

BusinessConnect  
A New Era of Smart  
June 11, 2014

# Security Intelligence

## A New Era of Security

*for a New Era of Computing*

Glen Gooding

Security Business Leader  
IBM Asia Pacific



@gg00ding





# A New Security Reality Is Here

**61%** of organizations say  
**Data theft and cybercrime**  
are the greatest threats  
to their reputation

*2012 IBM Global Reputational Risk & IT Study*



Average Australian  
data breach cost


**\$2.59M**

*2013 Cost of Cyber Crime Study  
Ponemon Institute*

 **70%**  
of security exec's  
are concerned about  
**cloud and mobile security**


*2013 IBM CISO Survey*

**Mobile malware grew**

**614%**   
in one year

*from March 2012 to March 2013*

*2013 Juniper Mobile Threat Report*

 **83%**  
of enterprises  
have difficulty finding the  
security skills they need

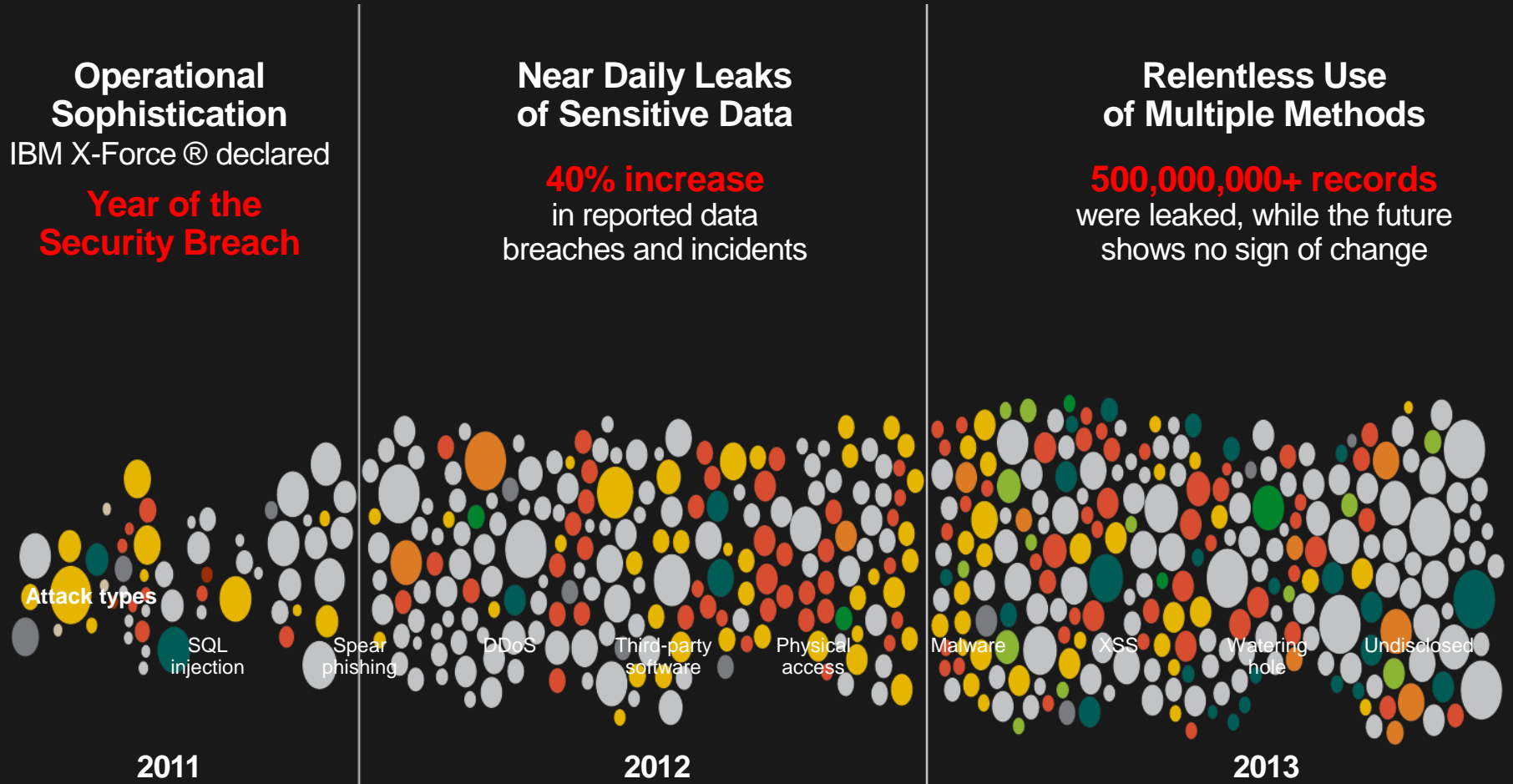
*2012 ESG Research*

**85**  tools from

**45**  vendors

*IBM client example*

# We are in an era of continuous breaches



# Why a New Approach

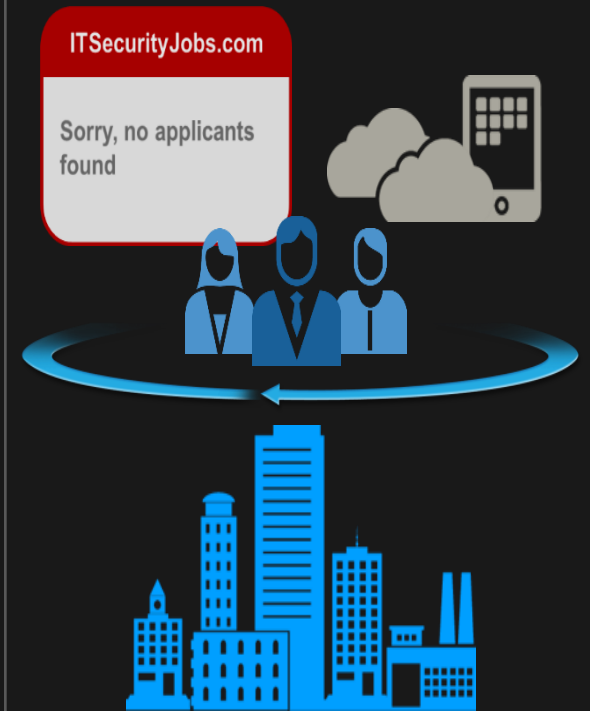
**Criminals will not relent  
and every business  
is a target**



**New technologies  
create opportunities  
to transform IT security**



**Security leaders  
are more accountable  
than ever before**



## INTELLIGENCE

*Use insights  
and analytics  
to identify  
outliers*

## INNOVATION

*Use cloud  
and mobile  
for better  
security*

## INTEGRATION

*Develop an integrated  
approach to  
stay ahead  
of the threat*

# Strategic imperative #1

*Use analytics and insights for smarter defense*

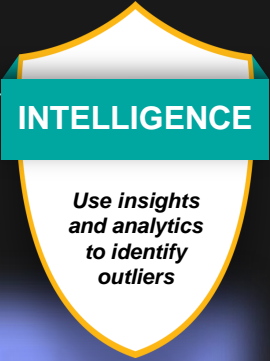
*Use insights and analytics to identify outliers*



**Use intelligence and anomaly detection across every domain**

**Build an intelligence vault around your crown jewels**

**Prepare your response for the inevitable**



# Use Intelligence & Anomaly Detection Across Every Domain

## Extensive Data Sources

-  Security devices
-  Servers and mainframes
-  Network and virtual activity
-  Data activity
-  Application activity
-  Configuration information
-  Vulnerabilities and threats
-  Users and identities
-  Global threat intelligence

## Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

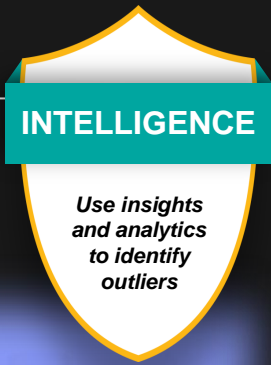
## Embedded Intelligence



Suspected Incidents

Prioritized Incidents





# Gain Insights to Prioritize What Is Most Critical



**2 Billion** logs and events per day



**25** high priority offenses



**QRadar Security Intelligence Platform**

# Build a Vault Around Your Crown Jewels

INTELLIGENCE

*Use insights  
and analytics  
to identify  
outliers*



Use insights and analytics to identify outliers

# Prepare your response for the inevitable



## Incident Forensics

- Full packet capture
- Detailed incident meta-data / evidence
- Reconstruction of content and user activity



Network Security



Insider Threat Analysis



Fraud and Abuse



Evidence Gathering

## Strategic imperative #2

*Use cloud and mobile to improve security*

INNOVATION

*Use cloud  
and mobile  
for better  
security*



**Own the security  
agenda  
for innovation**

**Employ  
innovation  
to improve security**

**Embed  
security  
on day one**

# Employ Cloud to Improve Security

**INNOVATION**

*Use cloud  
and mobile  
for better  
security*



## Traditional Security

Manual  
and static



## Cloud-enhanced Security

Automated, customizable,  
and elastic



# Build Security into Mobile from Day One

## Enterprise Applications and Cloud Services





# Device, Application, and Transaction Security



MaaS360 by Fiberlink

Trusteer Mobile Fraud Prevention

AppScan

Tealeaf

Worklight

Security Access Manager for Mobile

Discovered and enrolled **3,000 devices** in **under 5 minutes** each with ability to wipe the device if lost  
*Chemical company*

Helping prevent user access to fraudulent websites for **thousands** of mobile customers  
*Large European bank*

## Strategic Imperative #3

*Get help to develop an integrated approach*

**INTEGRATION**

*Develop an  
integrated  
approach to  
stay ahead  
of the threat*



**Develop a  
risk-aware  
security strategy**

**Deploy a  
systematic  
approach**

**Harness the  
knowledge  
of professionals**



# Develop a Risk-aware Security Strategy



 **Security Maturity**

**49%** of IT executives have no measure of the effectiveness of their security efforts

**31%** of IT professionals have no risk strategy

**Board of Directors**

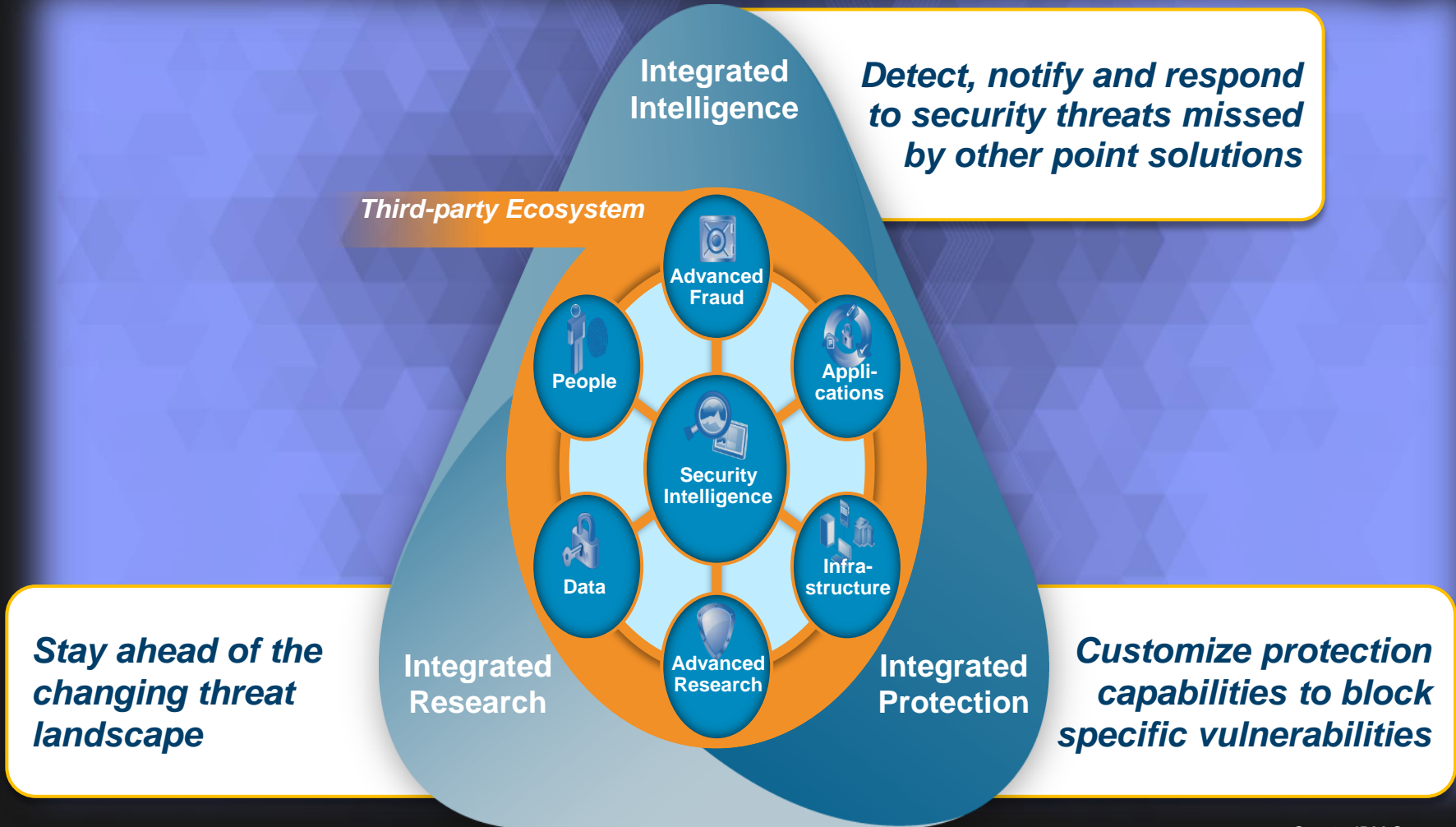
**Stakeholders**

**Compliance Mandates**

**Industry Standards**



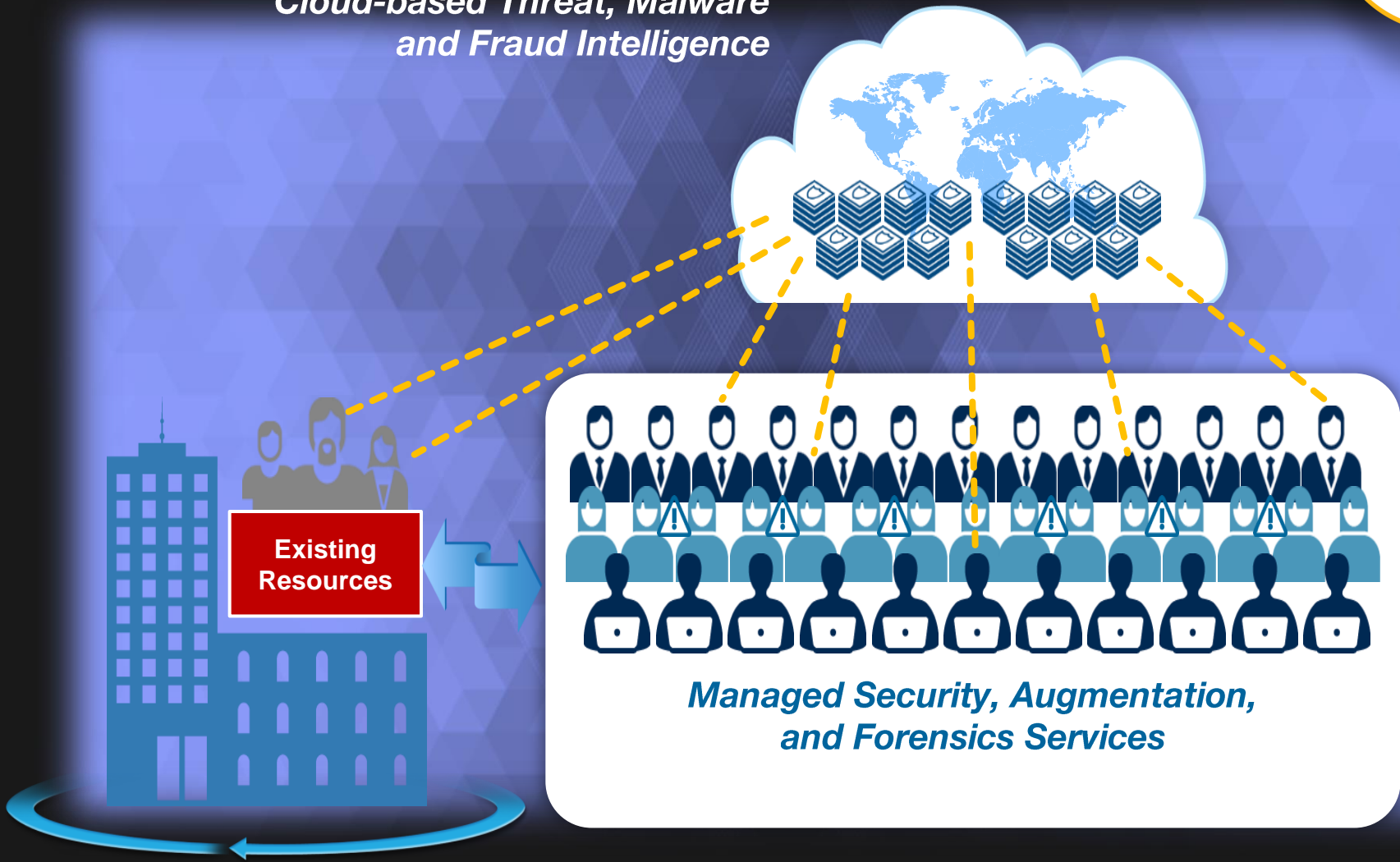
# Deploy a Systematic Approach with Integrated Capabilities



# Harness the Knowledge of Professionals

**INTEGRATION**  
*Develop an integrated approach to stay ahead of the threat*

**Cloud-based Threat, Malware and Fraud Intelligence**



# IBM Provides Unmatched Global Coverage and Security Awareness

**INTEGRATION**

*Develop an  
integrated  
approach to  
stay ahead  
of the threat*

**6,000+**

security specialists

**10**

security operations centers

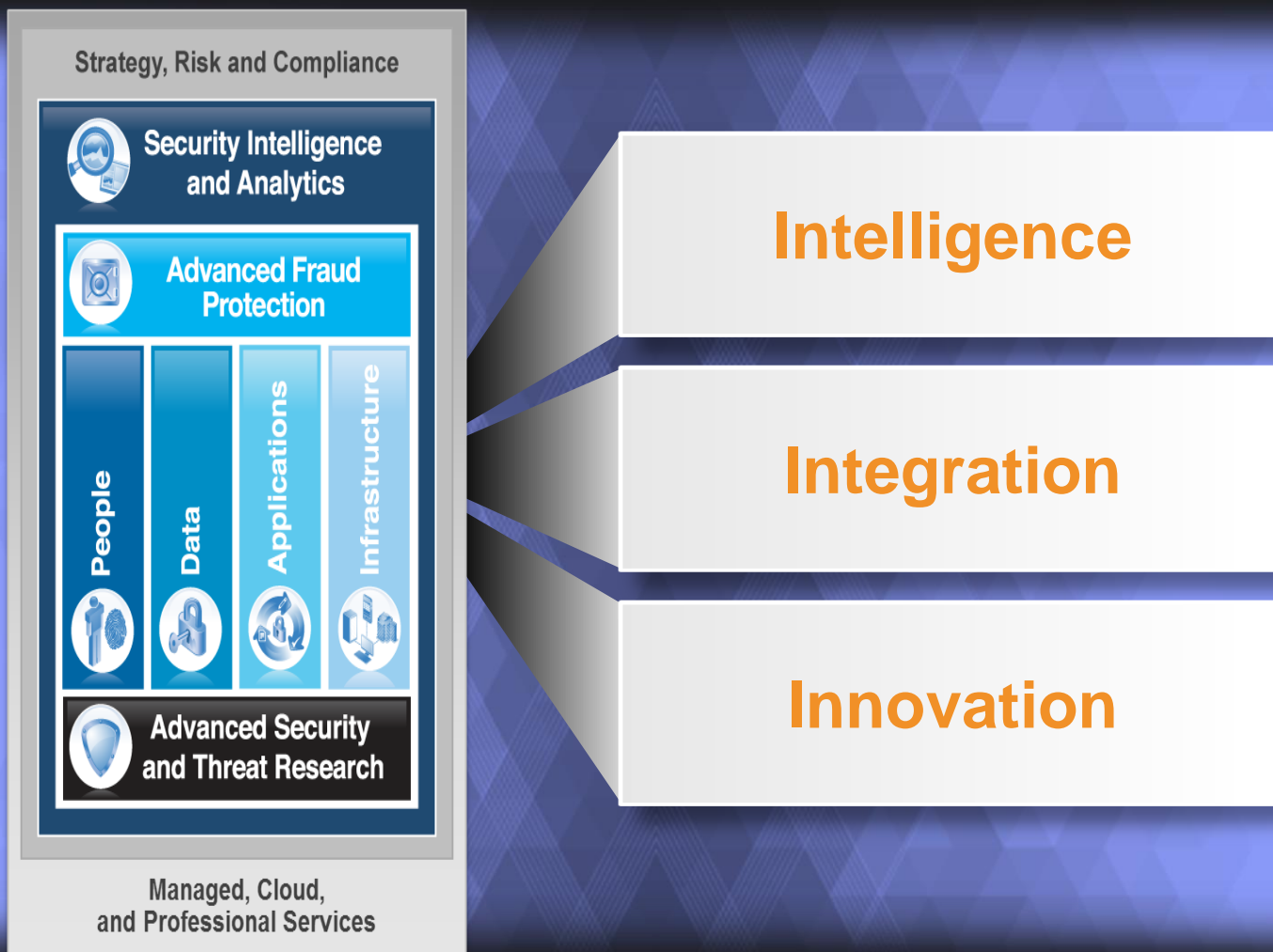
**133**

monitored countries

**18B**

events per day

# IBM Security Framework



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.

# Thank You

[www.ibm.com/security](http://www.ibm.com/security)

© Copyright IBM Corporation 2014. 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.

