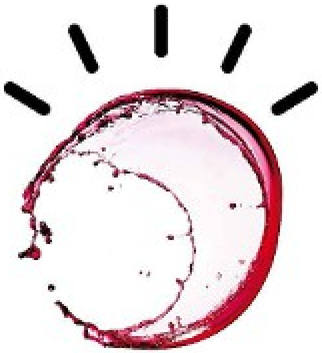
Degustare la crescita

Un percorso in 4 tappe alla scoperta delle soluzioni IBM

Security Intelligence:
un approccio integrato e proattivo



The current environment is putting new demands on security

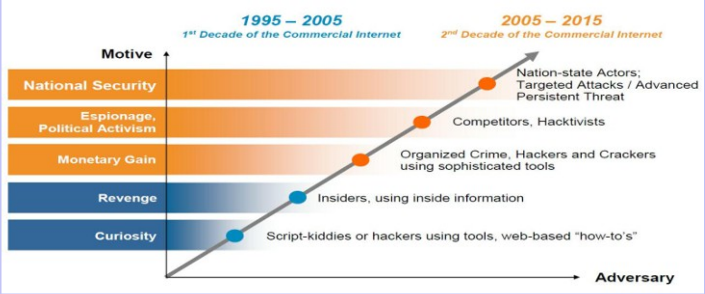
New Business Models, New Technologies

Mobile Collaboration / BYOD

Cloud / Virtualization

Large existing IT infrastructures with a globalized workforce, 3rd party services, and a growing customer base

Velocity of Threats

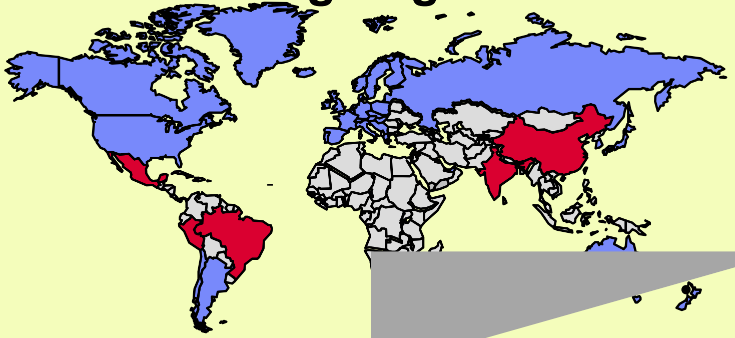


1995 – 2005
1st Decade of the Commercial Internet
2005 – 2015
2nd Decade of the Commercial Internet
Motive
National Security
Espionage, Political Activism
Monetary Gain
Revenge
Curiosity
Nation-state Actors; Targeted Attacks / Advanced Persistent Threat
Competitors, Hacktivists
Organized Crime, Hackers and Crackers using sophisticated tools
Insiders, using inside information
Script-kiddies or hackers using tools, web-based "how-to's"
Adversary

Social Business Blurring "Social" Identities

Professional
Personal
Risk & Trust Balance

Evolving Regulations



Potential Impacts

Data or Device Loss or Theft

Malware infection Loss of productivity

Regulatory Fines

$$$

Data Leakage

Security need to change and adapt rapidly to this new normal

Data Explosion

Consumerization of IT

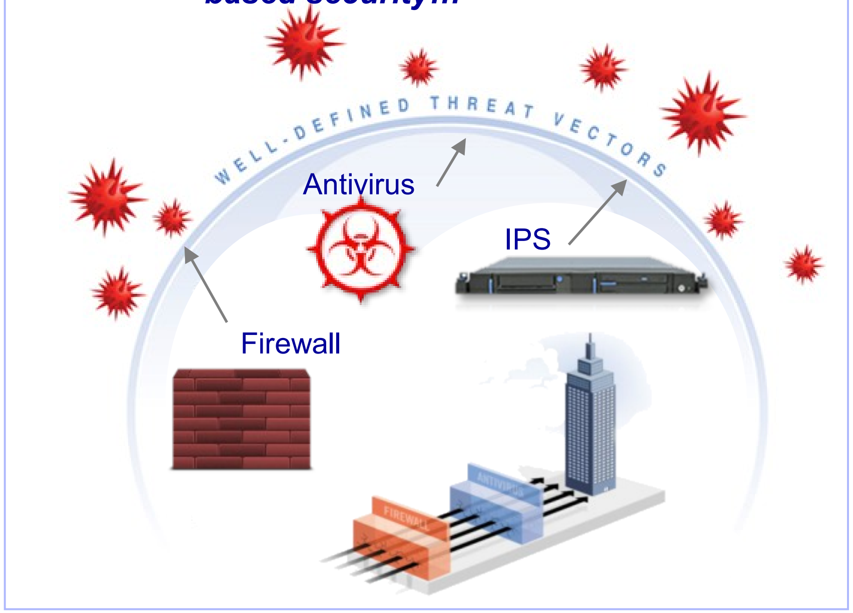
Everything is Everywhere

Attack Sophistication

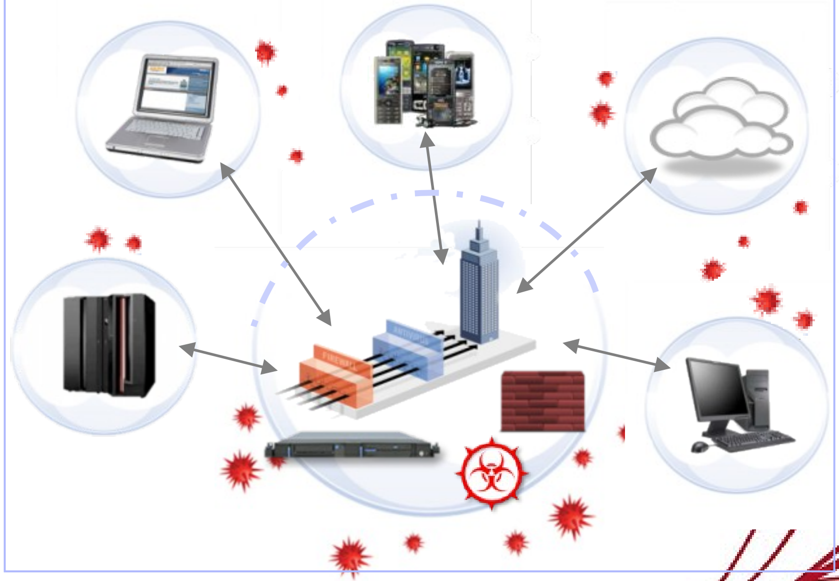
↓ ↓ ↓ ↓

Extending the Perimeter Shifts Protection Focus to Data

Moving from traditional perimeter-based security…



…to logical "perimeter" approach to security—focusing on the data and where it resides



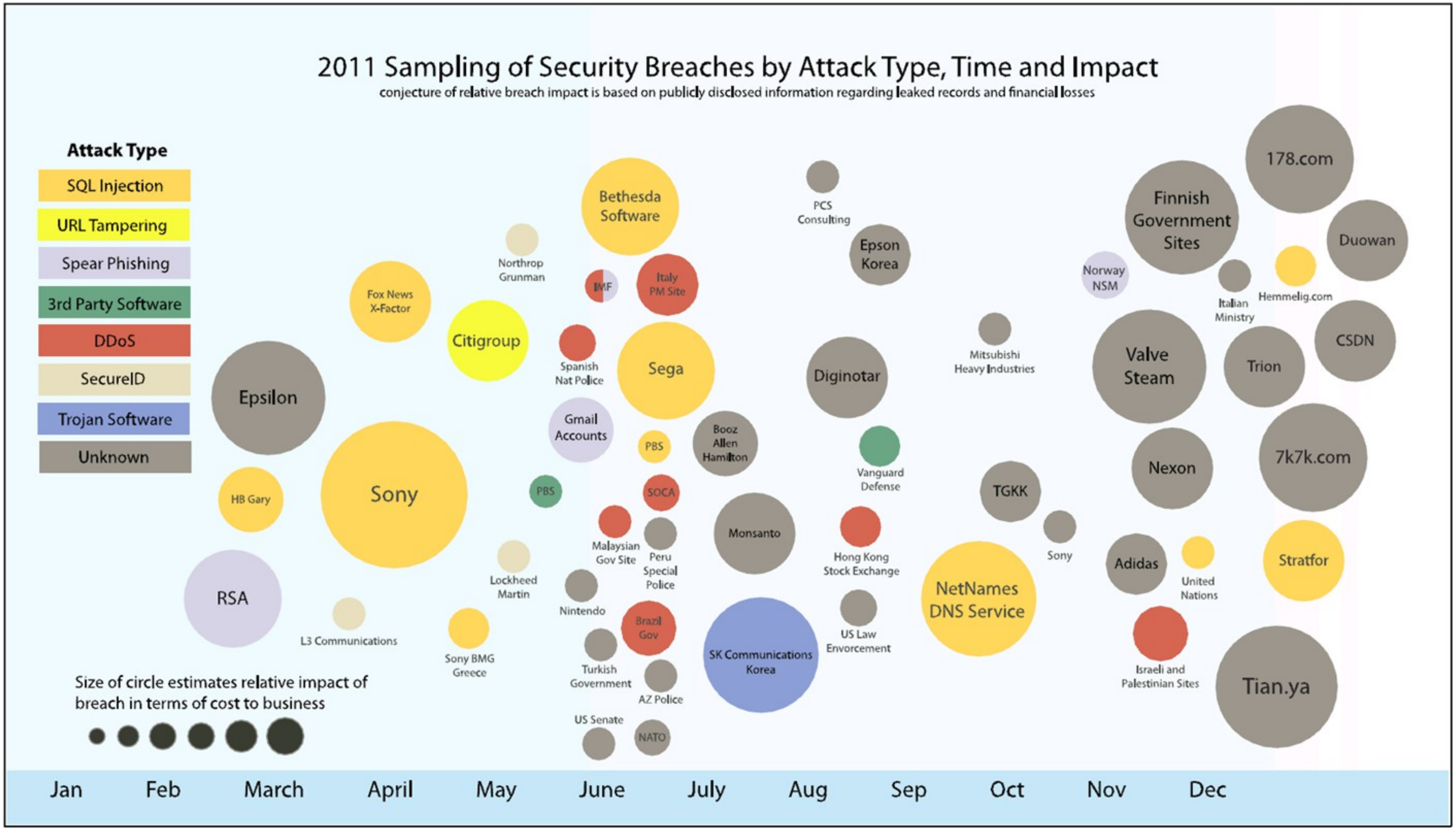
Today’s threats (actors) are more sophisticated

Potential impact

Threat	Type	% of Incidents	Threat Profile
Advanced, Persistent Threat / Mercenary	▪ National governments ▪ Organized crime ▪ Industrial spies ▪ Terrorist cells	Equals less than 10 percent	▪ Sophisticated tradecraft ▪ Foreign intelligence agencies, organized crime groups ▪ Well financed and often acting for profit ▪ Target technology as well as information ▪ Target and exploit valuable data ▪ Establish covert presence on sensitive networks ▪ Difficult to detect ▪ **Increasing in prevalence**
Hacktivist	▪ “White hat” and “black hat” hackers ▪ “Protectors of “Internet freedoms”	Equals less than 10 percent	▪ Inexperienced-to-higher-order skills ▪ Target known vulnerabilities ▪ Prefer denial of service attacks BUT use malware as means to introduce more sophisticated tools ▪ Detectable, but hard to attribute ▪ **Increasing in prevalence**
Opportunist	▪ Worm and virus writers ▪ Script Kiddie	20 percent	▪ Inexperienced or opportunistic behavior ▪ Acting for thrills, bragging rights ▪ Limited funding ▪ Target known vulnerabilities ▪ Use viruses, worms, rudimentary Trojans, bots ▪ Easily detected
Inadvertent Actor	▪ Insiders - employees, contractors, outsourcers	60 percent	▪ No funding ▪ Causes harm inadvertently by unwittingly carrying viruses, or posting, sending or losing sensitive data ▪ Increasing in prevalence with new forms of mobile access and social business

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434

Targeted attacks shake businesses and governments



Source: IBM X-Force® 2011 Trend and Risk Report

Top reasons WHY compromises occur

end users/endpoints

1. Double-clicking “on anything”
2. Disabling endpoint security settings
3. Using vulnerable, legacy software and hardware
4. Failing to install security patches
5. Failing to install anti-virus
6. Failing to report lost/stolen device
7. Connecting endpoint to a network from an insecure access point (e.g. Starbucks,McDonald)
8. Using a second access point (e.g. AirCard) creating a bypass
9. Using weak/default passwords and/or using business passwords for personal use
10. Giving passwords over the phone

infrastructure

1. Connecting systems/virtual images to the Internet before hardening them
2. Connecting test systems to the Internet with default accounts/passwords
3. Failing to update or patch systems/applications on a timely basis.
4. Failing to implement or update virus detection software
5. Using legacy/end-of-life software and hardware
6. Running unnecessary services
7. Using insecure back-end management software
8. Failing to remove old/unused user accounts
9. Implementing firewalls with rules that don't stop malicious or dangerous incoming or outgoing traffic
10. Failing to segment network and/or adequately monitor/block malicious traffic with IDS/IPS

80-90% of all security incidents can be easily avoided!

Security Pain Points .. in short

- Keeping up with regulatory and maintain compliance posture
- Data Security Compliance
- Cybercrimes/Attacks
- Cost Take-Out / Cost Reduction for Operational Expenses
- Increased risk of fraud and other criminal activity (inside/outside)
- Increased threats from disgruntled employees
- Information is money
- Protect security and privacy of critical assets (logical/physical)
- Improve operational efficiency – manage costs

IT Security is a board room discussion

Business results

Sony estimates potential $1B long term impact – $171M / 100 customers*

Brand image

HSBC data breach discloses 24K private banking customers

Supply chain

Epsilon breach impacts 100 national brands

Legal exposure

TJX estimates $150M class action settlement in release of credit / debit card info

Impact of hacktivism

Lulzsec 50-day hack-at-will spree impacts Nintendo, CIA, PBS, UK NHS, UK SOCA, Sony …

Audit risk

Zurich Insurance PLc fined £2.275M ($3.8M) for the loss and exposure of 46K customer records

Chief executive officers are under increasing pressure to deliver transformative business value—with limited resources available

Increased risk

40%

of Fortune 500 and popular web sites contain a vulnerability[2]

Budgetary constraints

71%

of the average IT budget is dedicated to ongoing operations[4]

Mobile in the enterprise

90%

of organizations will support corporate apps on a personal devices by 2014[6]

Social business

74%

of enterprise use social media today to communicate with clients[7]

Innovation in the cloud

60%

of chief information officers view cloud computing as critical to their plans[5]

Exploding data growth

2.7ZB

of digital content in 2012, a 50% increase from 2011[3]

Aging Infrastructure

71%

of data centers are over 7 years old[1]

For most clients, security skills shortages make even the simplest tasks a challenge for our clients

58%

are unable to find people with the right skills

53%

complain of the inability to measure the effectiveness of their current security efforts

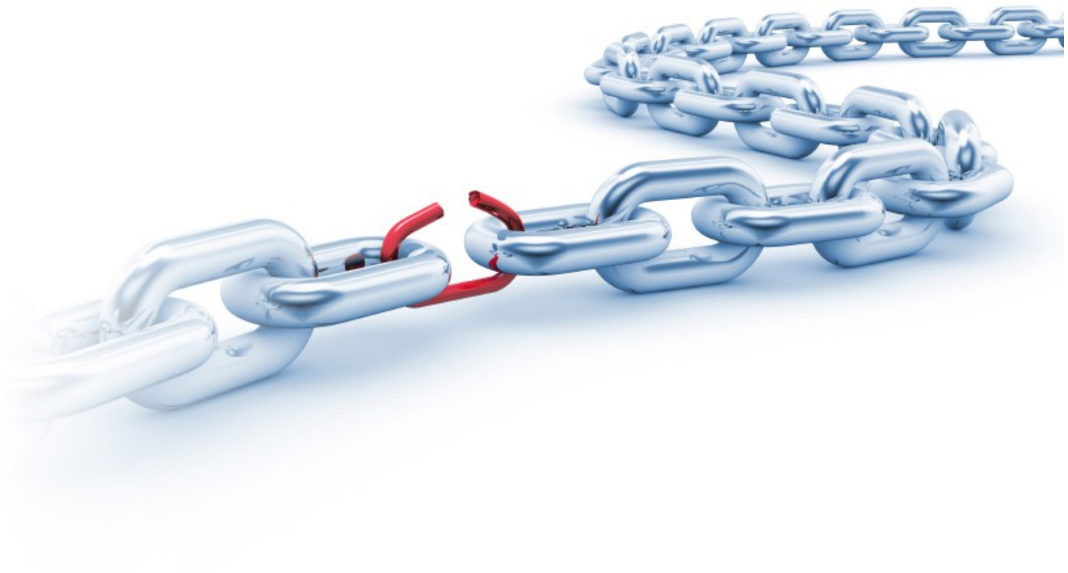
66%

struggle with an understaffed IT team

FORRESTER®

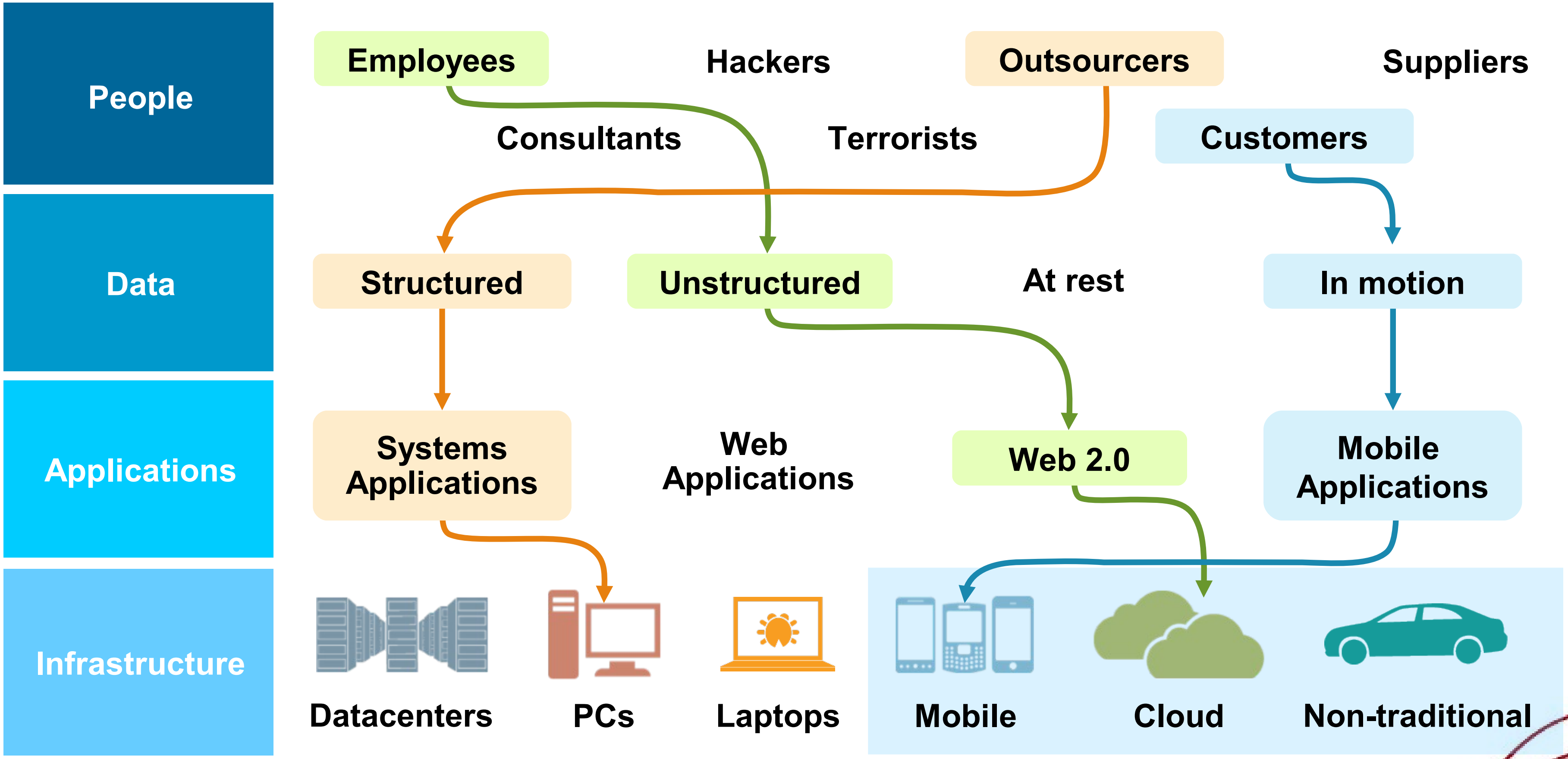
81% of chief information security officer functions are re-organizing or have been re-organized ***within the last six months***.

Corporate Executive Board, Information Risk Executive Council Study, July 2012



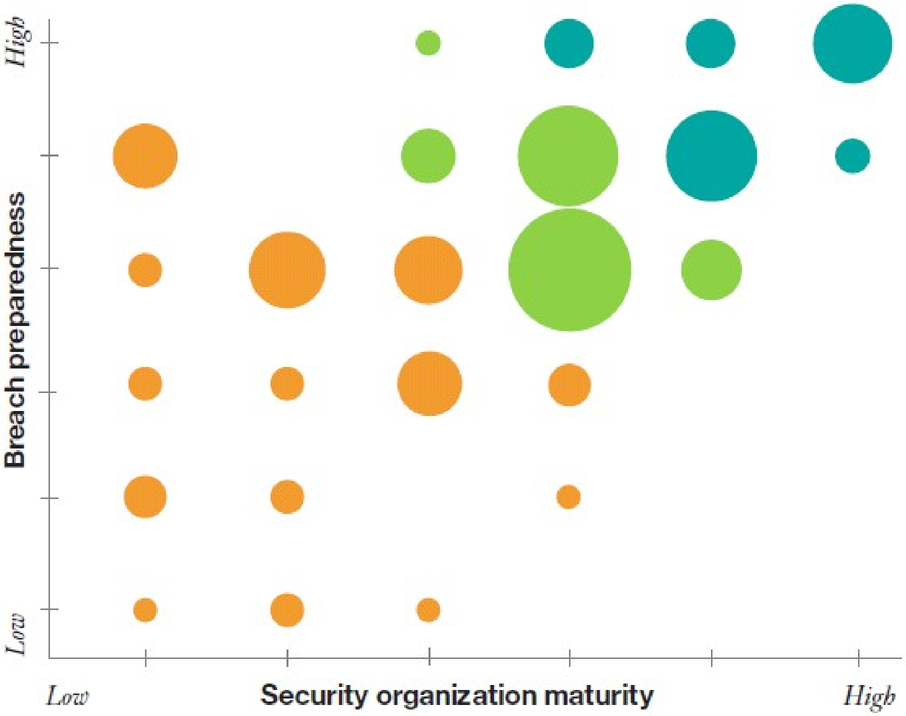
How do we solve this?

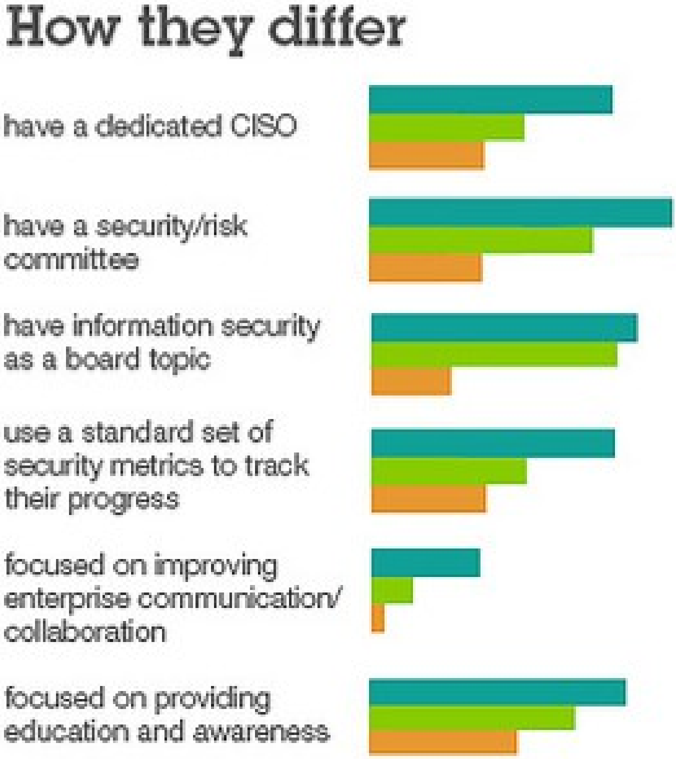
Security challenges are a complex, four-dimensional puzzle …



… that requires a new approach

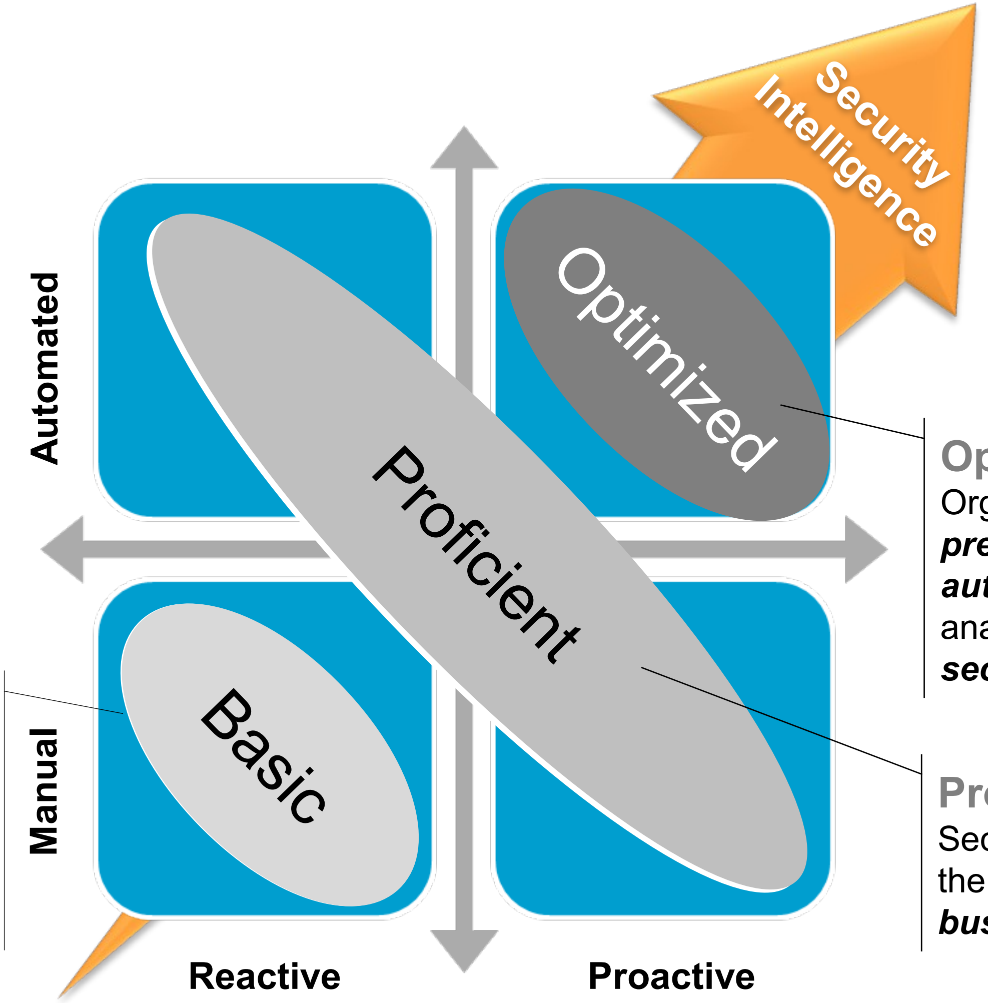
IBM CISO study revealed critical shift in the role of Chief Information Security Executives globally





● Influencers (25%) => **RISK**
● Protectors (47%) => **COMPLIANCE**
● Responders (28%) => **CRISIS**

In this “new normal”, organizations need an intelligent view of their security posture

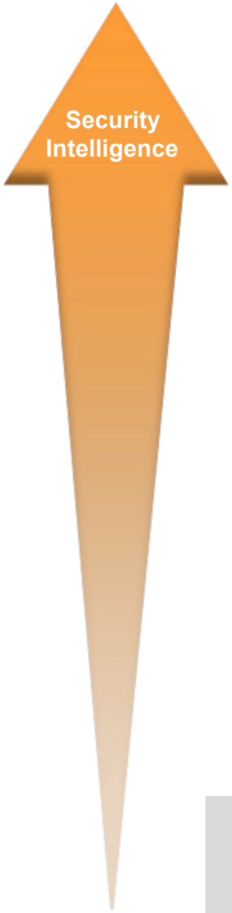


Optimized
Organizations use ***predictive and automated*** security analytics to drive toward ***security intelligence***

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

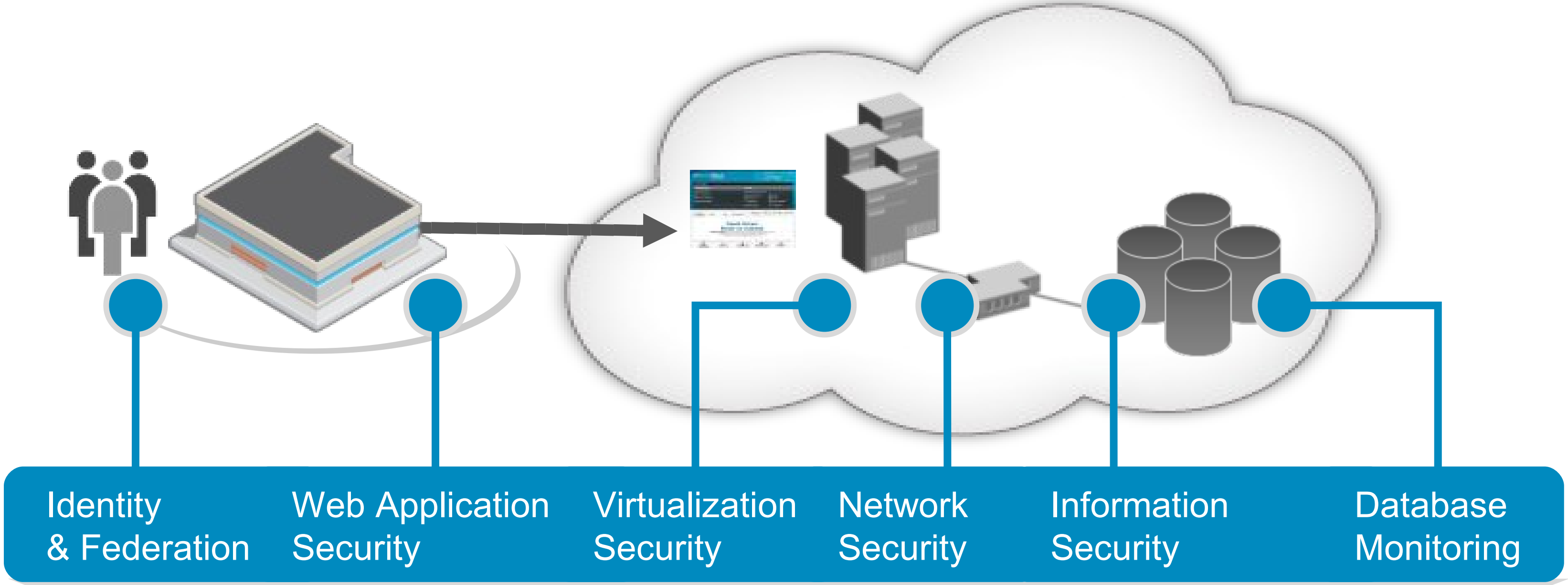
Basic
Organizations employ ***perimeter protection***, which regulates access and feeds manual reporting

Security intelligence helps clients build a more optimized security posture



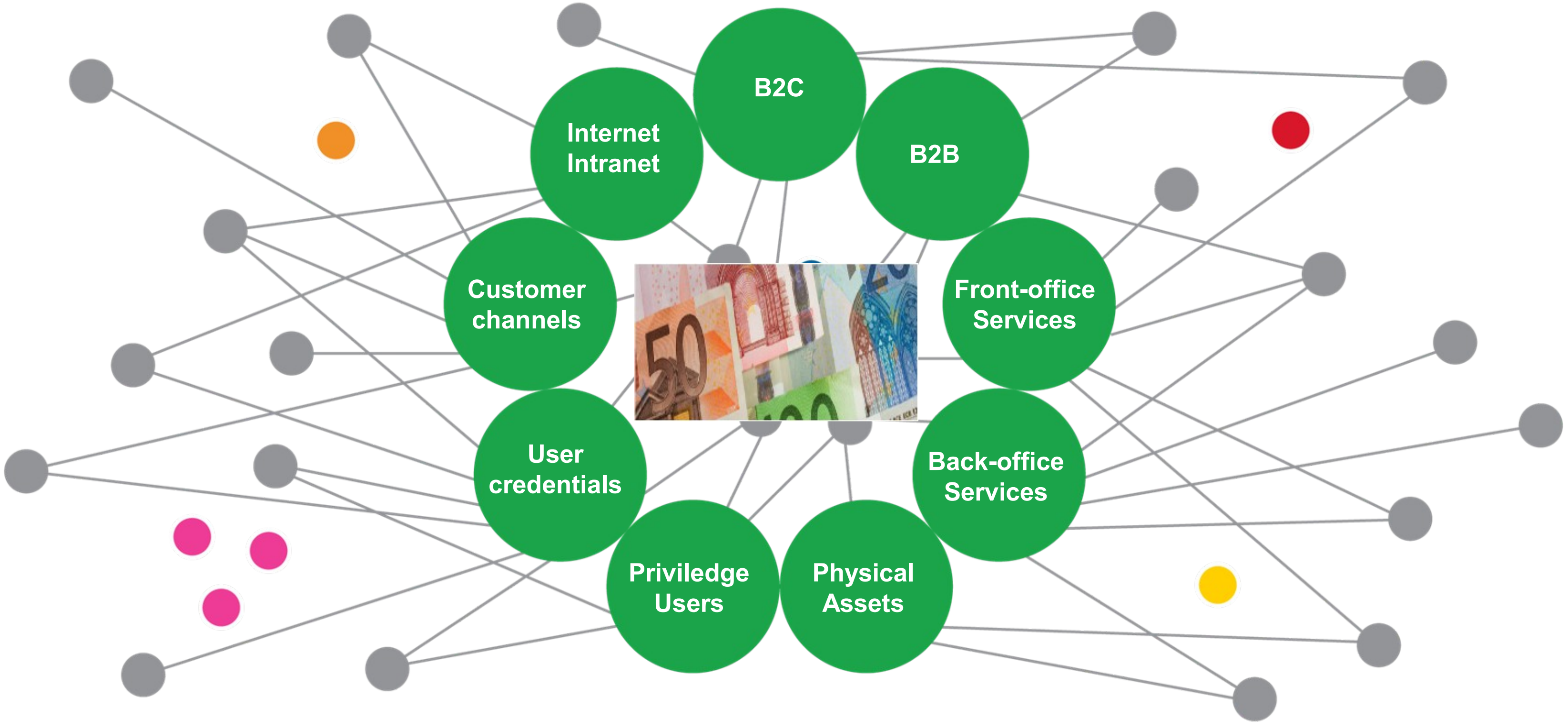
	People	Data	Applications	Infrastructure
	Security Intelligence: Information and event management Advanced correlation and deep analytics External threat research			
	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
	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

Our approach is to help clients adopt layered security across the entire company IT infrastructure ….



IBM Security Intelligence

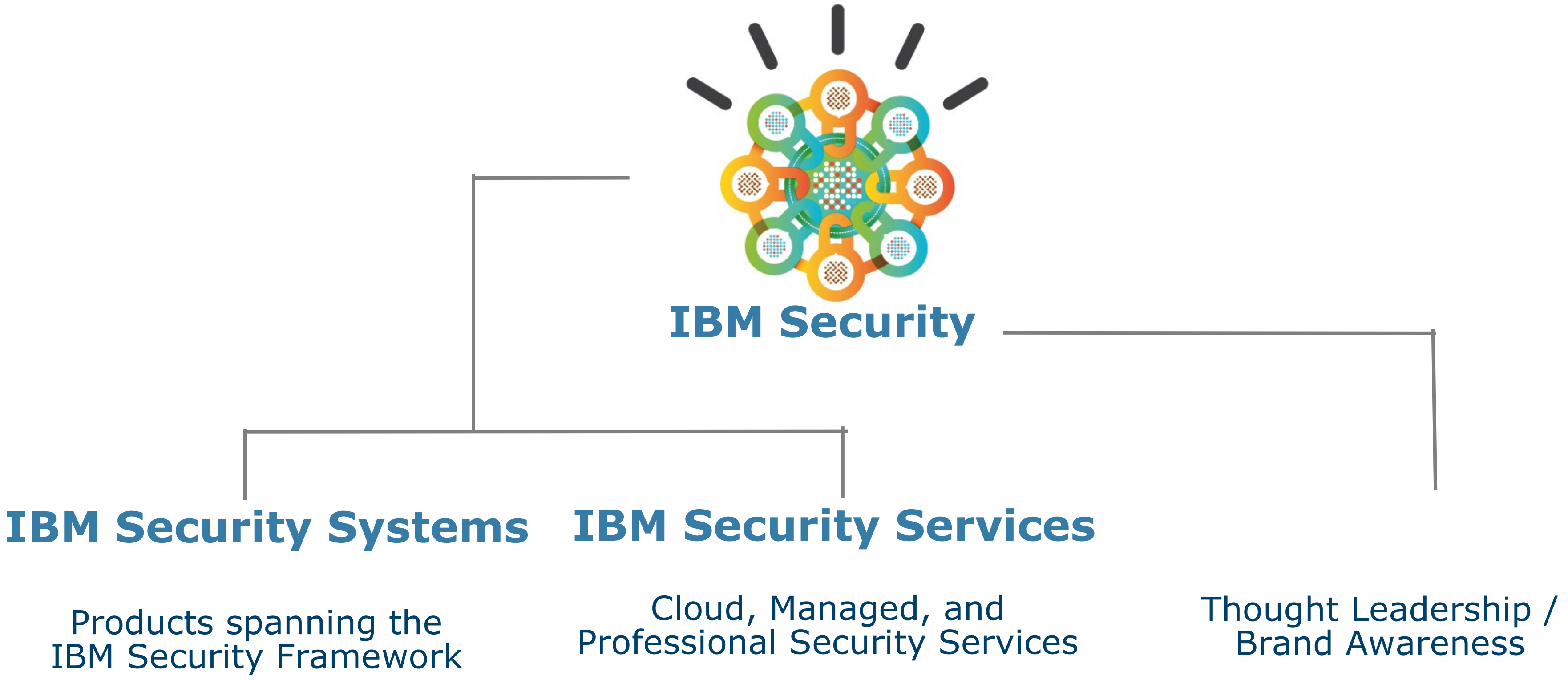
… with the right mix of control measures to proactively deal with financial cyber-crimes across all points of vulnerability



● Legitimate customers

● Rogue traders | ● Disgruntled employees | ● Money launderers | ● Terrorist financiers | ● Organized crime | ● Identity thieves

IBM Security



IBM Security

IBM Security Systems

Products spanning the IBM Security Framework

IBM Security Services

Cloud, Managed, and Professional Security Services

Thought Leadership / Brand Awareness

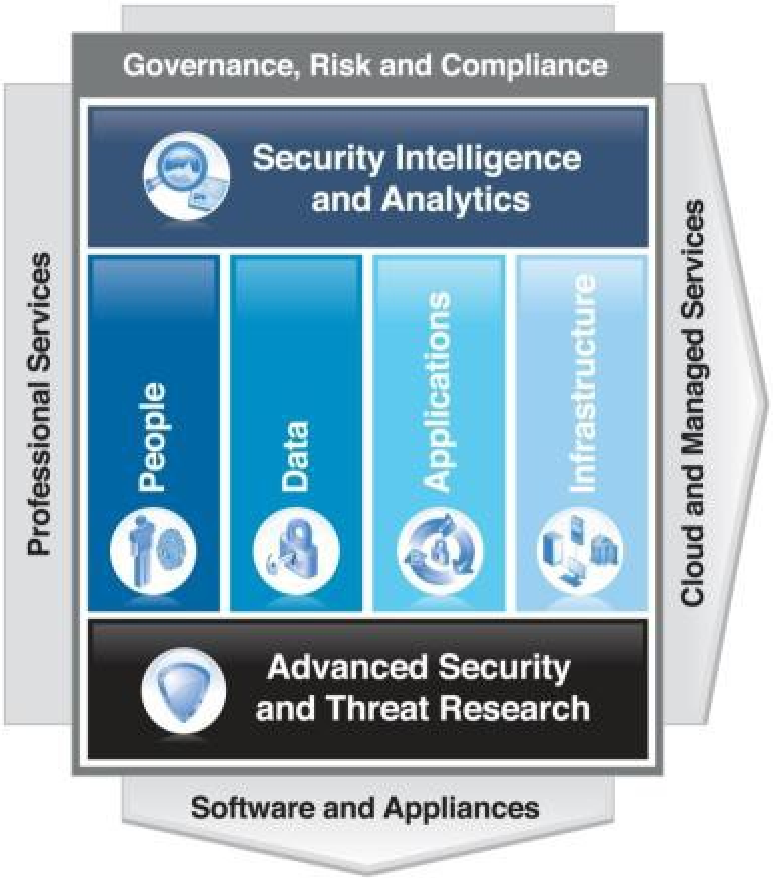
Leveraging IBM Research, Security Expertise, and Best-of-Breed Technologies

Intelligence, integration and expertise across a comprehensive framework is needed

IBM Security Intelligence

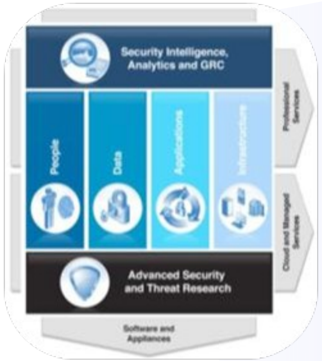
DASCOM
Softech
Guardium
NISC
METAMERGE
Internet Security Systems
watchfire
consul
access360
BIGFIX
Q1 Labs
ENCENTUATE
OUNCE LABS
DATAPOWER

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

Intelligence: Product Portfolio, Services and Research


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

Enterprise Governance, Risk and Compliance Management

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

IBM Security Portfolio

Security Intelligence, Analytics and GRC

QRadar SIEM	QRadar Log Manager	QRadar Risk Manager	IBM Privacy, Audit and Compliance Assessment Services

IT Infrastructure – Operational Security Domains

People	Data	Applications	Infrastructure: Network	Infrastructure: Endpoint
Identity & Access Management Suite	Guardium Database Security	AppScan Enterprise, Standard & Source	Network Intrusion Prevention	Endpoint Manager (BigFix)
Federated Identity Manager	InfoSphere Optim Data Masking	DataPower Security Gateway	SiteProtector Management System	Virtualization & Server Security
Enterprise Single Sign-On	Key Lifecycle Manager	Security Policy Manager	QRadar Anomaly Detection	Mainframe Security (zSecure, RACF)
Identity Assessment, Deployment and Hosting Services	Data Security Assessment Service Encryption and DLP Deployment	Application Assessment Service AppScan OnDemand - SaaS	Managed Firewall, UTM, and Intrusion Prevention Services	Penetration Testing Services Mobile Device Management

Security Ecosystem

Partner Programs (3rd party)

Standards

Security Consulting

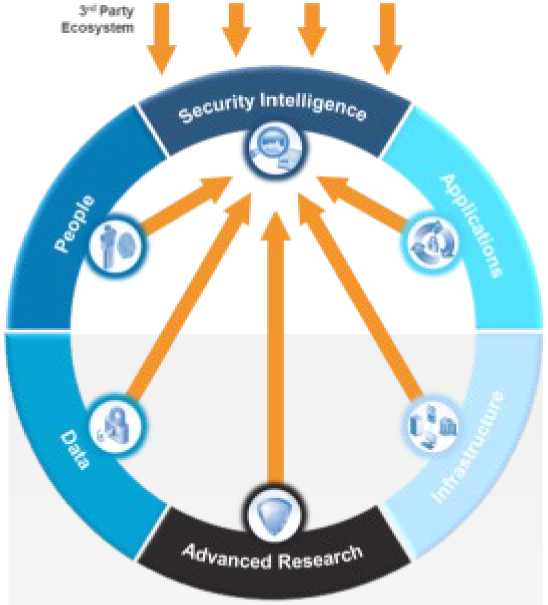
Managed Services

X-Force and IBM Research

Products Services

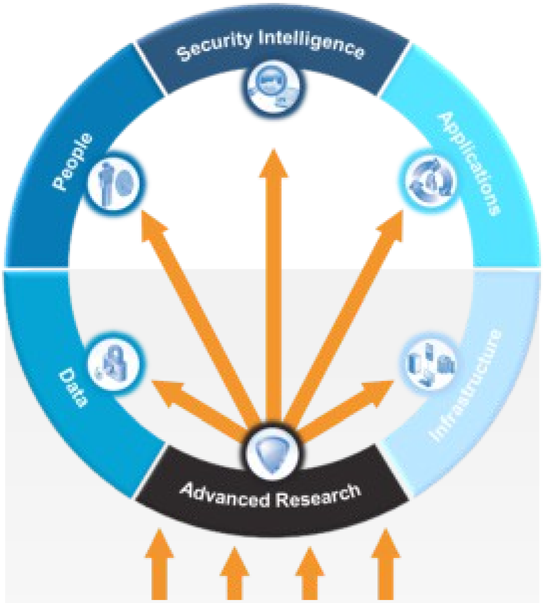
v12-03

Integrated Intelligence.



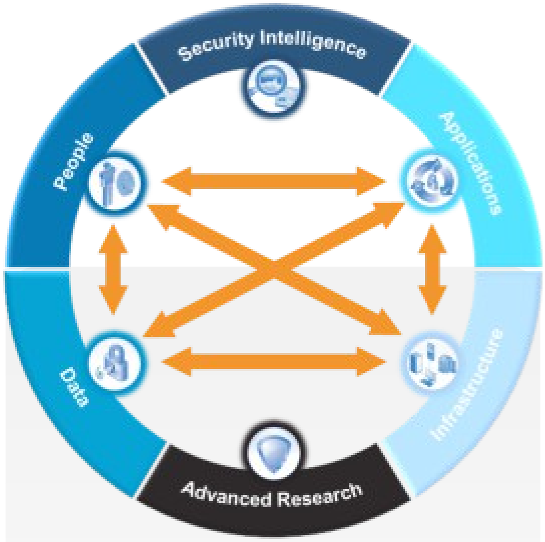
- Consolidate and correlate siloed information from hundreds of sources
- Detect, notify and respond to threats missed by other security solutions
- Automate compliance tasks and assess risks

Integrated Research.



- Stay ahead of the changing threat landscape
- Detect the latest vulnerabilities, exploits and malware
- Add security intelligence to non-intelligent systems

Integrated Protection.



- Customize protection to block specific vulnerabilities using scan results
- Converge access management with web service gateways
- Link identity information with database security

IBM's approach as an enterprise and service provider

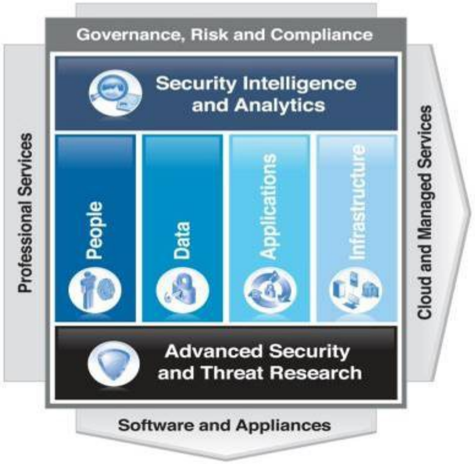
Focused on security essentials, informed by the IBM Security Framework

1. Build a risk-aware culture and management system

6. Control network access and help assure resilience

2. Manage security incidents with greater intelligence

IBM Security Framework


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

7. Address new complexity of cloud and virtualization

3. Defend the mobile and social workplace

8. Manage third-party security compliance

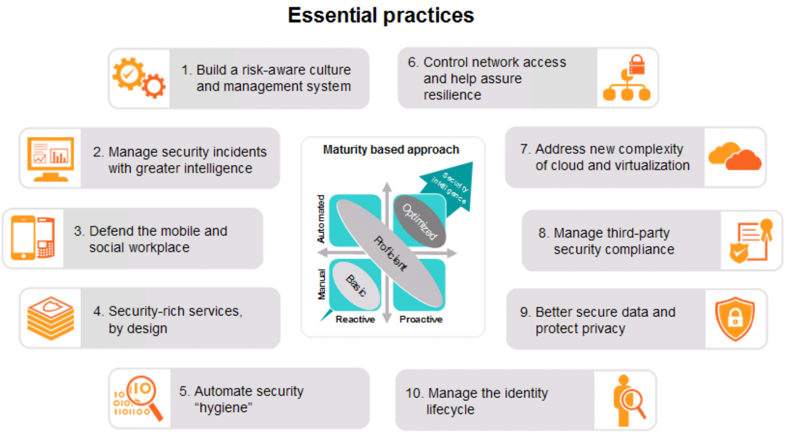
4. Security-rich services, by design

9. Better secure data and protect privacy

5. Automate security "hygiene"

10. Manage the identity lifecycle

Our strategy is to meet our Clients’ security needs with a range of high value services from consulting to managed services



Essential practices

1. Build a risk-aware culture and management system

2. Manage security incidents with greater intelligence

3. Defend the mobile and social workplace

4. Security-rich services, by design

5. Automate security “hygiene”

6. Control network access and help assure resilience

7. Address new complexity of cloud and virtualization

8. Manage third-party security compliance

9. Better secure data and protect privacy

10. Manage the identity lifecycle

Maturity based approach

Consulting services

Focus on strategy & benchmarking – showcasing our industry expertise

Architecture & Implementation services

Focused on consistent delivery methods and skills enablement on key platforms

Managed & Cloud services

Focused on platform support and analytics of existing services, while adding new, high value, cloud based services

An IBM Managed Security Services sourcing strategy can help your business gain competitive advantage

Potential opportunities at company level

- Access to innovation
- Core competence
- Competitiveness
- Focusing
- Shareholder value
- Flexibility
- Ability to react

Managed Security Services

X FORCE

IBM Research

Potential opportunities at IT level

- Reduction of costs
- Access to IT expertise
- Delivery of consistent service levels
- Sharing of responsibility
- Risk sharing
- Risk reduction
- Predictable pricing

IBM offers a broad managed security service portfolio to help address a variety of business requirements

Managed Security Services (CPE)

- ***Managed security incident and event management***
- **Managed firewall services**
- **Managed and monitored IPS and IDS services**
- **Managed Unified Threat Management (UTM) services**
- ***Managed protection services for networks, servers and desktops***

Managed Security Services (Cloud)

- **Hosted security event and log management services**
- **Hosted vulnerability management services**
- **Hosted application scanning**
- **Hosted managed e-mail and web security**
- **Hosted IBM X-Force threat analysis service**

Multiple device types and vendors supported

CPE: Customer Premise Equipment
IPS: Intrusion Prevention System
IDS: Intrusion Detection System

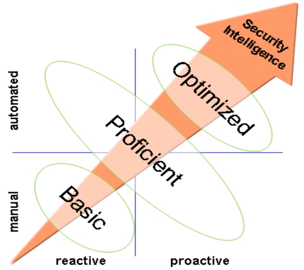
IBM Manages Services can help optimize your security intelligence

Add FW Logs	Add IDPS Events	Add vScan Results	Add OS & App Logs
Add Firewall Logs	Add IDPS Events:	Add Vulnerability Scan Results	Add Operating System and App logs:
Real-time identification of connections with known Attackers	Know the attacks levied against you	Know if the Attacks are Successful	Monitor suspicious internal activities
Good	Better	Enhanced	Superior

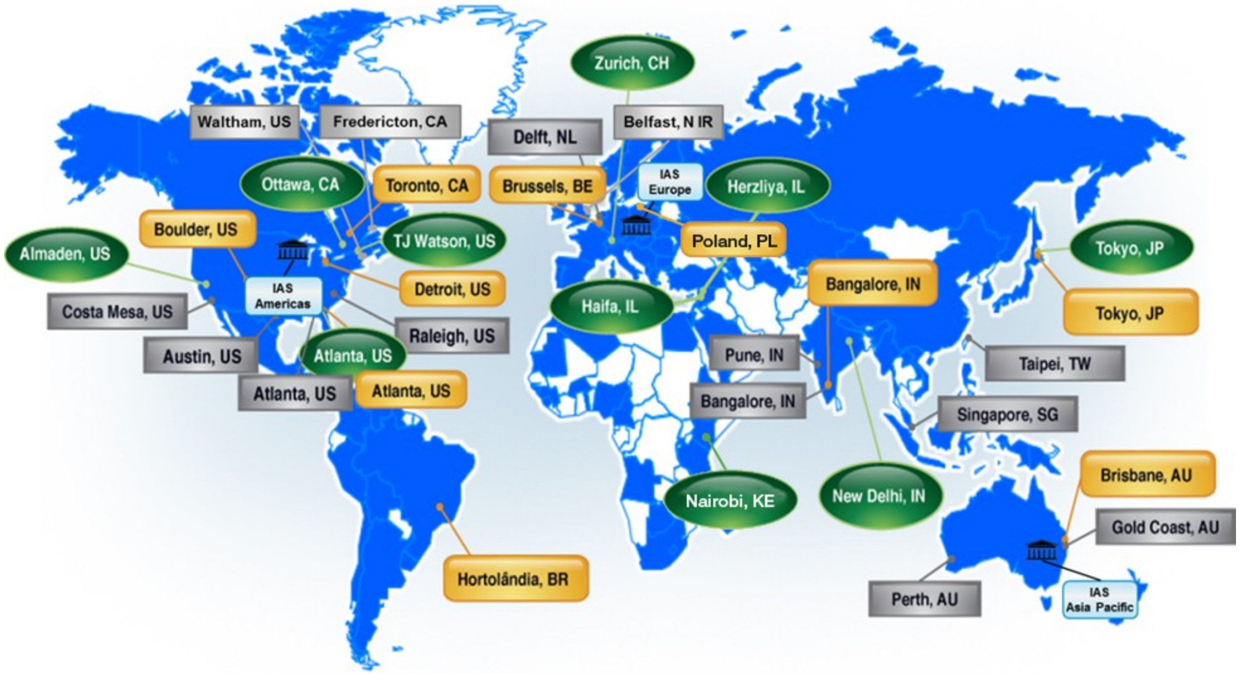
Services recommended to enable these capabilities:

(1) Firewall Mgmt (2) Managed UTM (3) Hosted SELM	(1) Managed IDPS (2) Managed UTM (3) MPS (4) Hosted SELM	(1) VMS 2.0	(1) Hosted SELM

Maturity Based Approach



Expertise: 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

54K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

X FORCE

World Wide Managed Security Services Coverage

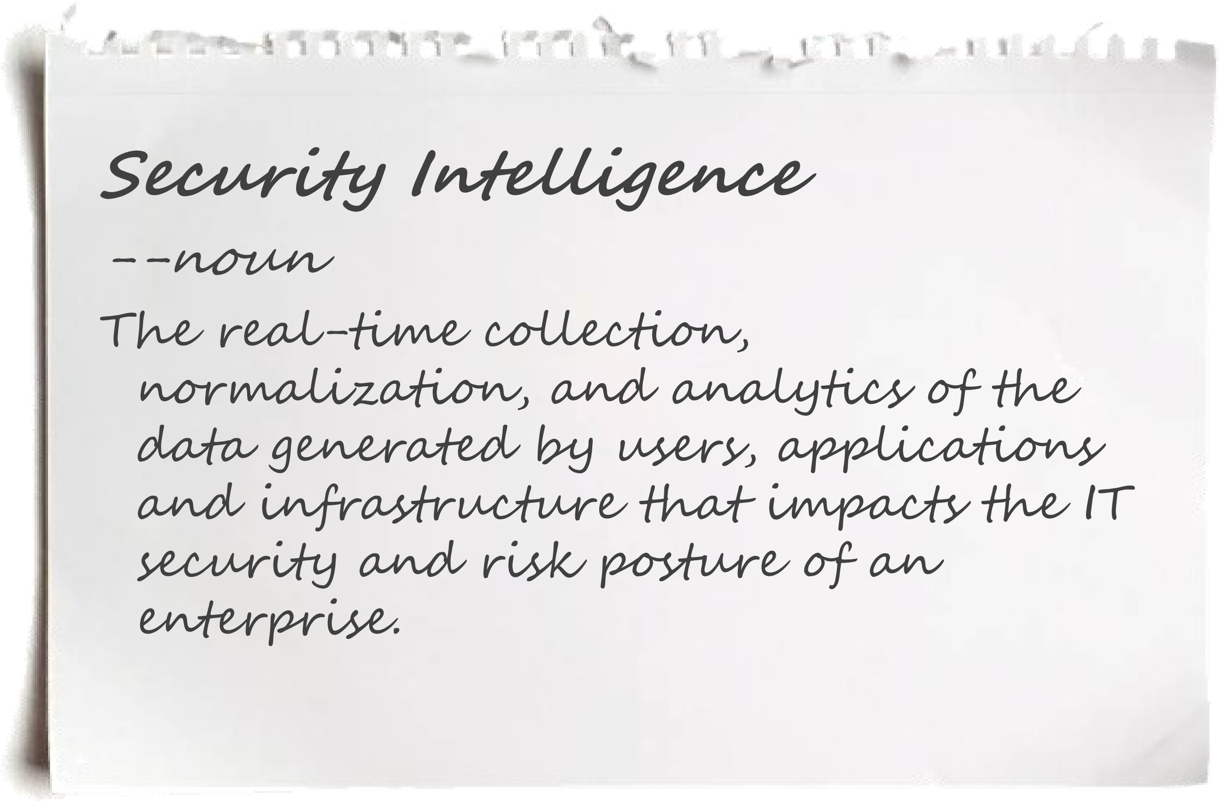
- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

Il costo della non-sicurezza

è

l’impossibilità di innovare

ai ritmi richiesti dal mercato



Security Intelligence

--noun

The real-time collection, normalization, and analytics of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise.

Security Intelligence provides actionable and comprehensive insight for managing risks and threats from protection and detection through remediation