

An abstract graphic on the left side of the slide consists of several thick, overlapping lines in various colors: orange, blue, green, red, purple, and pink. These lines are arranged in a way that suggests a network or data flow, with some lines crossing and others running parallel. The lines originate from the top-left and bottom-left corners and extend towards the right side of the slide.

# Stream Keynote: Security Intelligence

**Pulse2013**  
Optimizing the World's Infrastructure

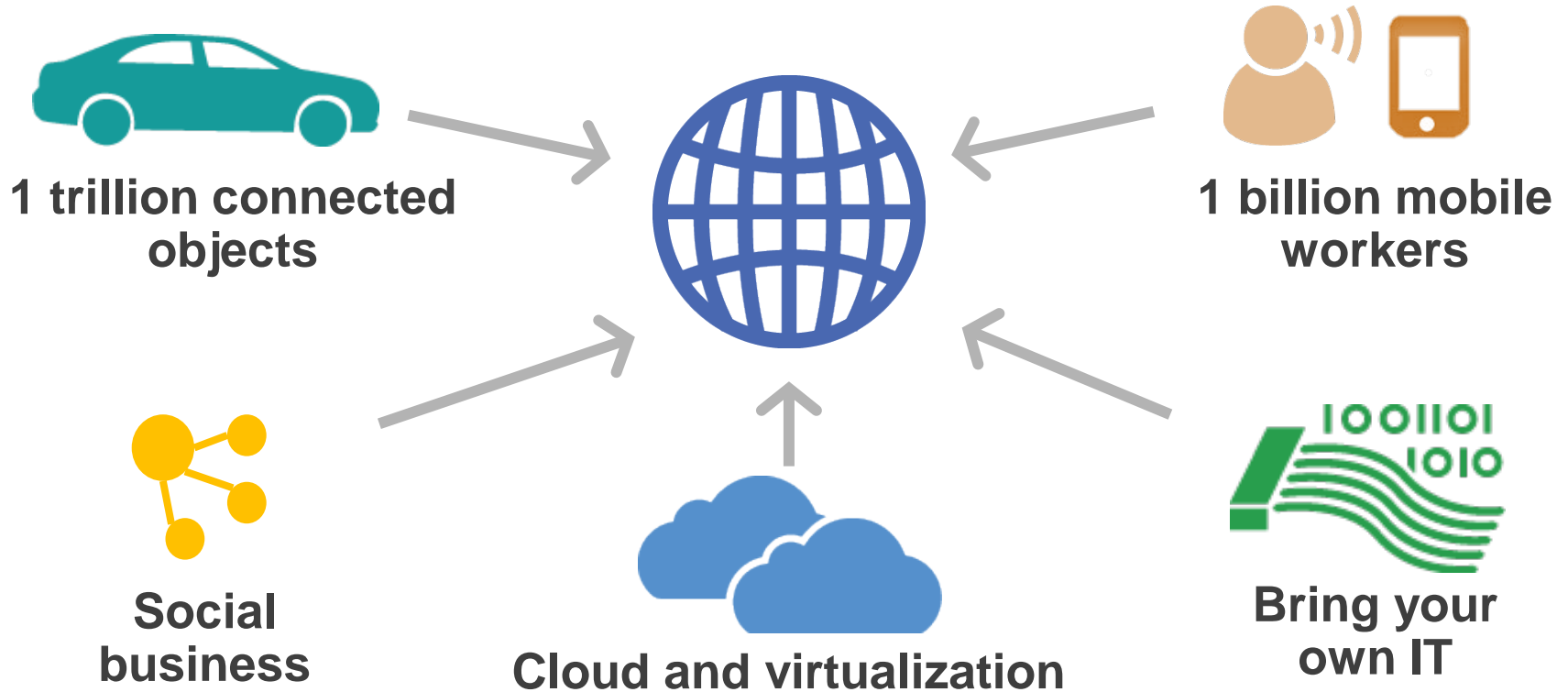


# Security Intelligence Keynote

**Brendan Hannigan**

General Manager, IBM Security Systems Division  
IBM Software Group

# Innovative technology changes everything



# Motivation and sophistication is evolving rapidly

1995 – 2005  
*1<sup>st</sup> Decade of the  
Commercial Internet*

2005 – 2015  
*2<sup>nd</sup> Decade of the  
Commercial Internet*

## Motive

National Security, Infrastructure Attack

State actors

Espionage, Political Activism

Competitors, hacktivists

Monetary Gain

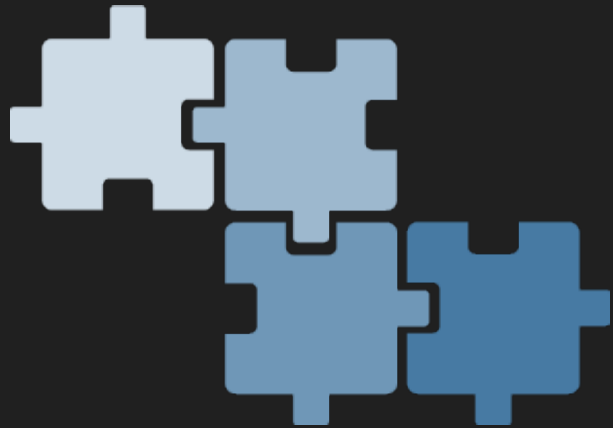
Organized crime

Revenge

Insiders

Curiosity

Script-kiddies or hackers



How do we  
solve this?

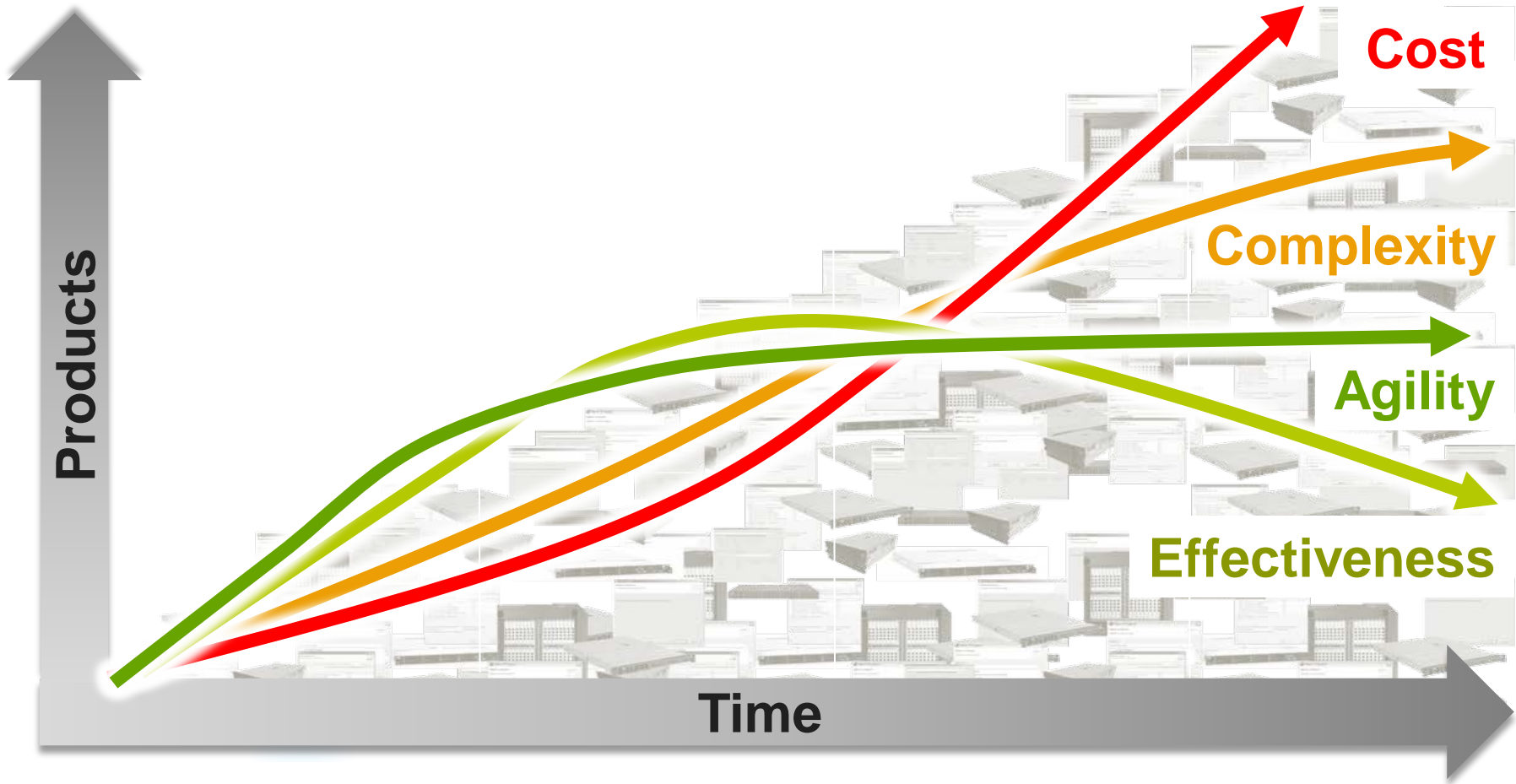


Products



Time





**Cost**

**Complexity**

**Agility**

**Effectiveness**

**Products**

**Time**

**Your security team sees noise**



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

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

Infrastructure



**Datacenters**



**PCs**



**Laptops**

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

Infrastructure



**Datacenters**



**PCs**



**Laptops**



**Mobile**

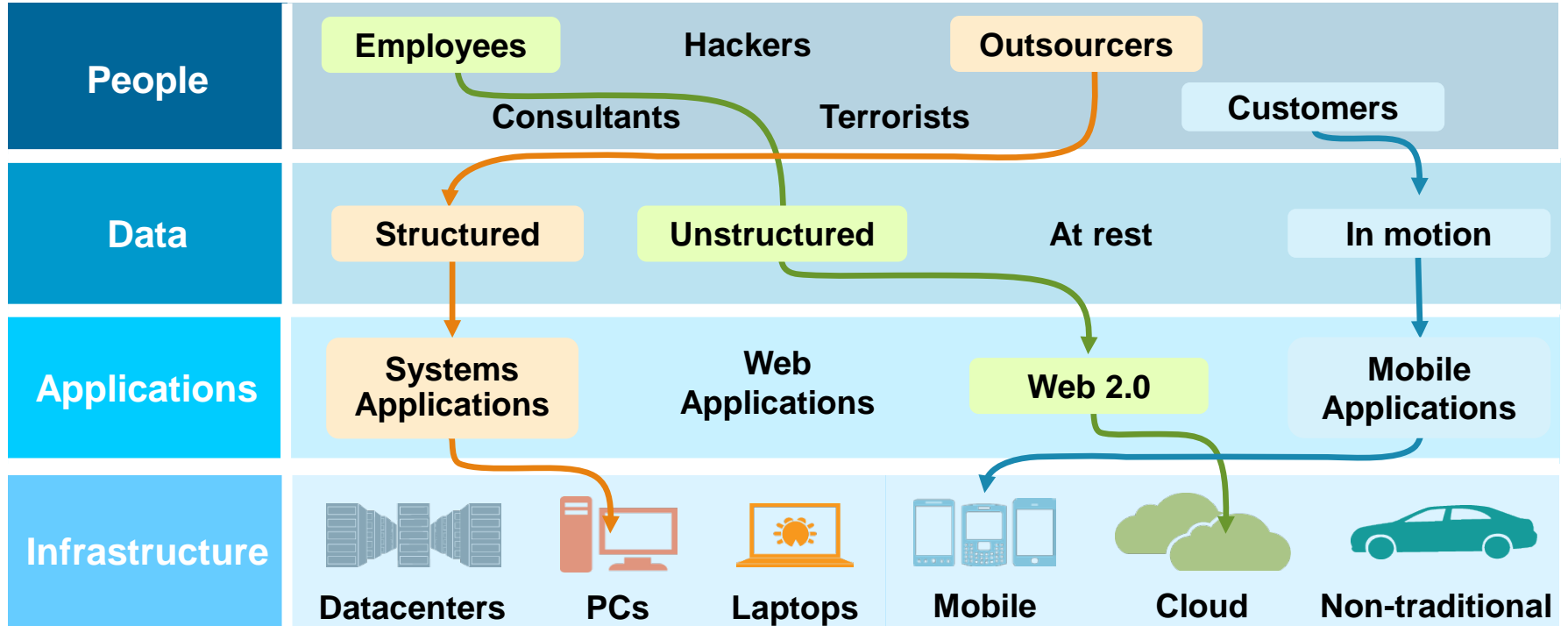


**Cloud**



**Non-traditional**

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



... that requires a new approach

Then

Now

---

# ... that requires a new approach

Then

Now



**People**

Administration

# ... that requires a new approach



# ... that requires a new approach

Then

Now



**People**

Administration



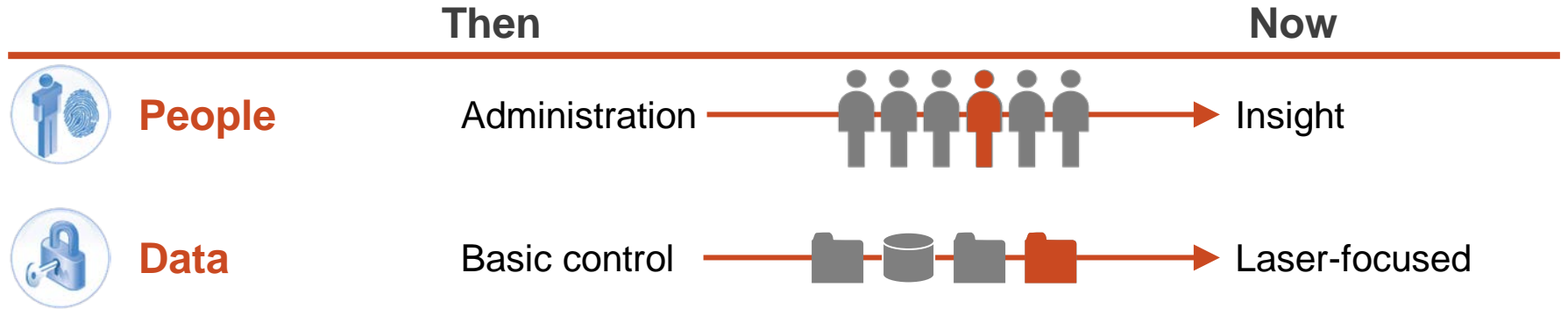
Insight



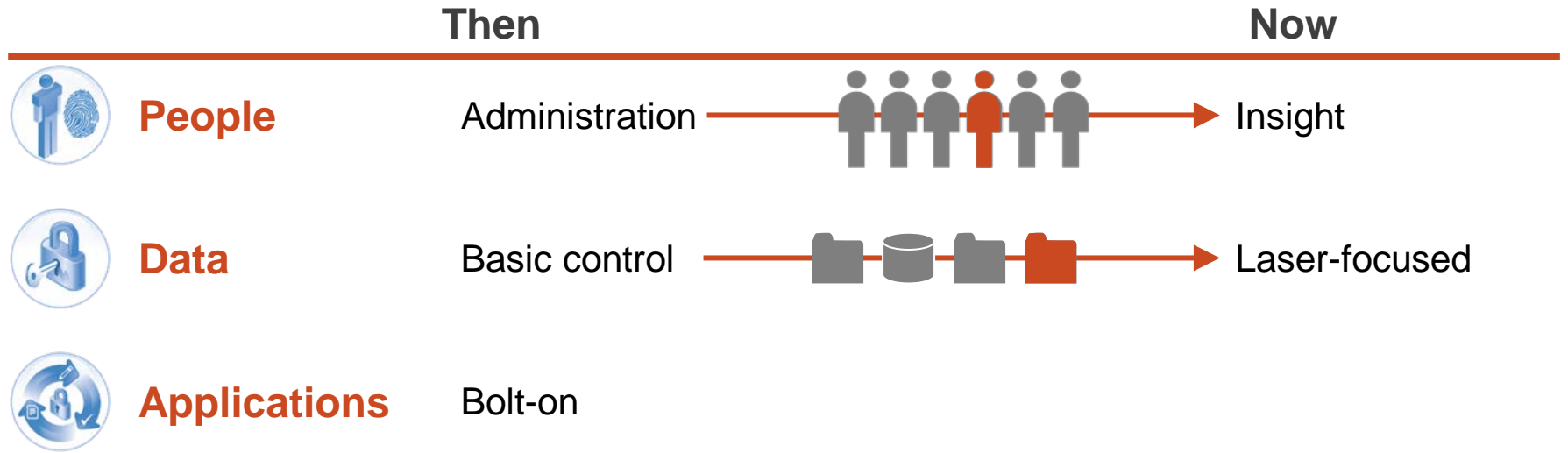
**Data**



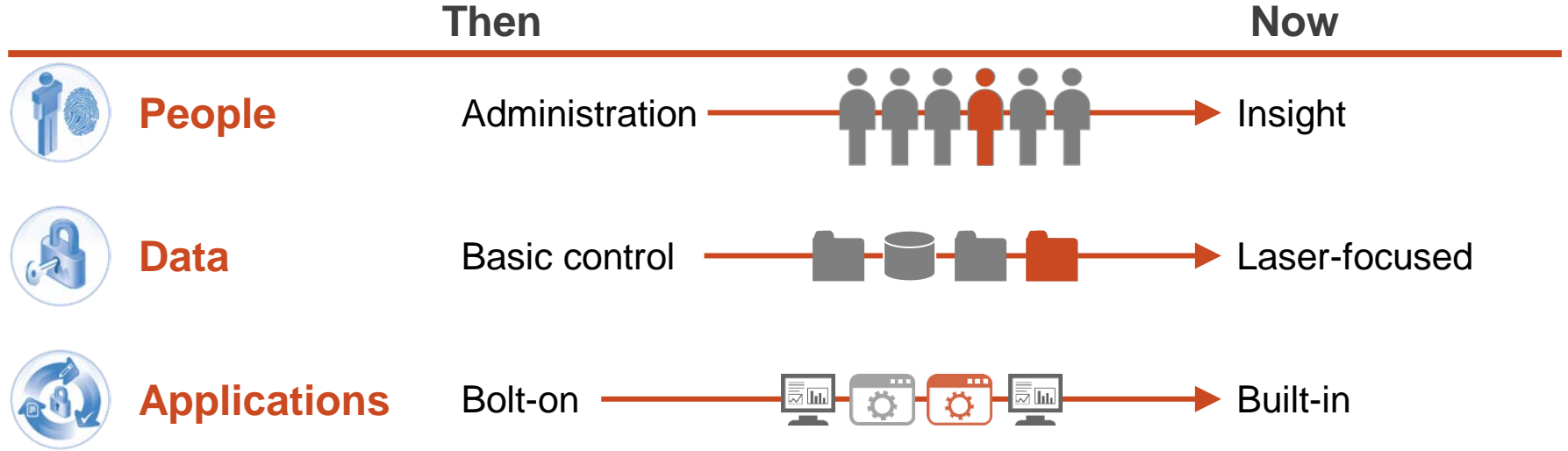
# ... that requires a new approach



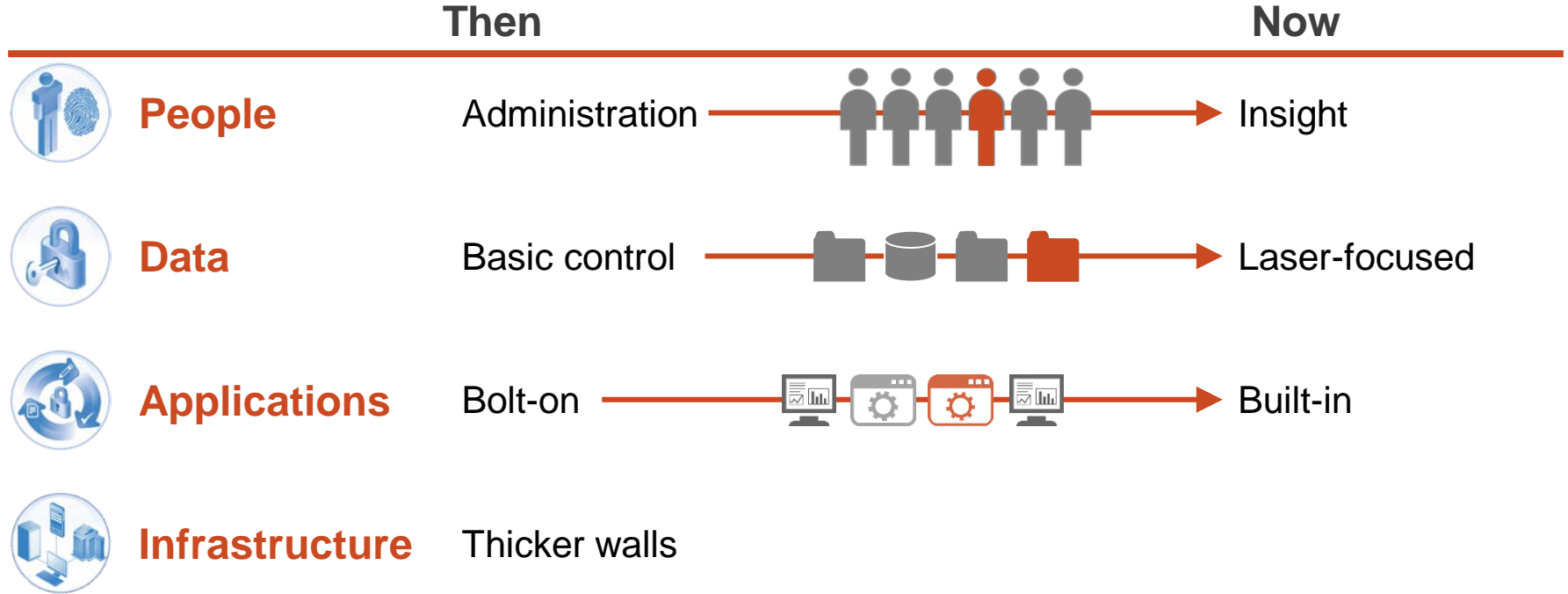
# ... that requires a new approach



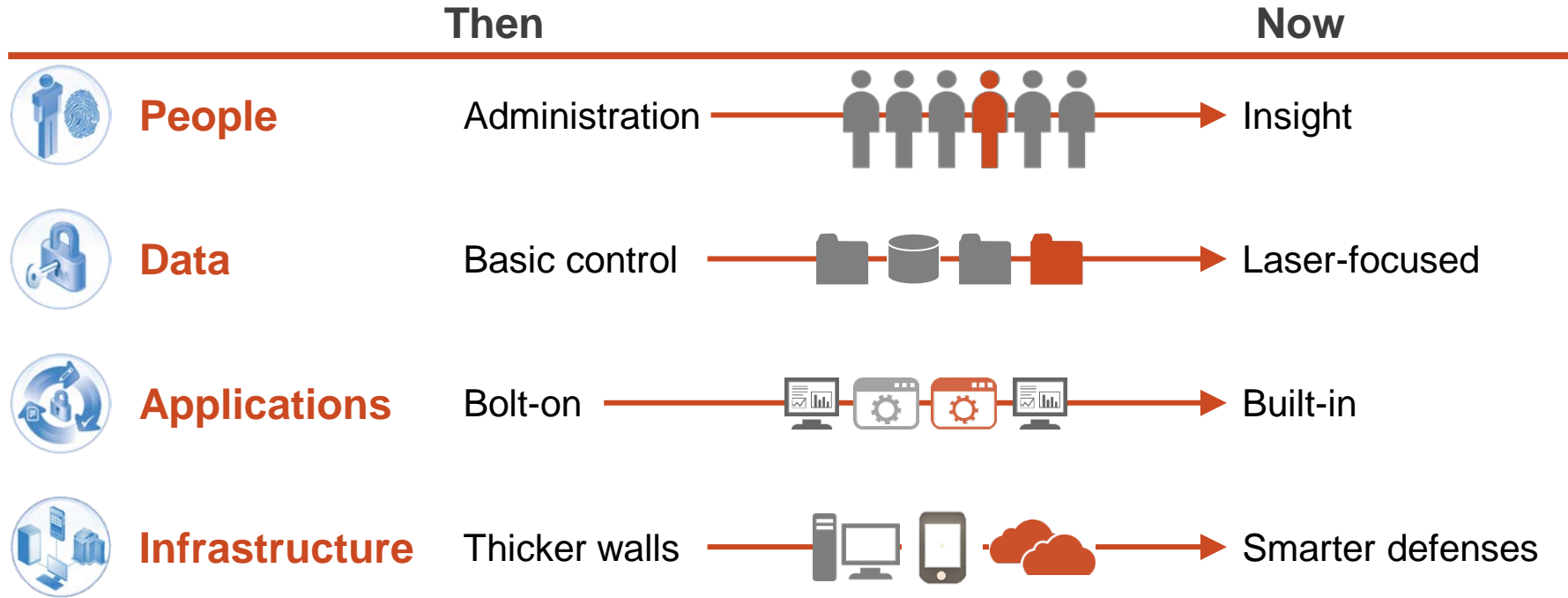
# ... that requires a new approach



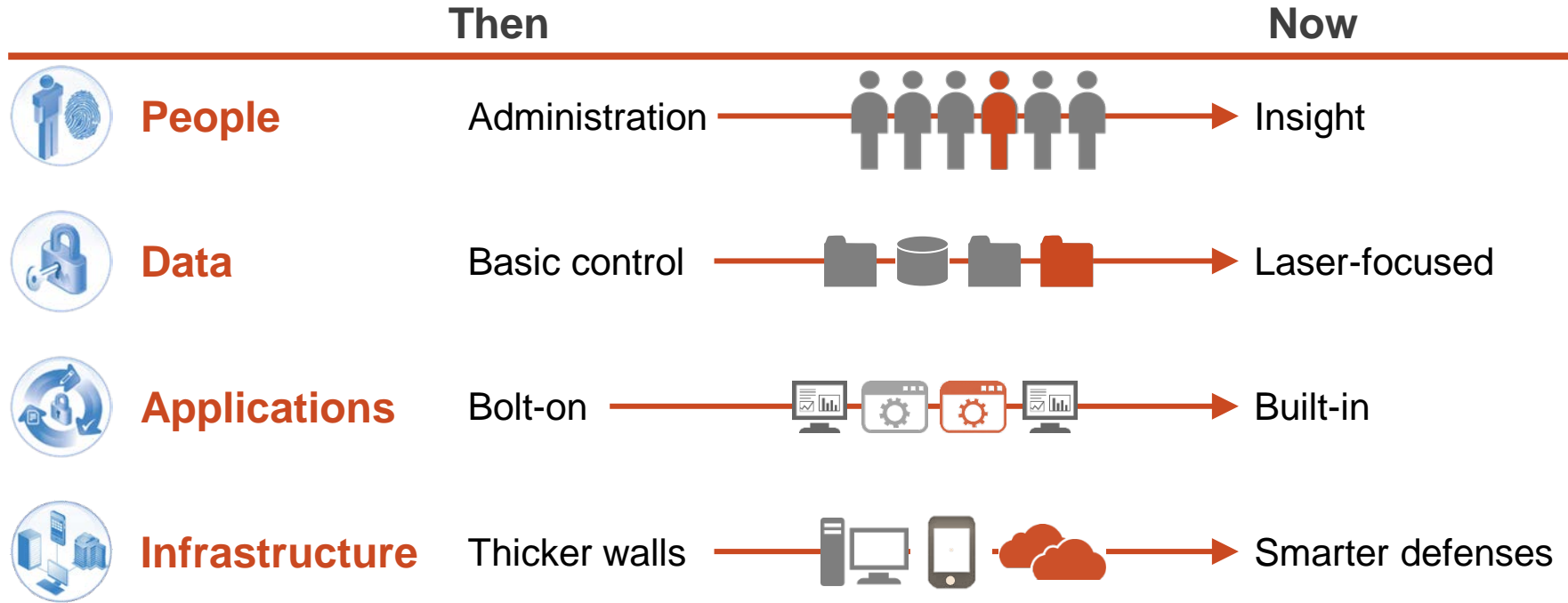
# ... that requires a new approach



# ... that requires a new approach

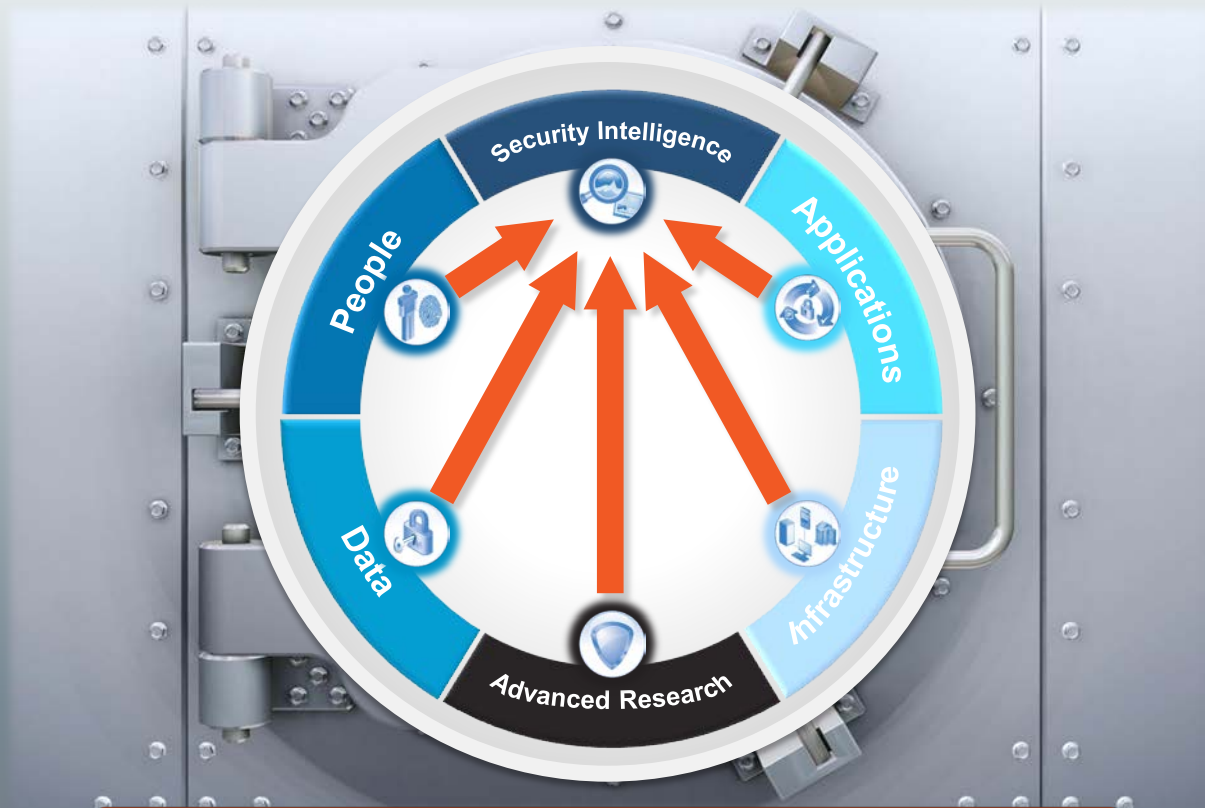


# ... that requires a new approach



**Collect and Analyze Everything**





**Monitor Everything**

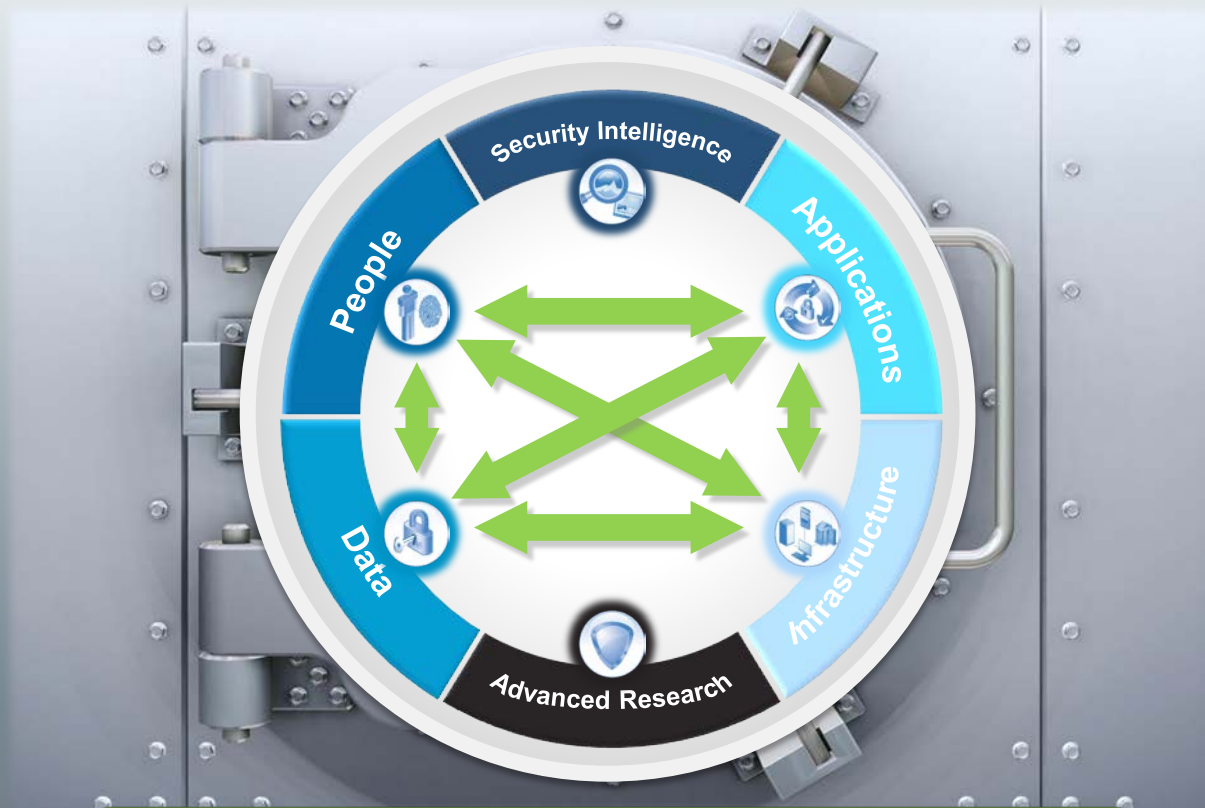






**Consume Threat Intelligence**





**Integrate Across Domains**

Applying these  
principles

**IBM**

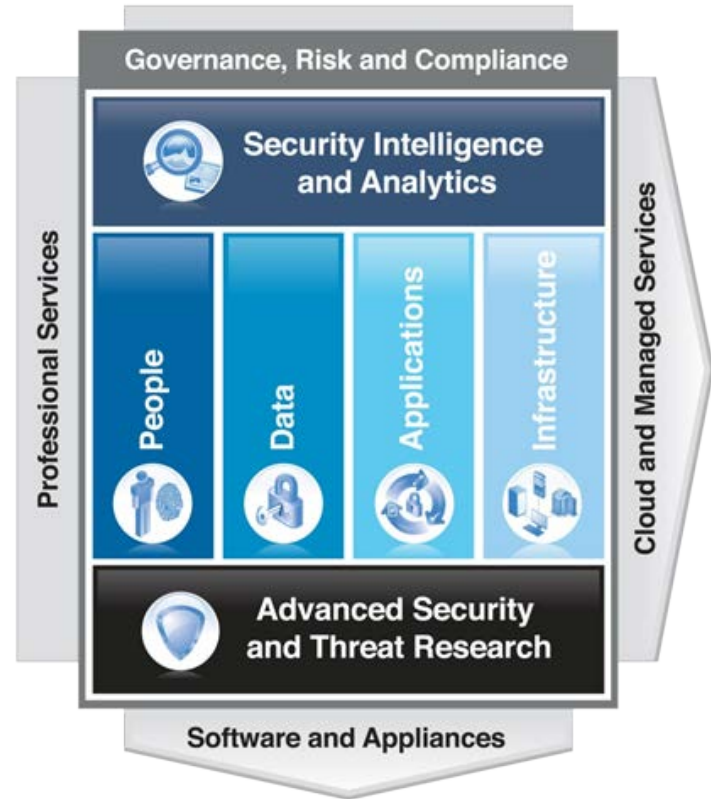
The IBM logo is rendered in a large, bold, blue font. The letters are filled with a vibrant image of the Earth from space, showing swirling white clouds and deep blue oceans. The logo is set against a dark blue background and has a subtle reflection effect below it.

# IBM delivers security solutions across a comprehensive framework

**Intelligence**

**Integration**

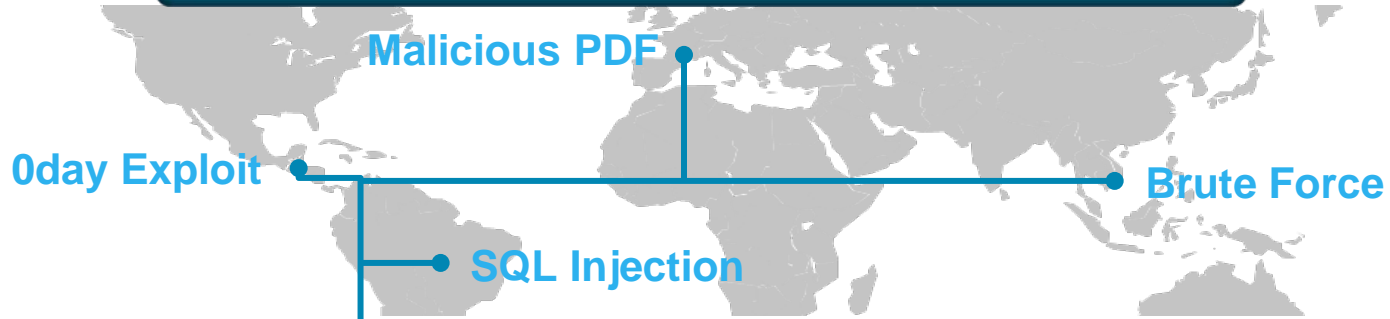
**Expertise**



# IBM Advanced Threat Protection Platform



# IBM Advanced Threat Protection Platform



## IBM Advanced Threat Protection

Application Control

Network Anomaly Detection

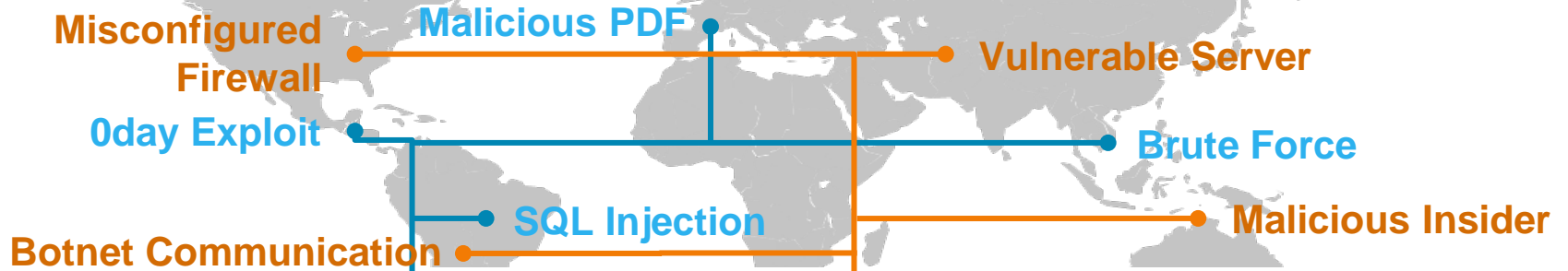
Web Application Protection

Content and Data Security

Intrusion Prevention



# IBM Advanced Threat Protection Platform



## IBM Advanced Threat Protection

Application Control

Network Anomaly Detection

Web Application Protection

Content and Data Security

Intrusion Prevention

## IBM QRadar Security Intelligence

Risk Management

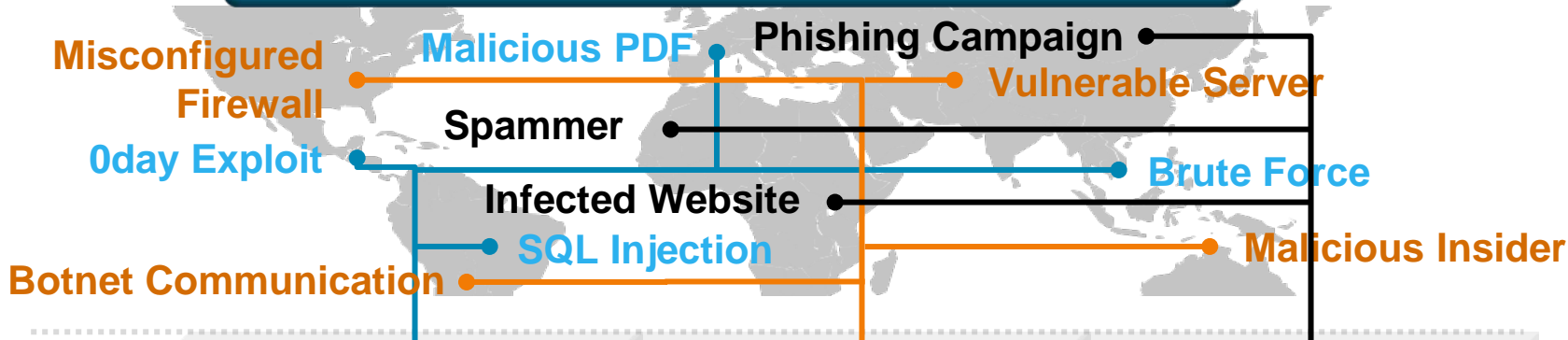
Vulnerability Management

Network Activity Monitoring

SIEM

Log Management

# IBM Advanced Threat Protection Platform



## IBM Advanced Threat Protection

Application Control

Network Anomaly Detection

Web Application Protection

Content and Data Security

Intrusion Prevention

## IBM QRadar Security Intelligence

Risk Management

Vulnerability Management

Network Activity Monitoring

SIEM

Log Management

## IBM X-Force® Threat Intelligence

Threat Advisories

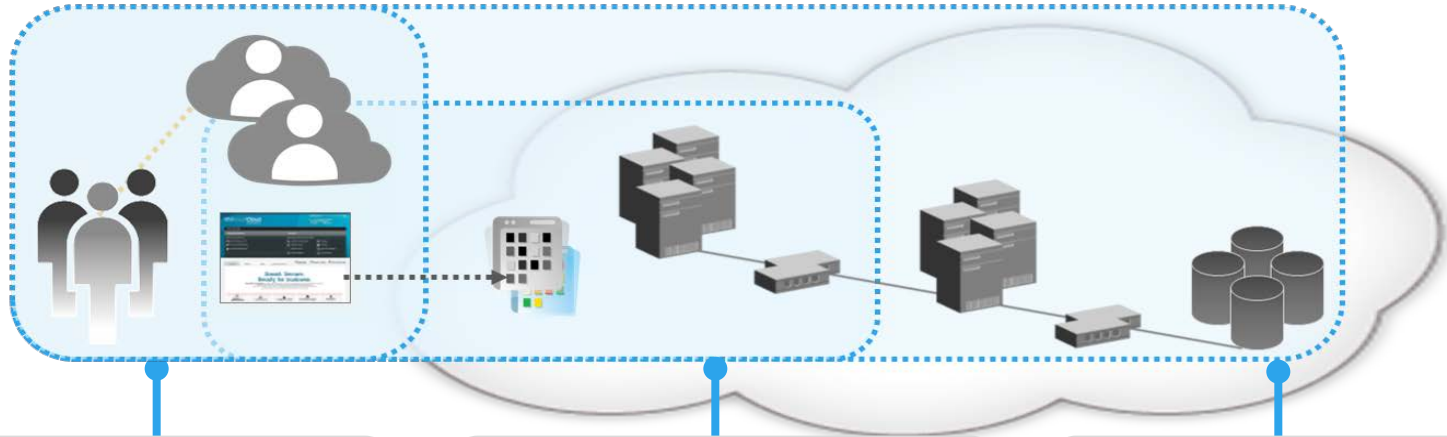
IP Reputation

Malware Information

Malicious Websites

Vulnerability Database

# IBM SmartCloud Security



## Identity Protection

- Administer, extend and help secure identity and access to / from the cloud

## Data and Application Protection

- Help secure enterprise databases
- Build, test and maintain cloud applications

## Threat Protection

- Help prevent advanced threats with layered protection and analytics

# 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

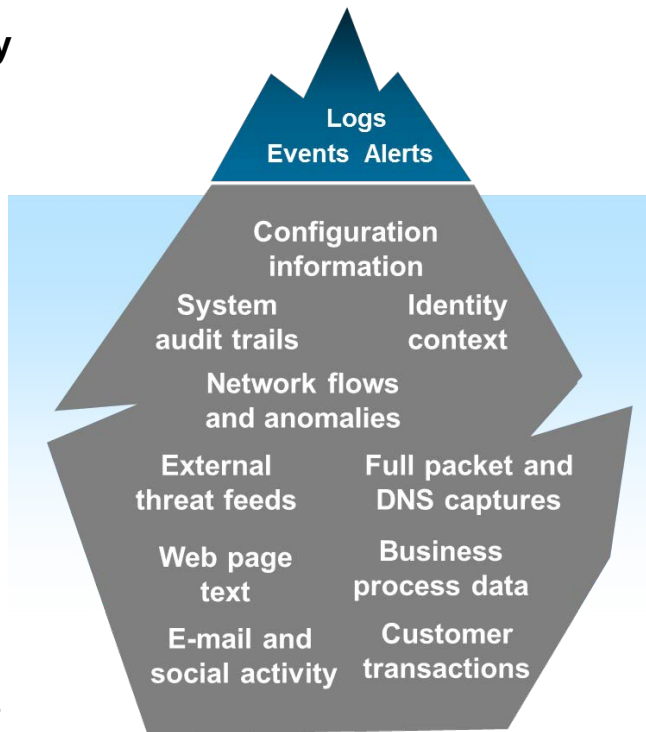
Develop and test applications

# Variety and volume of data is driving new Big Data use cases

Traditional Security  
Operations and  
Technology



Big Data Analytics



## Large FSS Customer

**250,000** managed firewalls

**30,000** network devices

**500,000** open port combinations

**410,455** Windows client systems

**36,109** Windows servers

**24,000** \*NIX servers

**1200+** vulnerability assessment products

## Size estimates of scale and volume of events and logs

**1.5 – 2 TB** per month /major security service

**200 – 750GB** total / minor security service

**Your security team sees...**

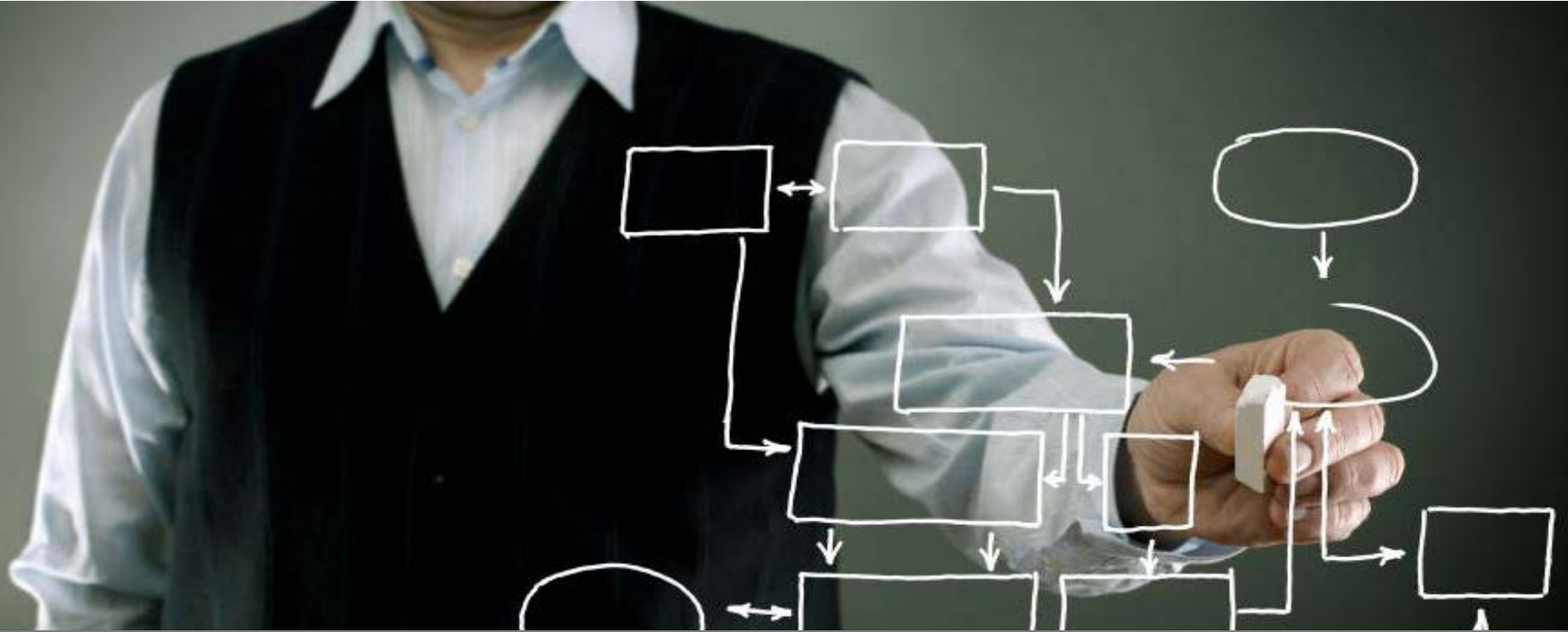


**Clarity...**



**Insights...**





**Everything**

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.**

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated there.

© Copyright IBM Corporation 2013. 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.

An abstract graphic on the left side of the slide consists of several thick, overlapping lines in various colors: orange, blue, green, red, purple, and pink. These lines are arranged in a way that suggests a network or data flow, with some lines crossing and others following parallel paths. The lines originate from the top-left and bottom-left corners and extend towards the right side of the slide.

# Stream Keynote: Security Intelligence

**Pulse2013**  
Optimizing the World's Infrastructure