

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



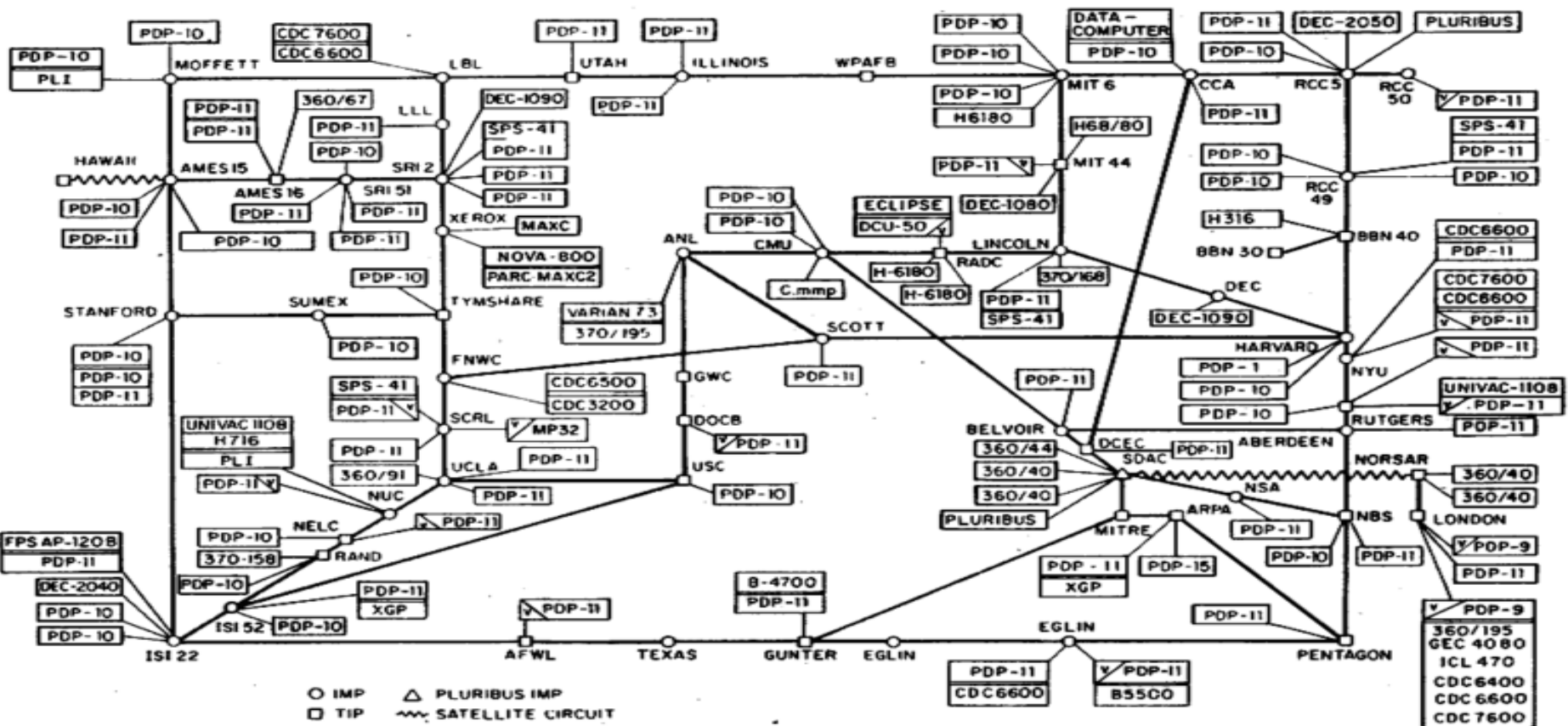
www.facebook.com/barlow.caleb



www.youtube.com/calebbarlow



ARPANET LOGICAL MAP, MARCH 1977



○ IMP △ PLURIBUS IMP
 □ TIP ~ SATELLITE CIRCUIT

(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



361 million

people using the Internet.¹

5.8%

of the world's population.¹

In 2012



2.67 billion

people using the Internet.¹

33%

of the world's population.¹



.... And Becoming Mobile



In 2000

720 million
mobile subscribers worldwide.⁴

12%
of the world's population.⁴



In 2012

6 billion
mobile subscribers worldwide.⁵

87%
of the world's population.⁴

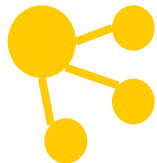




Innovative technology changes everything



**1 trillion connected
objects**



**Social
business**



Cloud and virtualization



**1 billion mobile
workers**



**Bring your
own IT**



- 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?

“Google Earth” Would Like to Access Your Contacts

Search for a contact to fly to their address.

Don't Allow

OK

“Flashlight” Would Like to Use Your Current Location

For Compass Mini Map to work properly, location services need to be enabled.

Don't Allow

OK



Motivation and sophistication is evolving rapidly

National Security



Nation-state actors **Stuxnet**

Espionage, Activism



Competitors and Hacktivists **Aurora**

Monetary Gain



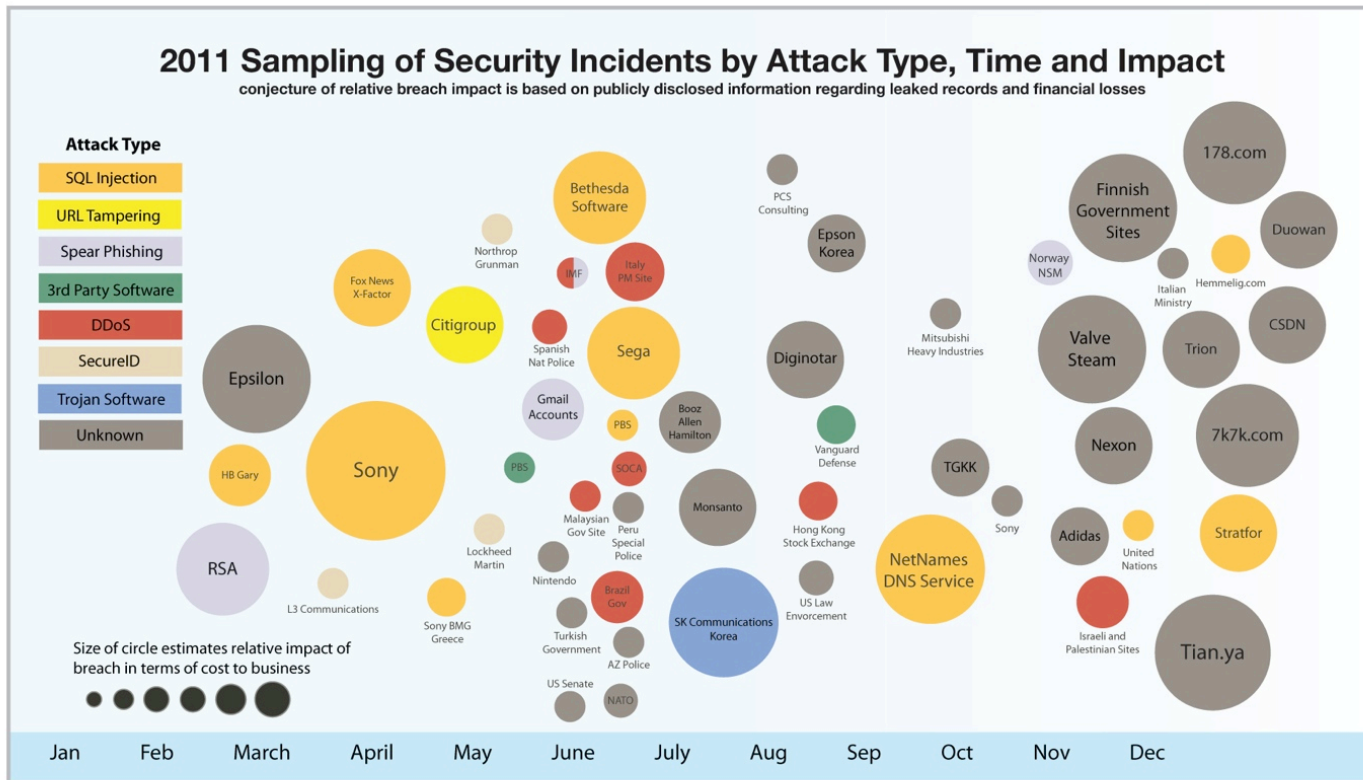
Organized crime **Zeus**

Revenge, Curiosity



Insiders and Script-kiddies **Code Red**

Reported security breaches continue to increase

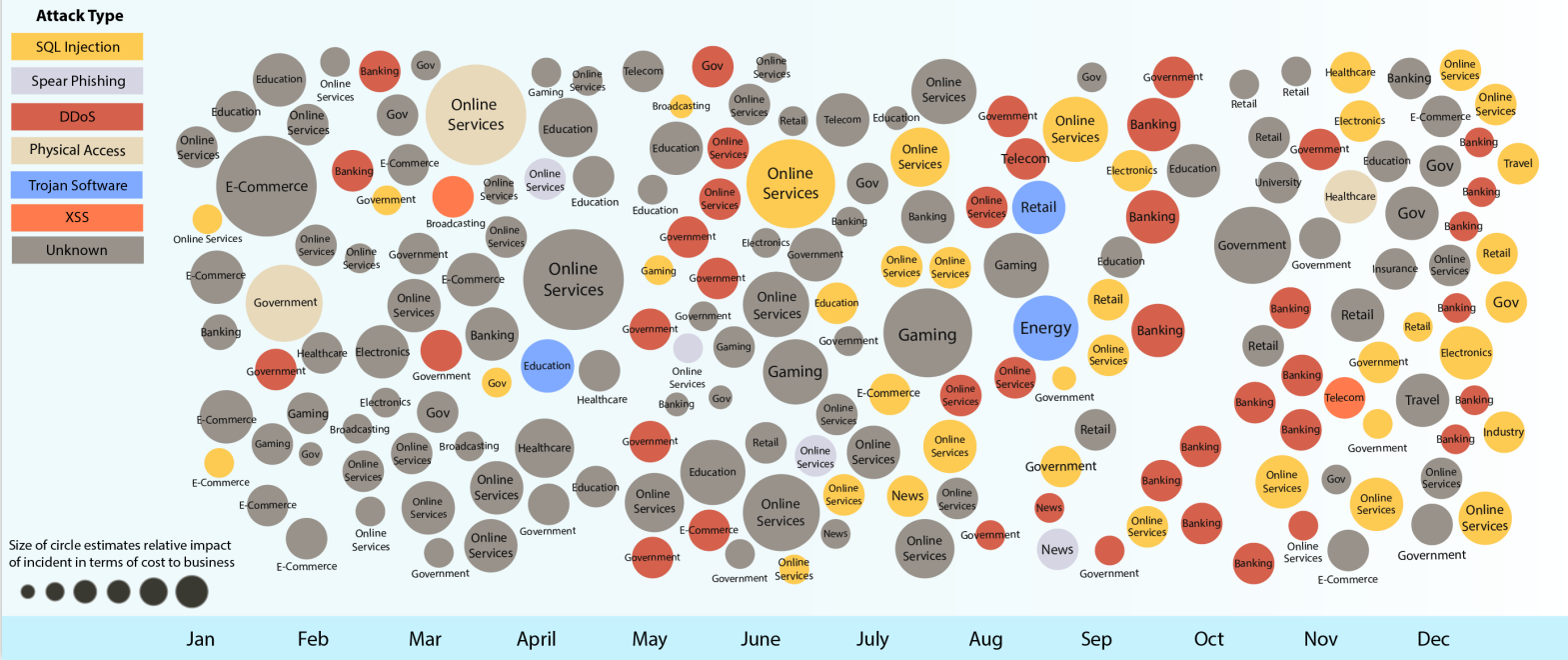


Source: IBM X-Force® 2011 Full Year Trend and Risk Report

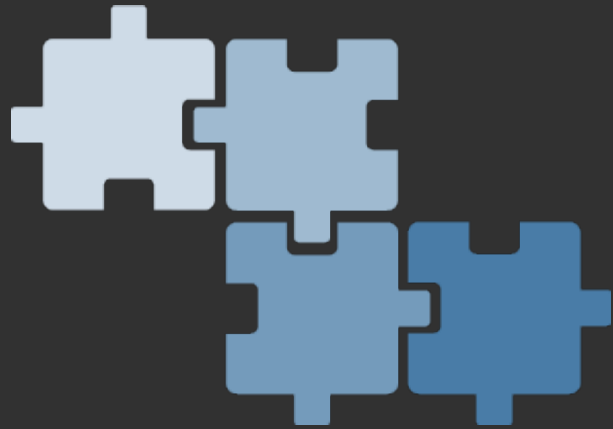
Reported security breaches continue to increase

2012 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



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



How do we
solve this?

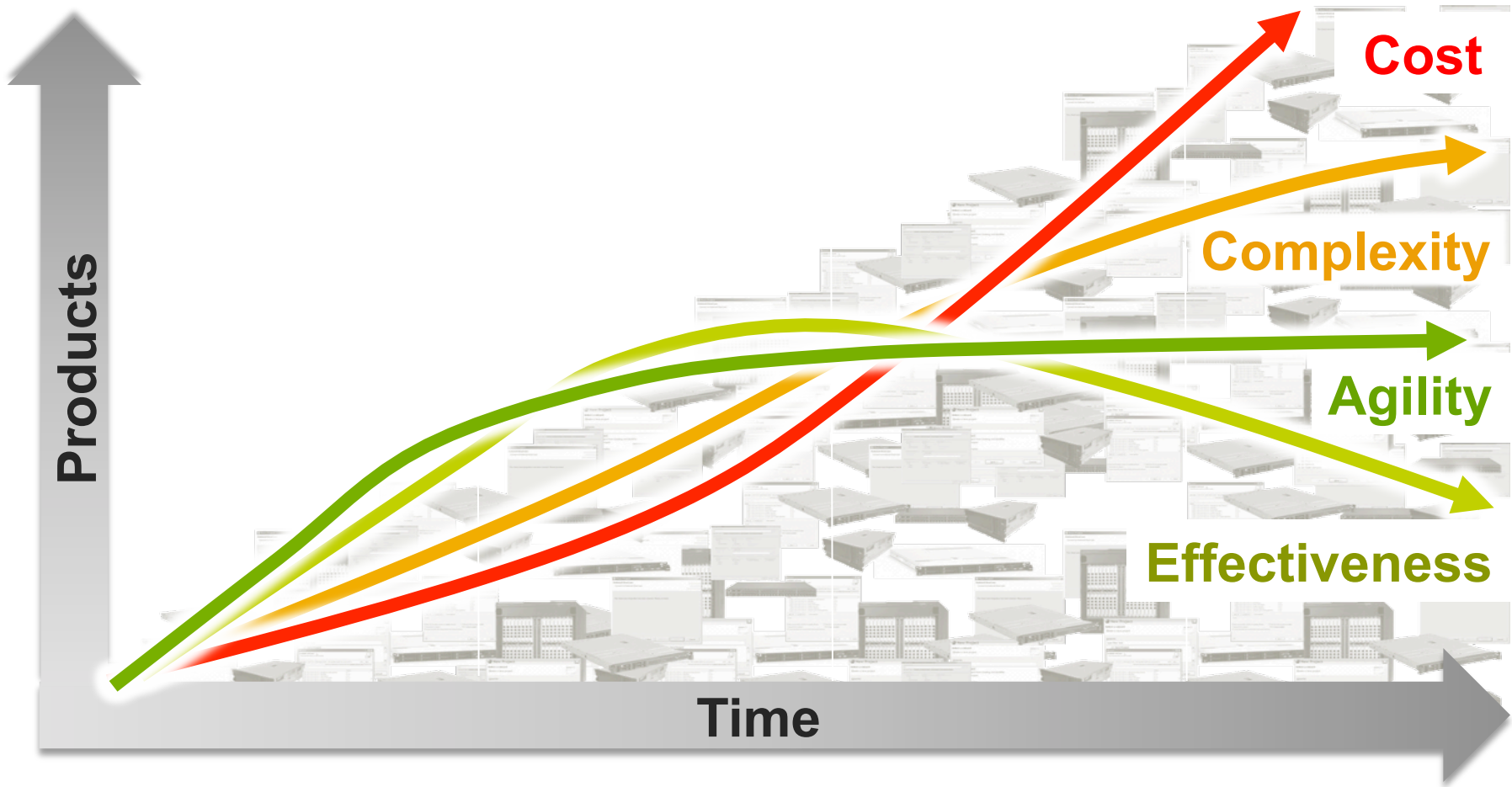


Products



Time





Cost

Complexity

Agility

Effectiveness

Products

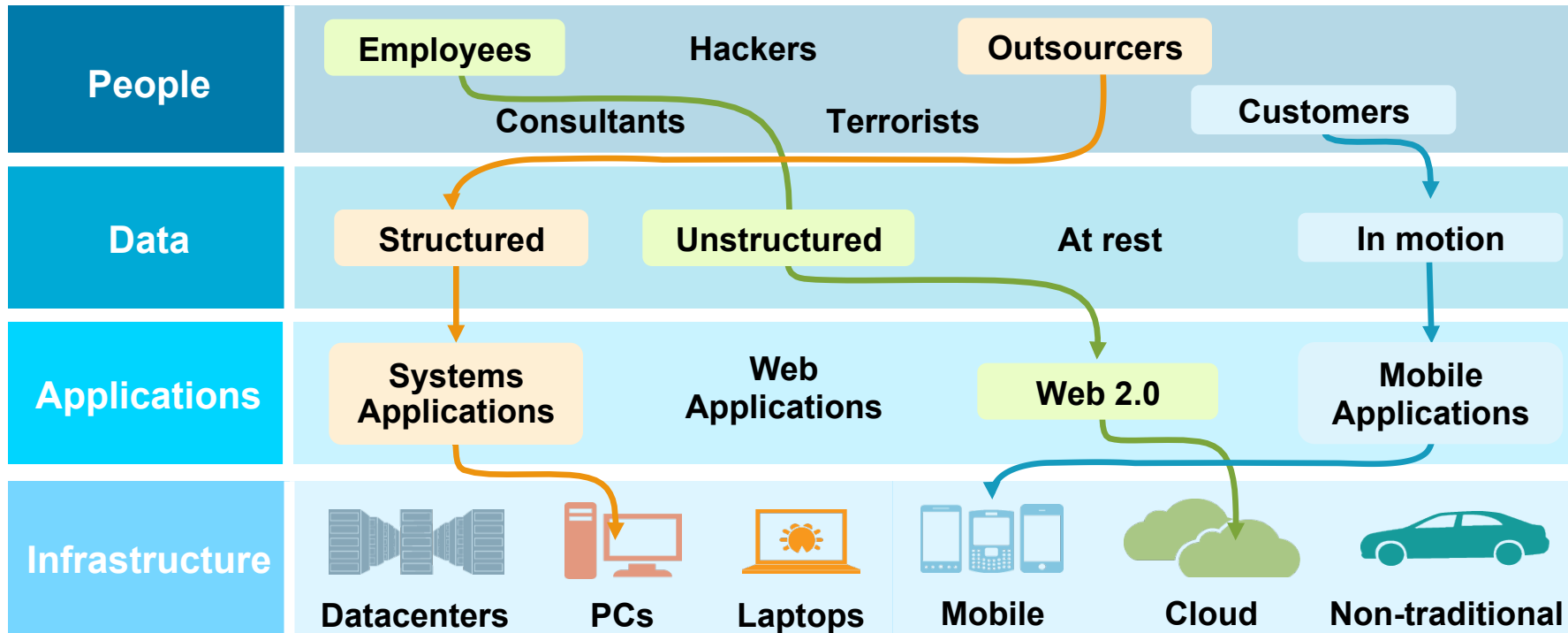
Time

The image features a horizontal banner with a white central band and dark, textured borders above and below. The text is centered in the white band.

Your security team sees noise

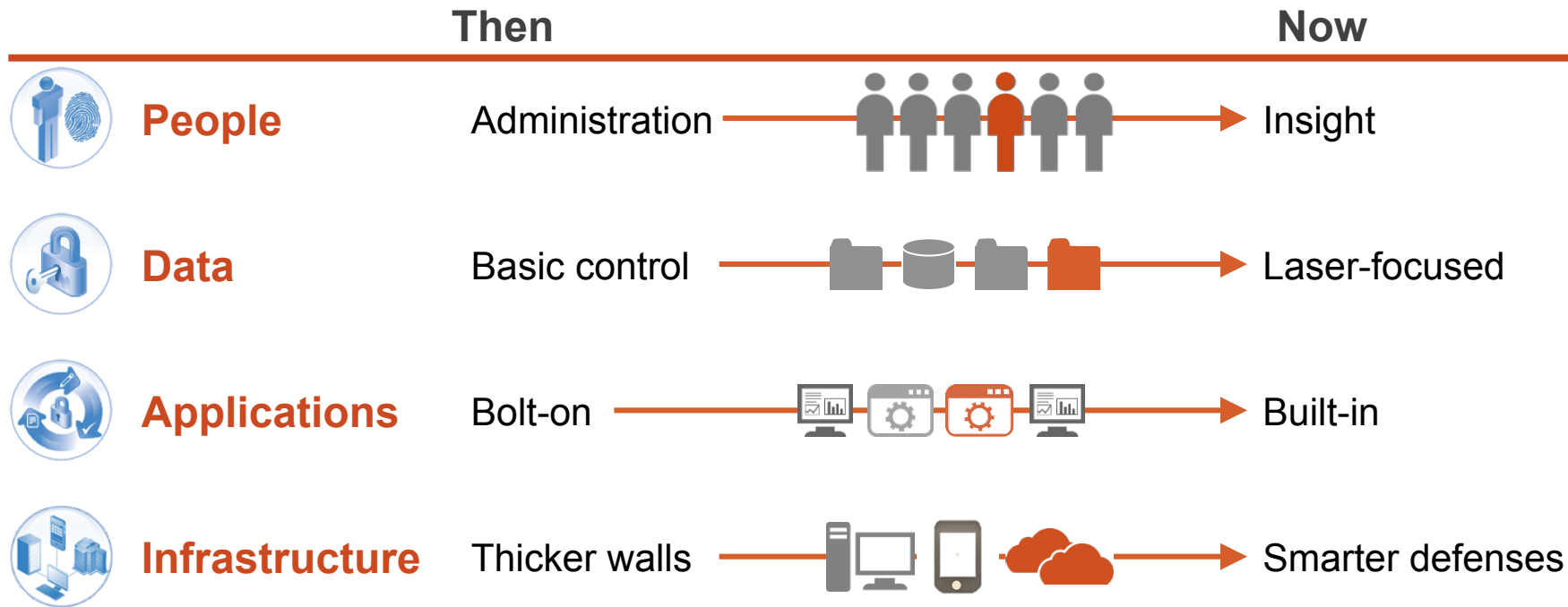


Security challenges are a complex, four-dimensional puzzle ...





... that requires a new approach



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

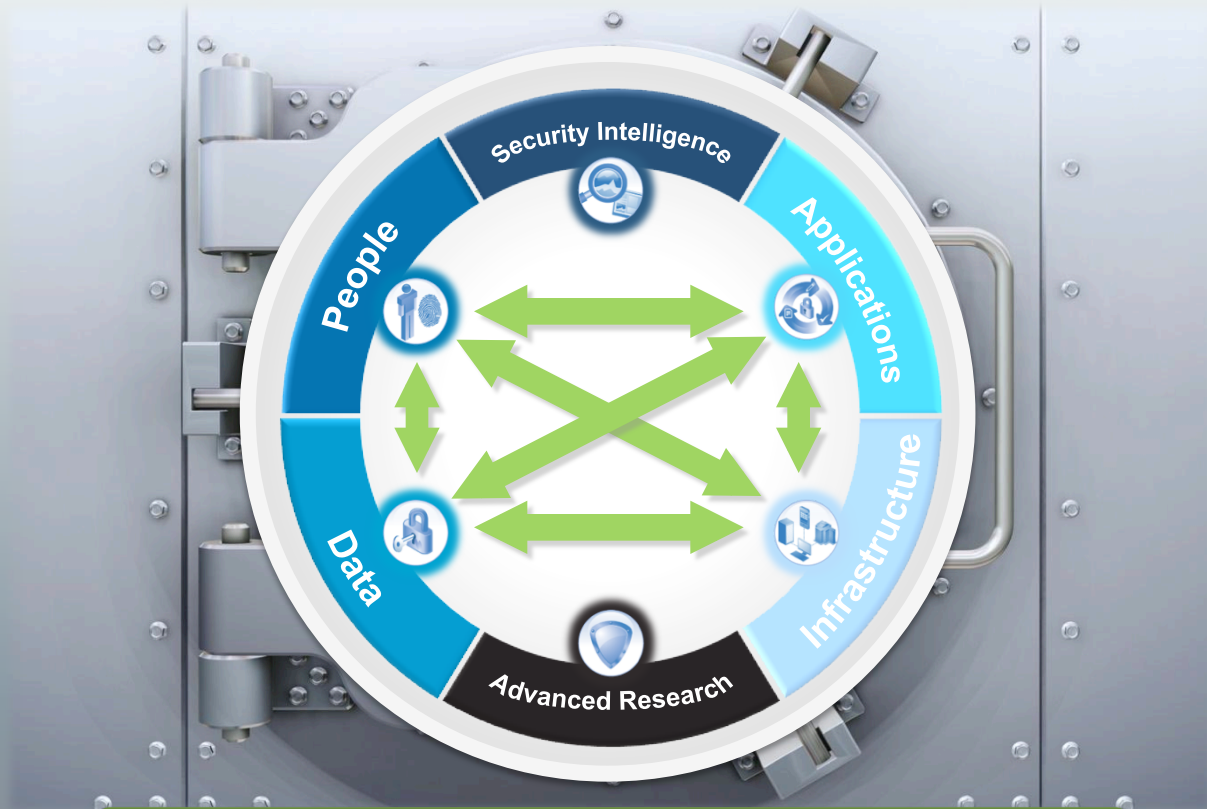




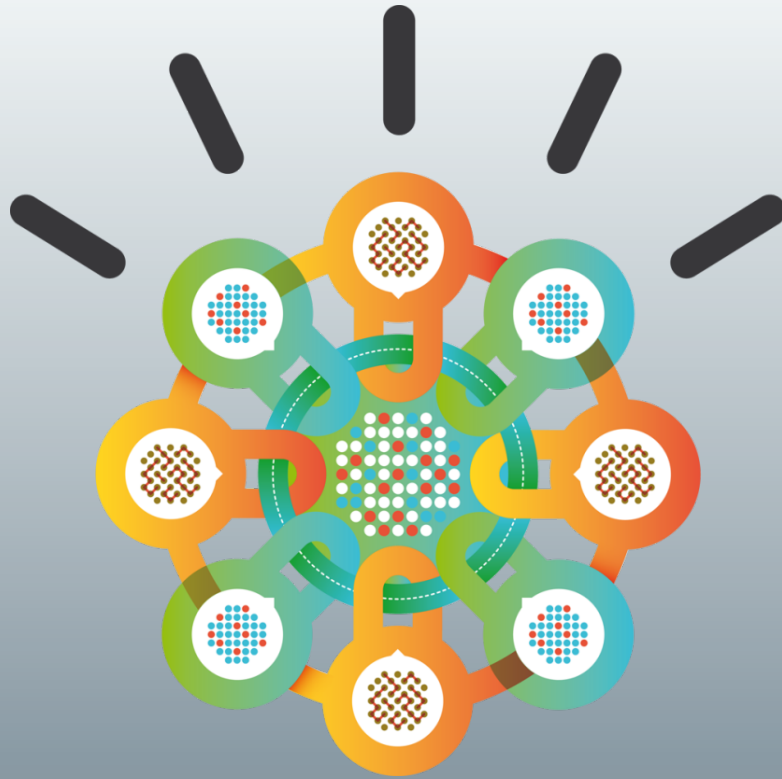
Monitor Everything



Consume Threat Intelligence



Integrate Across Domains



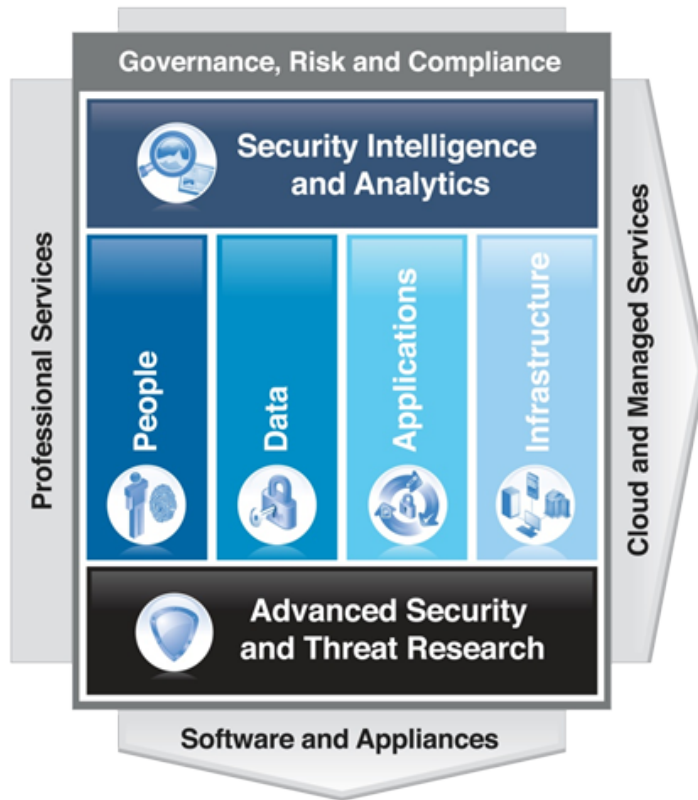
Security Intelligence



Intelligence

Integration

Expertise



IBM Mobile Security



Device Management

Security for endpoint device and data

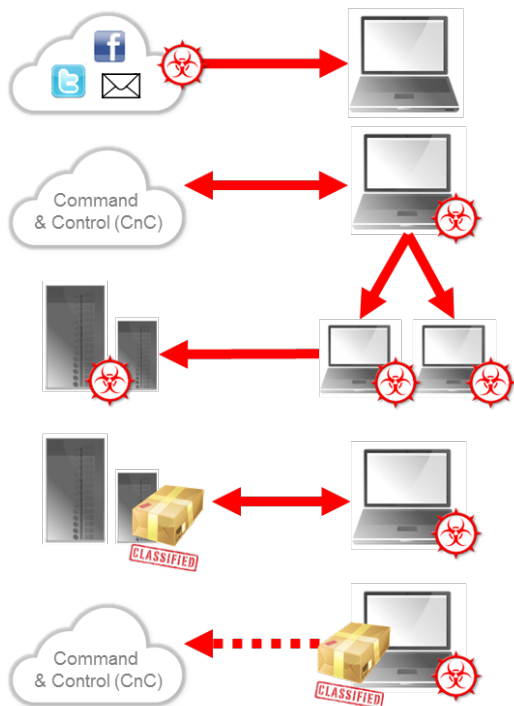
Network, Data, and Access Security

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

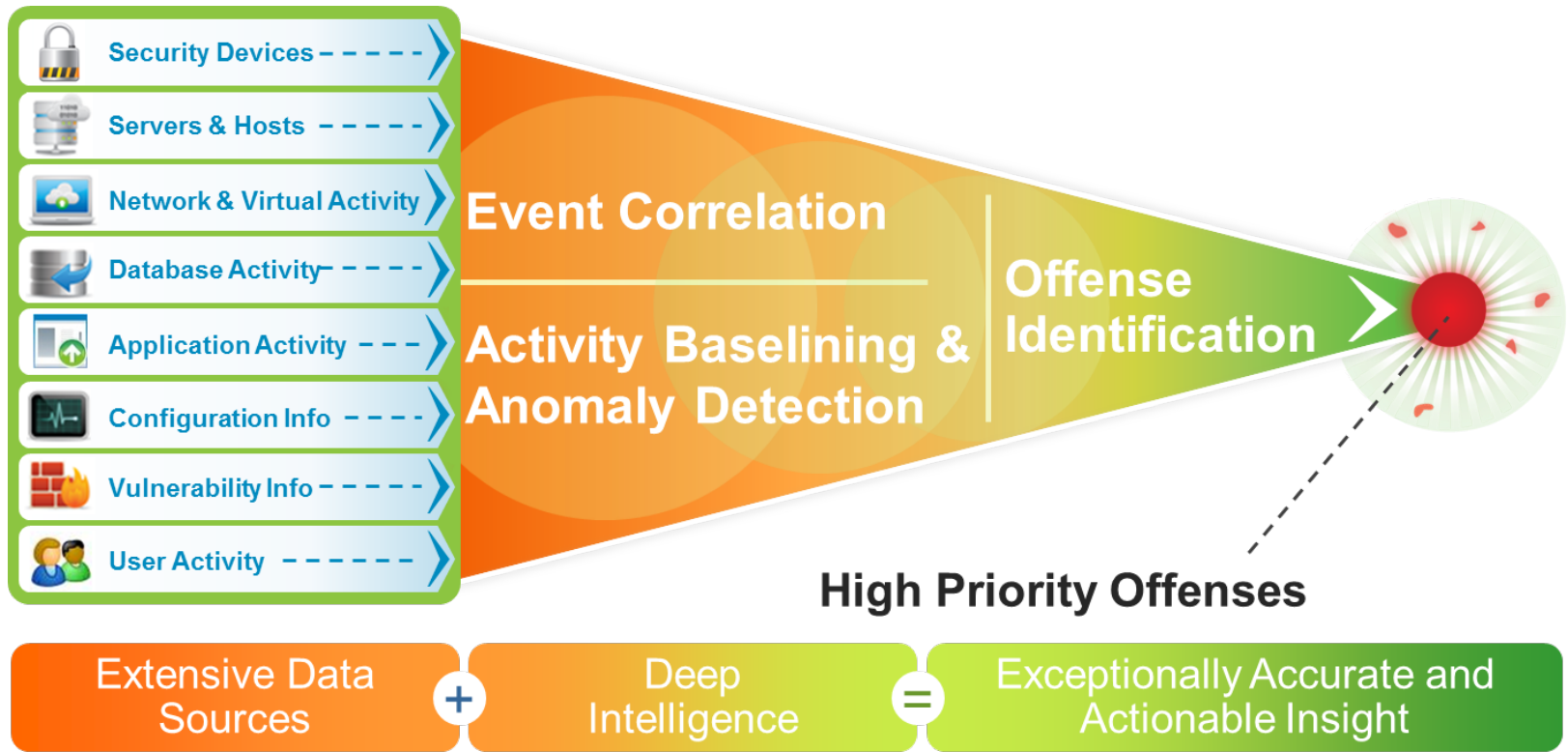
Deep data security, access controls

Network anomaly detection, blocking

Security Big Data Analytics

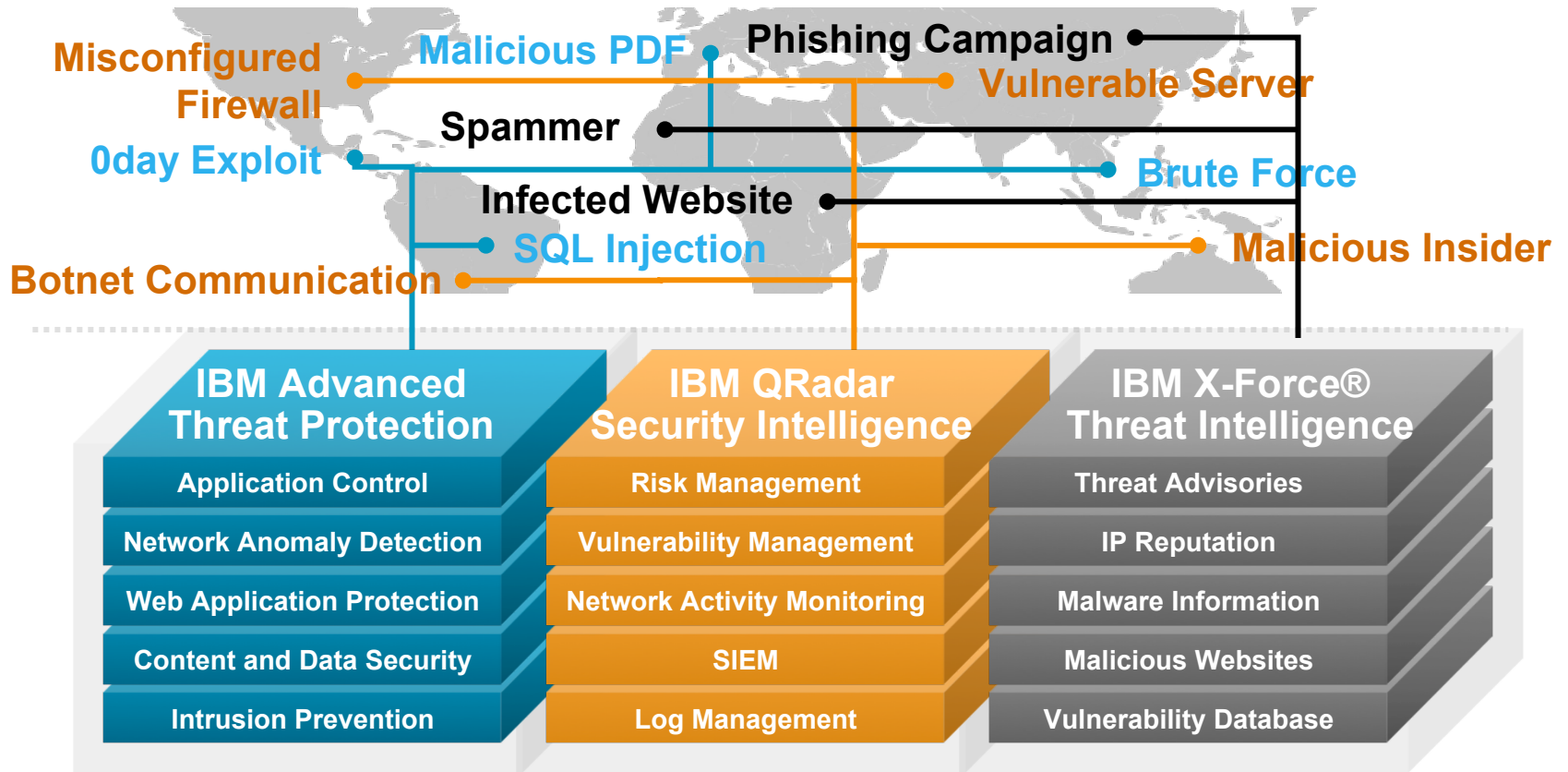


Security Intelligence: Integrating across IT silos

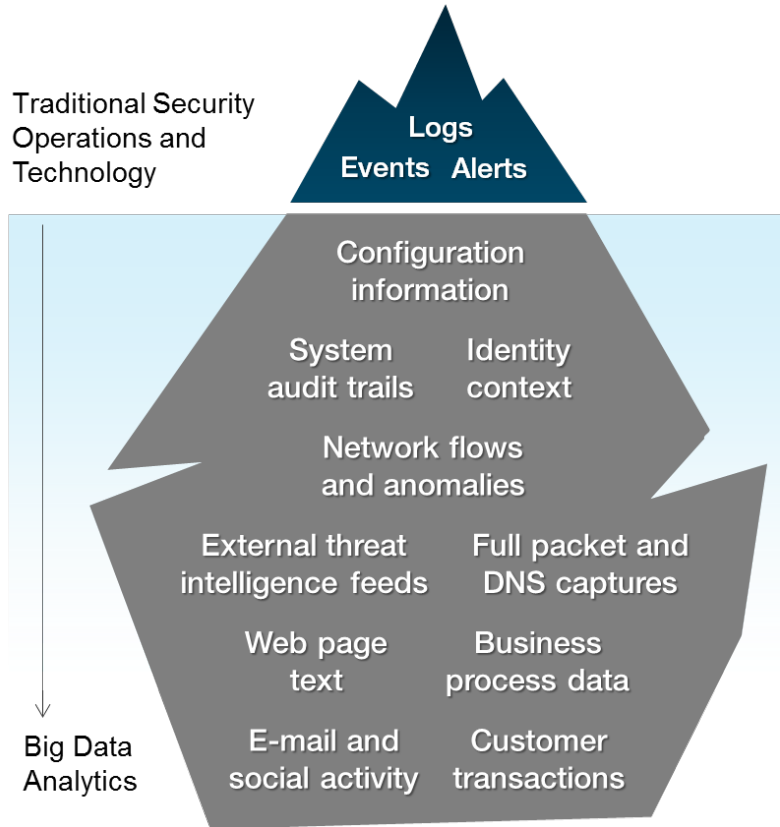


J1C/0120/04/03

IBM Advanced Threat Protection Platform



Customers want to build insights from broader data sets



New Considerations

Collection, storage and processing

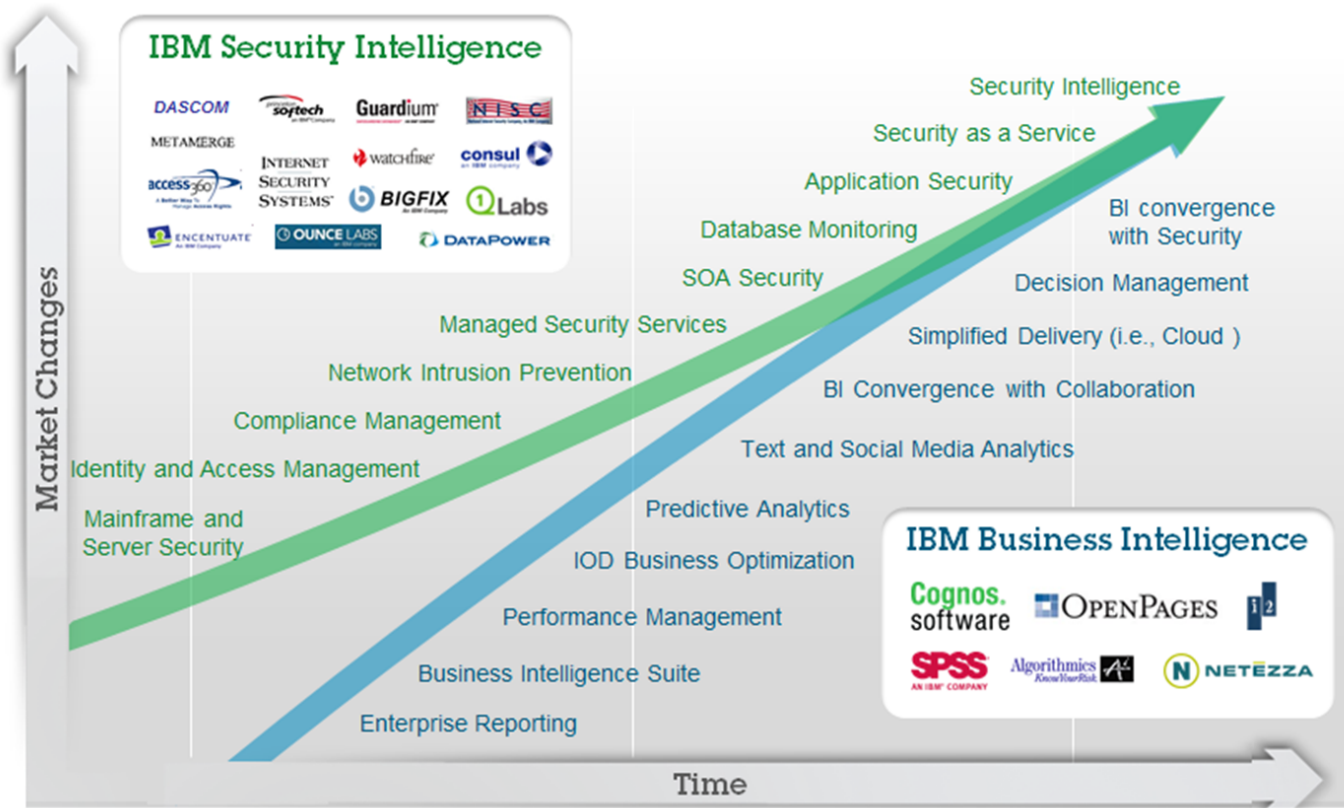
- Collection and integration
- Size and speed
- Enrichment and correlation

Analytics and workflow

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

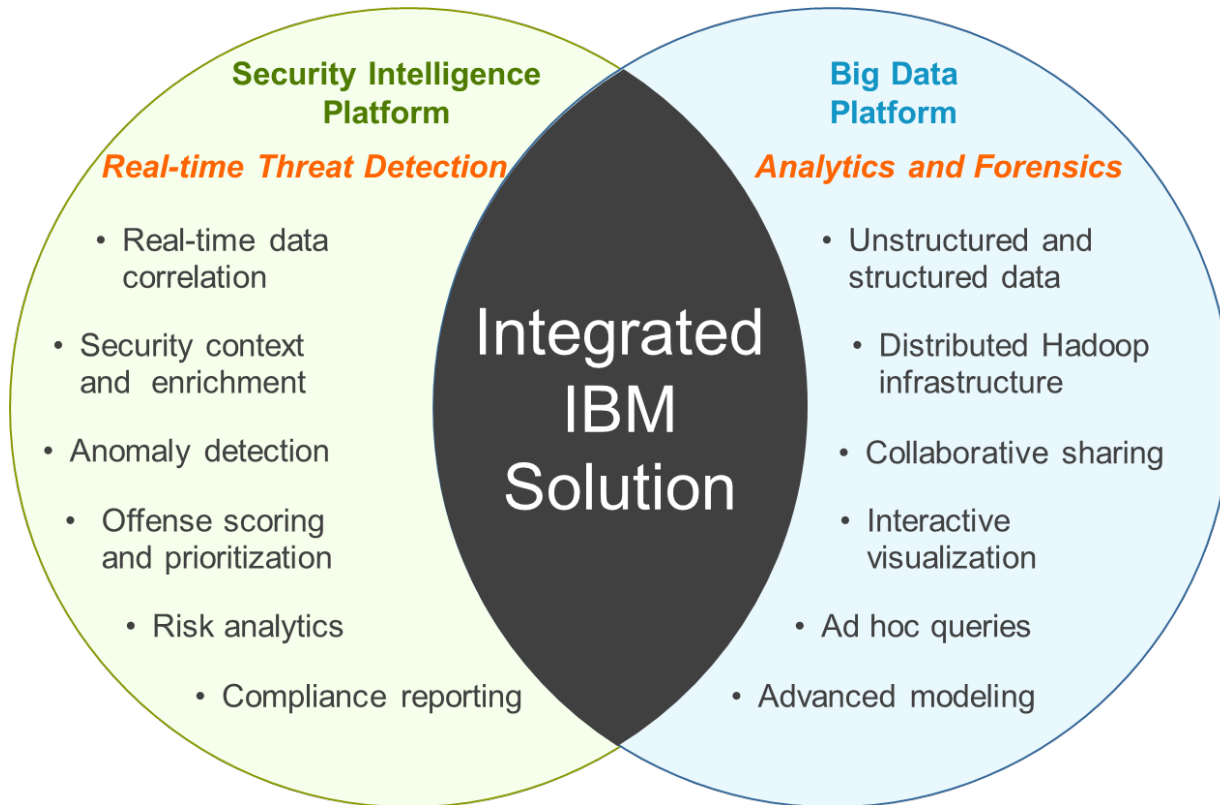


IBM is bringing together security and analytics



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



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.



© 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.