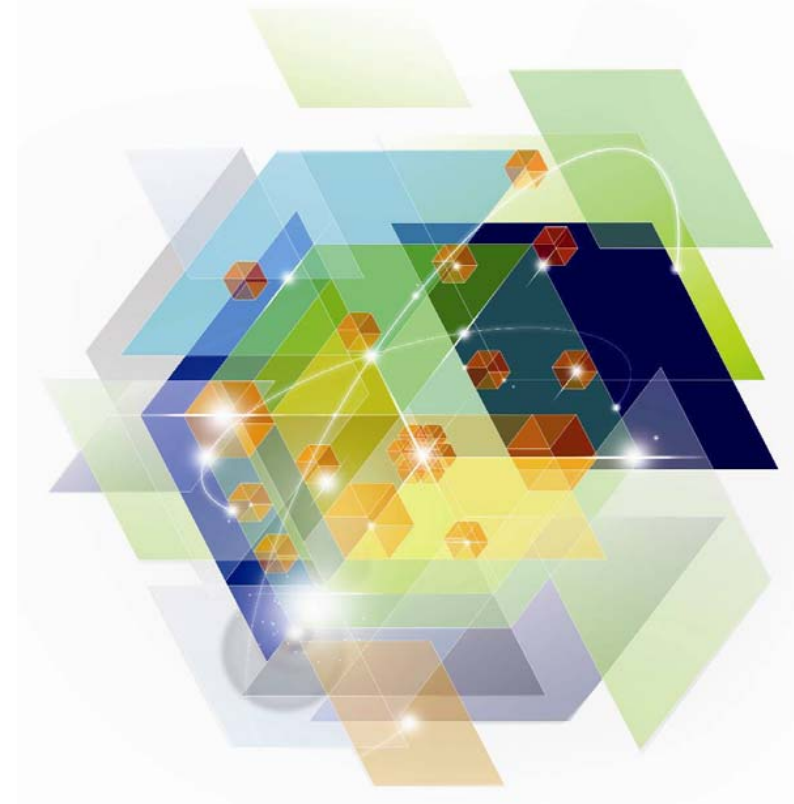




Strategy for Leveraging Mainframe Security in Today's Smarter Planet



Agenda

- **Current state of security**
- **How industry security practices need to evolve**
- **Introduction to IBM Security Products on System z**

The Planet is getting more...

Smart Supply Chains



Smart Countries



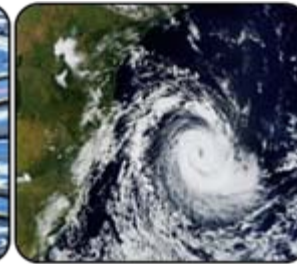
Smart Retail



Smart Water Management



Smart Weather



Smart Energy Grids



INSTRUMENTED



INTERCONNECTED



INTELLIGENT

Smart Oil Field Technologies



Smart Regions



Smart Healthcare



Smart Traffic Systems



Smart Cities



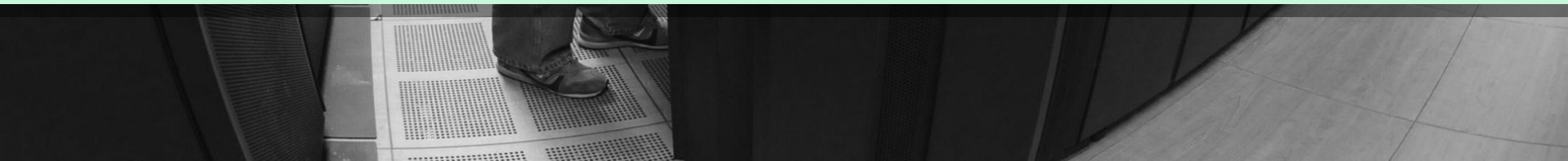
Smart Food Systems





DATA EXPLOSION

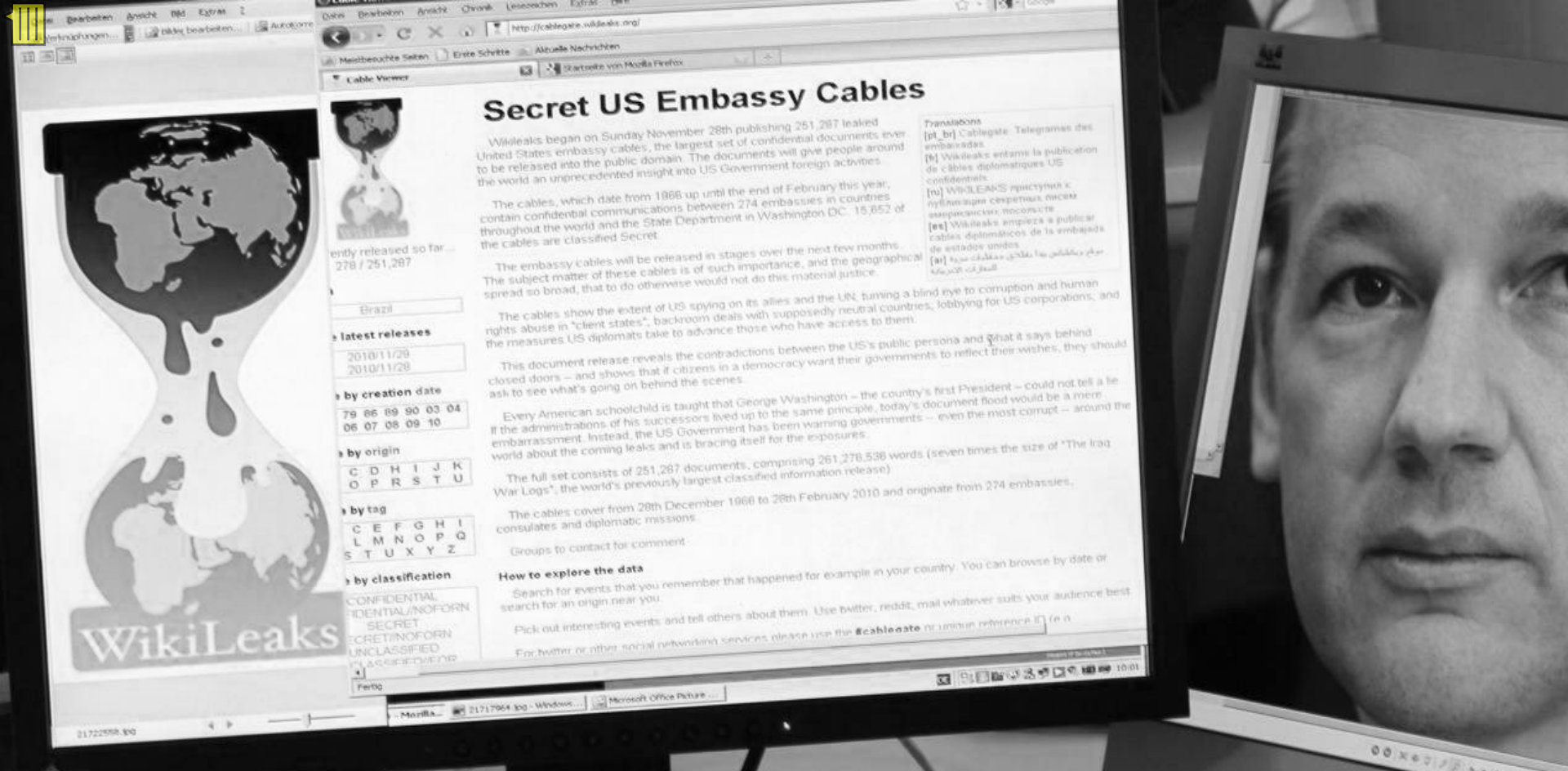
The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere.





CONSUMERIZATION OF IT

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



ATTACK SOPHISTICATION

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

Targeted Attacks Shake Businesses and Governments

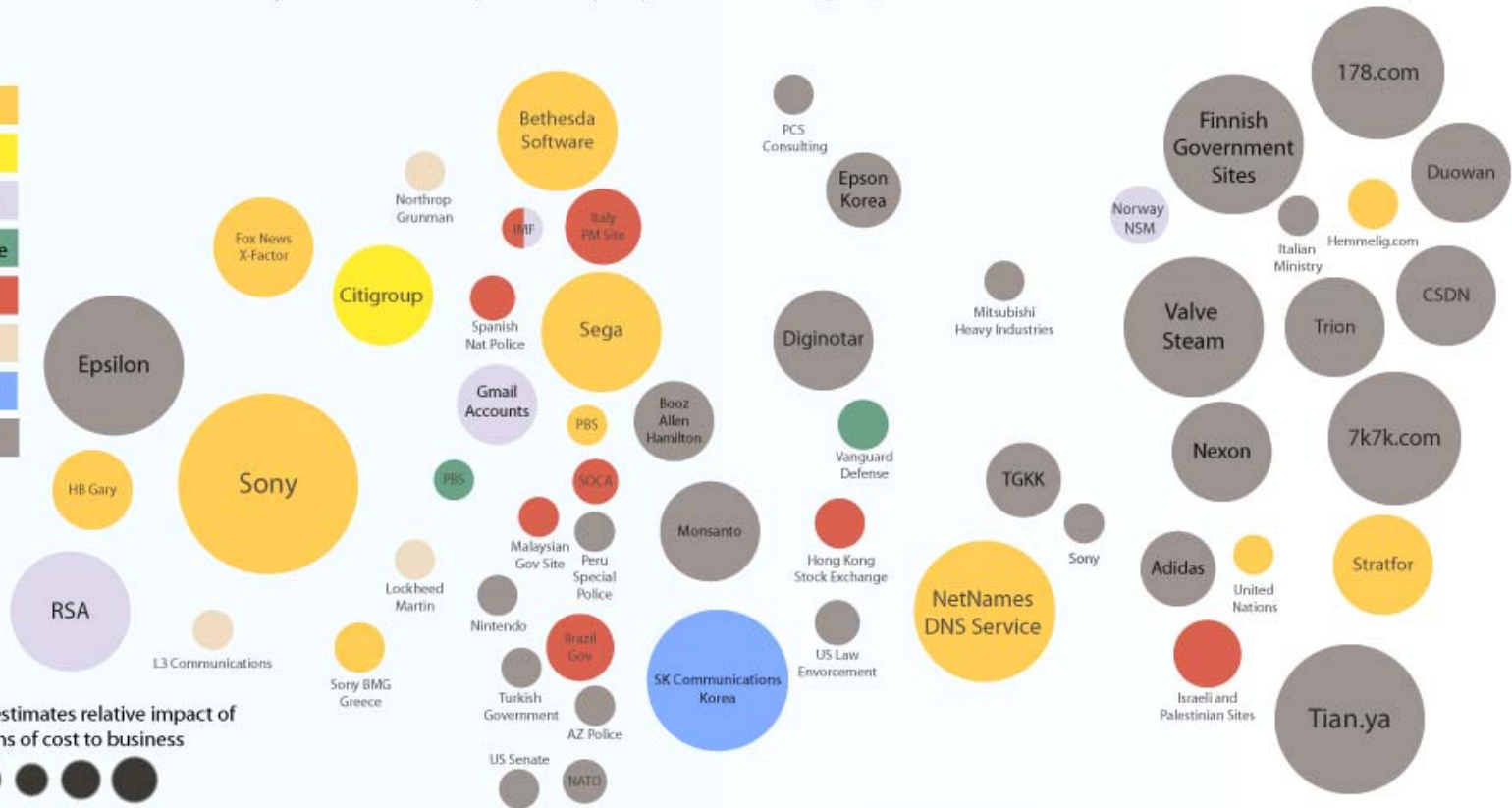
2011 Sampling of Security Incidents by Attack Type, Time and Impact
 conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

- 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 March April May June July Aug Sep Oct Nov Dec





EVERYTHING IS EVERYWHERE

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



Security challenges are impacting innovation

External threats

Sharp rise in external attacks from non-traditional sources

- Cyber attacks
- Organized crime
- Corporate espionage
- State-sponsored attacks

Internal threats

Ongoing risk of careless and malicious insider behavior

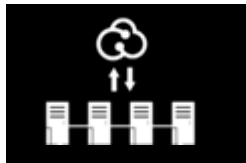
- Administrative mistakes
- Careless inside behavior
- Internal breaches
- Disgruntled employee actions

Compliance

Growing need to address an increasing number of mandates

- National regulations
- Industry standards
- Local mandates

Impacting innovation



Cloud Computing



Mobile Computing

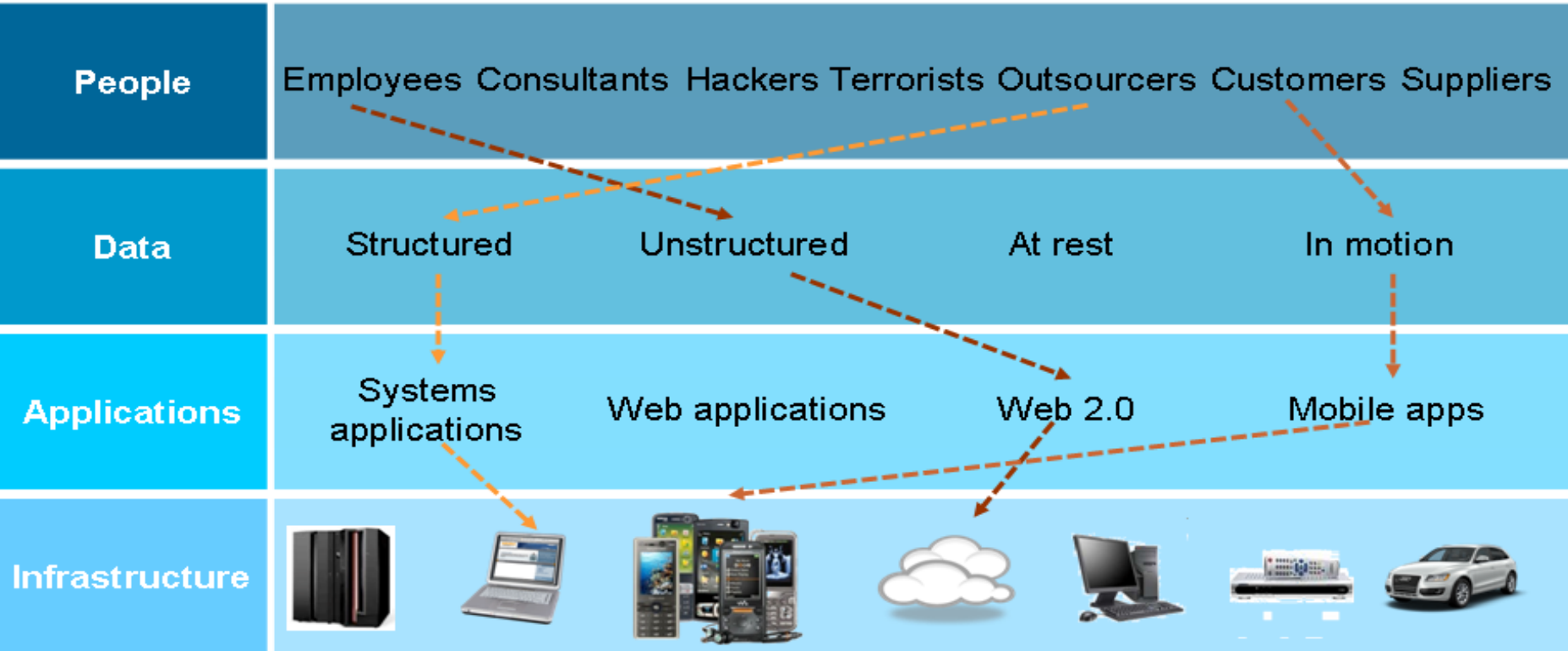


Social Business



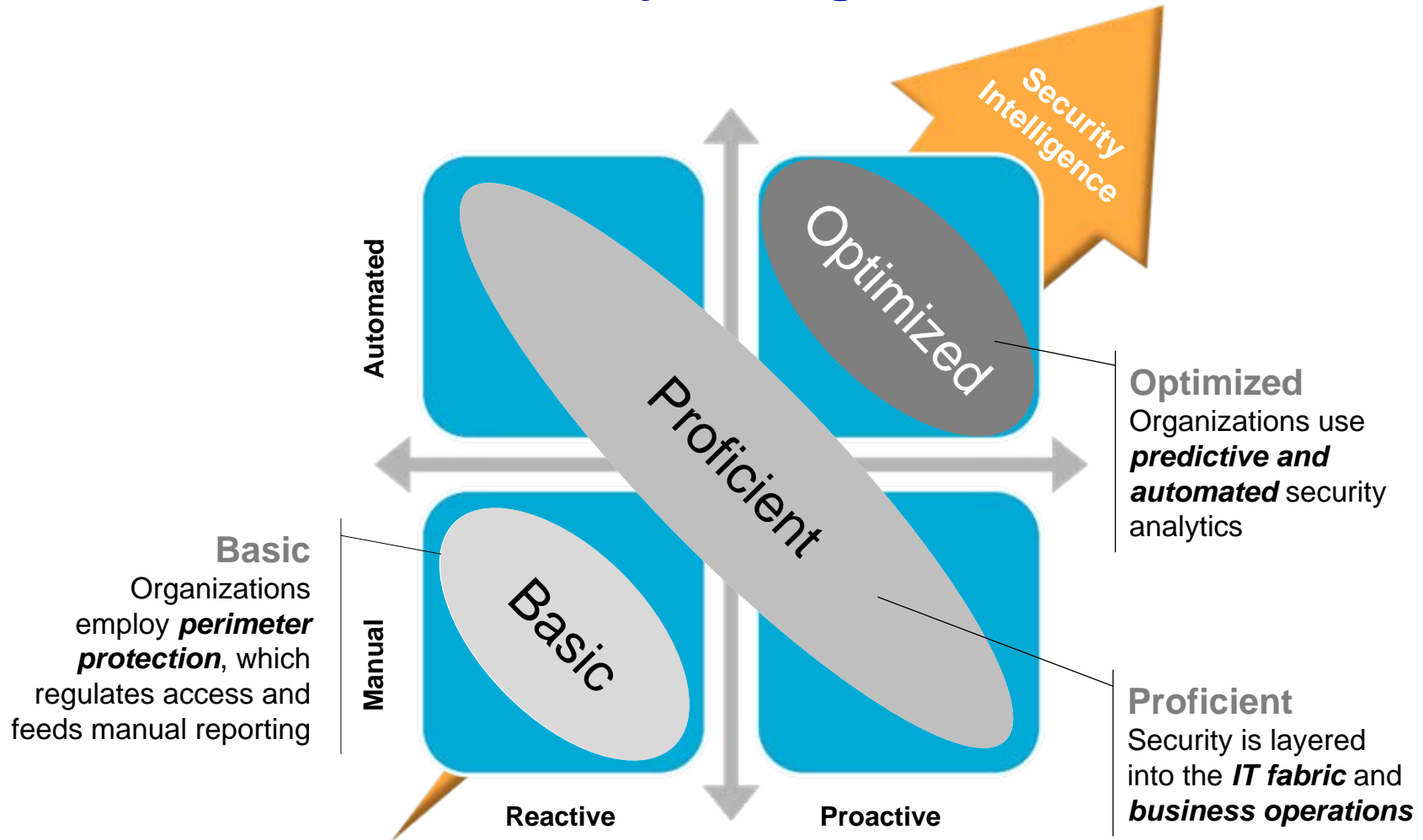
Business Analytics

Solving a security issue is a complex, four-dimensional puzzle



It is no longer enough to protect the perimeter – siloed point products will not secure the enterprise

In this “new normal”, IBM is helping organizations usher in an era of Security Intelligence



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

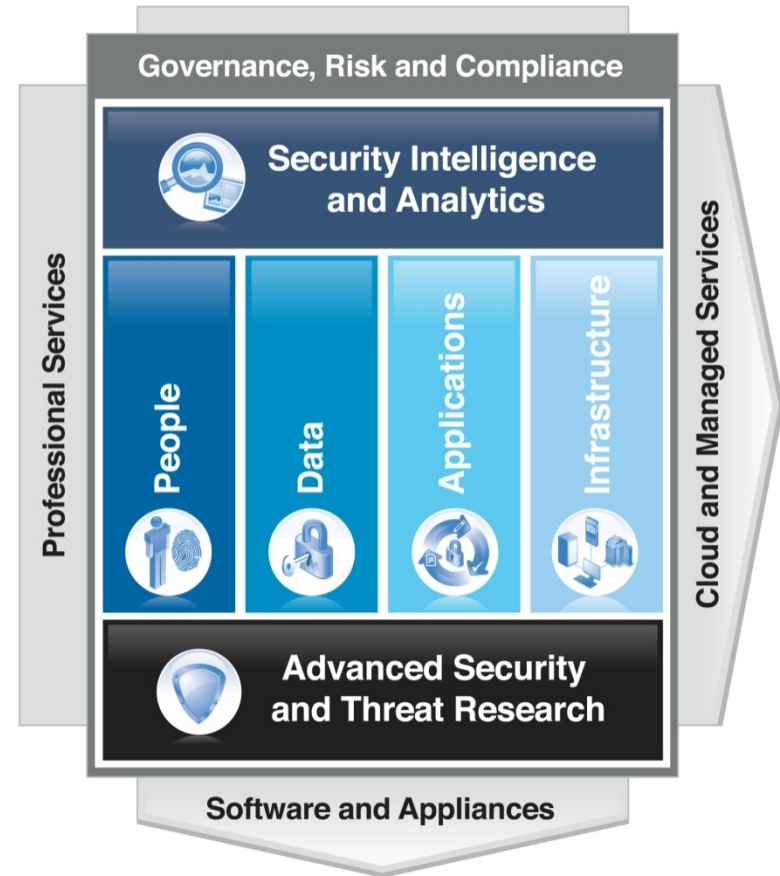


IBM Security Systems

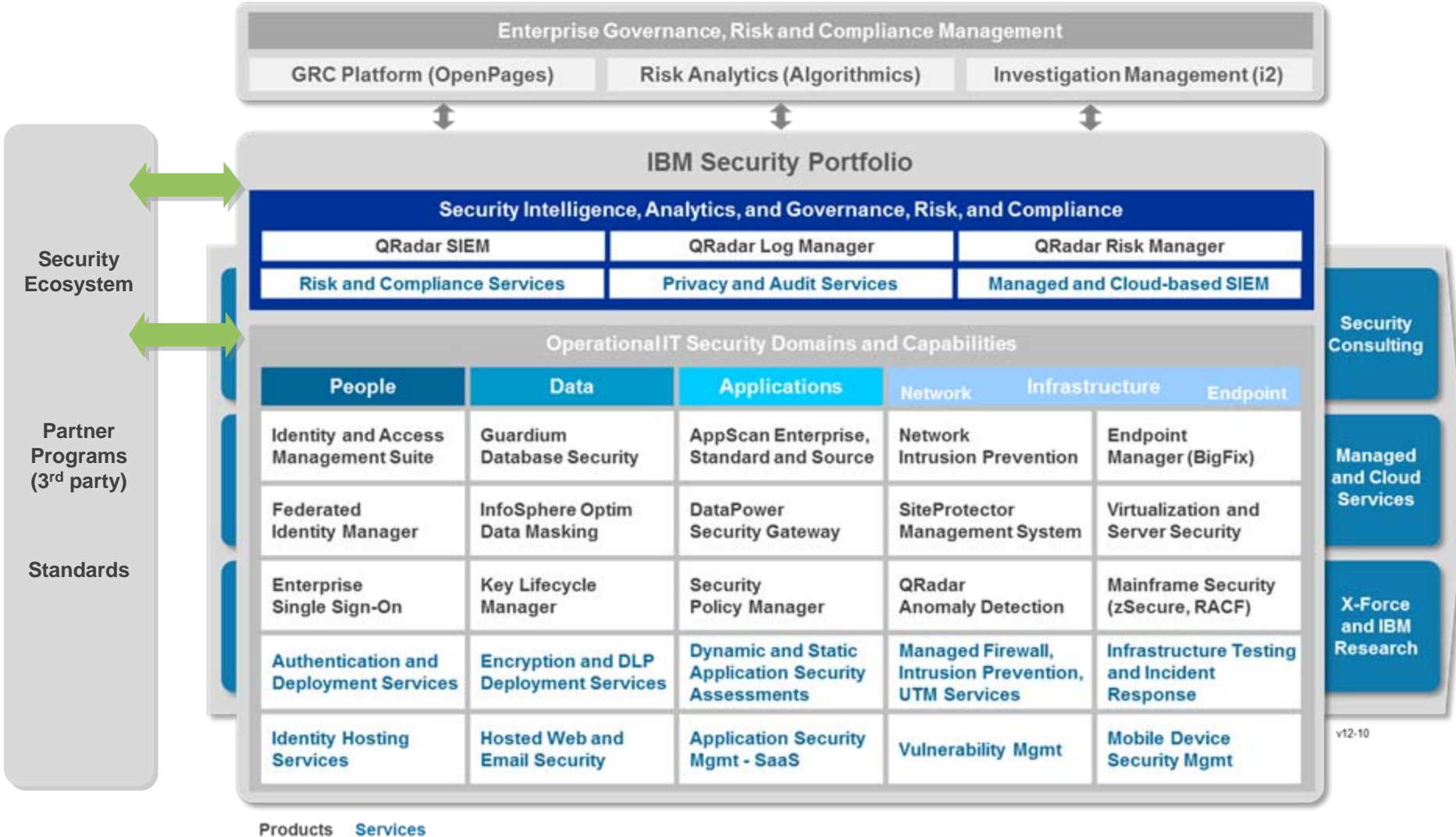
- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise

IBM Security Framework

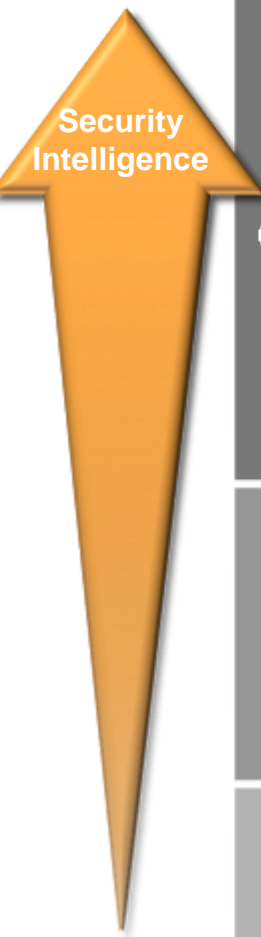


A comprehensive portfolio of products and services across all domains



v12-10

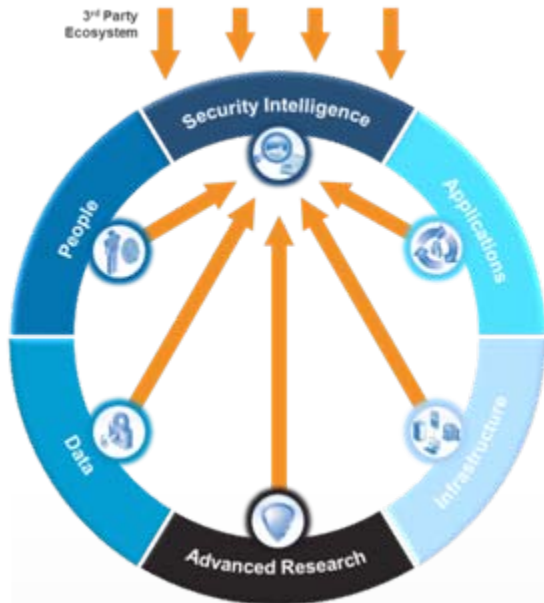
Security Intelligence enables progress to optimized security



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

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

Integrated Intelligence.



- Consolidate and correlate siloed information from hundreds of sources
- Designed to 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 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: Unmatched global coverage and security awareness



IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration



10B analyzed Web pages & images
 150M intrusion attempts daily
 40M spam & phishing attacks
 46K documented vulnerabilities
 Millions of unique malware samples



World Wide Managed Security Services Coverage

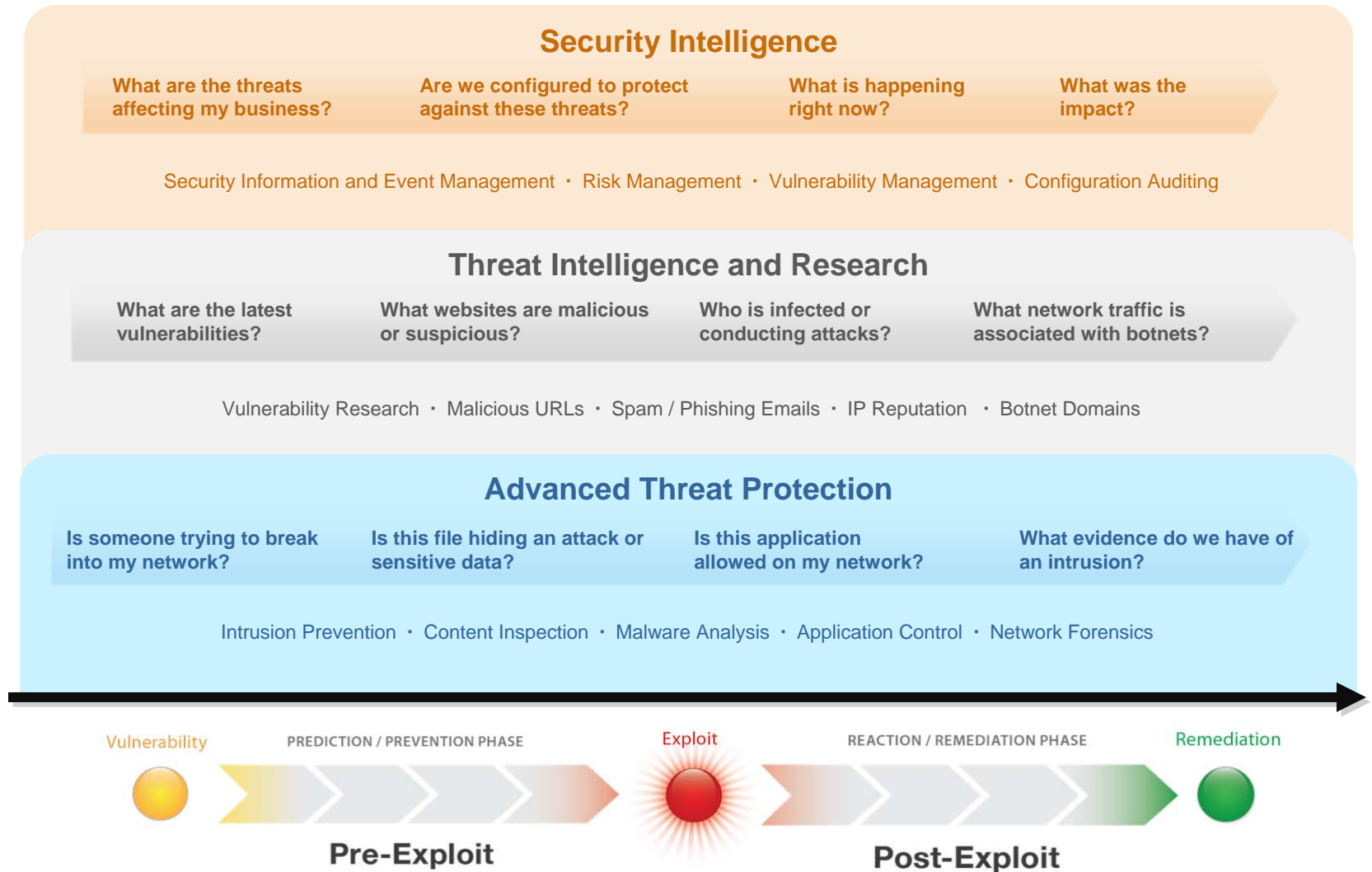
- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)



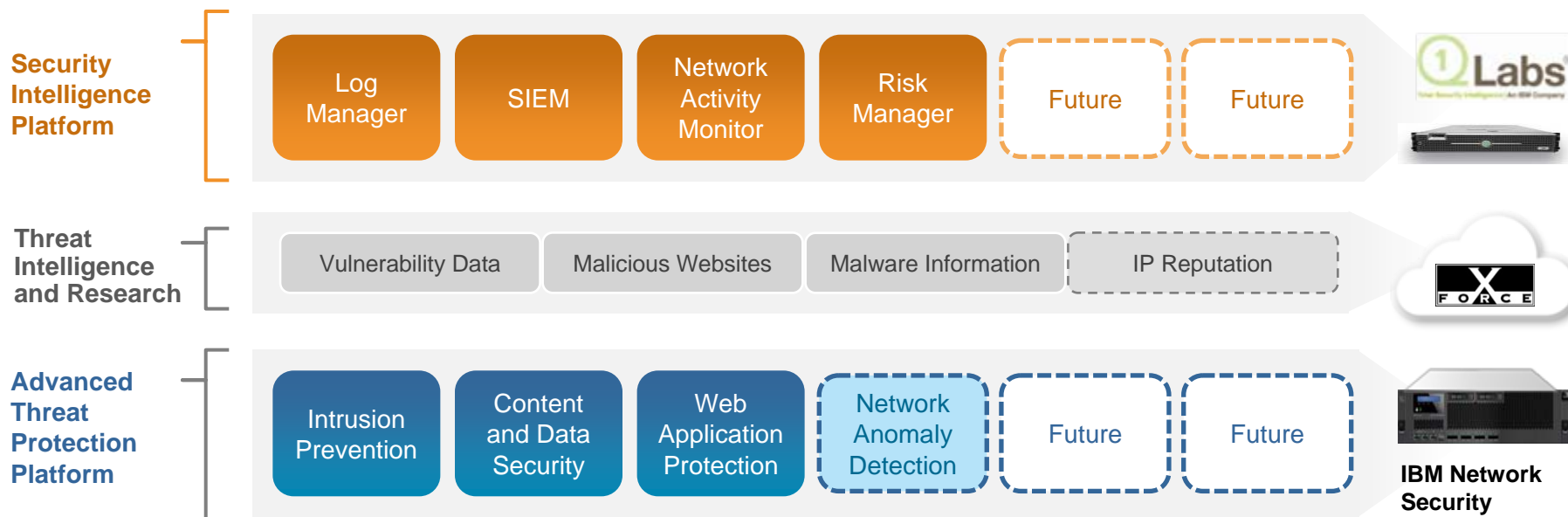
Advanced Threats

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

The Requirements for an Advanced Threat Protection Platform



IBM's Vision for Advanced Threat Protection



Advanced Threat Protection Platform

Ability to prevent sophisticated threats and detect abnormal network behavior by leveraging 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 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 detect, investigate and remediate threats

System z Self-protection guards against network threats

- *Self-protection is a key element in a total defense in depth strategy*
- z/OS provides network security to protect the system from network intrusions:
 - Policy-based network security helps ensure compliance and eases auditing
 - Integrated Intrusion Detection Services integrated into z/OS
 - TCP/IP stacks, ports and network addresses can be RACF protected
 - Protects against network attacks even for encrypted data
 - Can prevent rogue programs from taking over ports between guests (Linux, z/OS)
 - Highly secure internal networking between virtual servers limits external attacks
 - Unique HiperSockets that virtualizes network traffic within memory
 - Defense Manager enables rapid response to attack
 - Timed filter rules installed into network stack block attacking packets
 - Blocks access from remote resources and to System z resources
 - Easy installation and removal of blocking rules using authorized automation or manual commands

Network Security: Protecting data in flight

Encryption everywhere will become standard practice in response to new regulations and internal IT security policies.

z/OS provides network security that protects data in the network:

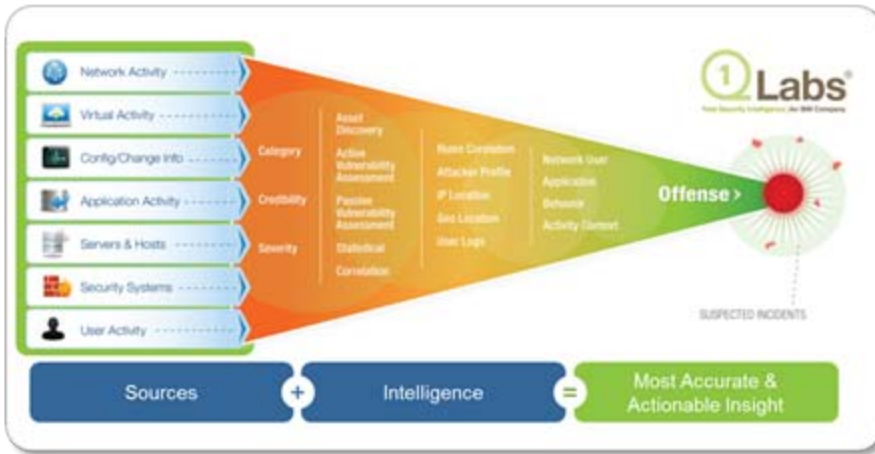
- Easy to configure policy-based network security options
 - Encryption for file transmissions (FTP, OpenSSH, TLS/SSL)
 - Application encryption (TLS/SSL, IPsec)
 - Secure tunneling (Virtual Private Networks)
- Faster time to deploy for network encryption for applications
 - Application Transparent TLS (AT-TLS) secures application network traffic
 - No application changes needed
- Transparent use of built-in acceleration by network security protocols
 - Utilizes the System z CPACF and cryptographic coprocessors
 - zIIP specialty engine security protocol offload improves encrypted bulk data workload throughput



Security Intelligence

The consolidation and correlation of security data to provide new insights and protection

QRadar: Security Intelligence in a unified console



Integrated Intelligence.



Recent integration announcements:

- **People:** IBM Identity Manager and Access Manager
- **Data:** IBM Guardium Database Security
- **Applications:** IBM AppScan
- **Infrastructure:** zSecure, IBM End-Point Manager (+ *Site Protector and IBM Security NIPS today*)
- **Threat Intelligence:** IBM X-Force real-time feeds
- Integration with **non-IBM products** such as Symantec DLP, WebSense, Stonesoft, Guidance, ...

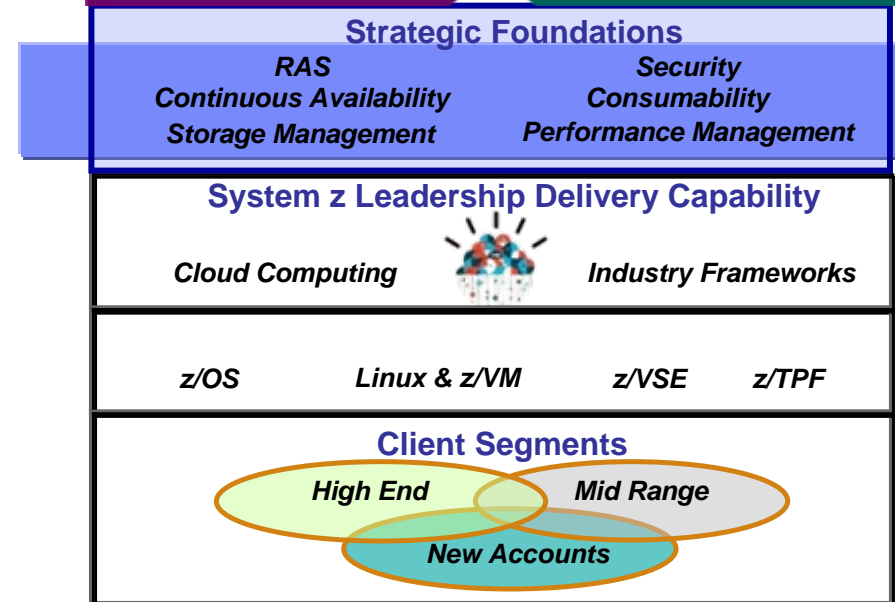
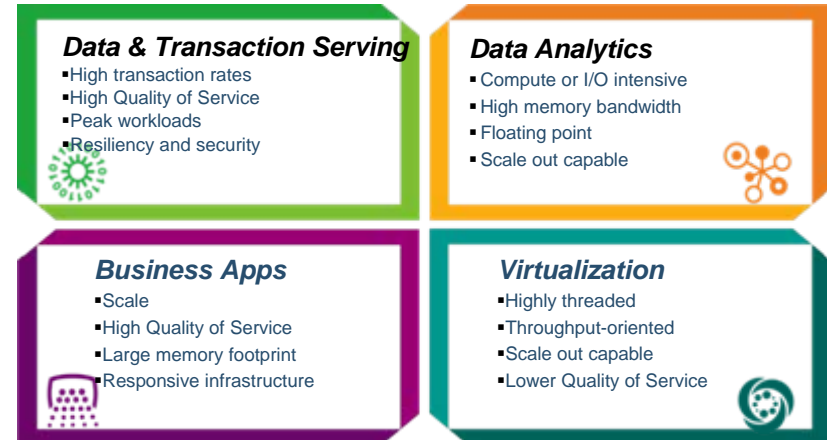
System z specific capabilities

Security is one of the strategic foundations of System z

- Integrated security that spans from:
 - Hardware
 - Firmware
 - Hypervisors
 - System z Operating Systems
 - Middleware and applications
 - Network

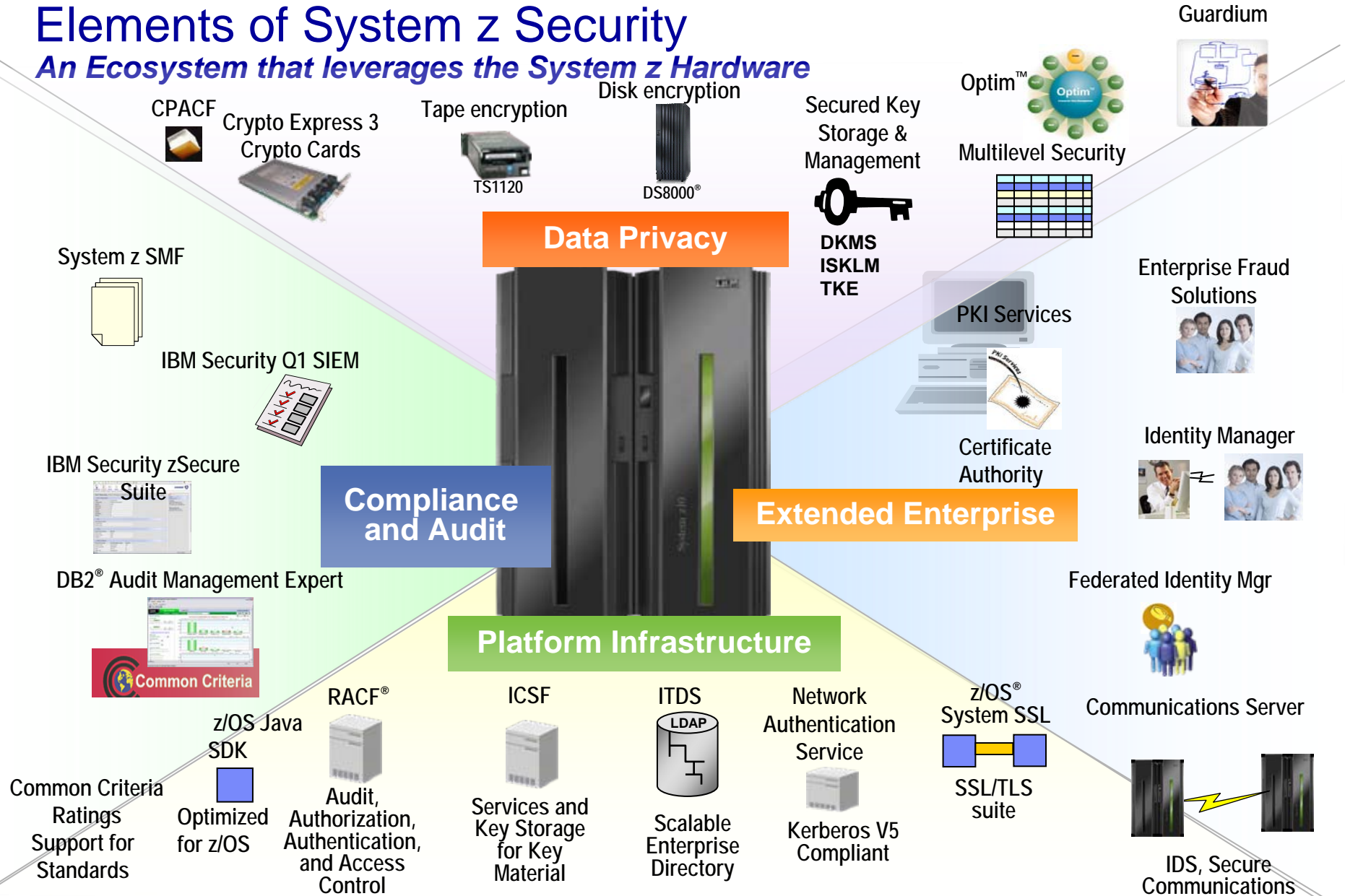
- Integrated security that spans to an zEnterprise ensemble
- Hardware and firmware assists enhance security QoS
- System z security is integrated at all “levels” of the platform
- From a strategic view -- multiple security strategies converge -- to create unified view of security on System z

Optimizing System z for Strategic Workloads & Industry-based Initiatives



Elements of System z Security

An Ecosystem that leverages the System z Hardware





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.