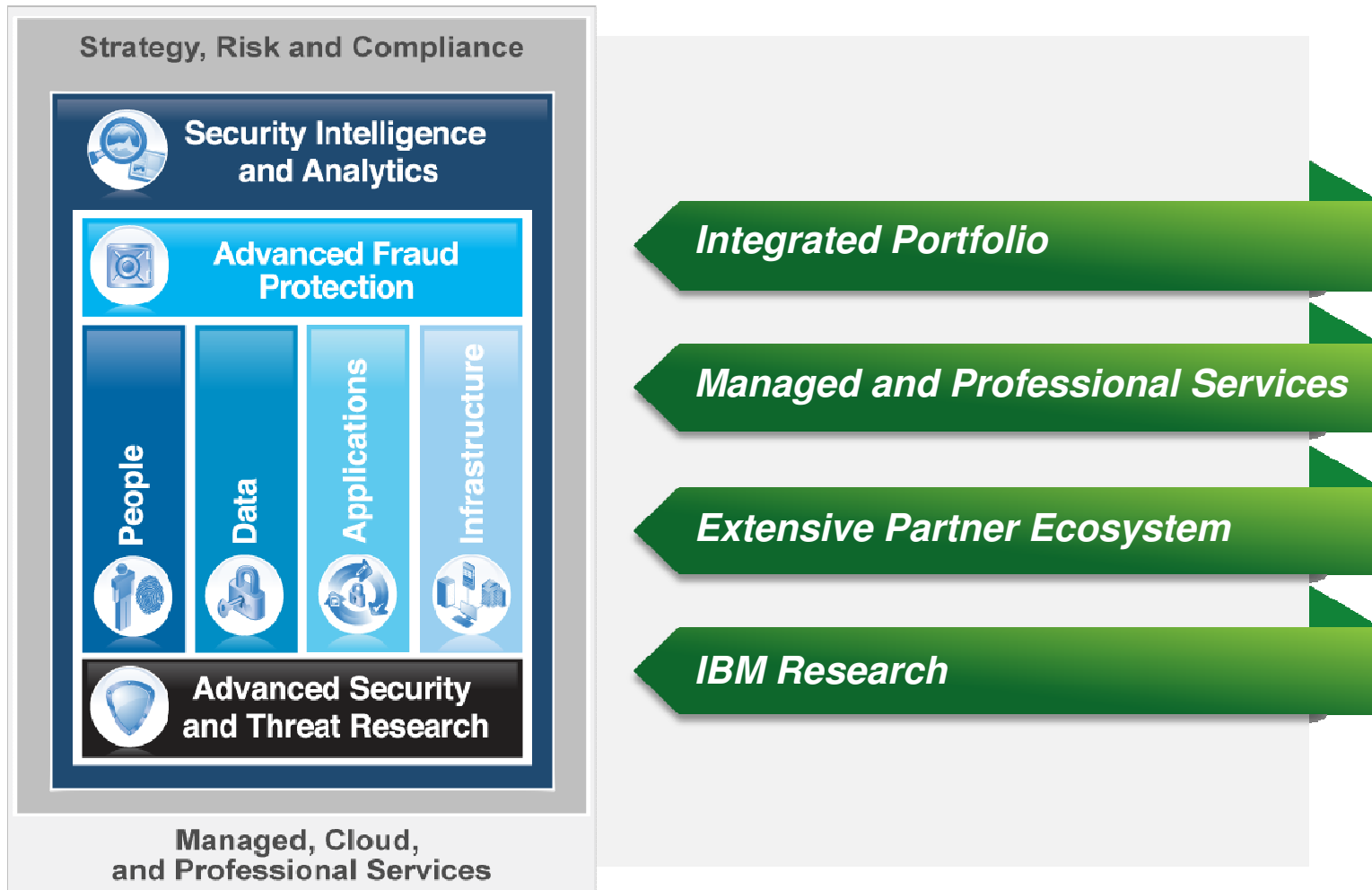
Disclaimer

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.

Thank You

www.ibm.com/security

IBM

A new security reality is here

Sophisticated attackers break through conventional safeguards every day

61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study
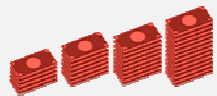
$3.5M

Average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Cloud, mobile, social and big data drive unprecedented change

70% of security executives have **cloud and mobile security** concerns

2013 IBM CISO Survey

614%

Mobile malware growth in just one year

2012 - 2013 Juniper Mobile Threat Report

Yesterday's security practices are unsustainable

83% of enterprises have difficulty finding the **security skills** they need

2012 ESG Research

85 **security tools** from

45 **vendors**

IBM client example

We are in an era of continuous breaches

Operational Sophistication	Near Daily Leaks of Sensitive Data	Relentless Use of Multiple Methods
IBM X-Force® declared **Year of the Security Breach**	**40% increase** in reported data breaches and incidents	**500,000,000+ records** were leaked, while the future shows no sign of change

2011   **2012**   **2013**

Attack types

🟨 SQL injection	⬛ Spear phishing	🟥 DDoS	🟫 Third-party software	🟧 Physical access	🟩 Malware	🟢 XSS	🟩 Watering hole	⬜ Undisclosed

Note: Size of circle estimates relative impact of incident in terms of cost to business.

Security is a board room discussion, and security leaders are more accountable than ever before

CEO	CFO/COO	CIO	CHRO	CMO
Loss of market share and reputation Legal exposure	Audit failure Fines and criminal charges Financial loss	Loss of data confidentiality, integrity and/or availability	Violation of employee privacy	Loss of customer trust Loss of brand reputation

Your Board and CEO demand a strategy

Source: Discussions with more than 13,000 C-suite executives as part of the IBM C-suite Study Series

A new approach to security is needed
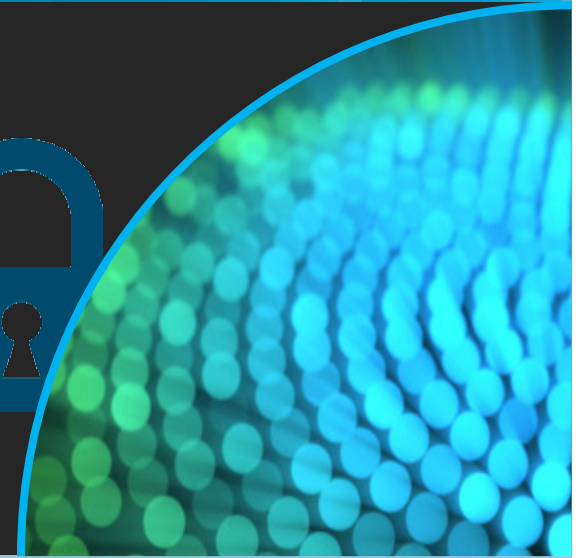
Strategic imperative #1

Use analytics and insights for smarter defense

| Use intelligence and anomaly detection across every domain | Build an intelligence vault around your crown jewels | Prepare your response for the inevitable |

Strategic imperative #2

Use cloud and mobile to improve security

| **Own the security agenda for innovation** | **Embed security on day one** | **Employ innovation to improve security** |

Strategic Imperative #3

Get help to develop an integrated approach

| **Develop a risk-aware security strategy** | **Deploy a systematic approach** | **Harness the knowledge of professionals** |

Security challenges are a complex, four-dimensional puzzle…

People	**EMPLOYEES** ATTACKERS **OUTSOURCERS** SUPPLIERS CONSULTANTS PARTNES **CONSUMERS**		
Data	**STRUCTURED** **UNSTRUCTURED** AT REST **IN MOTION**		
Applications	**SYSTEMS APPLICATIONS** WEB APPLICATIONS **WEB 2.0** **MOBILE APPLICATIONS**		
Infrastructure	DATACENTERS **PCs** LAPTOPS **MOBILE** **CLOUD** NON-TRADITIONAL		
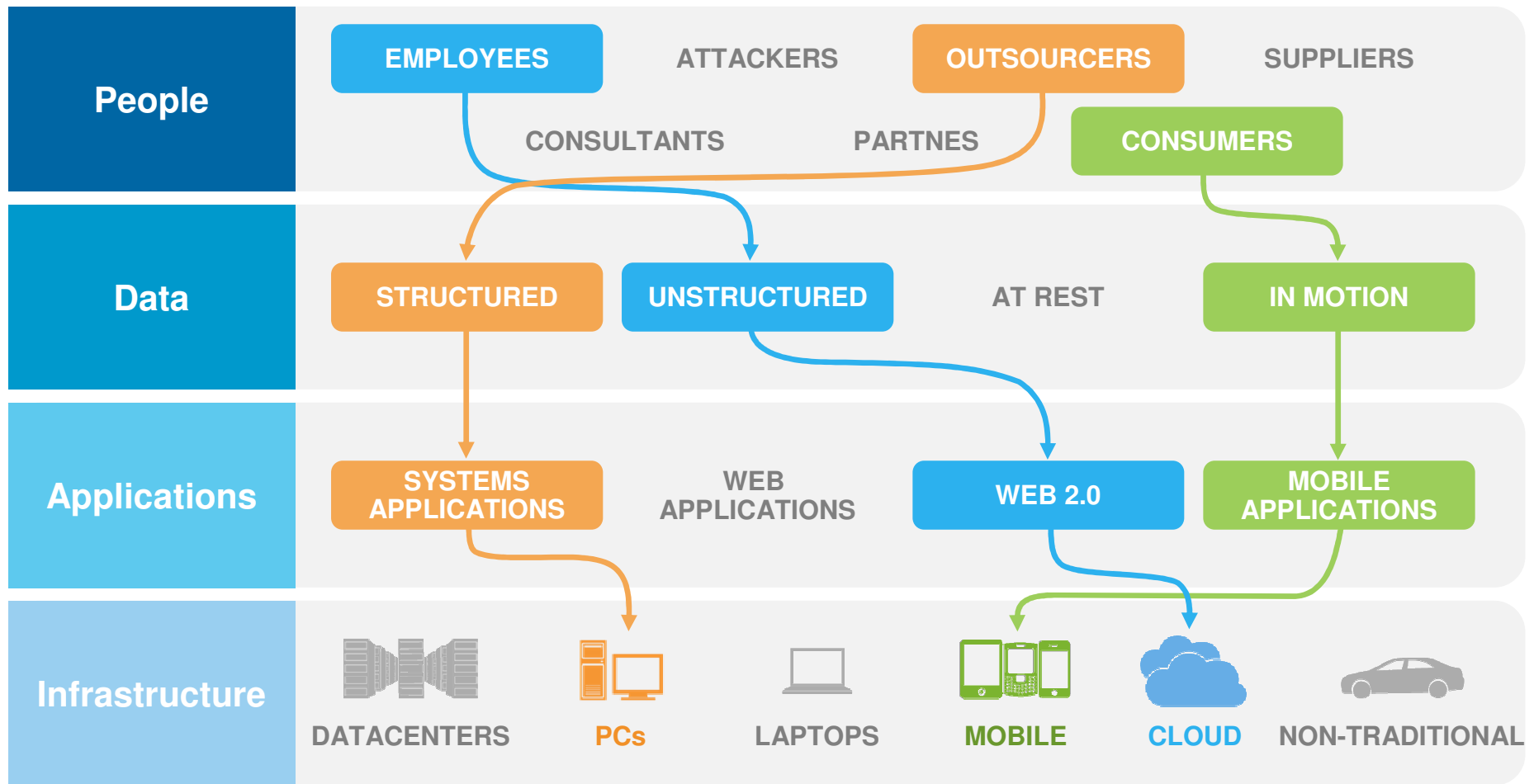
…a holistic approach is needed

IBM Security capabilities to help reach security maturity

ADVANCED FRAUD PROTECTION
- Prevent transactions from malware infected endpoints
- Login challenge questions
- Device ID rules

SECURITY INTELLIGENCE
- Predictive analytics
- Flow analysis
- Big data workbench
- Threat modeling
- SIEM
- Vulnerability management
- Log management

INFRASTRUCTURE
- Protocol analysis
- Anomaly detection
- Virtualization security
- App state awareness
- Endpoint / network security management
- Perimeter security
- Host security
- Anti-virus

PEOPLE
- Identity governance
- Fine-grained entitlements
- Privileged user management
- User provisioning
- Access management
- Directory management

DATA
- *Crown Jewel* protection
- Data governance
- Data masking
- DB activity monitoring
- Data loss prevention
- Encryption / key management

APPLICATIONS
- Hybrid scanning and correlation
- Mobile app scanning
- Web application protection
- Source code scanning
- Application scanning

ADVANCED
BASIC

- Advanced Threat
- Cloud
- Mobile
- Compliance