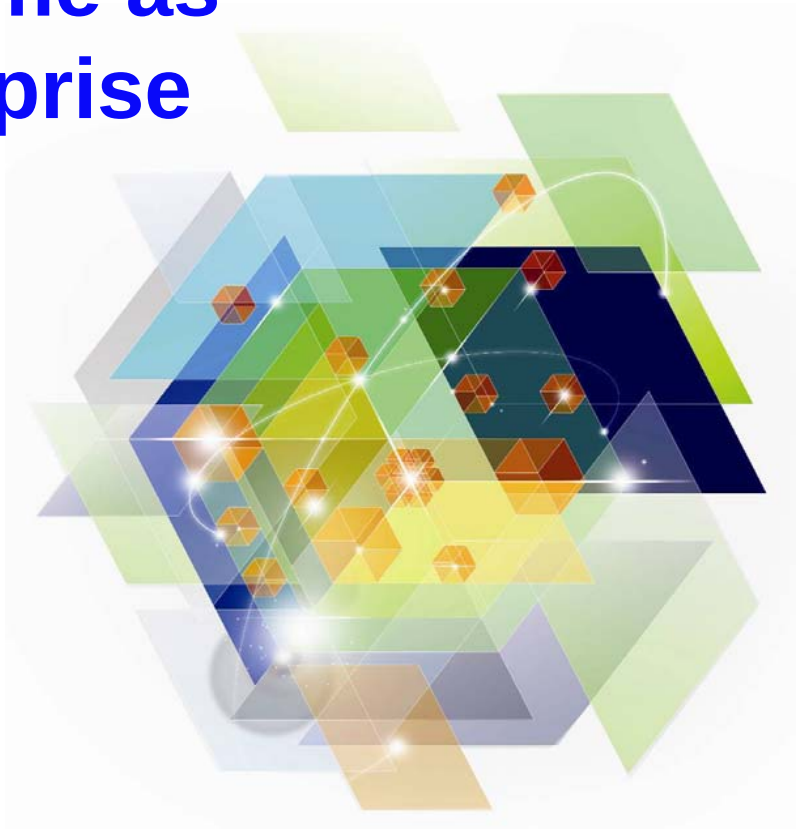
Leveraging your mainframe as part of your overall enterprise security strategy



Agenda

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

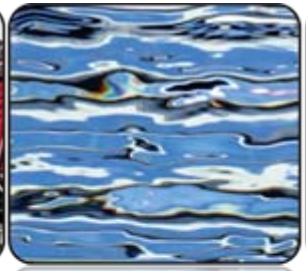
The Planet is getting more…

Smart Supply Chains

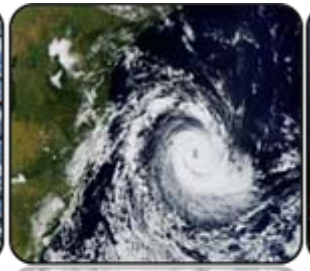
Smart Countries

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

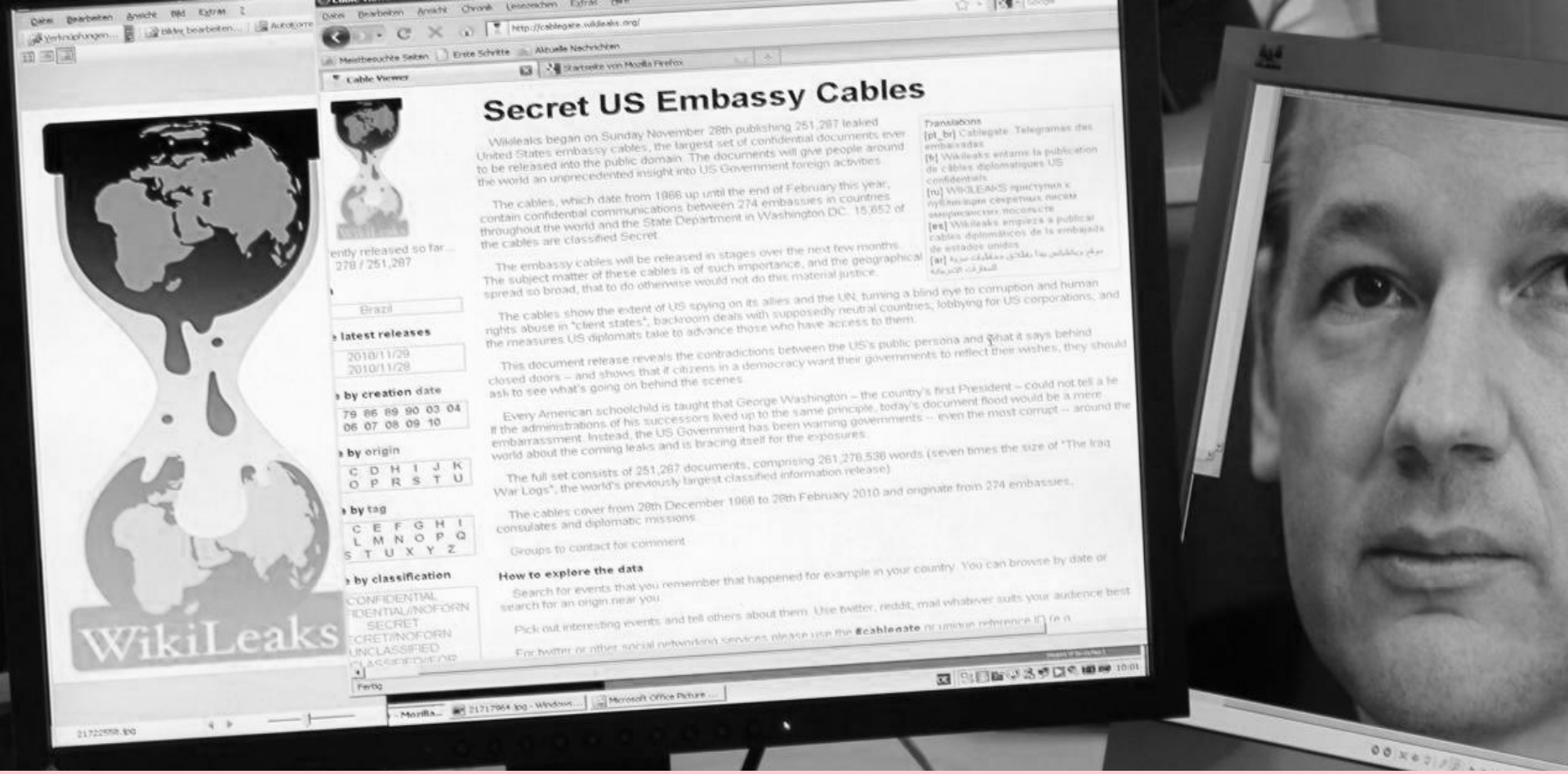
Smart Food Systems

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

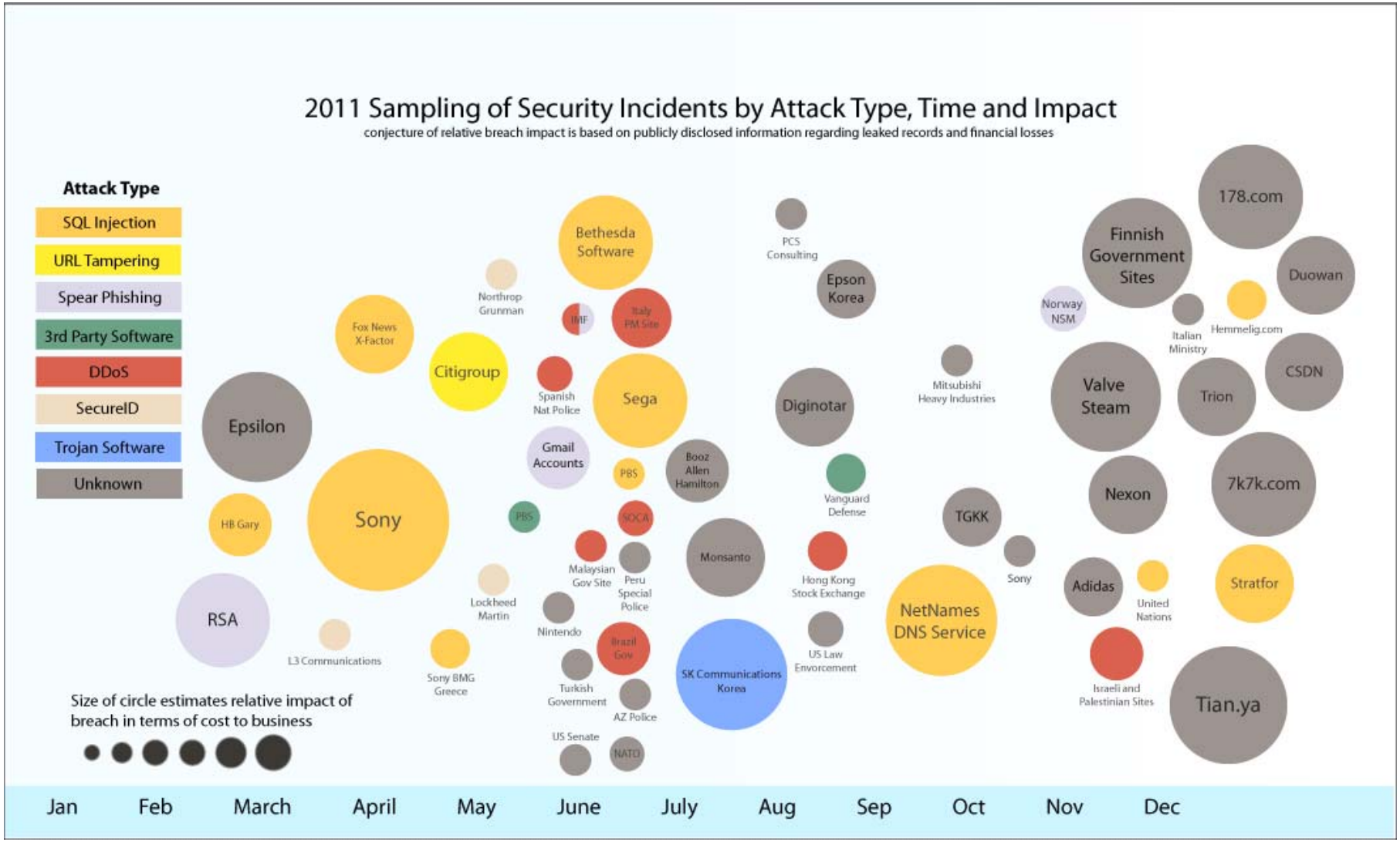
With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared.



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



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

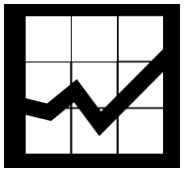
- National regulations
- Industry standards
- Local mandates

Impacting innovation

Cloud Computing

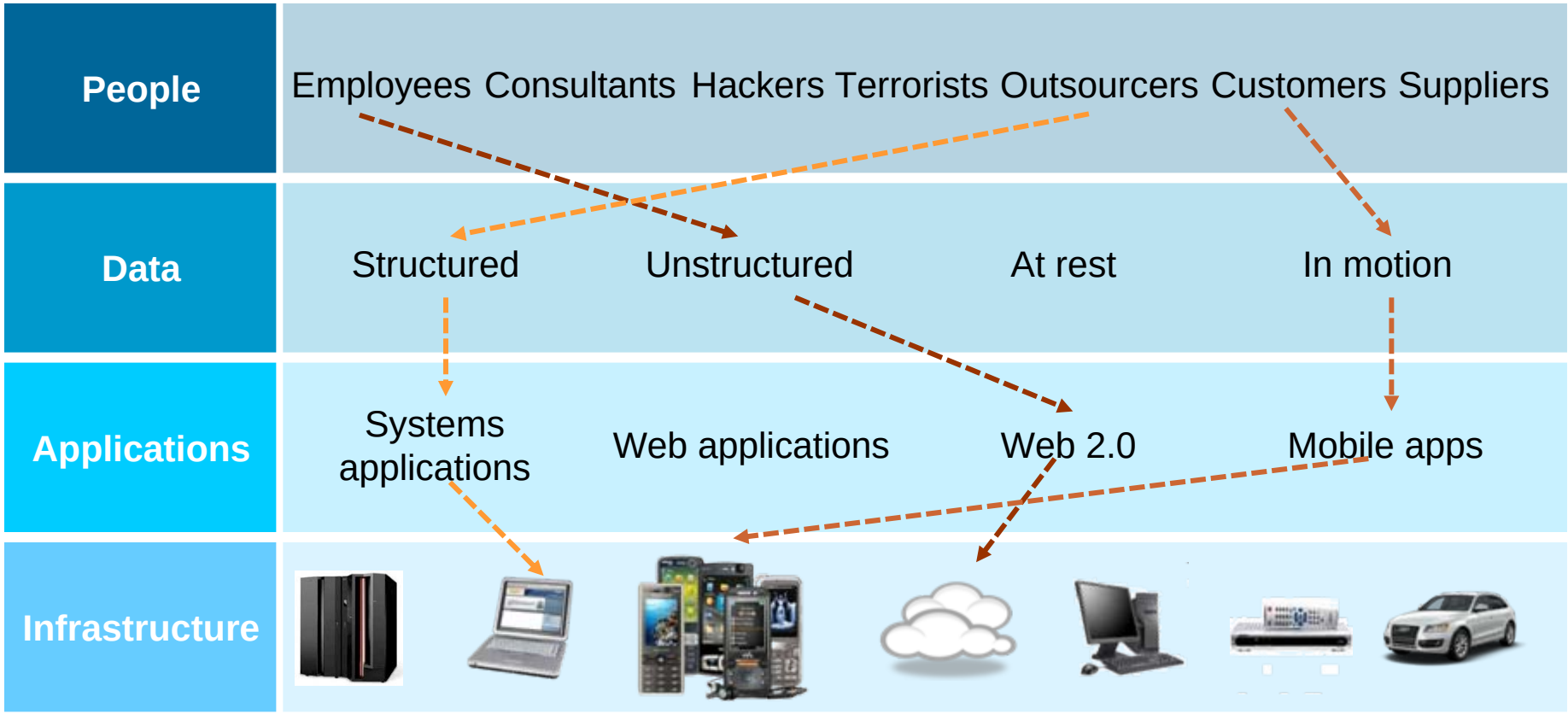
Mobile Computing

Social Business



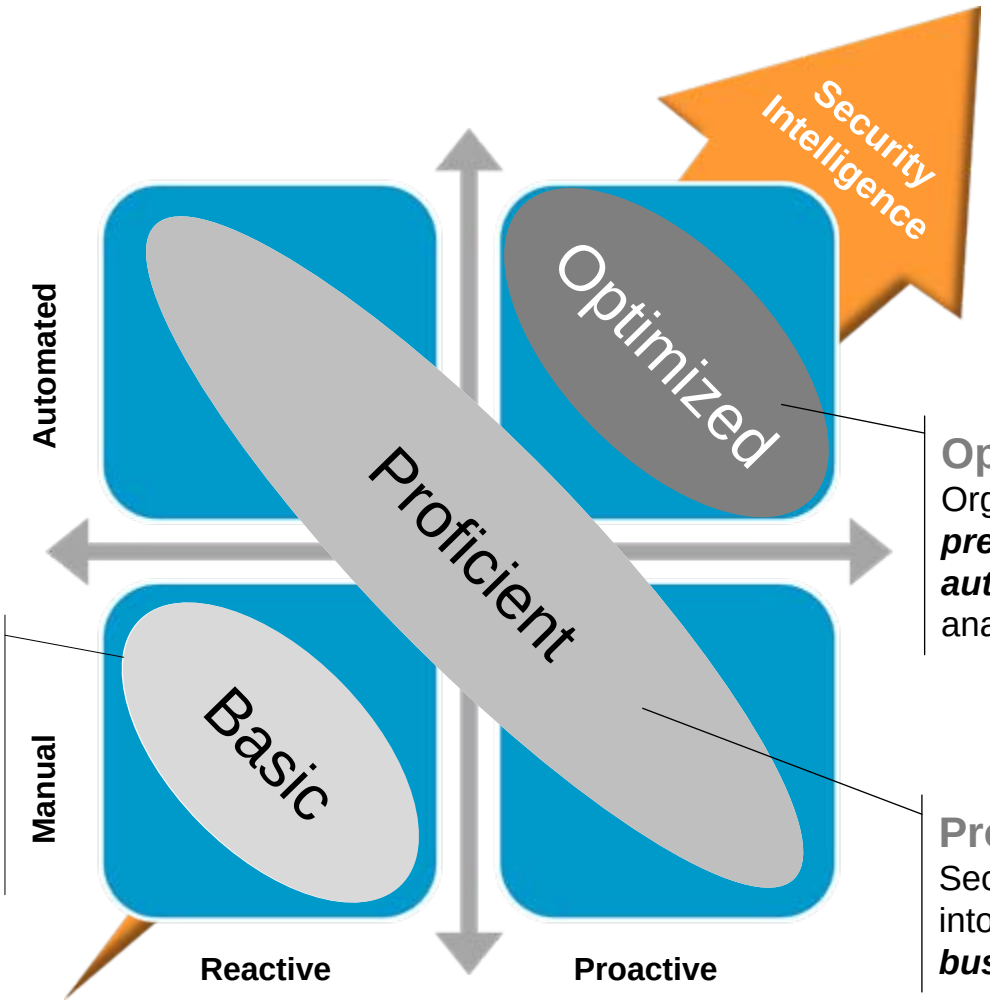
Business Analytics

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



Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Optimized
Organizations use ***predictive and automated*** security analytics

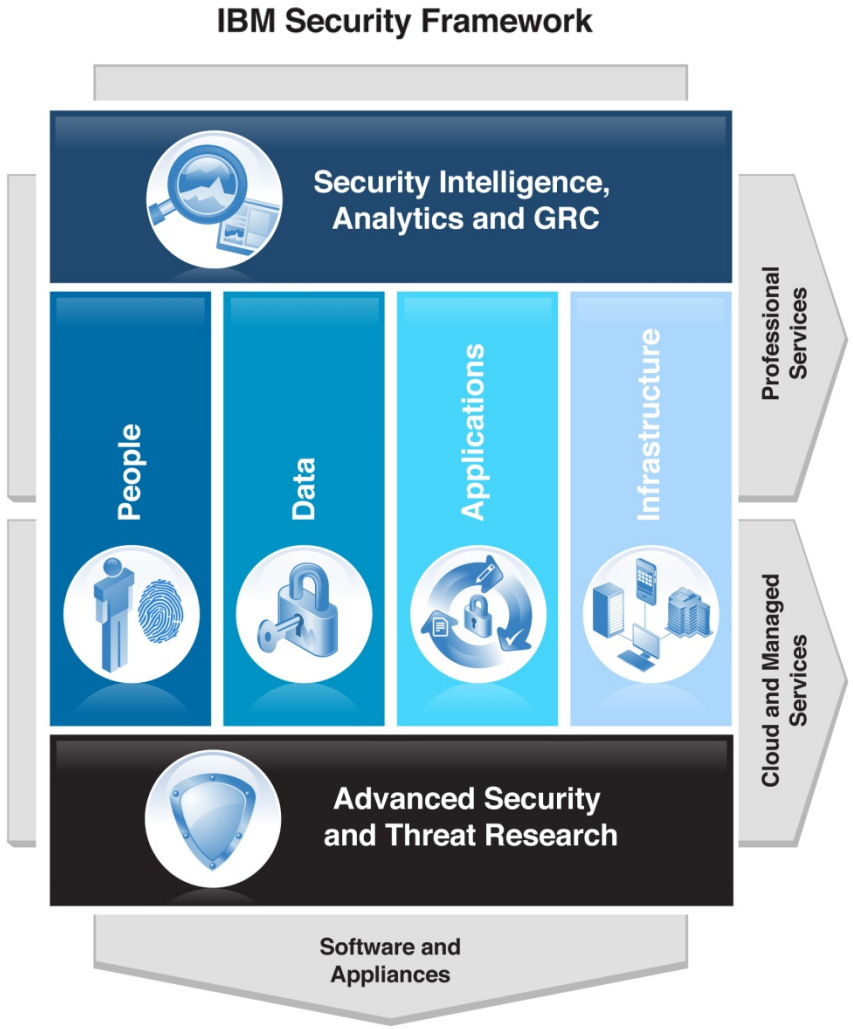
Proficient
Security is layered into the ***IT fabric*** and ***business operations***

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

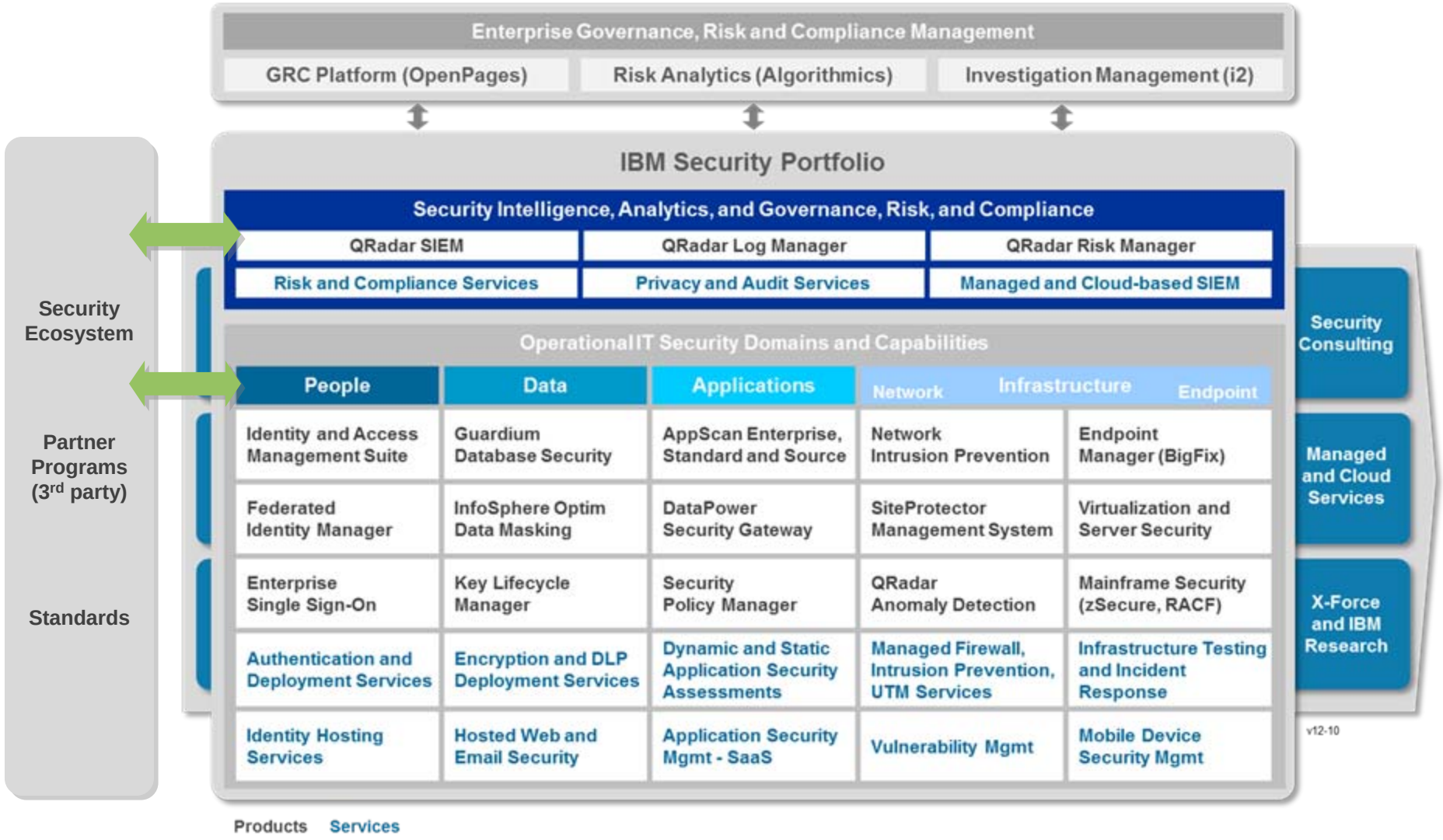
IBM Security Systems

- 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

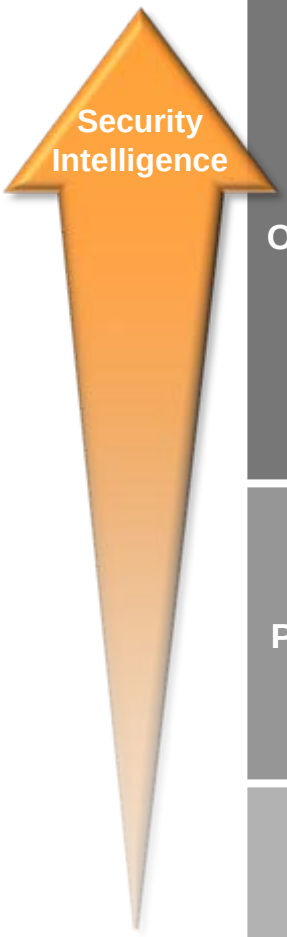
Intelligence • Integration • Expertise



A comprehensive portfolio of products and services across all domains



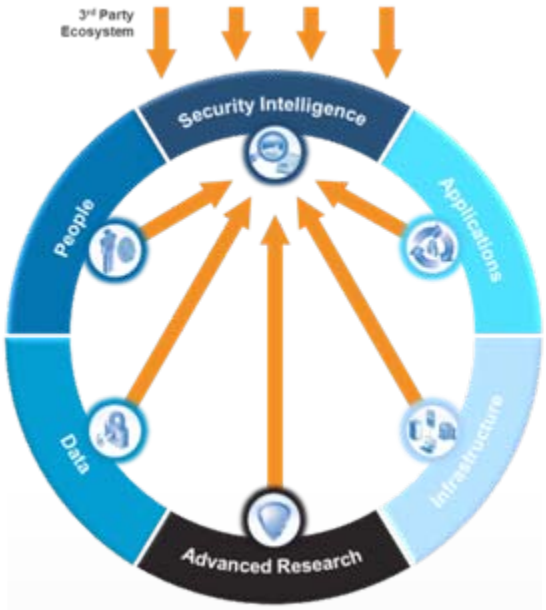
Security Intelligence is enabling progress to optimized security



	People	Data	Applications	Infrastructure
	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

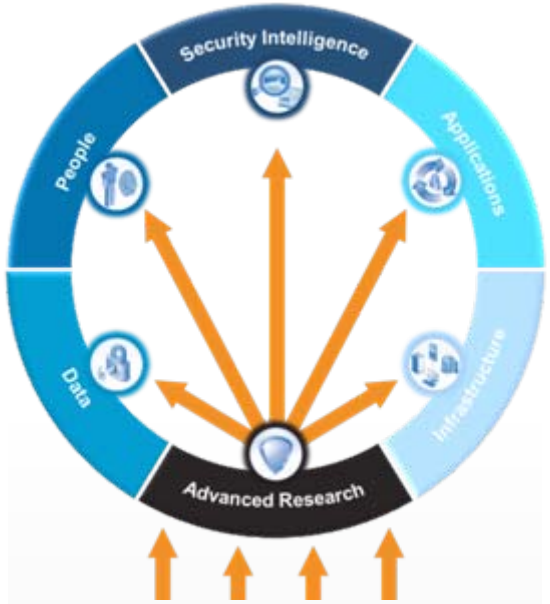
Integration: Help increase security, collapse silos, and reduce complexity

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

X-FORCE

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

Security Intelligence

What are the threats affecting my business? | **Are we configured to protect against these threats?** | **What is happening right now?** | **What was the impact?**

Security Information and Event Management · Risk Management · Vulnerability Management · Configuration Auditing

Threat Intelligence and Research

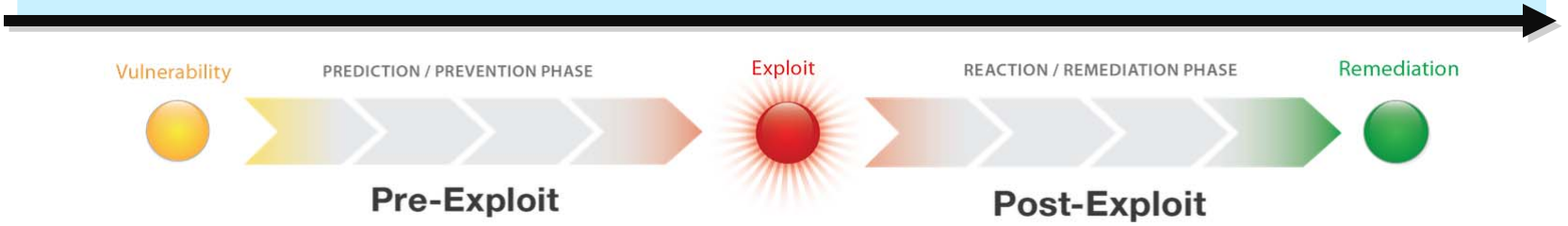
What are the latest vulnerabilities? | **What websites are malicious or suspicious?** | **Who is infected or conducting attacks?** | **What network traffic is associated with botnets?**

Vulnerability Research · Malicious URLs · Spam / Phishing Emails · IP Reputation · Botnet Domains

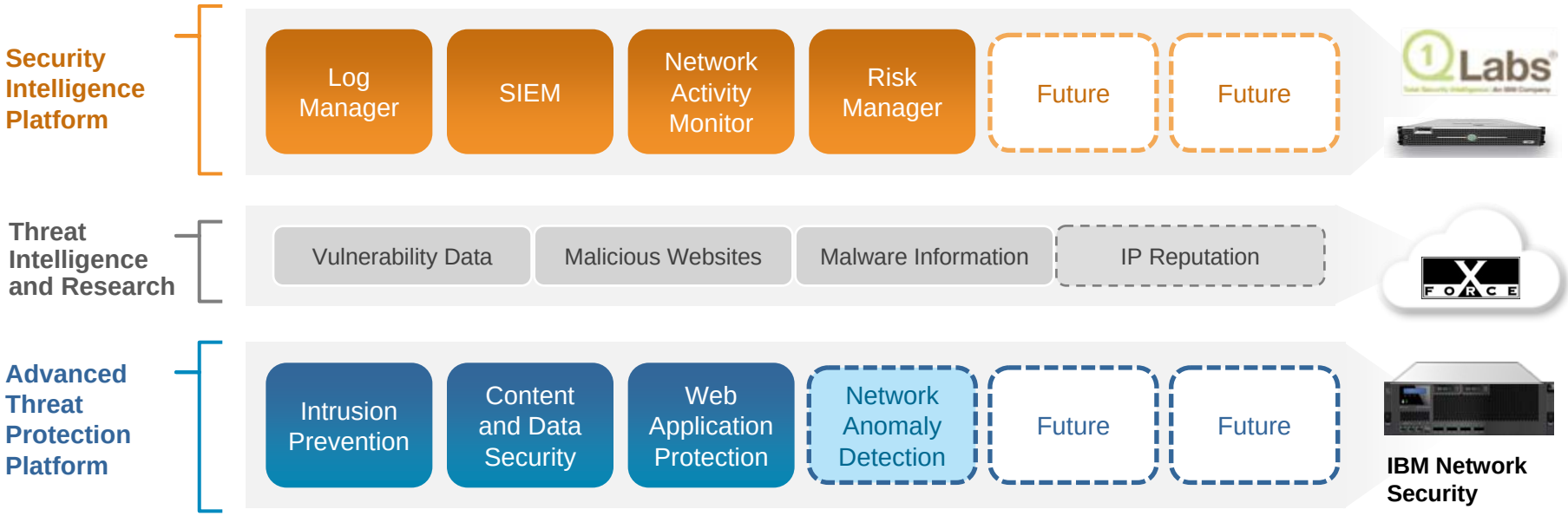
Advanced Threat Protection

Is someone trying to break into my network? | **Is this file hiding an attack or sensitive data?** | **Is this application allowed on my network?** | **What evidence do we have of an intrusion?**

Intrusion Prevention · Content Inspection · Malware Analysis · Application Control · Network Forensics



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
    - 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.

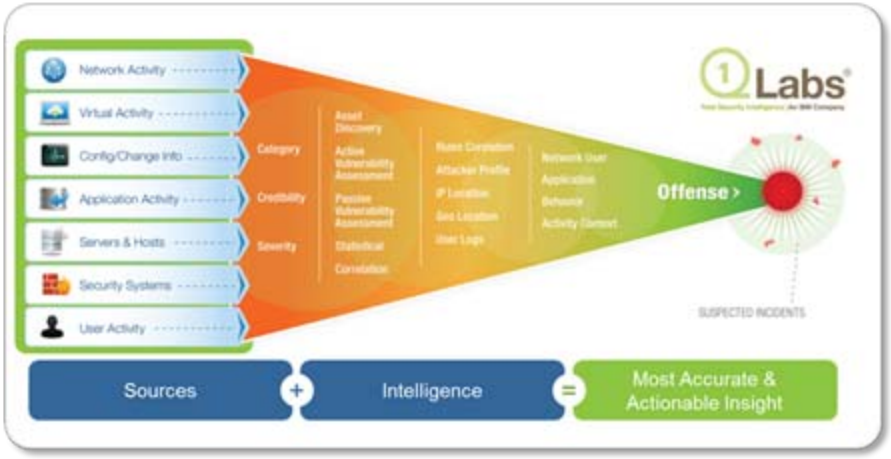
z/OS provides network security that protects data in the network:

- 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 through put

Security Intelligence

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

QRadar: Security Intelligence in a unified console



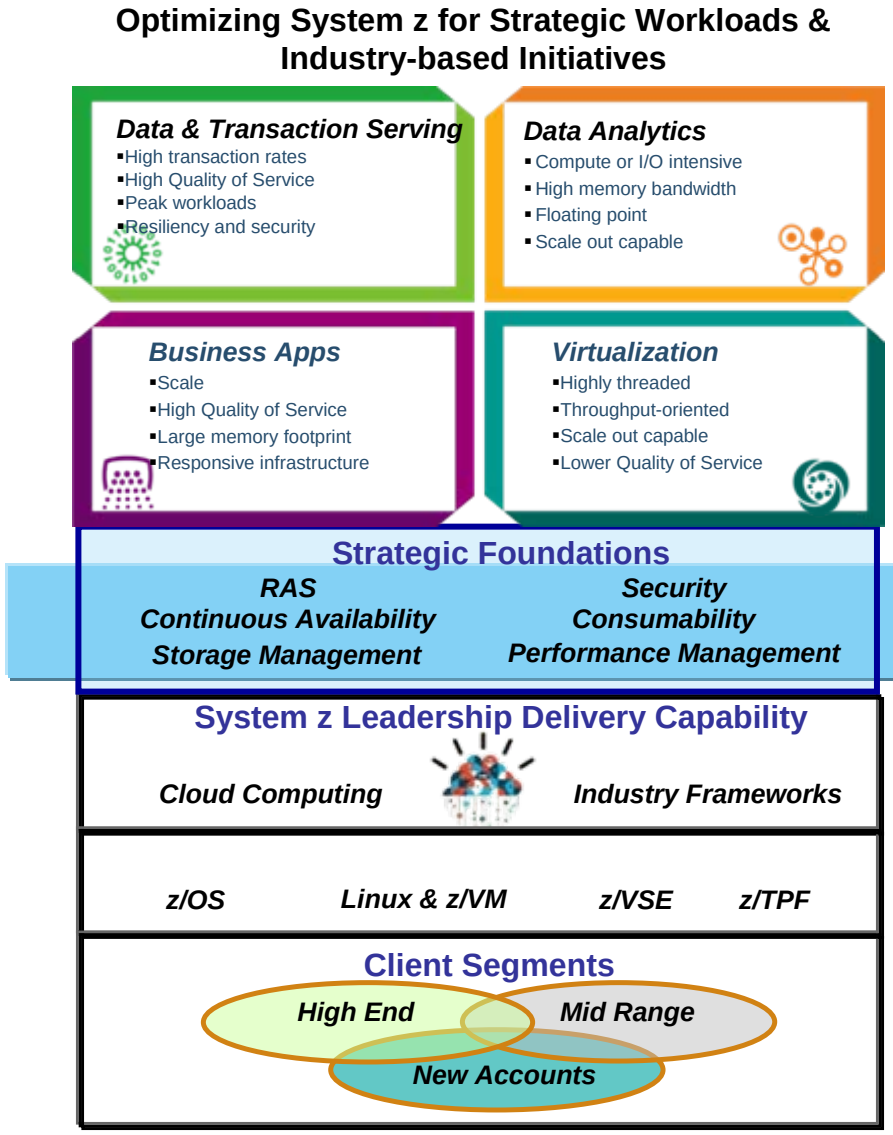
Recent integration announcements:

- **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



Elements of System z Security

An Ecosystem that leverages the System z Hardware

CPACF

Crypto Express 3 Crypto Cards

Tape encryption

TS1120

Disk encryption

DS8000®

Secured Key Storage & Management

DKMS
ISKLM
TKE

Optim™

Multilevel Security

Guardium

Data Privacy

System z SMF

IBM Security Q1 SIEM

IBM Security zSecure Suite

Compliance and Audit

DB2® Audit Management Expert

PKI Services

Certificate Authority

Enterprise Fraud Solutions

Identity Manager

Extended Enterprise

Platform Infrastructure

Common Criteria

Common Criteria Ratings Support for Standards

z/OS Java SDK

Optimized for z/OS

RACF®

Audit, Authorization, Authentication, and Access Control

ICSF

Services and Key Storage for Key Material

ITDS

LDAP

Scalable Enterprise Directory

Network Authentication Service

Kerberos V5 Compliant

z/OS® System SSL

SSL/TLS suite

Federated Identity Mgr

Communications Server

IDS, Secure Communications

ibm.com/security