Stream Keynote 4: Security & Compliance

Pulse2012

Optimizing the World's Infrastructure

Brendan Hannigan

GM, IBM Security Systems

Sandy Bird

CTO, IBM Security Systems

Pulse2012

Optimizing the World's Infrastructure

IBM Security: Intelligence. Integration. Expertise.

3 Takeaways

IT is at a crossroads, with organizations facing a threat landscape that is increasingly complex and that requires a fundamentally different approach to security. Clients want an integrated view of security and existing point products are not meeting their needs

1. IBM’s Security Intelligence solutions leverage real time processing and predictive analytics capabilities to help clients tackle difficult security challenges such as insider threat and advanced persistent threat

2. Critical controls are becoming more optimized and integrated across key security domains such as identity management, application security, and advanced network security

3. IBM has committed major resources to and organized around a broad, integrated framework of products and solutions to help organizations meet current and emerging threats

The Journey Toward a Smarter Planet Continues

Smart Supply Chains

Smart Countries

Smart Retail

Smart Water Management

Smart Weather

Smart Energy Grids

INSTRUMENTED

INTERCONNECTED

INTELLIGENT

Smart Oil Field Technologies

Smart Regions

Smart Healthcare

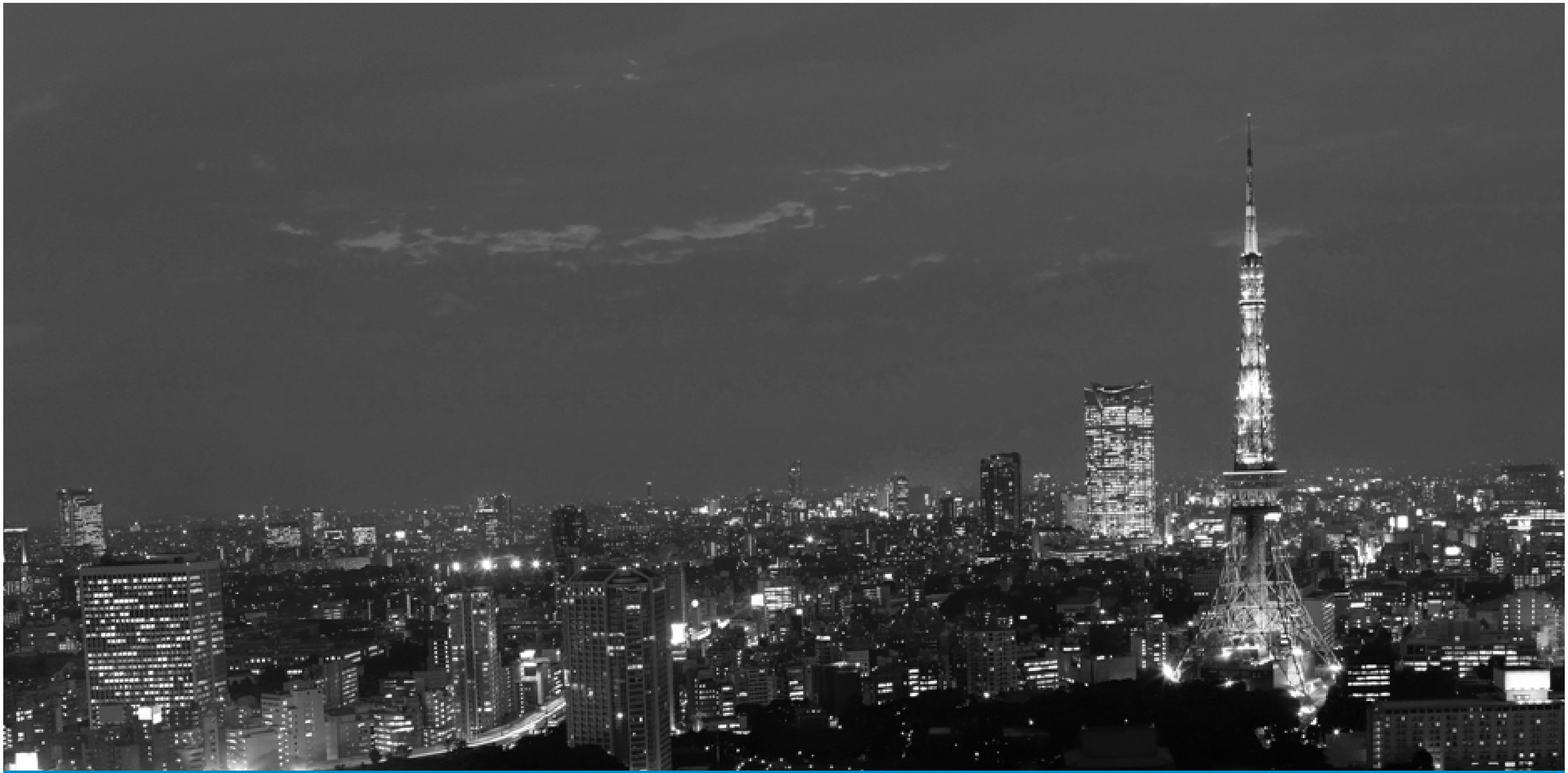
Smart Traffic Systems

Smart Cities

Smart Food Systems

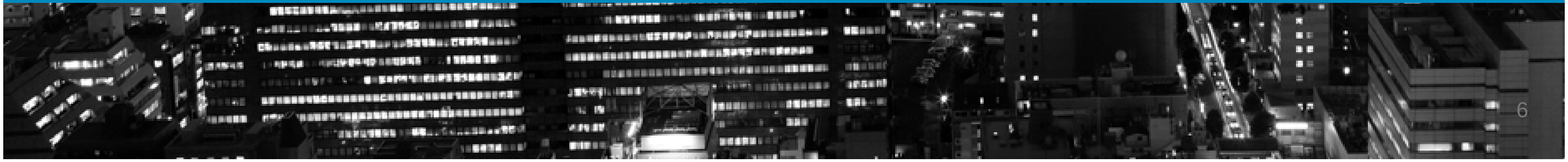
ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new motivations from cyber crime to state sponsored to terror inspired.



CLOUD

Continued movement of business to new platforms including cloud, virtualization, mobile, social business and more. Everything is everywhere.



CONSUMERIZATION OF IT

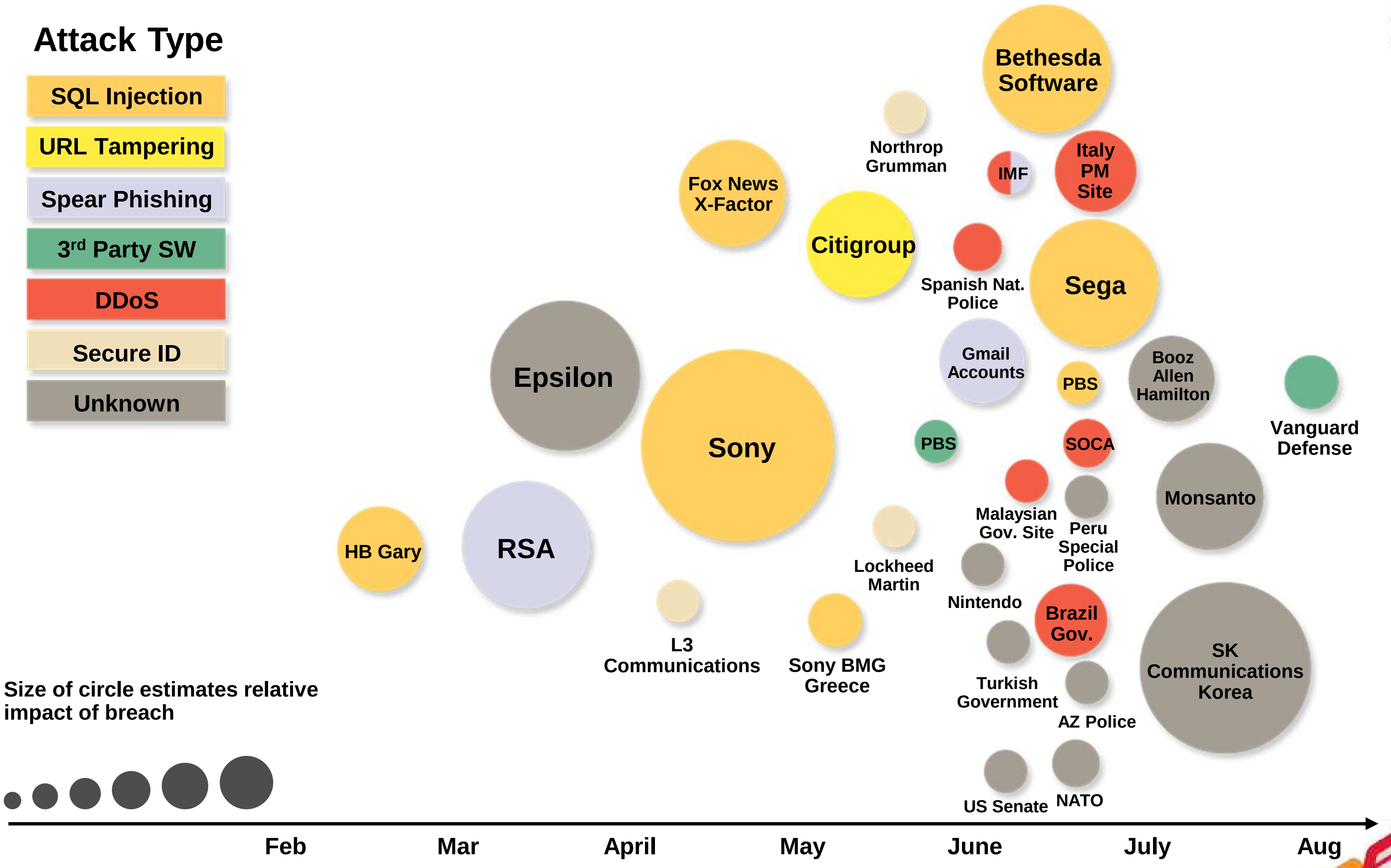
With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data is disappearing.

DATA EXPLOSION

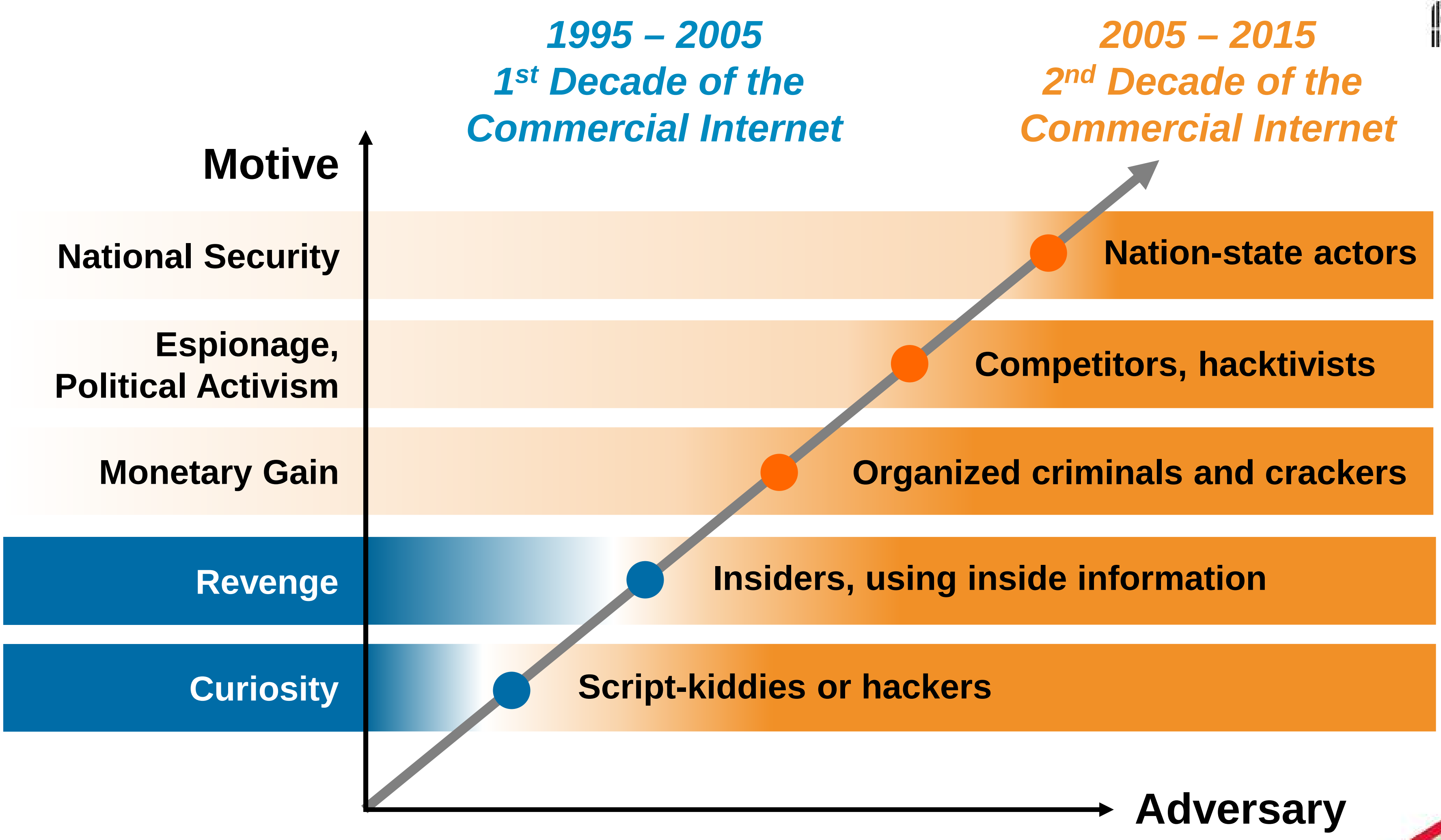
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

Security Threats Are Accelerating

Targeted Attacks Shake Businesses and Governments



Motivation and Sophistication Are Evolving



1995 – 2005
1st Decade of the Commercial Internet

2005 – 2015
2nd Decade of the Commercial Internet

Motive

National Security — Nation-state actors

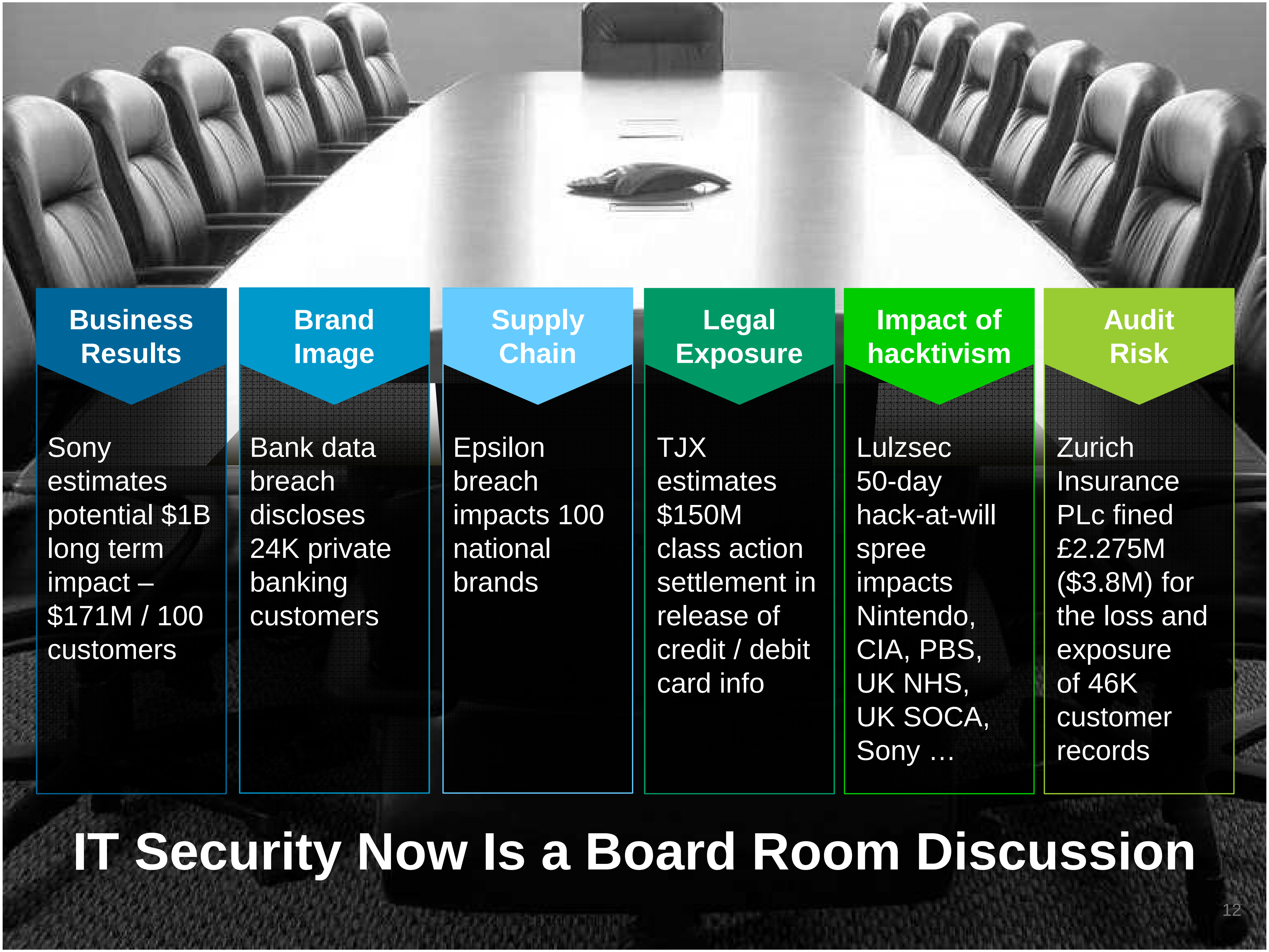
Espionage, Political Activism — Competitors, hacktivists

Monetary Gain — Organized criminals and crackers

Revenge — Insiders, using inside information

Curiosity — Script-kiddies or hackers

Adversary

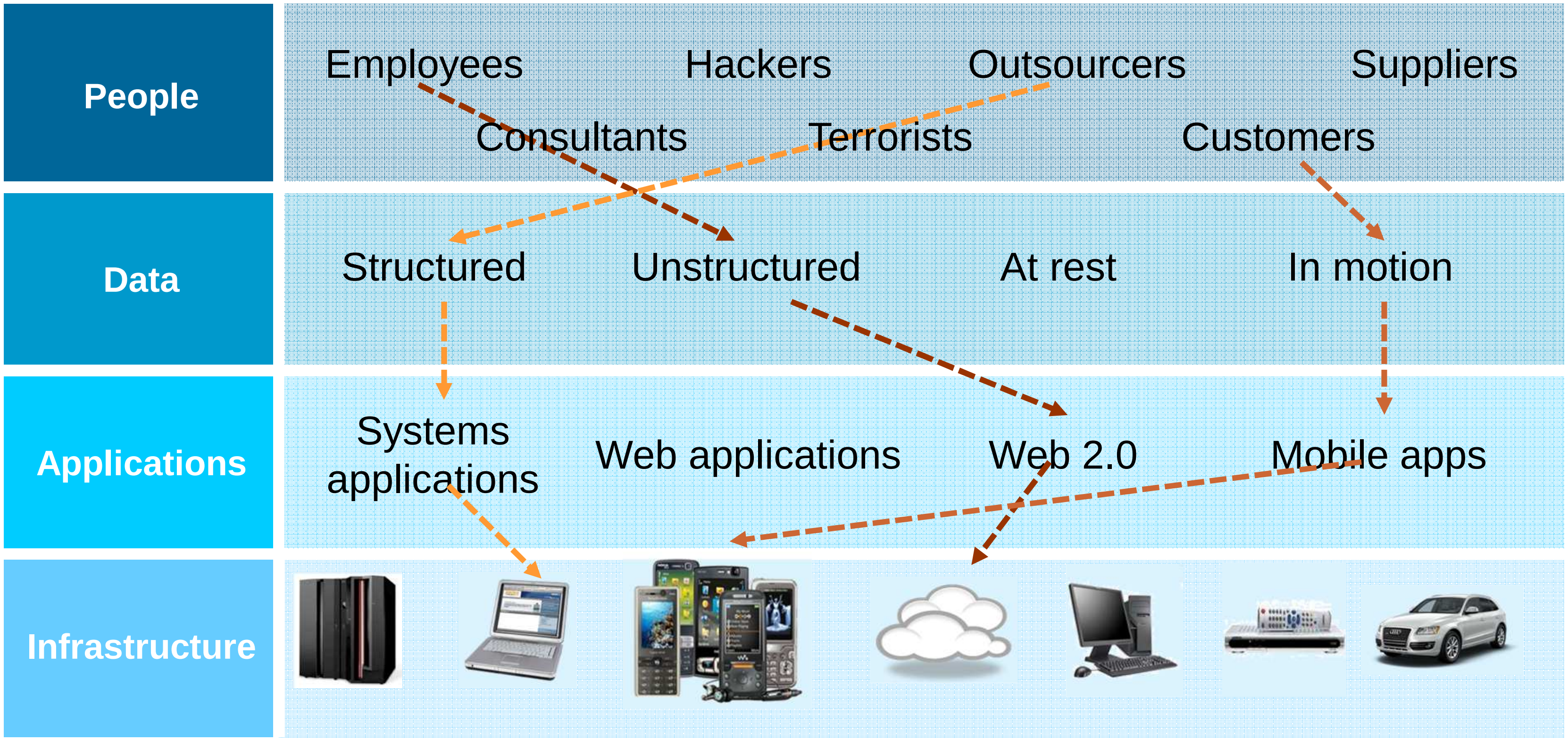


Business Results	Brand Image	Supply Chain	Legal Exposure	Impact of hacktivism	Audit Risk
Sony estimates potential $1B long term impact – $171M / 100 customers	Bank data breach discloses 24K private banking customers	Epsilon breach impacts 100 national brands	TJX estimates $150M class action settlement 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

IT Security Now Is a Board Room Discussion

IBM’s Security Strategy

Solving a Security Issue Is a Complex, Four-dimensional Puzzle



People

Employees Hackers Outsourcers Suppliers

Consultants Terrorists Customers

Data

Structured Unstructured At rest In motion

Applications

Systems applications Web applications Web 2.0 Mobile apps

Infrastructure

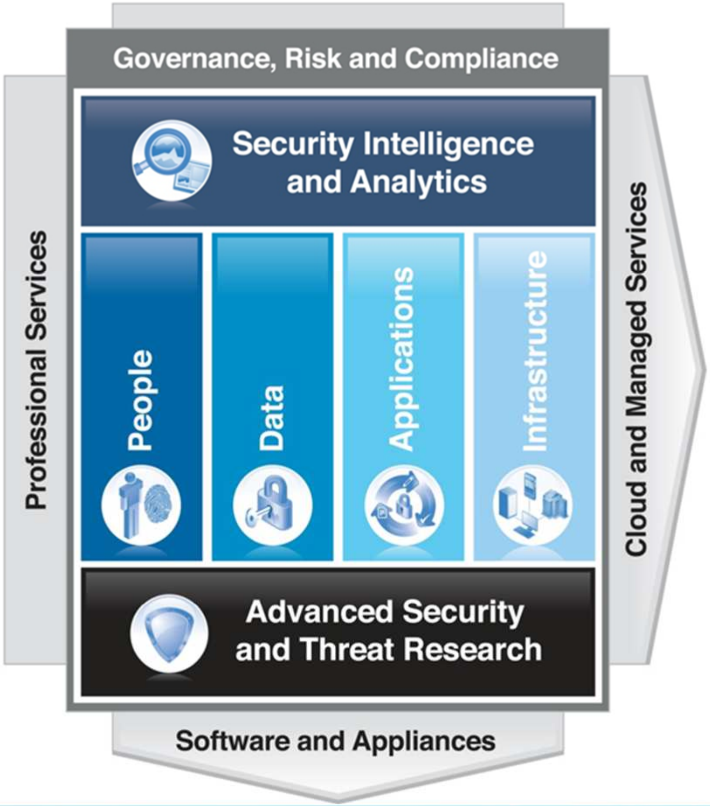
Attempting to protect the perimeter is not enough –
siloed point products cannot adequately secure the enterprise

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

IBM Security Systems

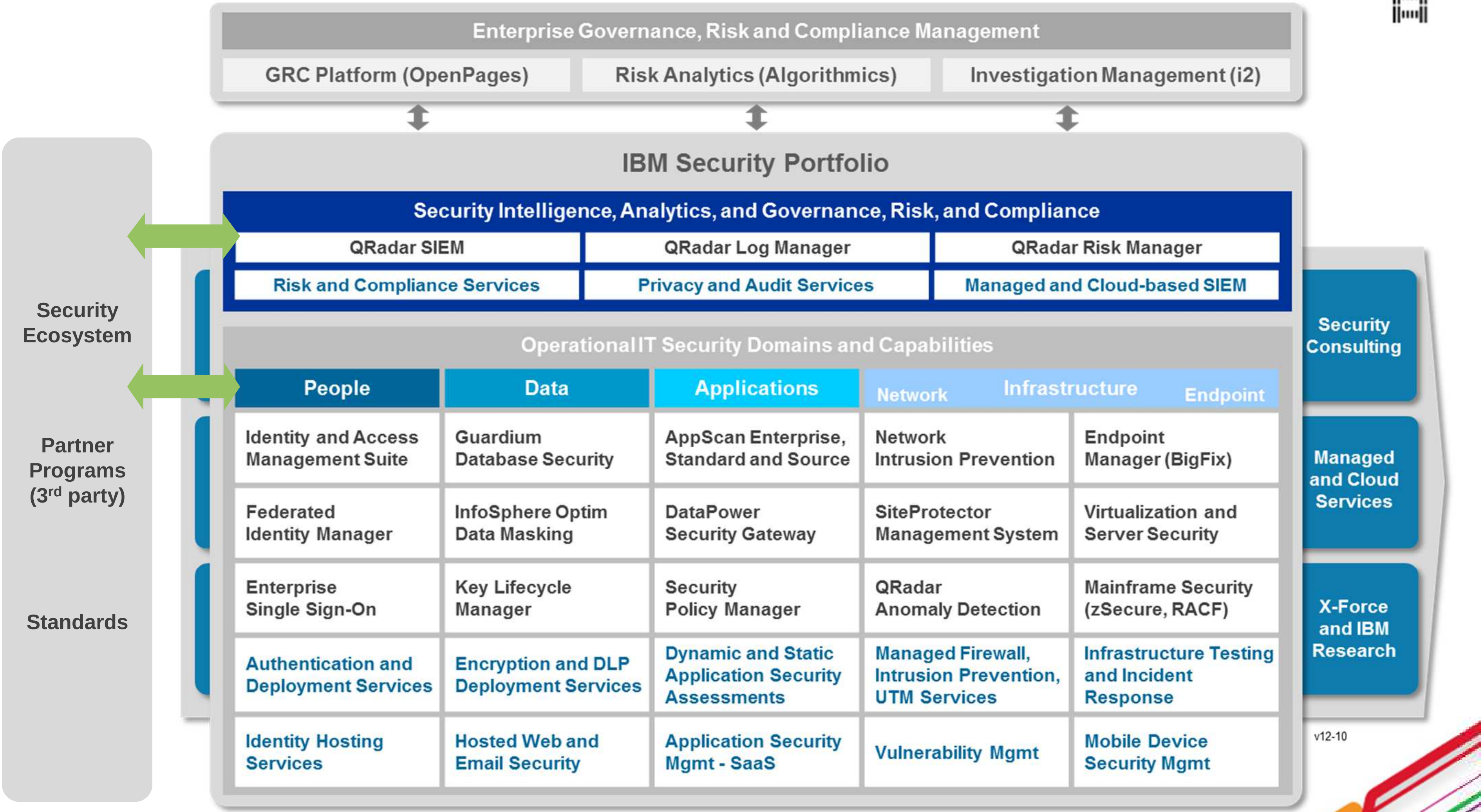
- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- One of the largest vulnerability databases

IBM Security Framework


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Intelligence ● Integration ● Expertise

A Comprehensive Portfolio of Products and Services Across All Domains



Enterprise Governance, Risk and Compliance Management

GRC Platform (OpenPages) | Risk Analytics (Algorithmics) | Investigation Management (i2)

IBM Security Portfolio

Security Intelligence, Analytics, and Governance, Risk, and Compliance

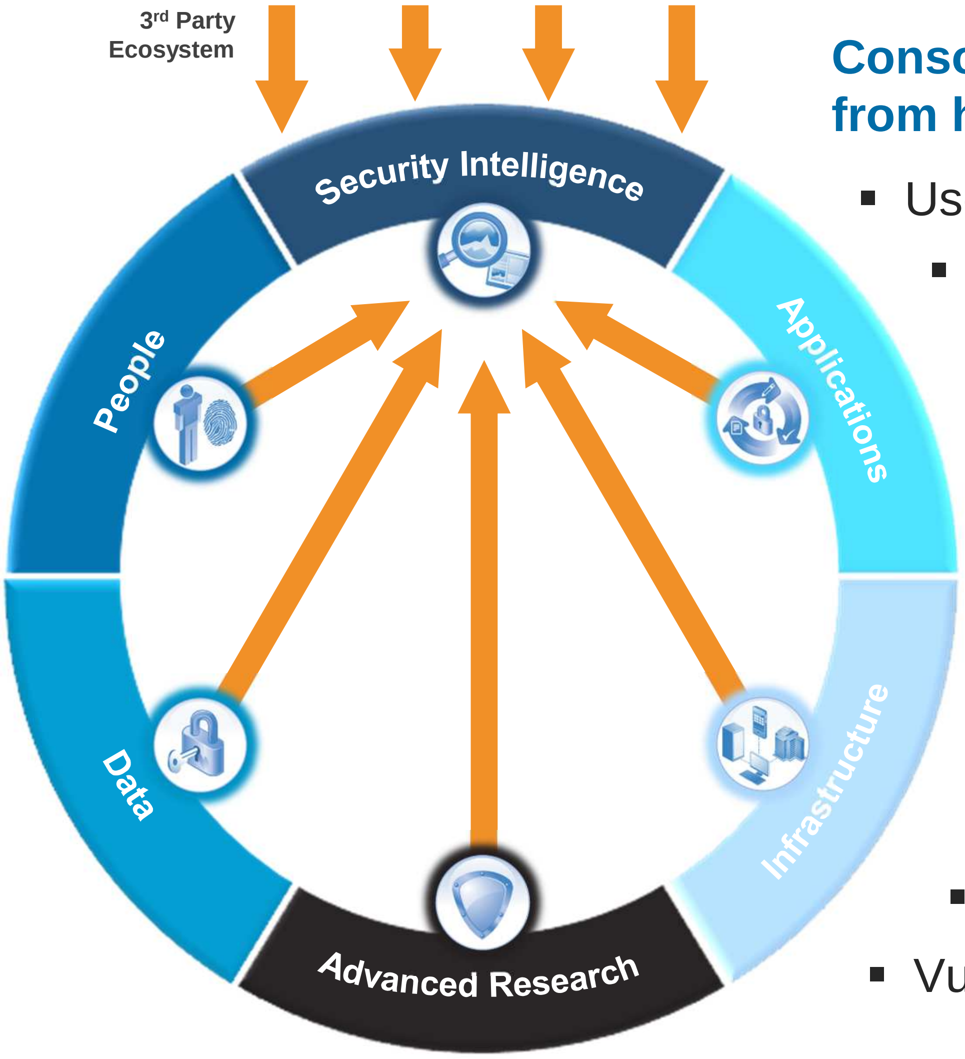
QRadar SIEM	QRadar Log Manager	QRadar Risk Manager
Risk and Compliance Services	Privacy and Audit Services	Managed and Cloud-based SIEM

Operational IT Security Domains and Capabilities

People	Data	Applications	Infrastructure	
			Network	Endpoint
Identity and Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard and Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization and Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Authentication and Deployment Services	Encryption and DLP Deployment Services	Dynamic and Static Application Security Assessments	Managed Firewall, Intrusion Prevention, UTM Services	Infrastructure Testing and Incident Response
Identity Hosting Services	Hosted Web and Email Security	Application Security Mgmt - SaaS	Vulnerability Mgmt	Mobile Device Security Mgmt

Products Services

Integrated Intelligence



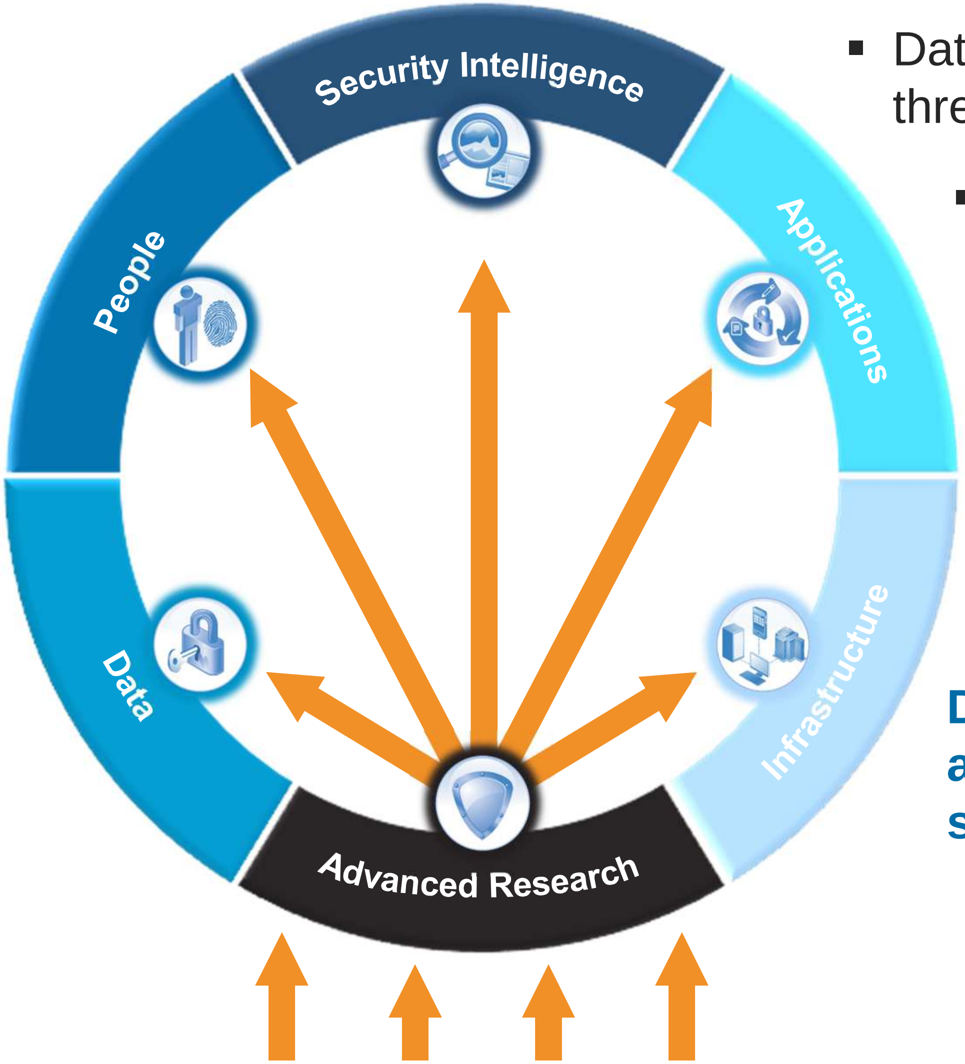
Consolidate siloed information from hundreds of sources

- User and asset contextual data
- Application logs
- Network events
- Network activity context
- Security events from firewalls, VPNs, IPS, etc.

Automate compliance tasks and assess risks

- Network and security configuration
- Vulnerability assessment
- Vulnerability assessment

Integrated Research



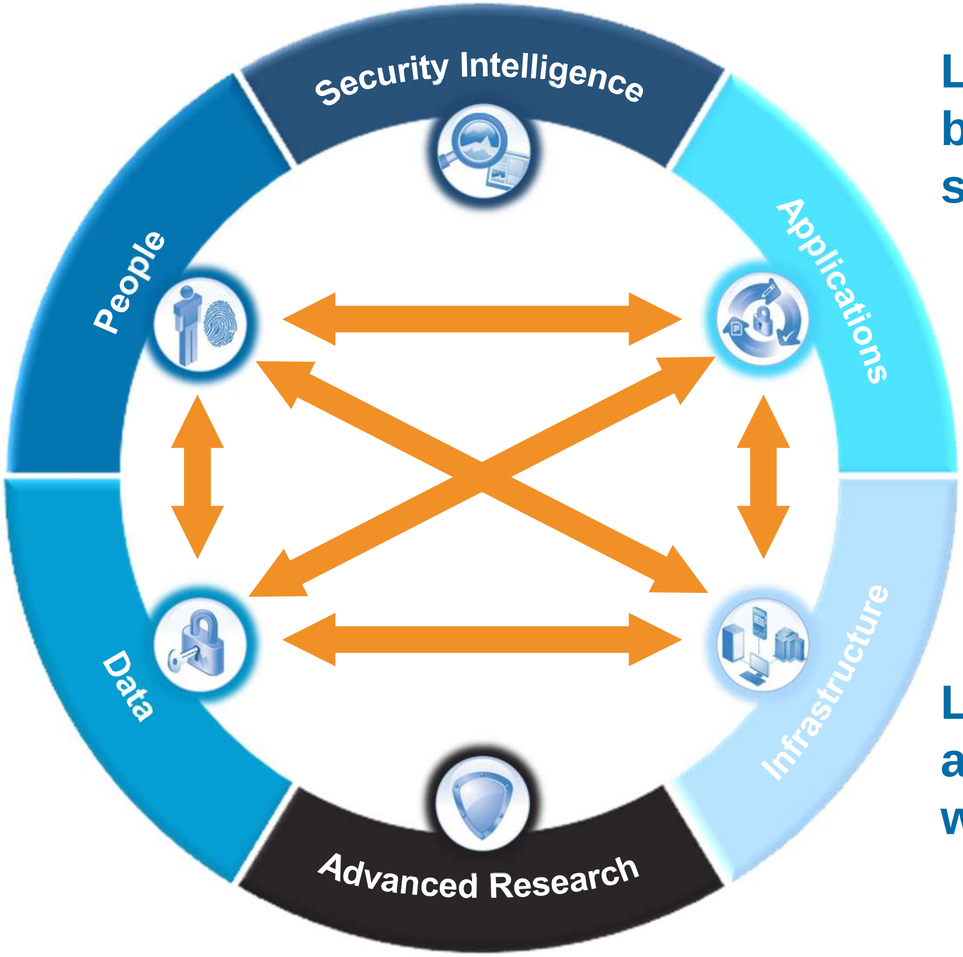
X-Force® Advanced Research

- Database of 63K+ unique vulnerabilities, threats and security checks
  - Virtual Patch for network intrusion prevention
    - X-Force® hosted threat analysis service

100s of preconfigured database vulnerability tests

Detect web application vulnerabilities and automatically update network security devices and software

Integrated Protection

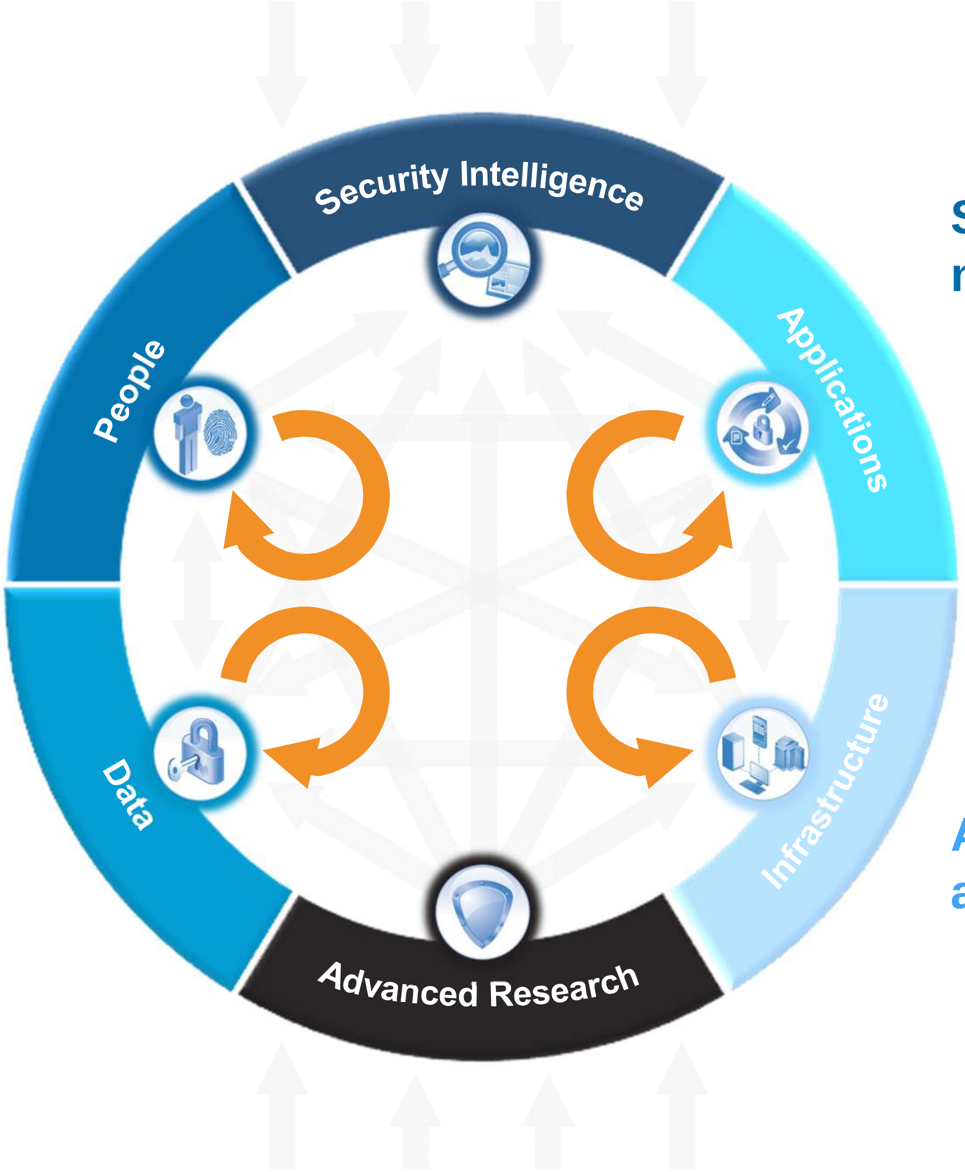


Link customized web attack blocking with network and server security appliances

Link automated identity and access policy enforcement with SOA gateways

Link user identification, authentication, and authorization with suspicious database activity

Integrated Lifecycle Management



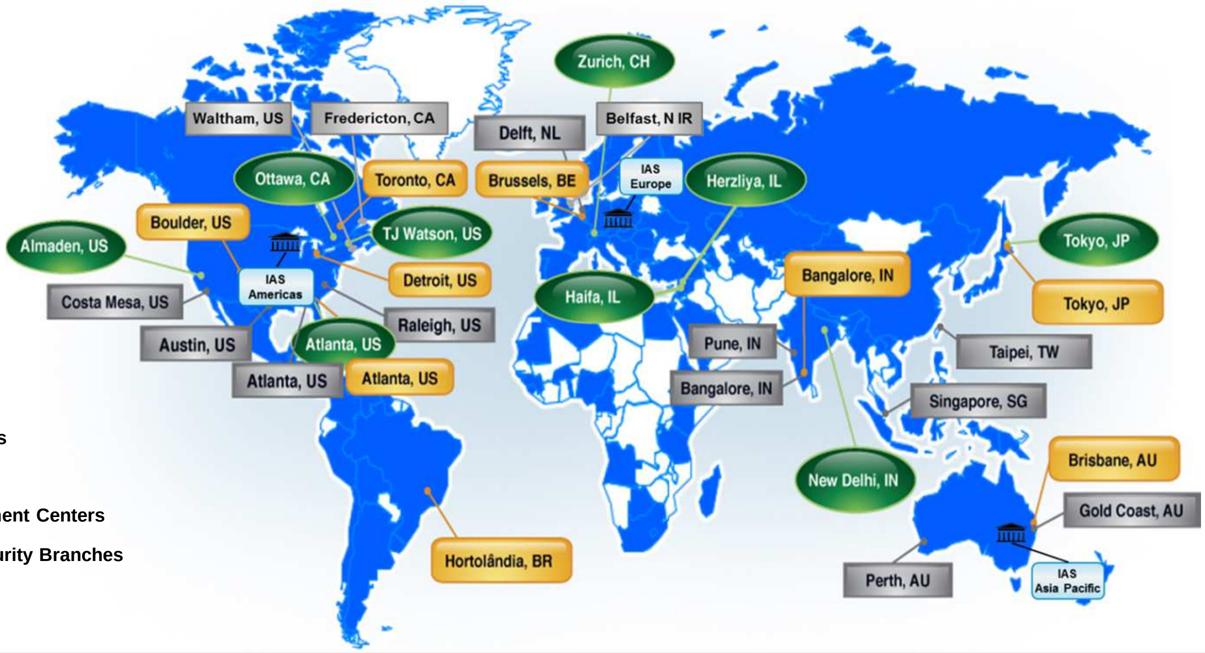
Simplify identity and access management

Deliver trusted information to the business

Operationalize application and web security

Automate endpoint security and compliance

Expertise: Unmatched Global Coverage and Security Awareness



🟨 Security Operations Centers

● Security Research Centers

▭ Security Solution Development Centers

🏛 Institute for Advanced Security Branches

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

14B analyzed Web pages & images

40M spam & phishing attacks

63K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

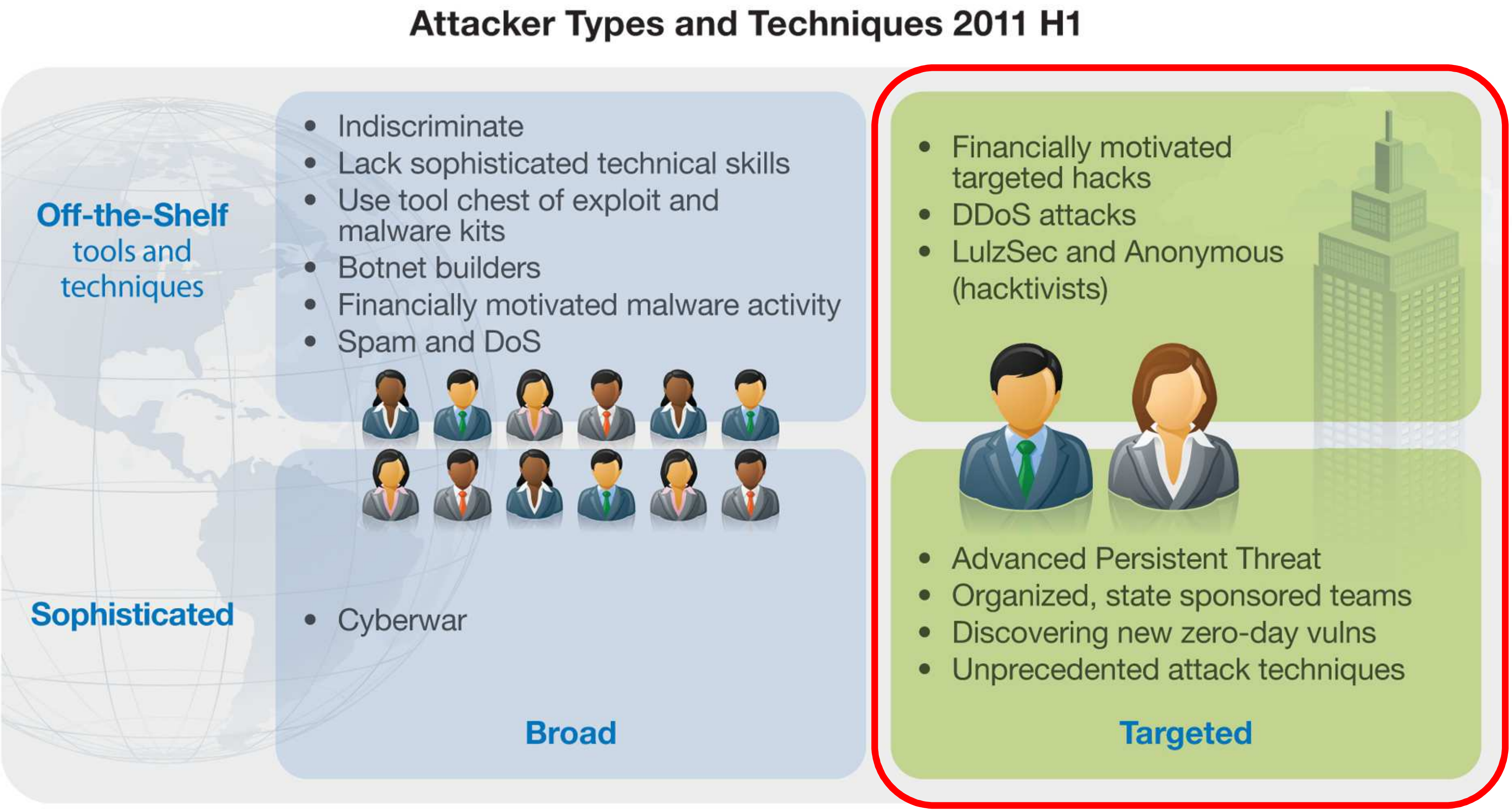
X FORCE

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 Is Helping Clients Tackle Complex Security Challenges

Who Is Attacking Our Networks?



Attacker Types and Techniques 2011 H1

	Broad	Targeted
Off-the-Shelf tools and techniques	• Indiscriminate • Lack sophisticated technical skills • Use tool chest of exploit and malware kits • Botnet builders • Financially motivated malware activity • Spam and DoS	• Financially motivated targeted hacks • DDoS attacks • LulzSec and Anonymous (hacktivists)
Sophisticated	• Cyberwar	• Advanced Persistent Threat • Organized, state sponsored teams • Discovering new zero-day vulns • Unprecedented attack techniques

Source: IBM X-Force® Research and Development

Advanced Persistent Threat (APT) Is Different

1 **Advanced**

- Exploiting unreported vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, researched attacks using multiple vectors

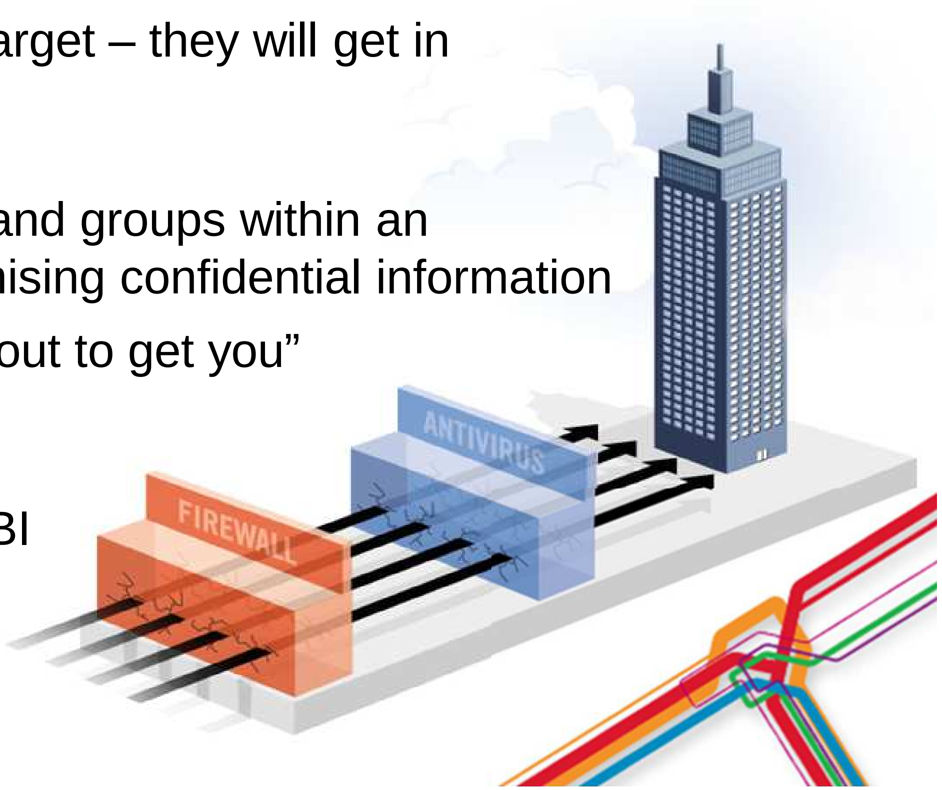
2 **Persistent**

- Attacks lasting for months or years
- Attackers are dedicated to the target – they will get in

3 **Threat**

- Targeted at specific individuals and groups within an organization, aimed at compromising confidential information
- Not random attacks – they are "out to get you"

4 Responding is different too –
Watch, **Wait**, **Plan** … and call the FBI



Internet Intelligence Collection

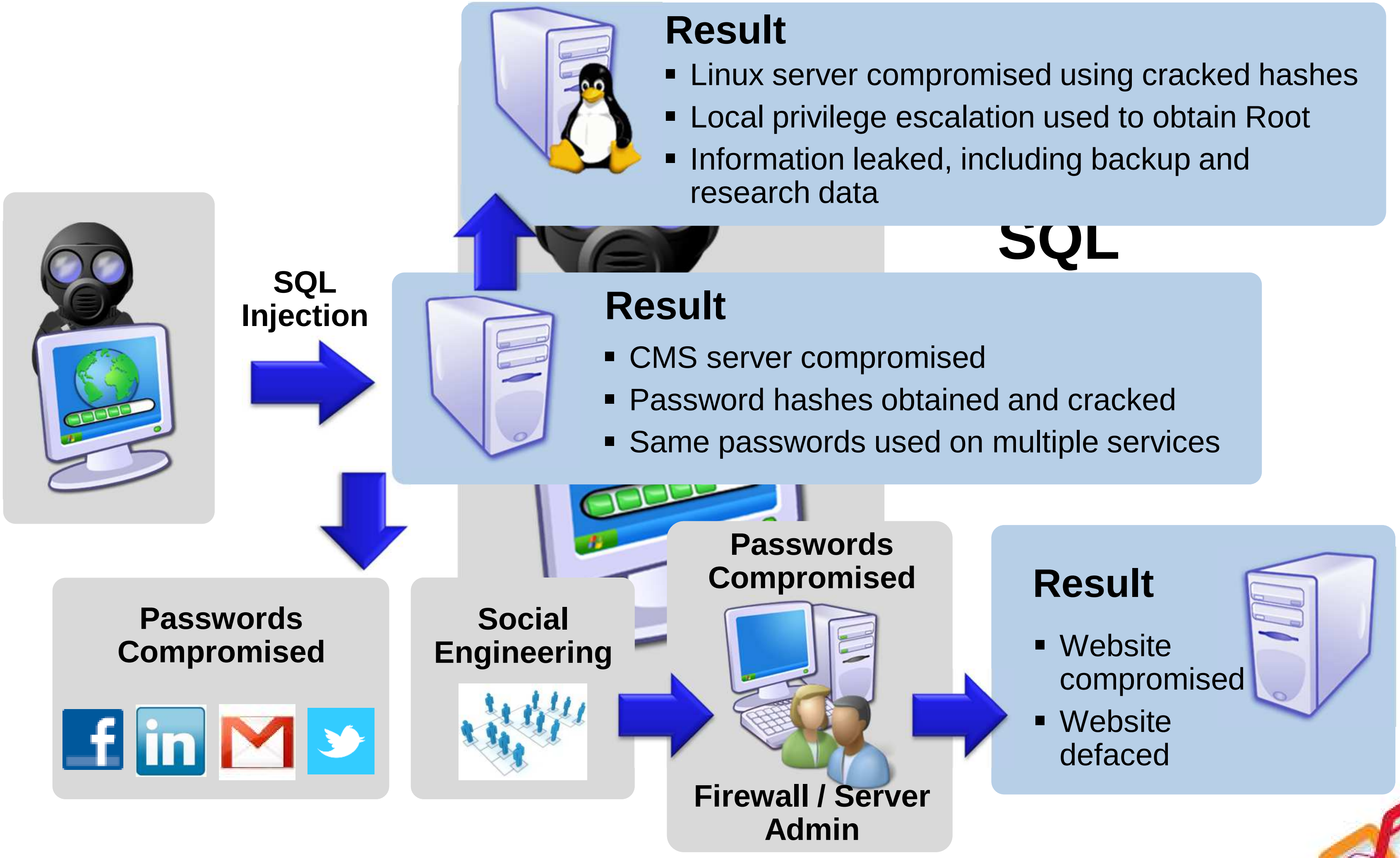
- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?

- Search for Linkedin, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart

- Who works with the information we want to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?

Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



SQL Injection

Result

- CMS server compromised
- Password hashes obtained and cracked
- Same passwords used on multiple services

Result

- Linux server compromised using cracked hashes
- Local privilege escalation used to obtain Root
- Information leaked, including backup and research data

SQL

Passwords Compromised

Social Engineering

Passwords Compromised

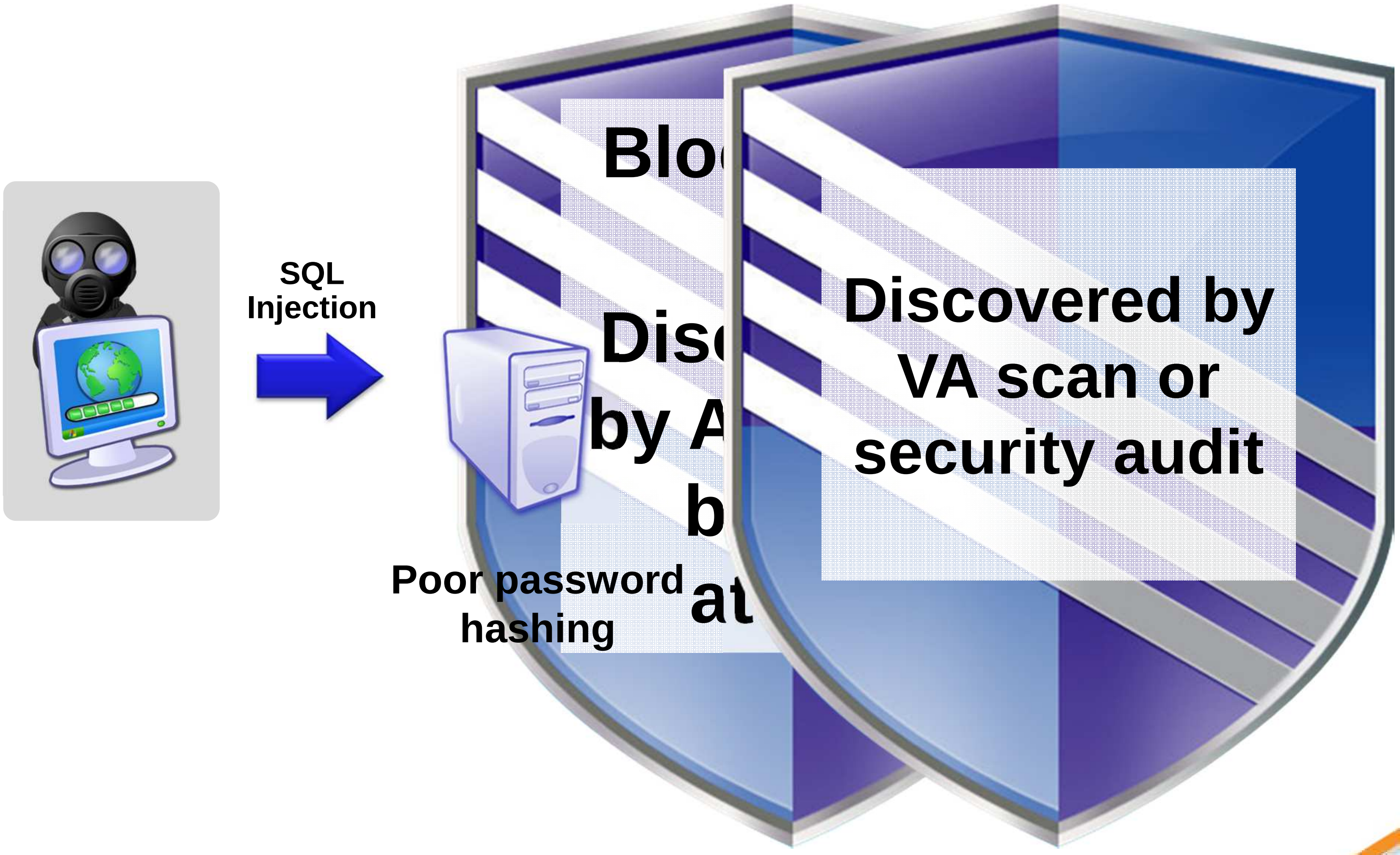
Firewall / Server Admin

Result

- Website compromised
- Website defaced

Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



SQL Injection

Poor password hashing

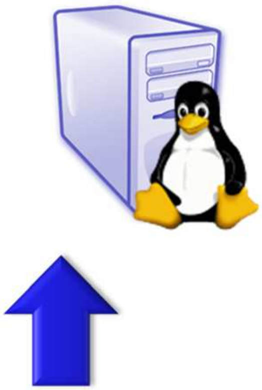
Blo

Disc by A b at

Discovered by VA scan or security audit

Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



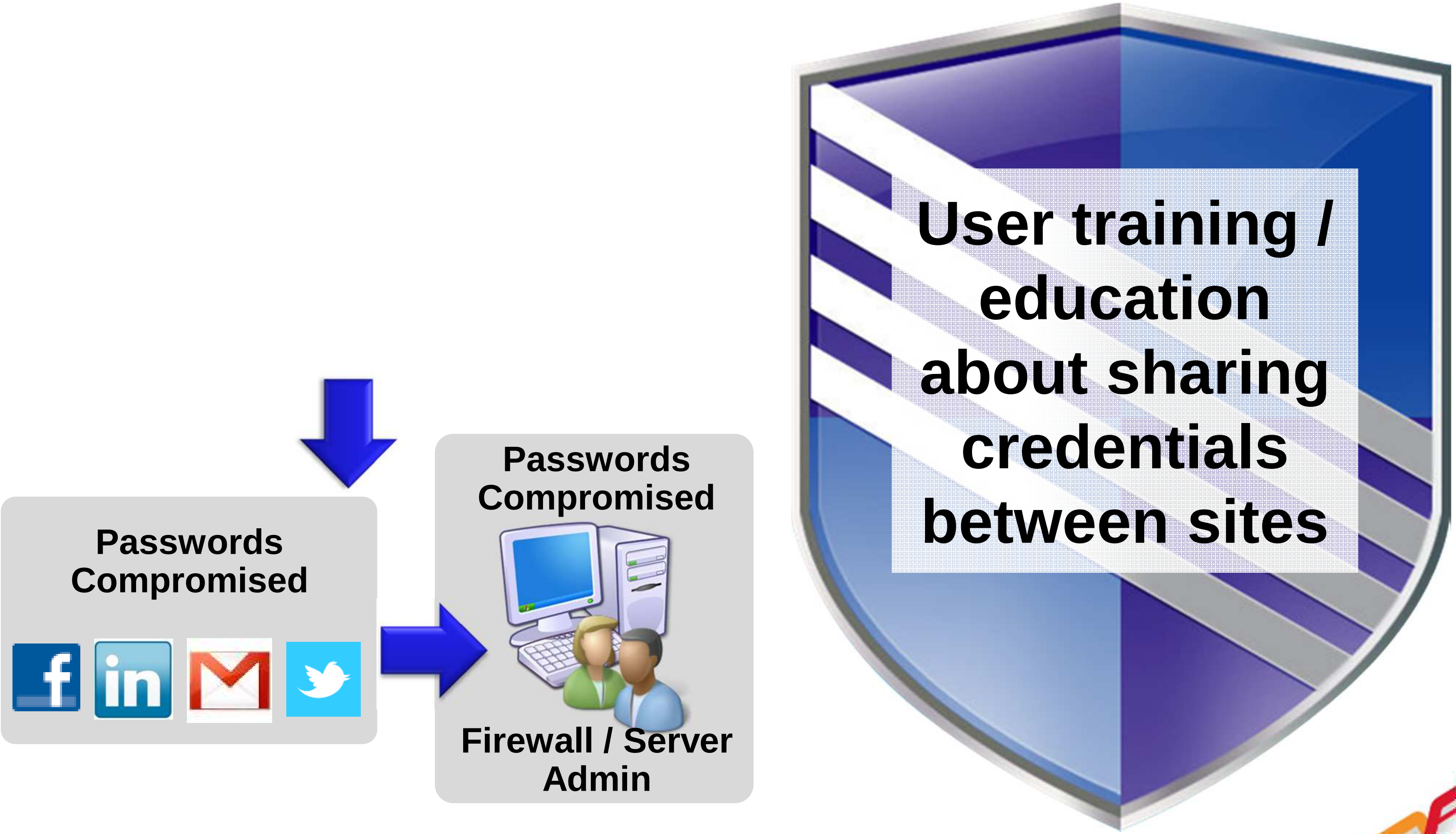
Privilege escalation

SSH

Patch management to fix privilege escalation

Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1



Passwords Compromised

Passwords Compromised

Firewall / Server Admin

User training / education about sharing credentials between sites

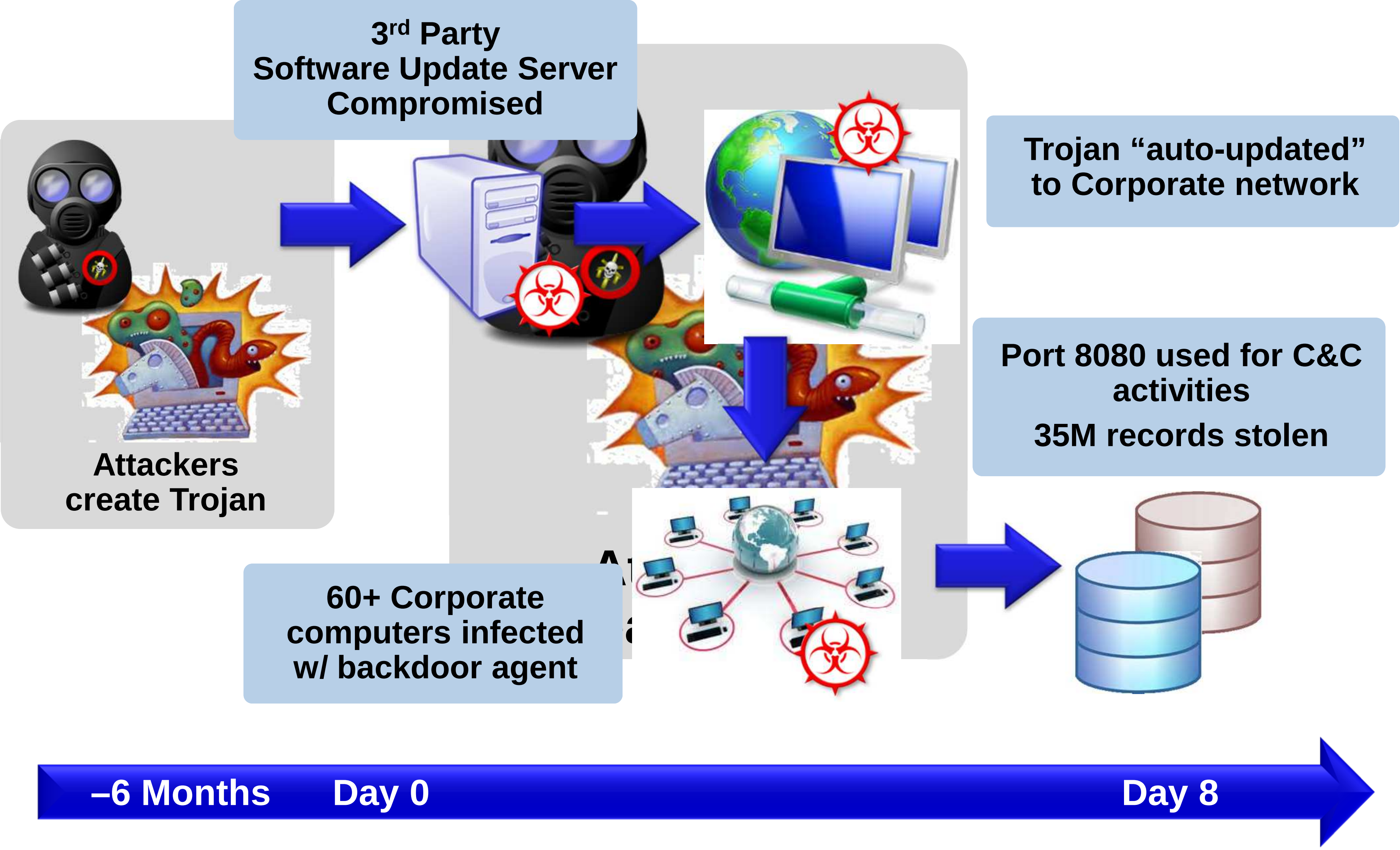
Well Known, Off the Shelf Attack Techniques Are All That It Takes

Anatomy of an APT – Scenario 1

So many ways to stop an attack

They Will Get In…Then What?

Anatomy of an APT – Scenario 2



3rd Party Software Update Server Compromised

Attackers create Trojan

Trojan “auto-updated” to Corporate network

Port 8080 used for C&C activities

35M records stolen

60+ Corporate computers infected w/ backdoor agent

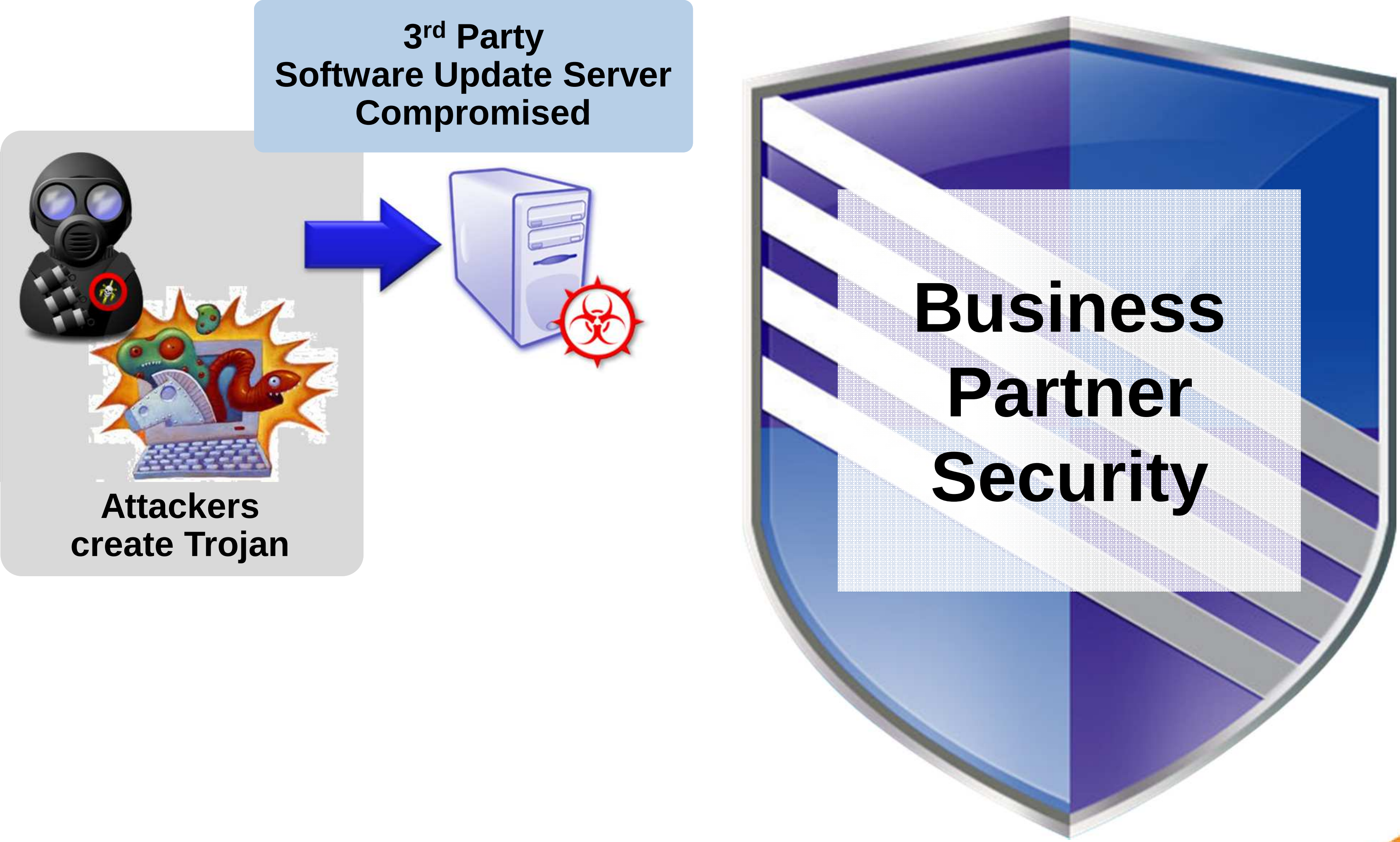
–6 Months

Day 0

Day 8

They Will Get In…Then What?

Anatomy of an APT – Scenario 2



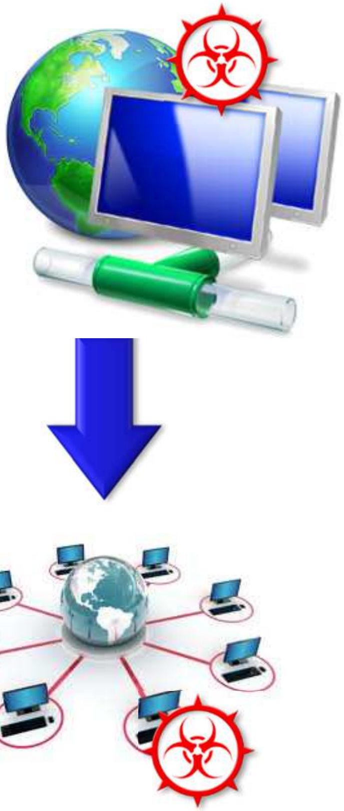
Attackers create Trojan

3rd Party Software Update Server Compromised

Business Partner Security

They Will Get In…Then What?

Anatomy of an APT – Scenario 2



60+ Corporate computers infected w/ backdoor agent

Recon Detection

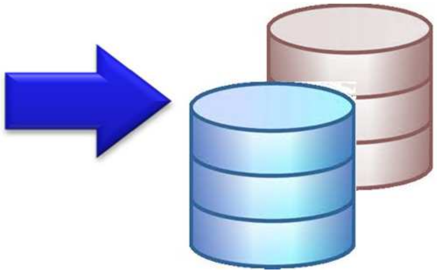
They Will Get In…Then What?

Anatomy of an APT – Scenario 2

Anomaly Detection Database Monitoring & Protection

Port 8080 used for C&C activities

35M records stolen



They Will Get In…Then What?

Anatomy of an APT – Scenario 2

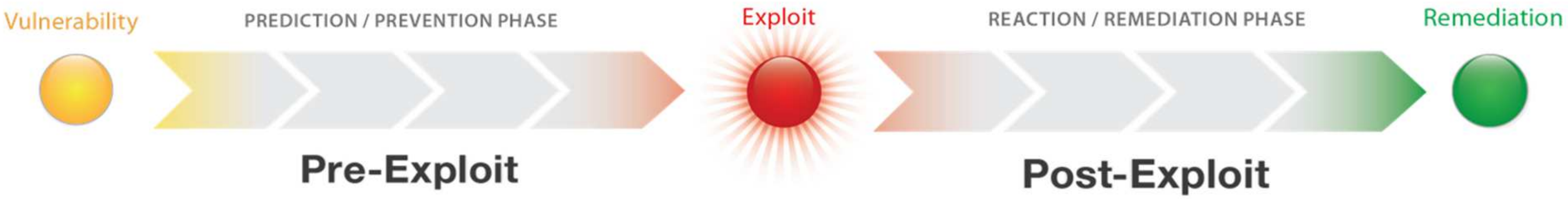
**An attack will happen…
You need Security Intelligence**

The Path to Security Intelligence

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 help protect against these threats?	What is happening right now?	What was the impact?



Prediction & Prevention

Risk Management.
Vulnerability Management.
Network and Host Intrusion Prevention.
Configuration and Patch Management.
X-Force® Research and Threat Intelligence.
Compliance Management.
Reporting and Scorecards.

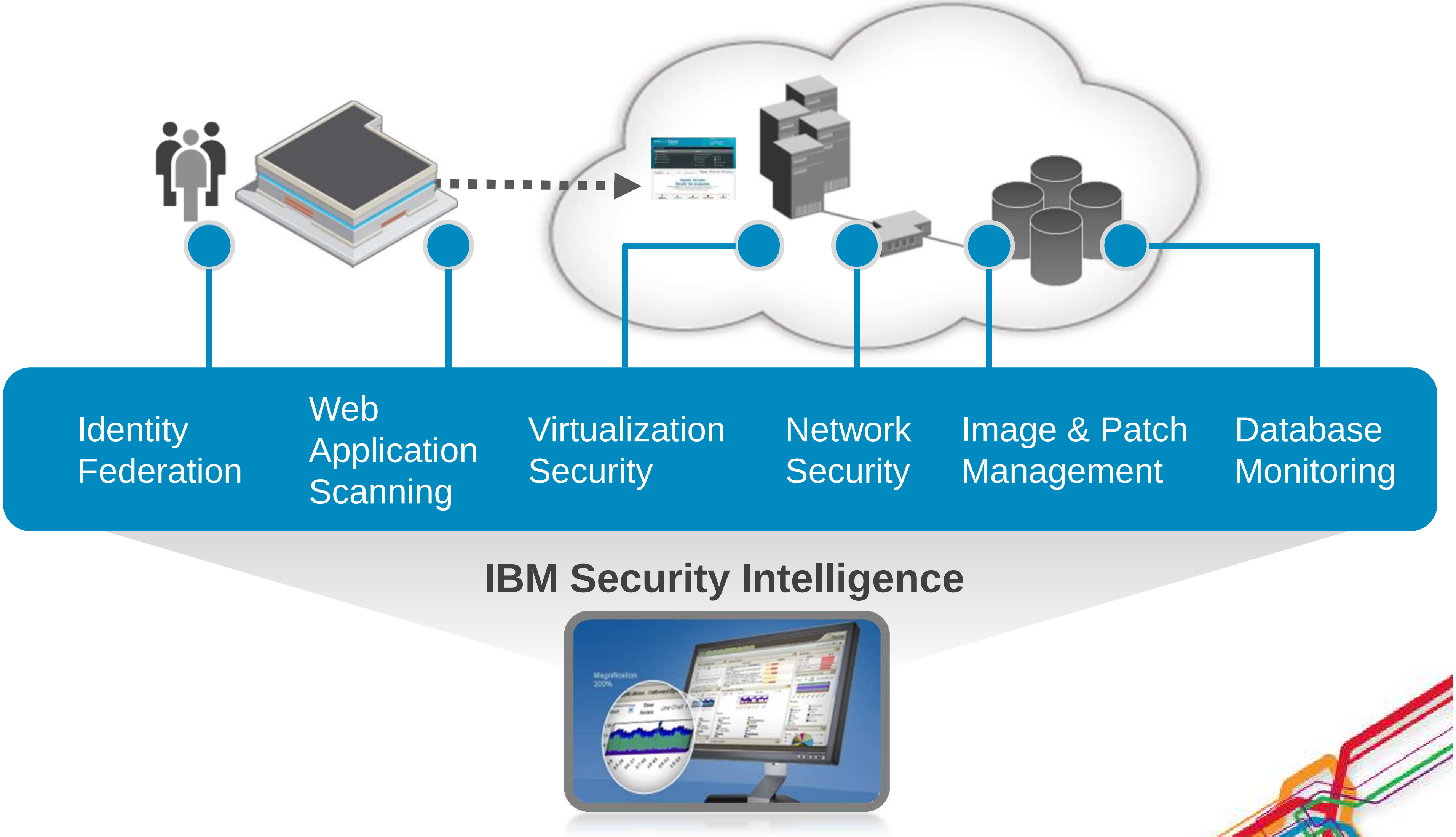
Reaction & Remediation

Network Anomaly Detection.
Packet Forensics.
Data Leak Prevention.
Database Activity Monitoring.
Security Intelligence and Event Management.
Log Management.
Incident Response.

IBM Security Intelligence

Cloud

Helping clients adopt cloud with flexible, layered security solutions



Identity Federation

Web Application Scanning

Virtualization Security

Network Security

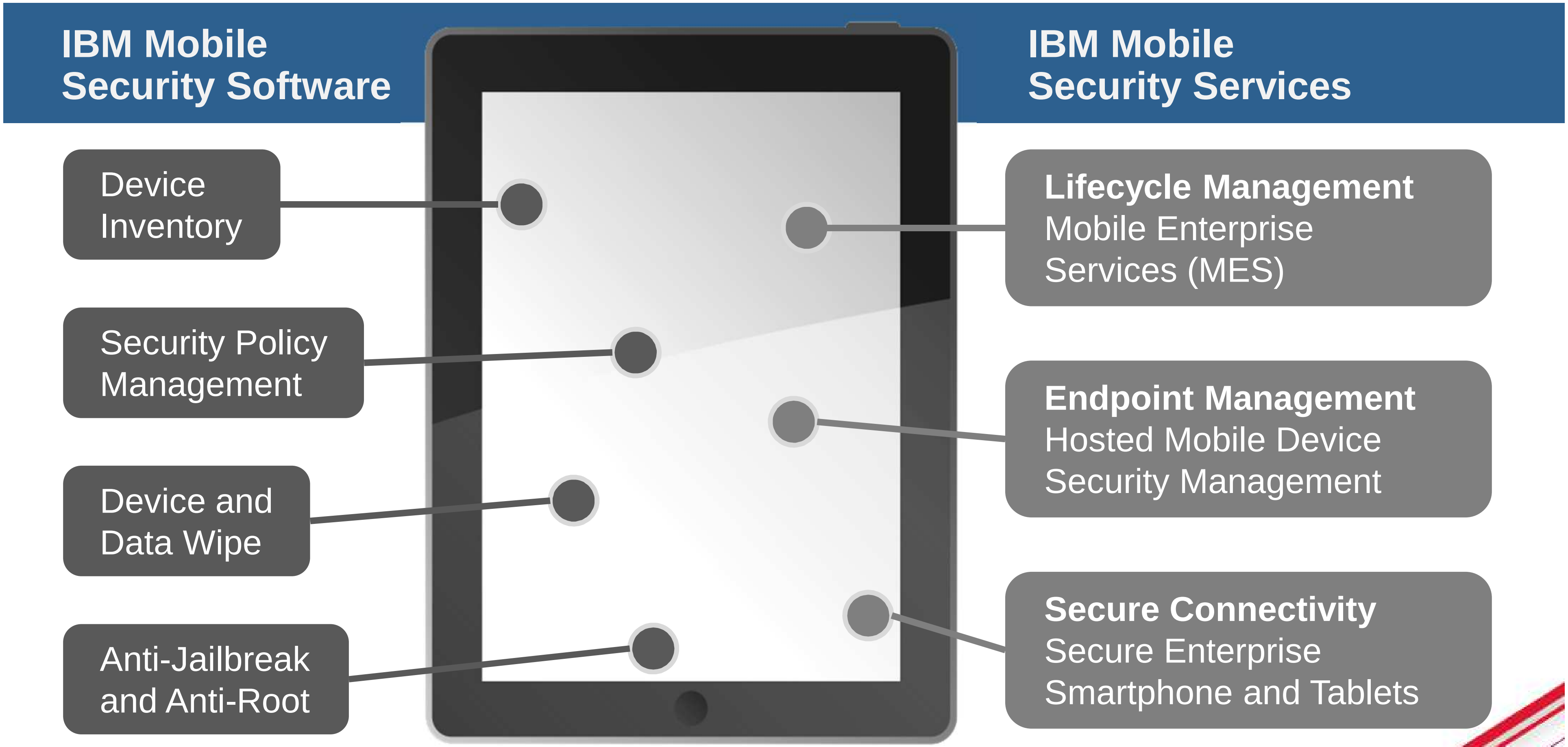
Image & Patch Management

Database Monitoring

IBM Security Intelligence

Consumerization of IT

Converging endpoint and mobile security management into a single solution with complementary services



IBM Mobile Security Software

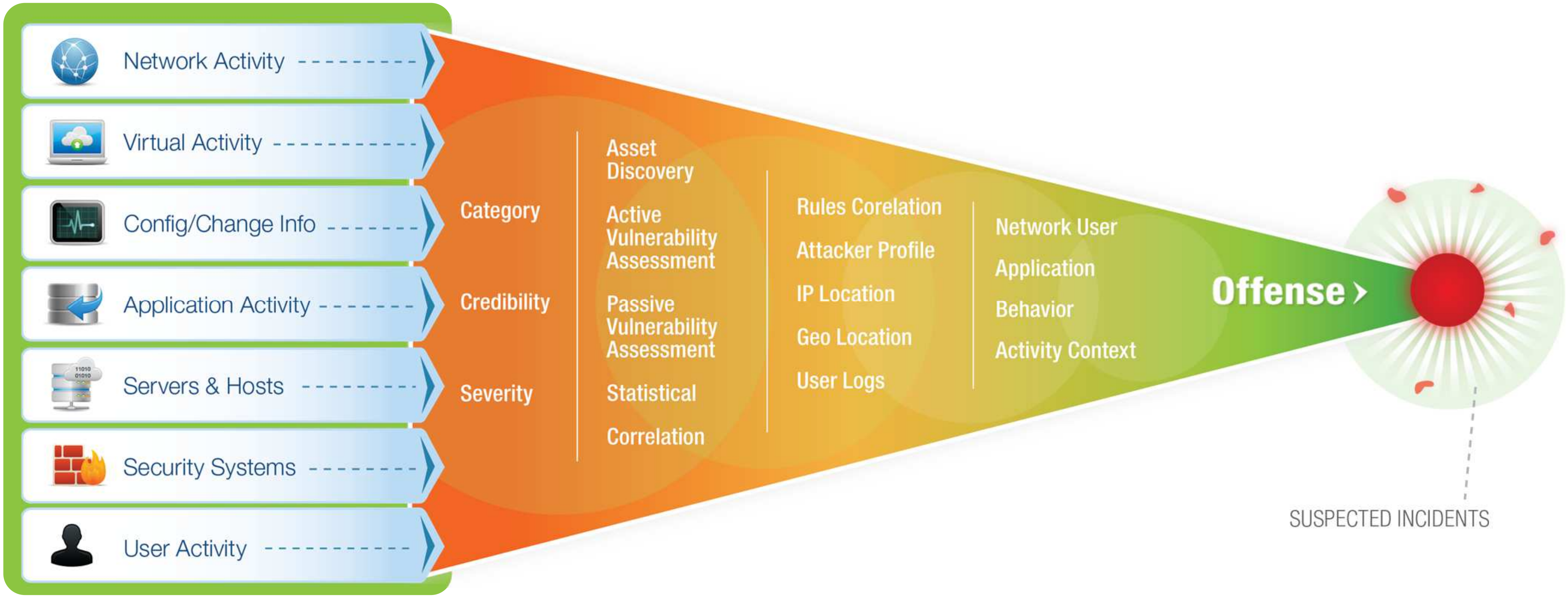
- Device Inventory
- Security Policy Management
- Device and Data Wipe
- Anti-Jailbreak and Anti-Root

IBM Mobile Security Services

- **Lifecycle Management** Mobile Enterprise Services (MES)
- **Endpoint Management** Hosted Mobile Device Security Management
- **Secure Connectivity** Secure Enterprise Smartphone and Tablets

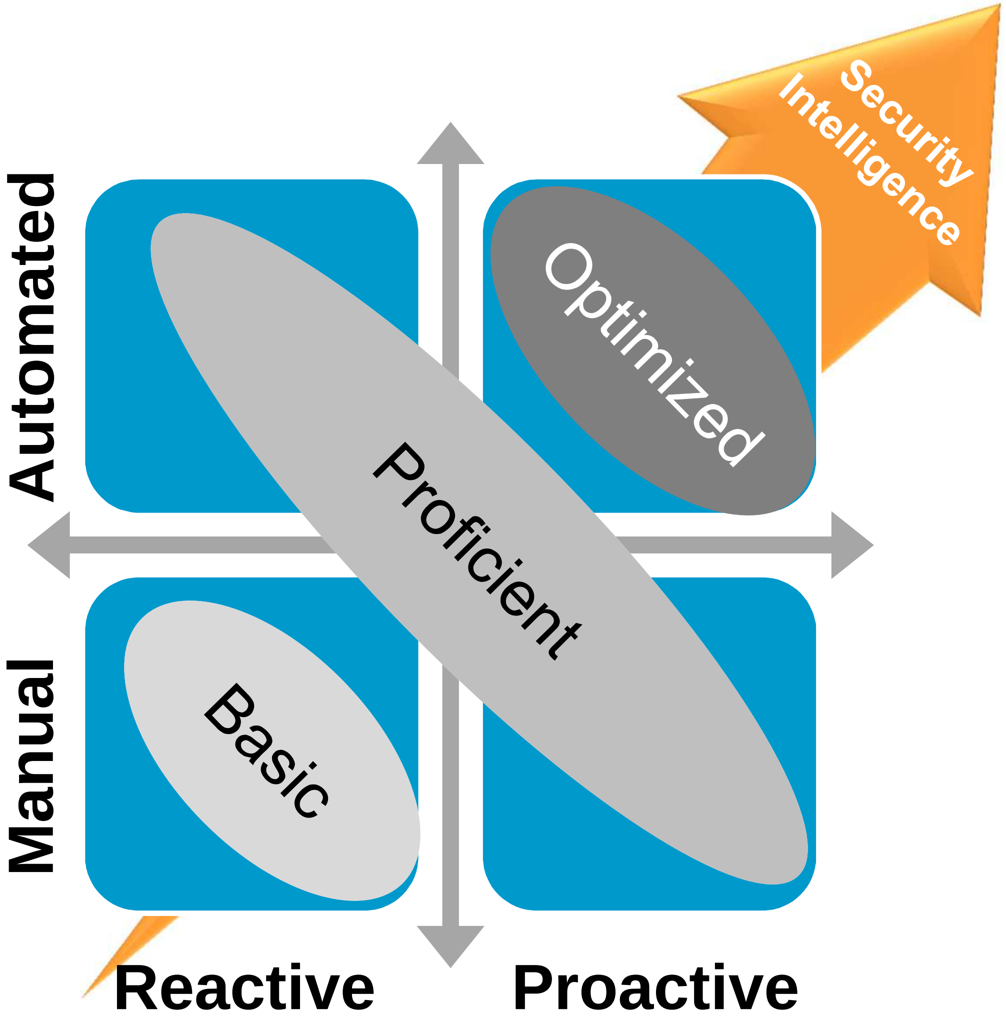
Data Explosion

Integrating across IT silos with Security Intelligence solutions

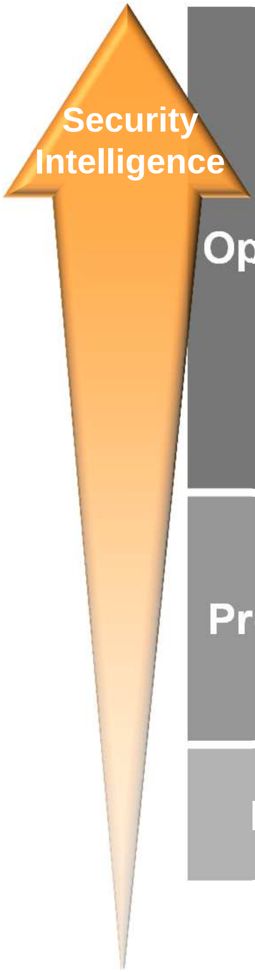


Sources + Intelligence = Most Accurate & Actionable Insight

In This "New Normal", Organizations Need an Intelligent View of Their Security Posture



Security Intelligence Is Enabling Progress to Optimized Security



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

IBM Security: Intelligence. Integration. Expertise.

3 Takeaways

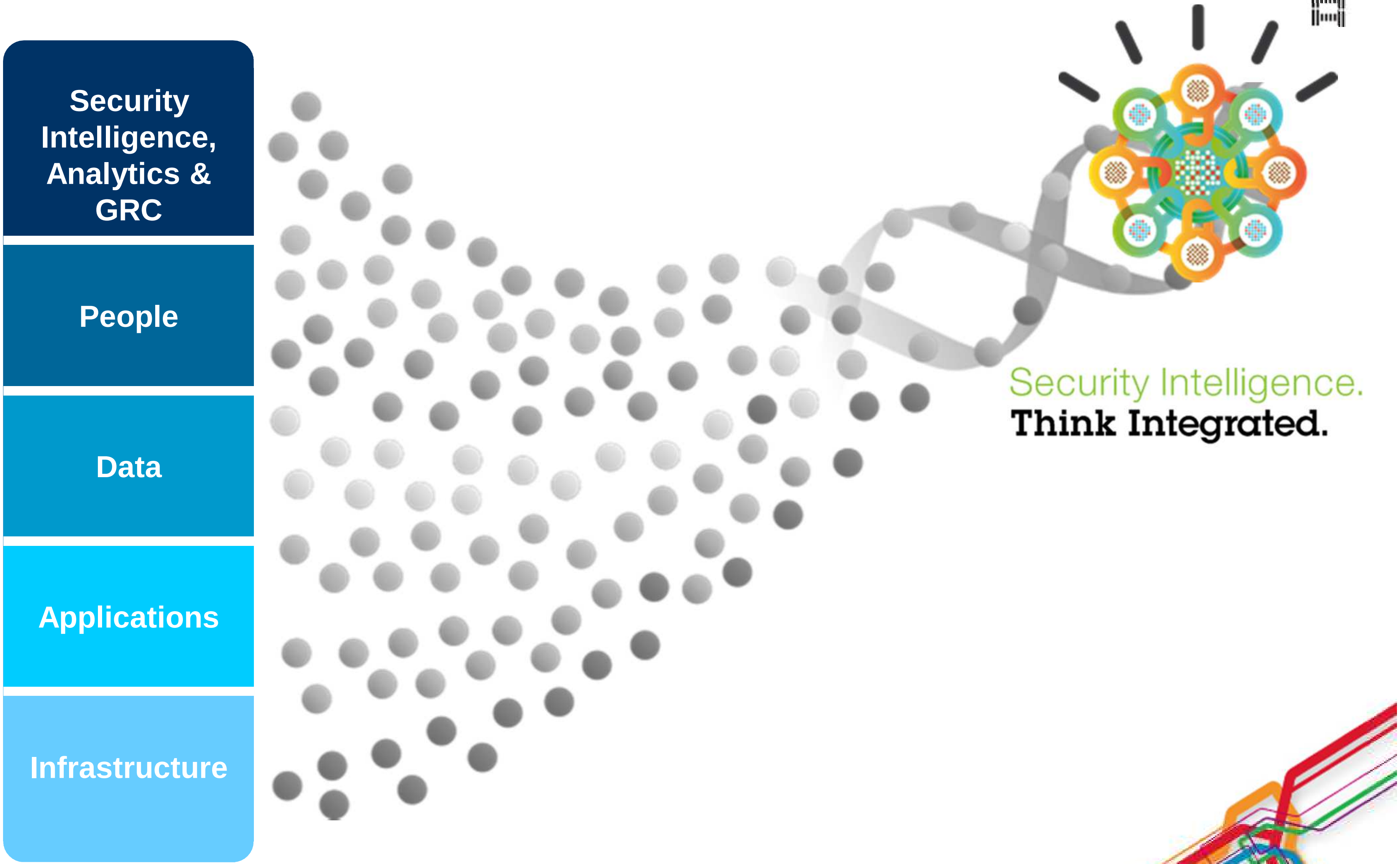
IT is at a crossroads, with organizations facing a threat landscape that is increasingly complex and that requires a fundamentally different approach to security. Clients want an integrated view of security and existing point products are not meeting their needs

1 IBM’s Security Intelligence solutions leverage real time processing and predictive analytics capabilities to help clients tackle difficult security challenges such as insider threat and advanced persistent threat

2 Critical controls are becoming more optimized and integrated across key security domains such as identity management, application security, and advanced network security

3 IBM has committed major resources to and organized around a broad, integrated framework of products and solutions to help organizations meet current and emerging threats

Intelligent Solutions Provide the DNA to Secure a Smarter Planet



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

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.

Stream Keynote 4: Security & Compliance

Pulse2012

Optimizing the World's Infrastructure