Pulse

IBM SolutionsConnect 2013

Getting Ahead of the Threat with Security Intelligence

Caleb Barlow

Director – Application, Data, Mobile, Critical Infrastructure Security

twitter.com/calebbarlow

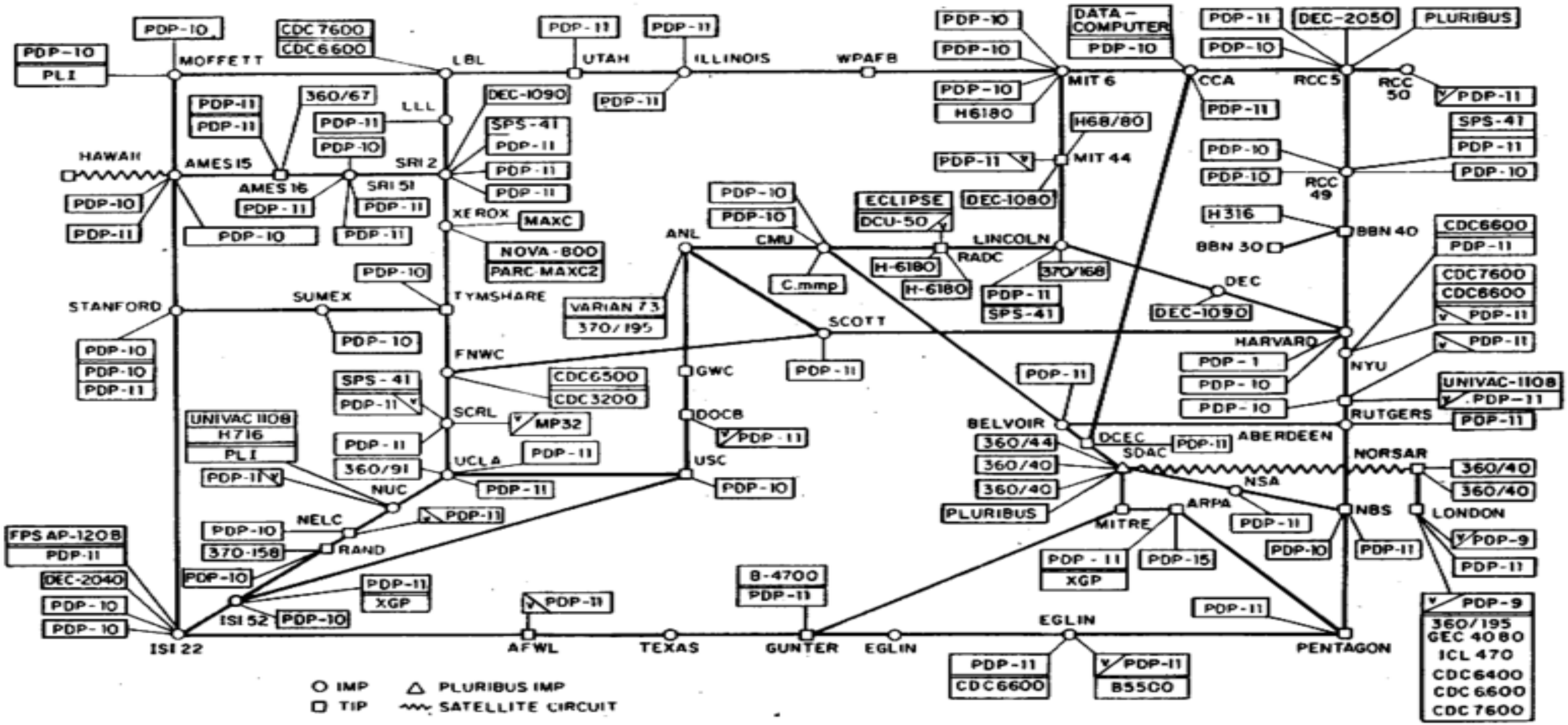
blogtalkradio.com/itsecurity

www.facebook.com/barlow.caleb

www.youtube.com/calebbarlow

IBM

ARPANET LOGICAL MAP, MARCH 1977



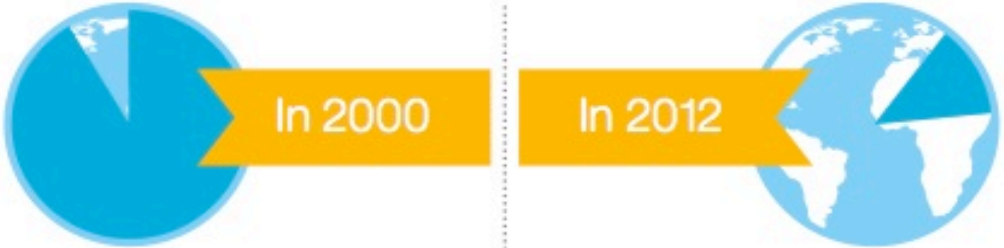
(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Threat Landscape Is Growing Fast

In 2000	In 2012
	
361 million people using the Internet.[1]	**2.67 billion** people using the Internet.[1]
5.8% of the world's population.[1]	**33%** of the world's population.[1]

…. And Becoming Mobile



720 million
mobile subscribers worldwide.[4]

12%
of the world's population.[4]

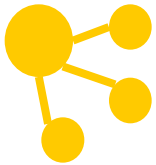
6 billion
mobile subscribers worldwide.[5]

87%
of the world's population.[4]

Innovative technology changes everything

1 trillion connected objects

1 billion mobile workers



Social business

Cloud and virtualization

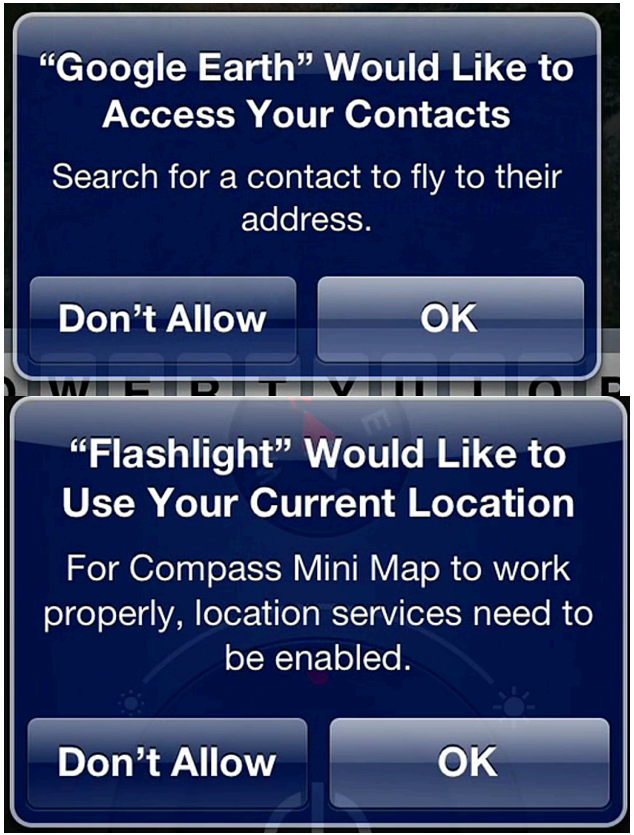
Bring your own IT

QR Codes

- QR Code can contain a URL to download malware
- The malware can then send SMS messages to a premium rate number (US $6 per message)

  http://siliconangle.com/blog/2011/10/21/infected-qr-malware-surfaces-on-smartphones-apps/

How do Mobile Applications Treat You?



Motivation and sophistication is evolving rapidly

National Security

Nation-state actors **Stuxnet**

Espionage, Activism

Competitors and Hacktivists **Aurora**

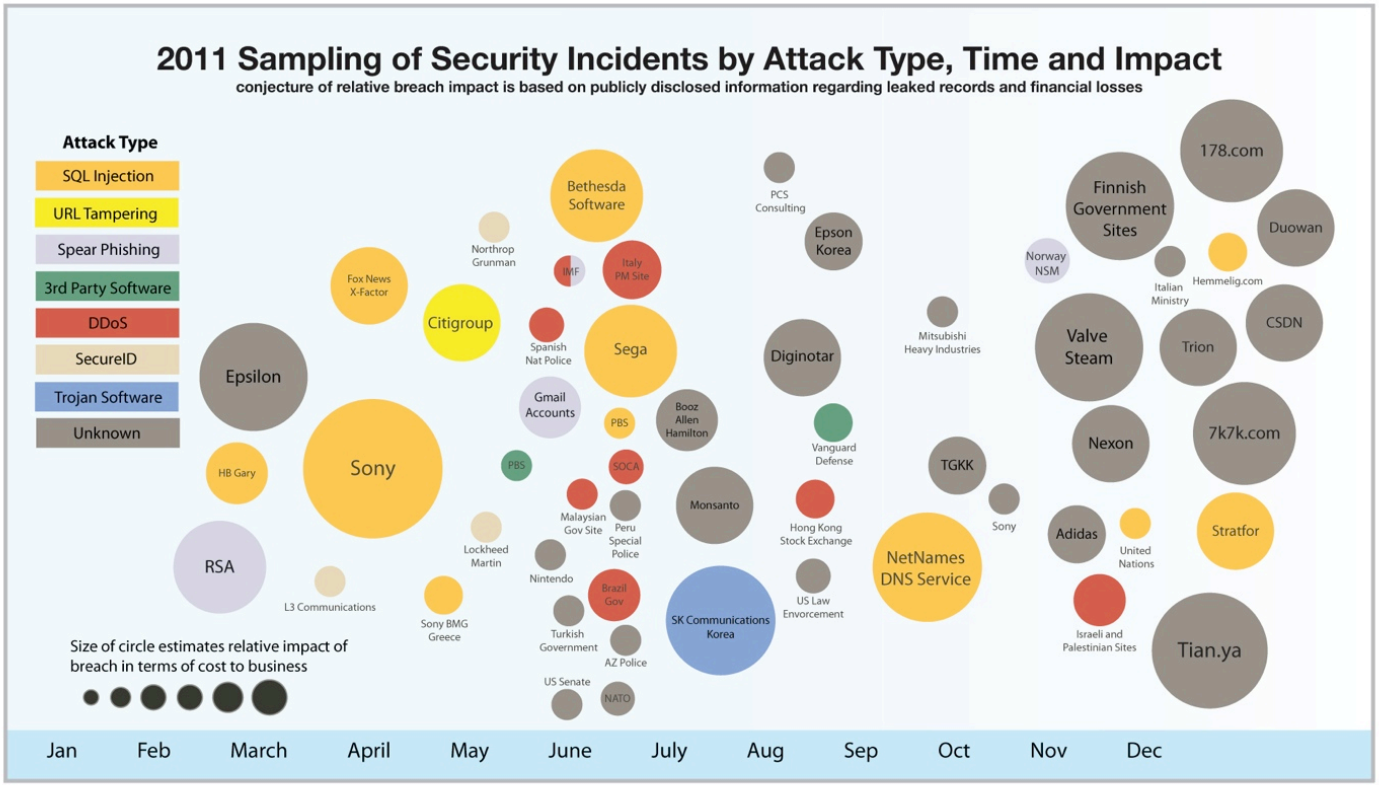
Monetary Gain

Organized crime **Zeus**

Revenge, Curiosity

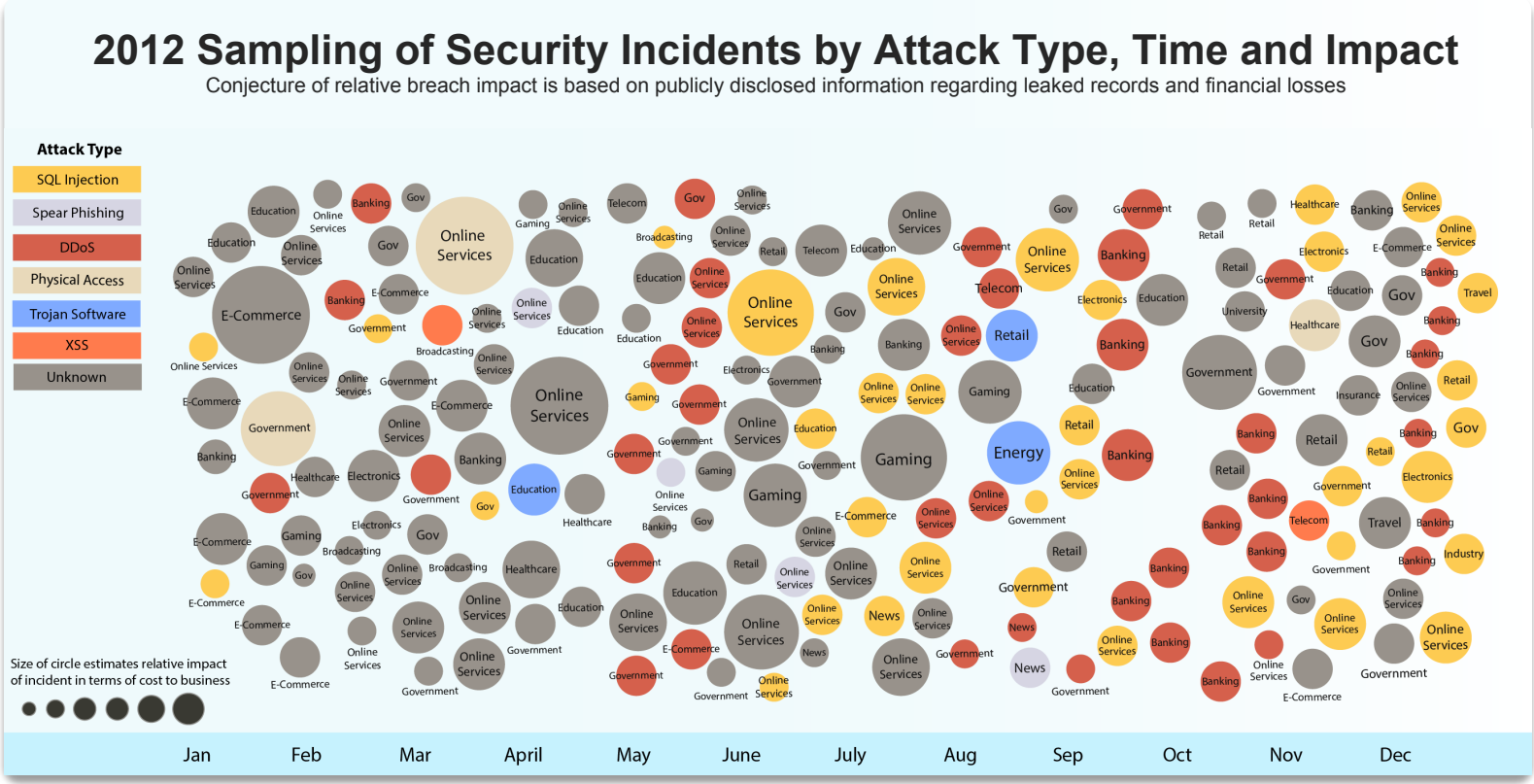
Insiders and Script-kiddies **Code Red**

Reported security breaches continue to increase

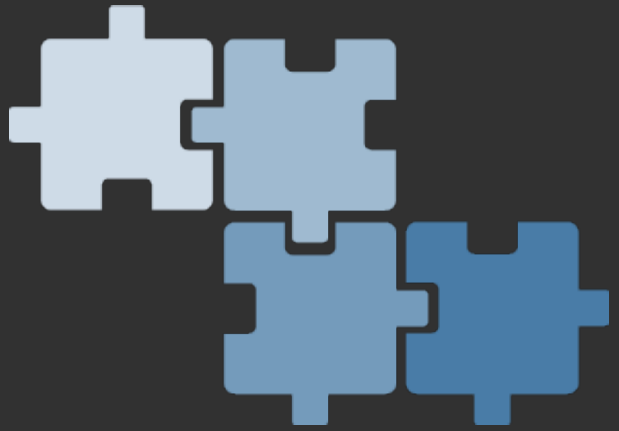


Source: IBM X-Force® *2011 Full Year Trend and Risk Report*

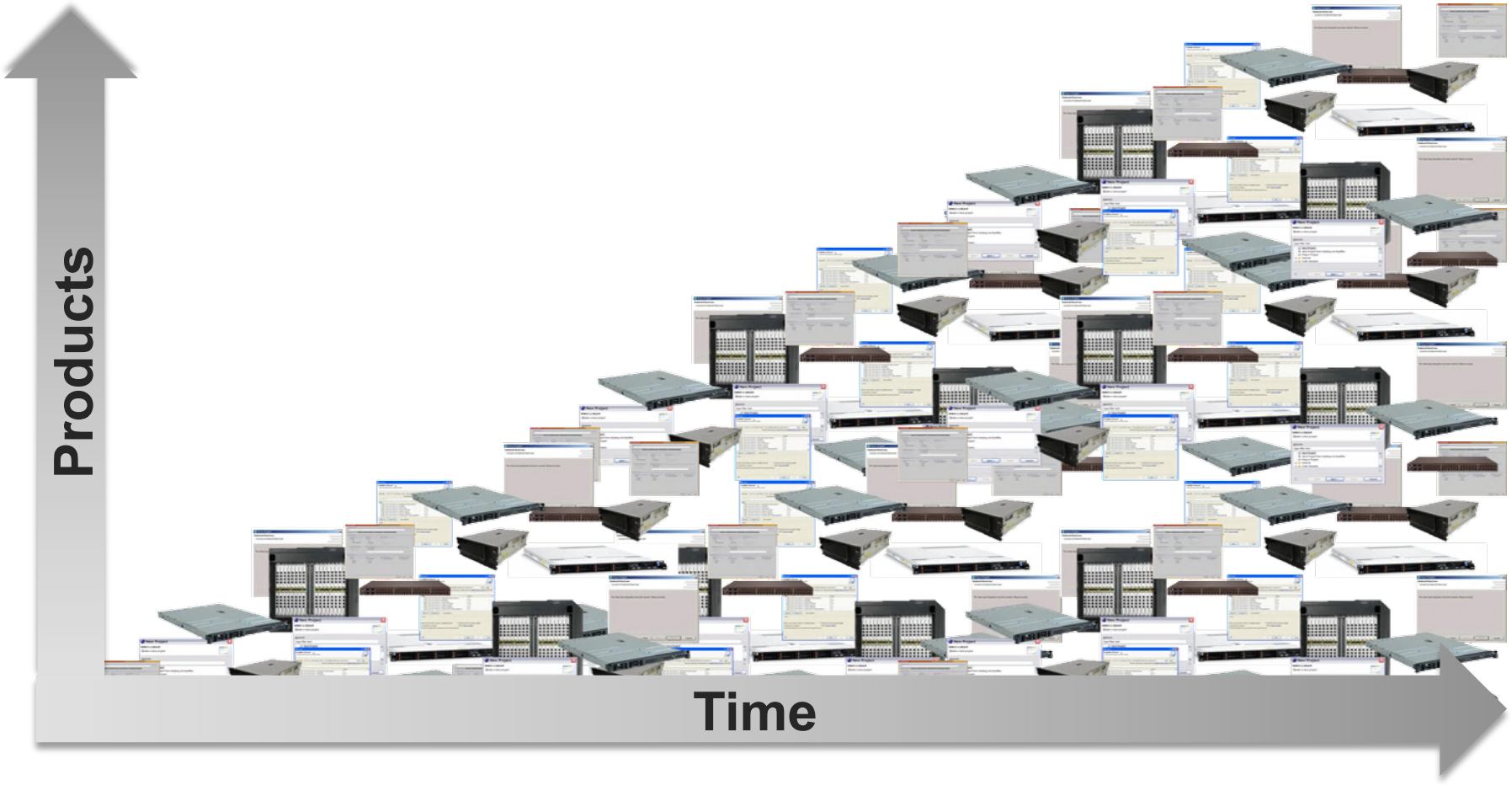
Reported security breaches continue to increase

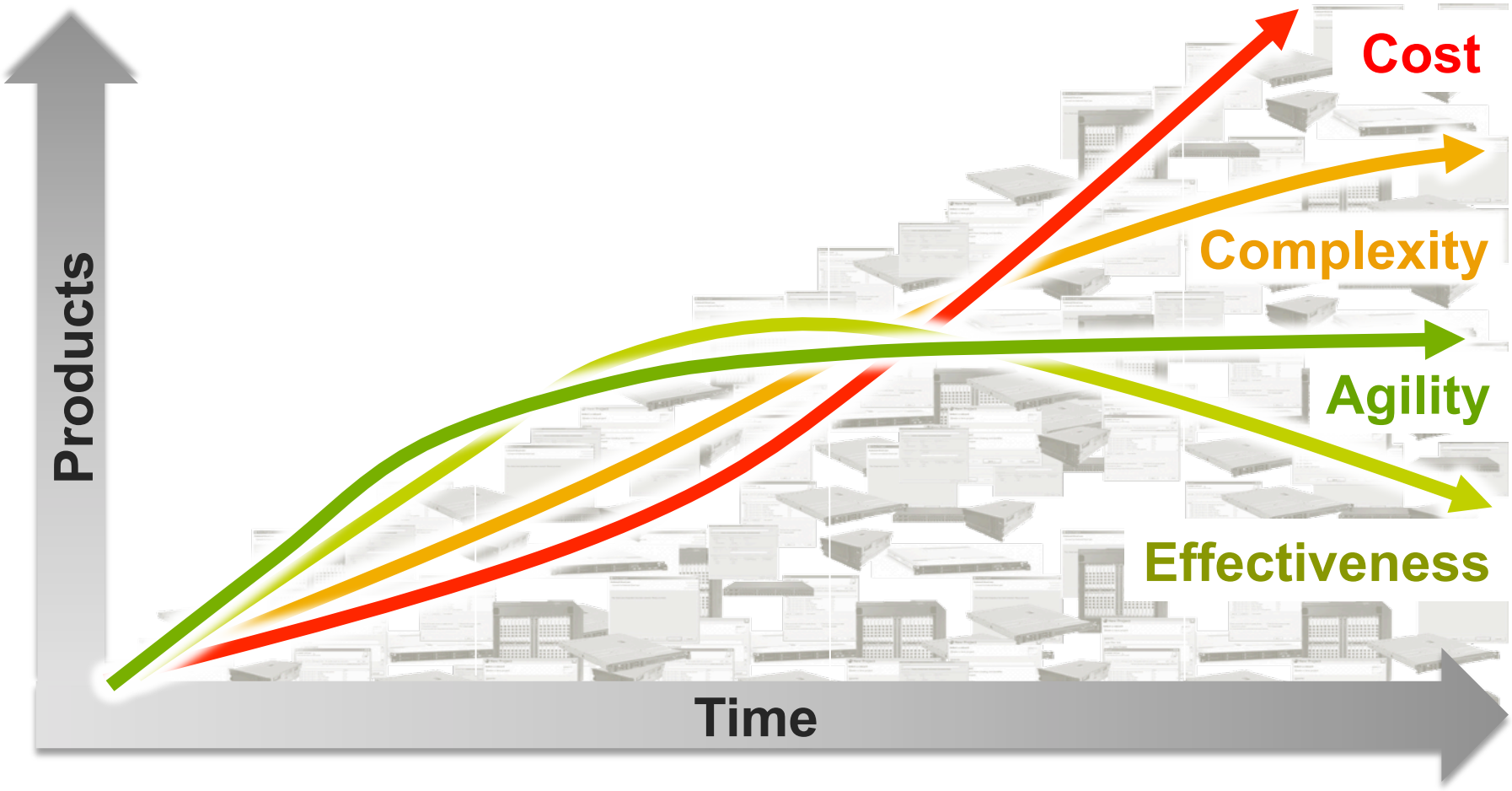


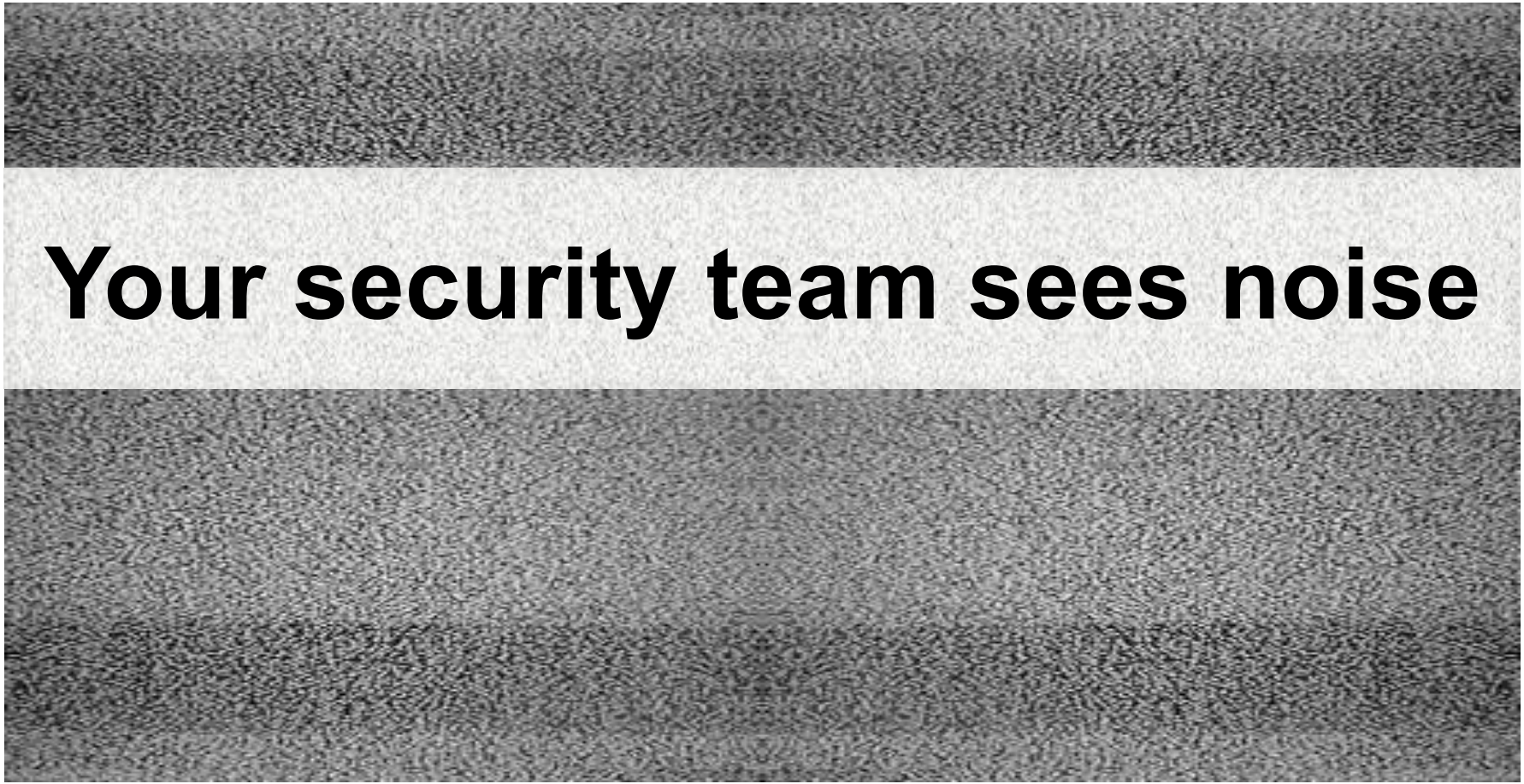
Source: IBM X-Force® *2012 Full Year Trend and Risk Report*



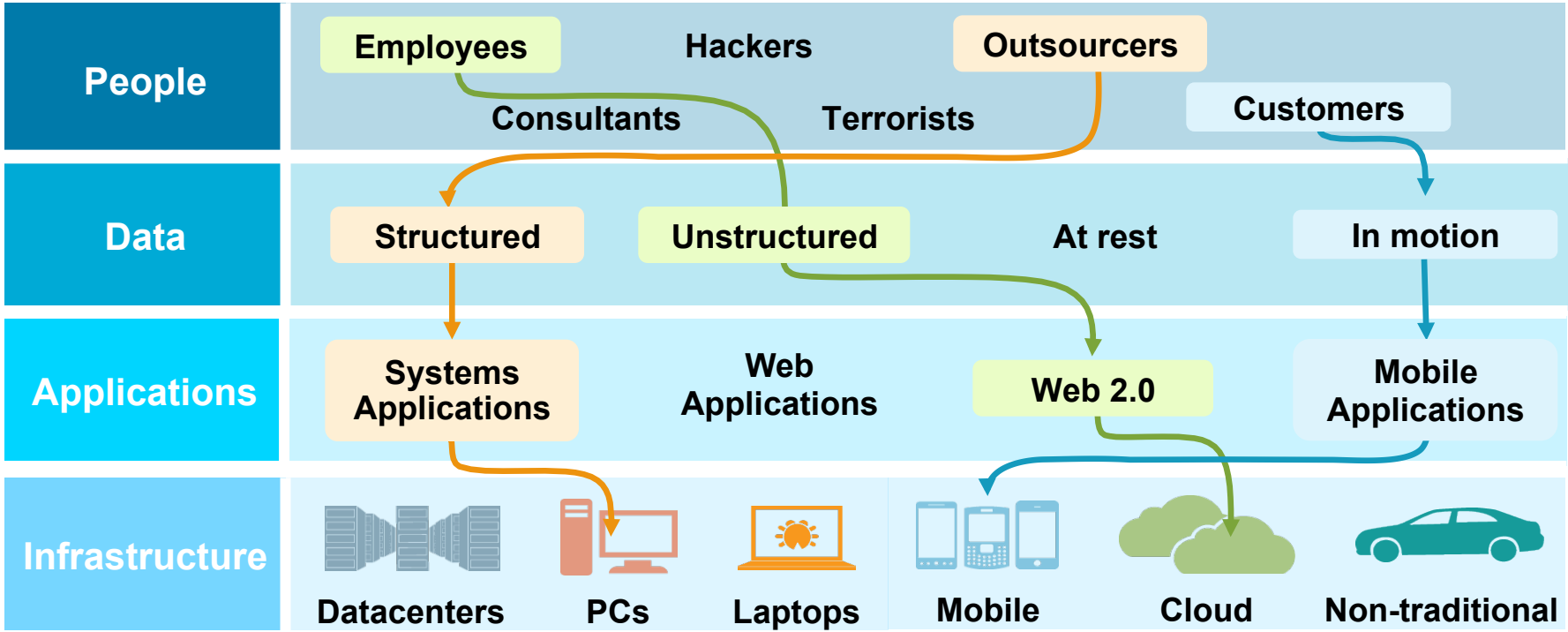
How do we solve this?


Products
Time


Products
Time
Cost
Complexity
Agility
Effectiveness


Your security team sees noise

Security challenges are a complex, four-dimensional puzzle …



… that requires a new approach

	Then		Now
People	Administration		Insight
Data	Basic control		Laser-focused
Applications	Bolt-on		Built-in
Infrastructure	Thicker walls		Smarter defenses

Collect and Analyze Everything

A change in mindset is already happening

Audit, Patch & Block

Think like a defender, defense-in-depth

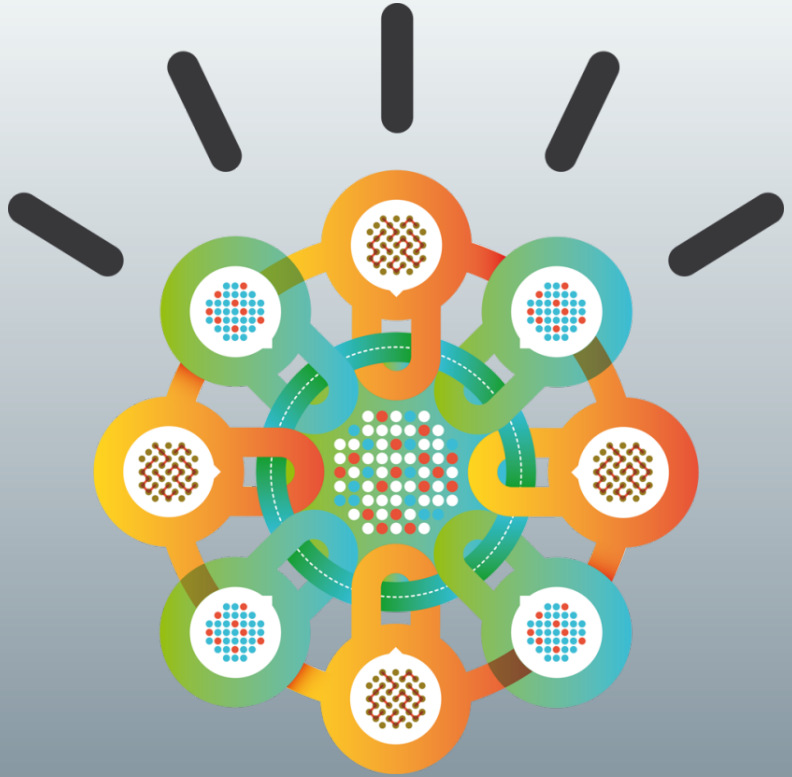
Detect, Analyze & Remediate

Think like an attacker, counter intelligence

Monitor Everything

Consume Threat Intelligence

Integrate Across Domains



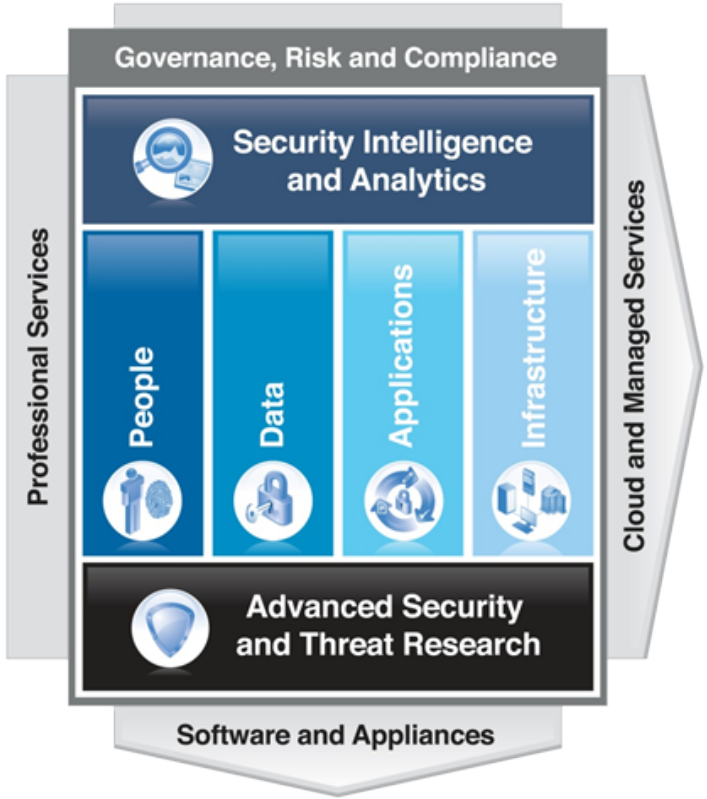
Security Intelligence

IBM Security solutions across a comprehensive framework

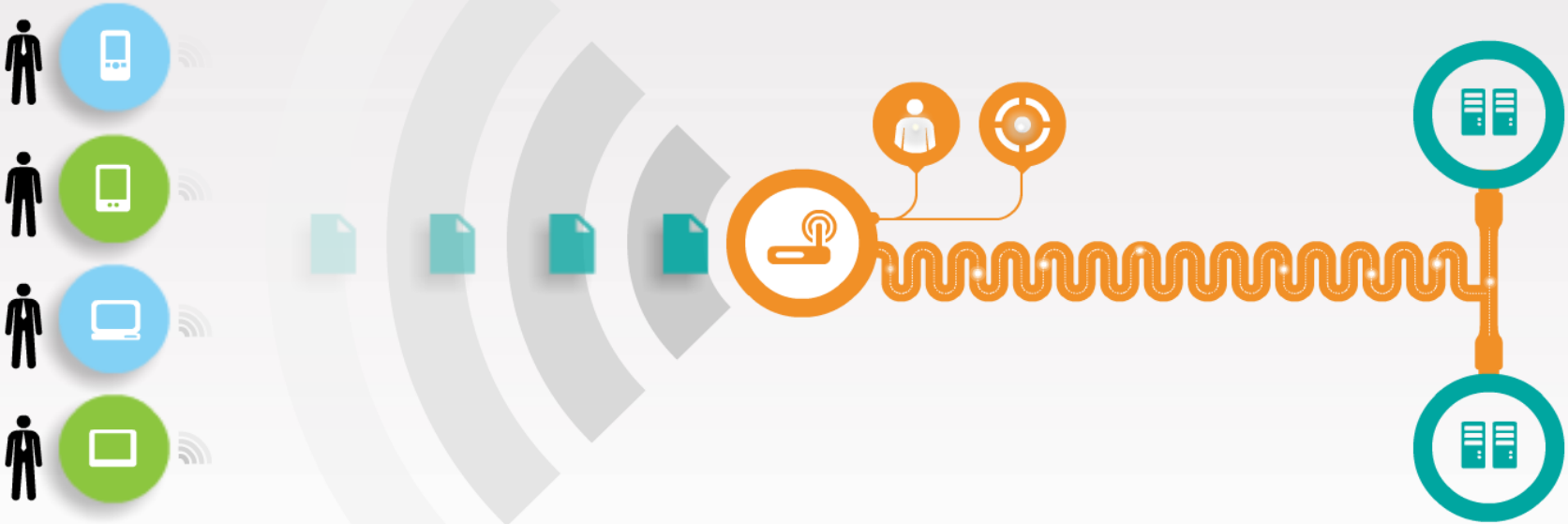
Intelligence

Integration

Expertise



IBM Mobile Security



Device Management

Security for endpoint device and data

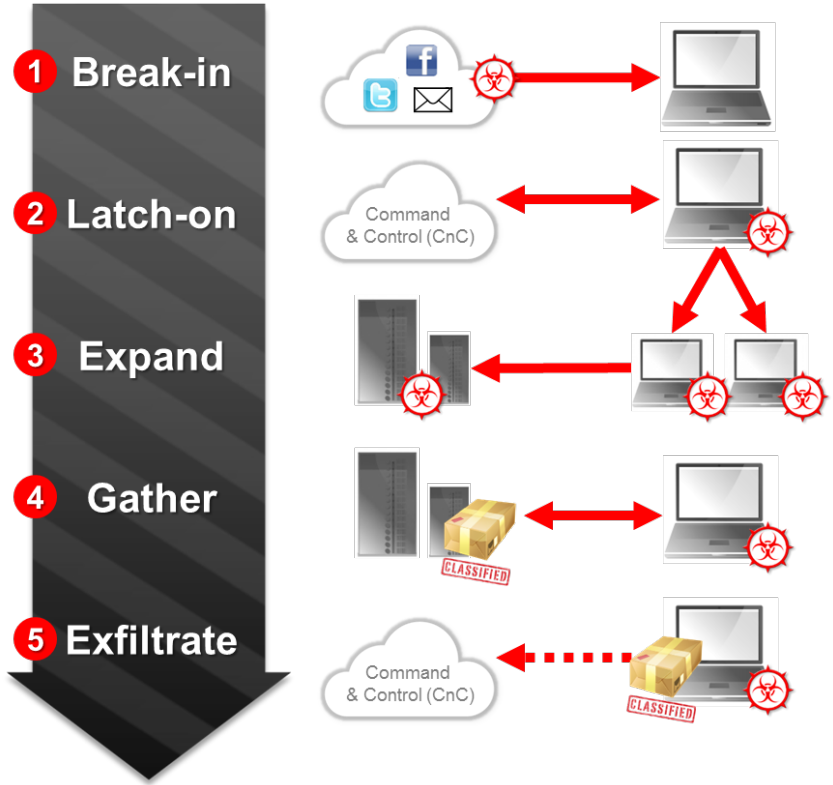
Network, Data, and Access Security

Achieve visibility and adaptive security policies

Application Layer Security

Develop and test applications

Advanced threats require a multifaceted approach

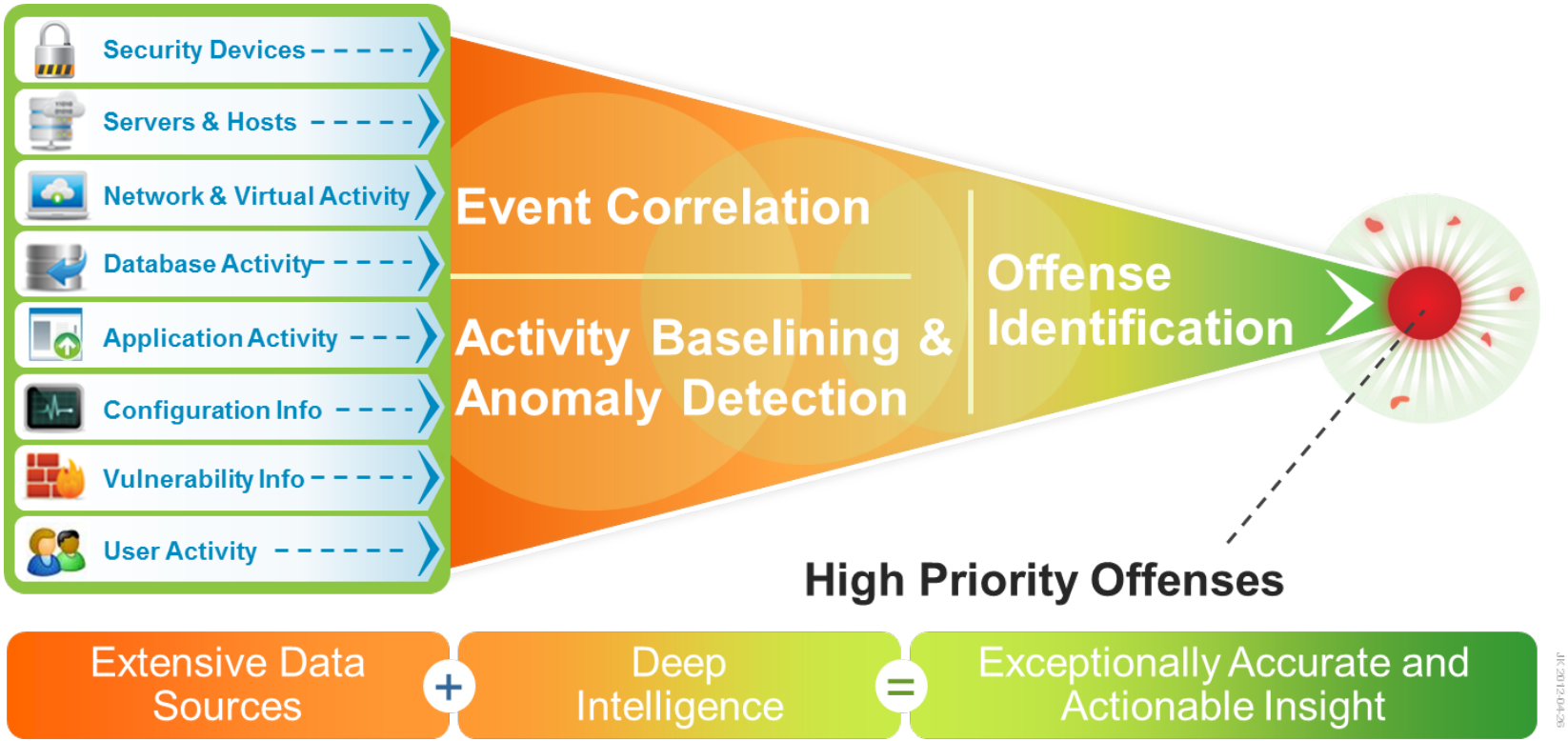


IBM Approach

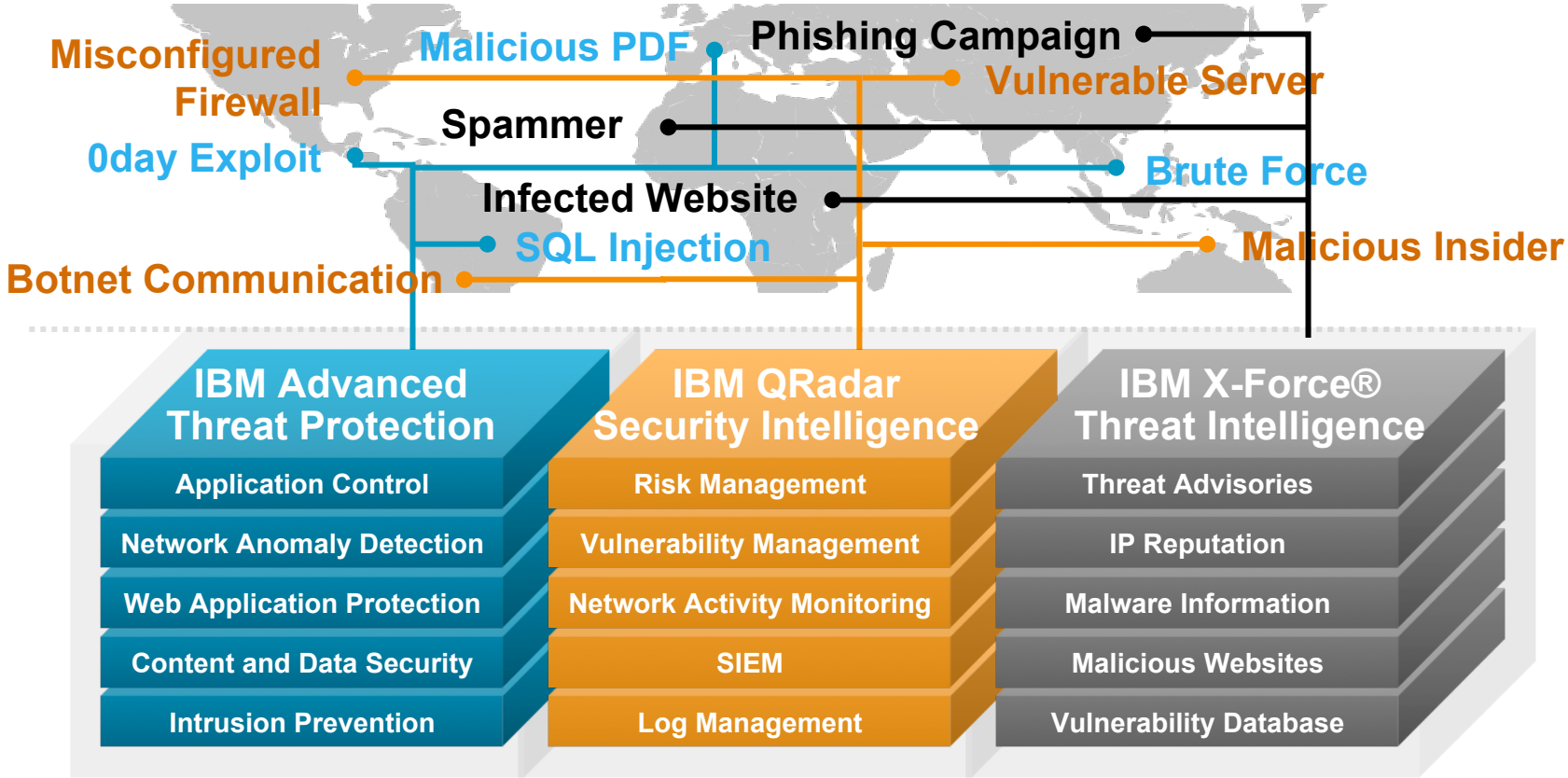
- Network and endpoint threat mitigation
- Data correlation, network protection
- Identity mgmt, control privileges, user monitoring
- Deep data security, access controls
- Network anomaly detection, blocking

Security Big Data Analytics

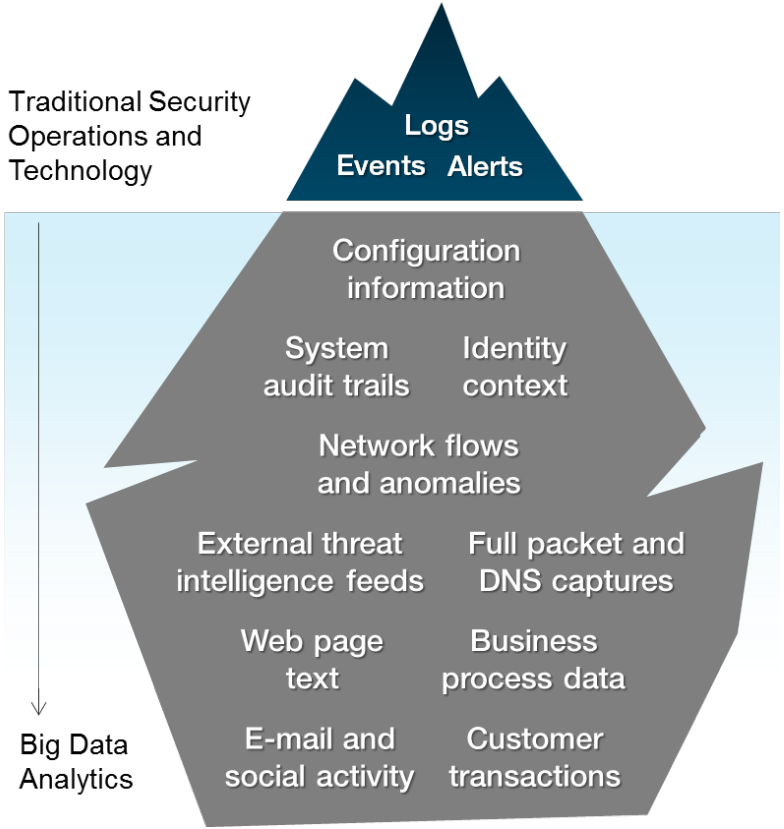
Security Intelligence: Integrating across IT silos



IBM Advanced Threat Protection Platform



Customers want to build insights from broader data sets



New Considerations

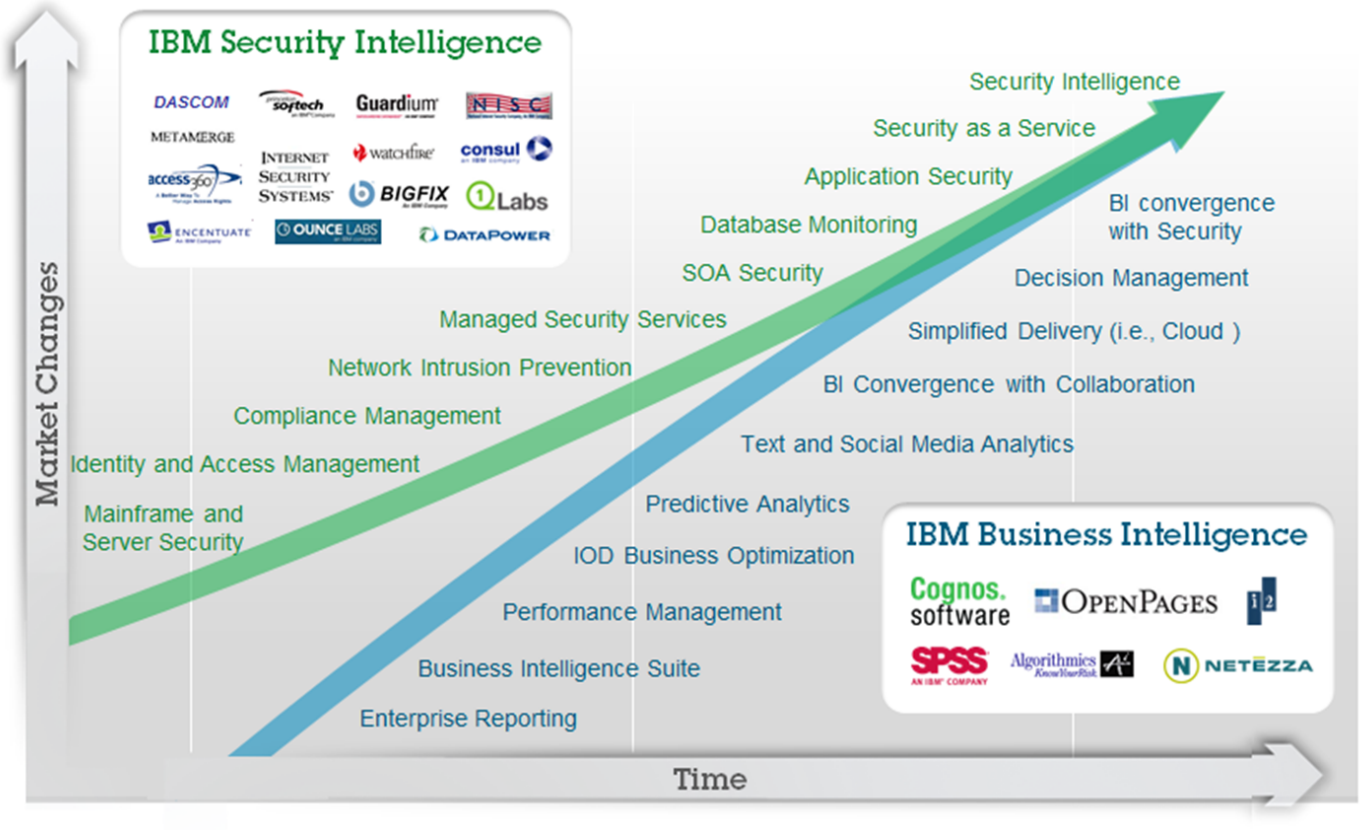
Collection, storage and processing

- Collection and integration
- Size and speed
- Enrichment and correlation

Analytics and workflow

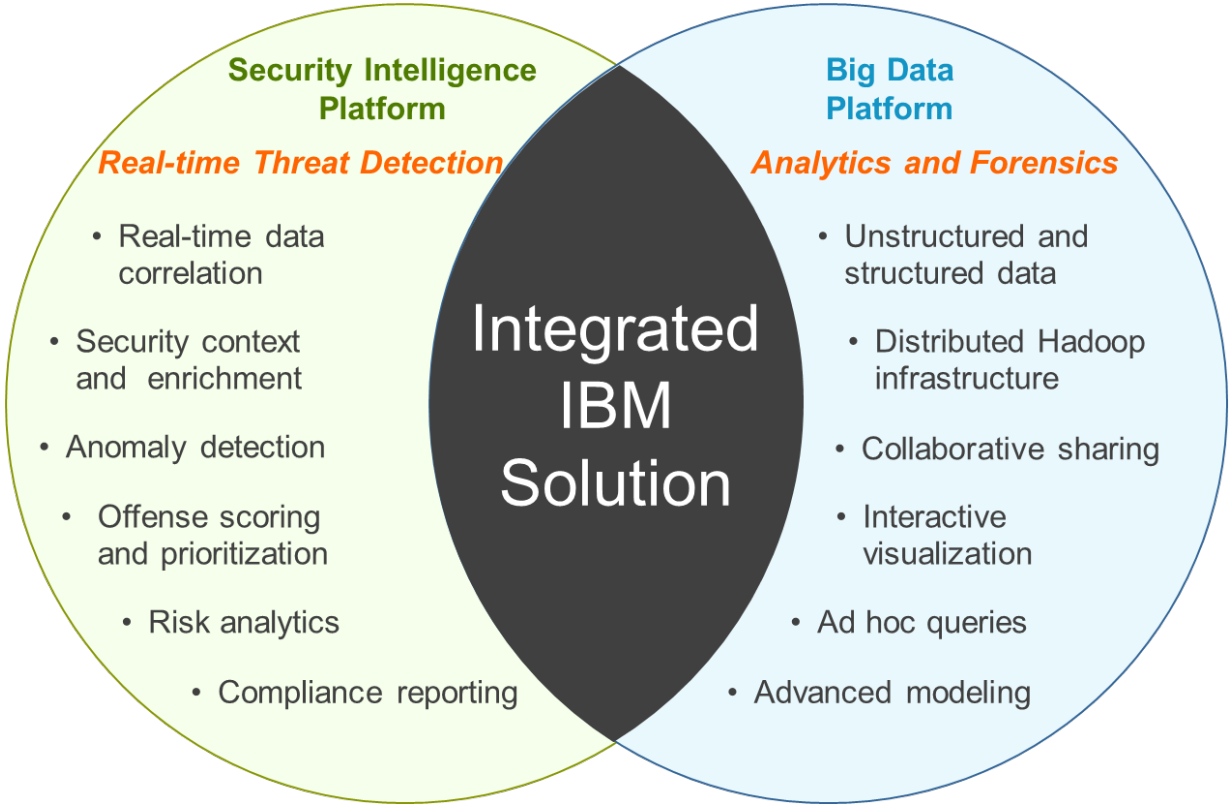
- Visualization
- Unstructured analysis
- Learning and prediction
- Customization
- Sharing and export

IBM is bringing together security and analytics



Integrated analytics and exploration in a new architecture

Structured, analytical, repeatable



Creative, exploratory, intuitive

Your security team sees…

Clarity…

Insights…

Everything

Pulse

IBM SolutionsConnect 2013

Getting Ahead of the Threat with Security Intelligence

Caleb Barlow

Director – Application, Data, Mobile, Critical Infrastructure Security

twitter.com/calebbarlow

blogtalkradio.com/itsecurity

www.facebook.com/barlow.caleb

www.youtube.com/calebbarlow

IBM

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.