– VIDEO –

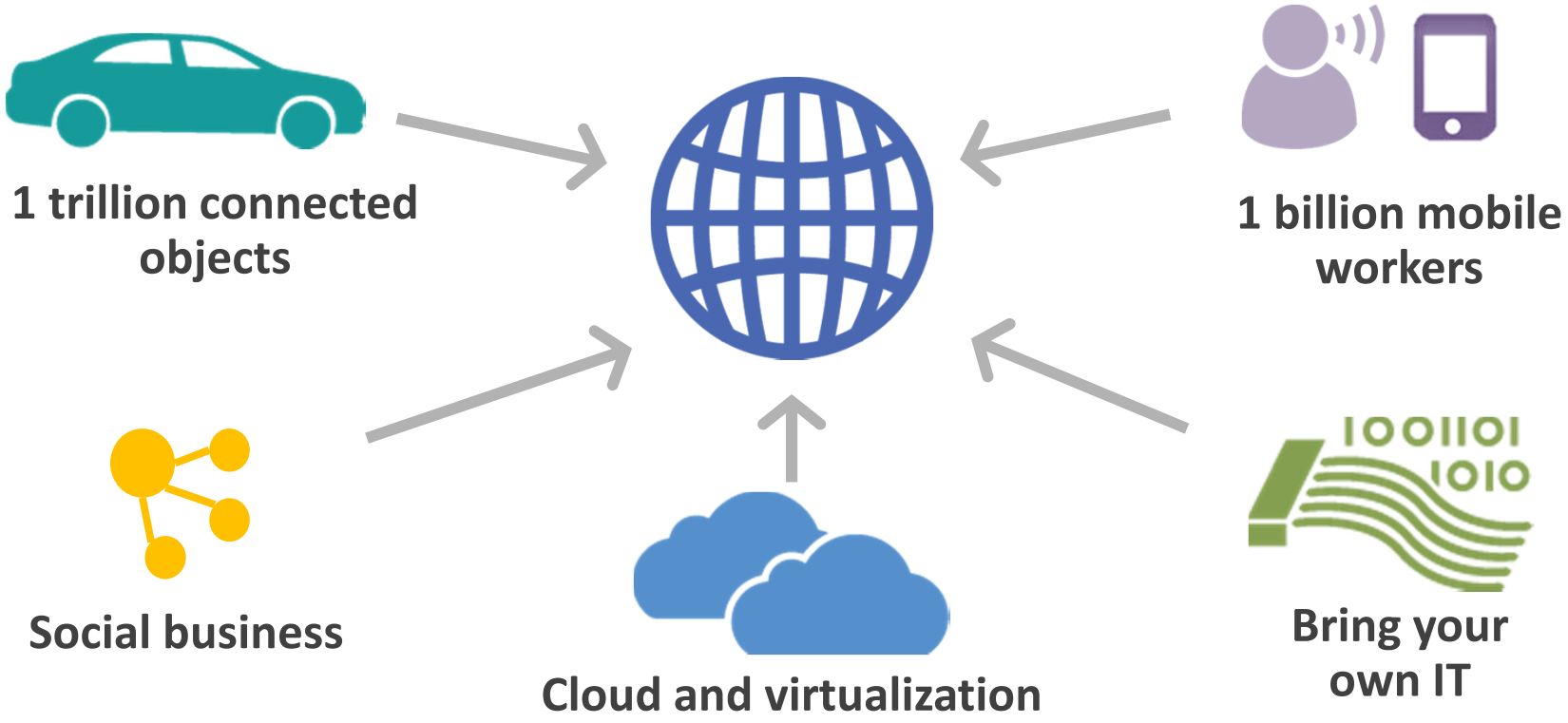
Security Intelligence Integration Expertise

IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

Security Intelligence

Erno Doorenspleet

Innovative technology changes everything



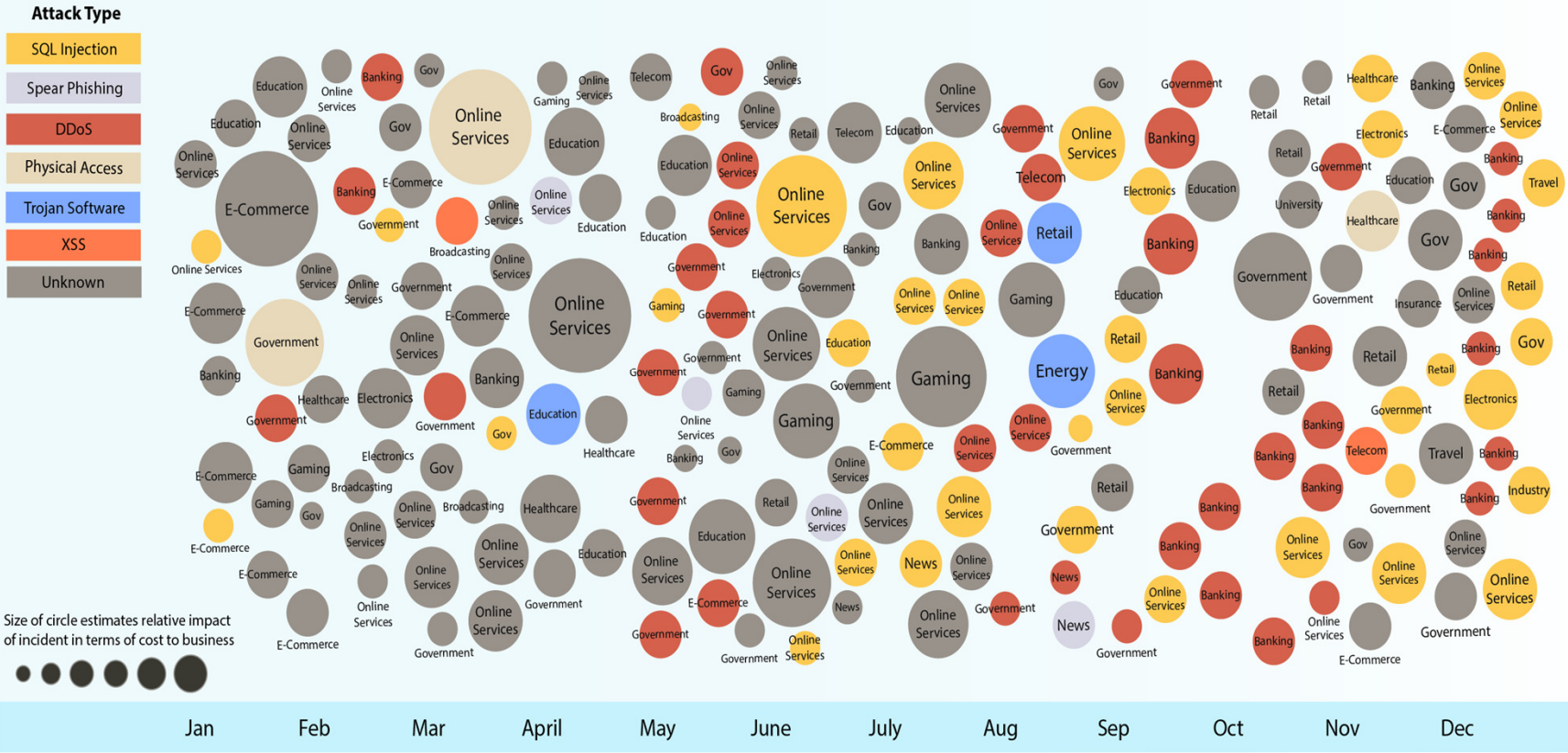
Motivation and sophistication is evolving rapidly

Motive	1995 – 2005 1st Decade of the Commercial Internet	2005 – 2015 2nd Decade of the Commercial Internet
National Security, Infrastructure Attack		State actors
Espionage, Political Activism		Competitors, hacktivists
Monetary Gain		Organized crime
Revenge	Insiders	
Curiosity	Script-kiddies or hackers	

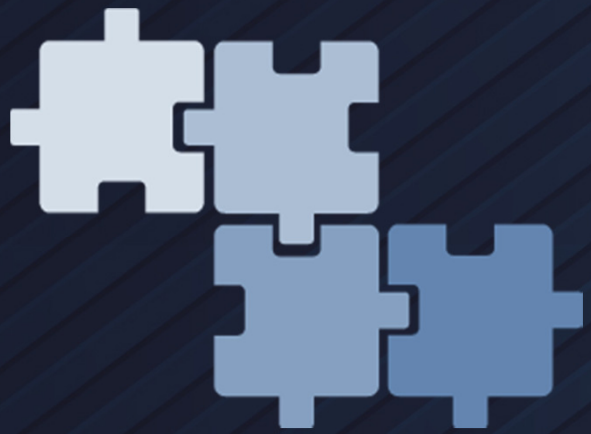
Nobody is immune

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

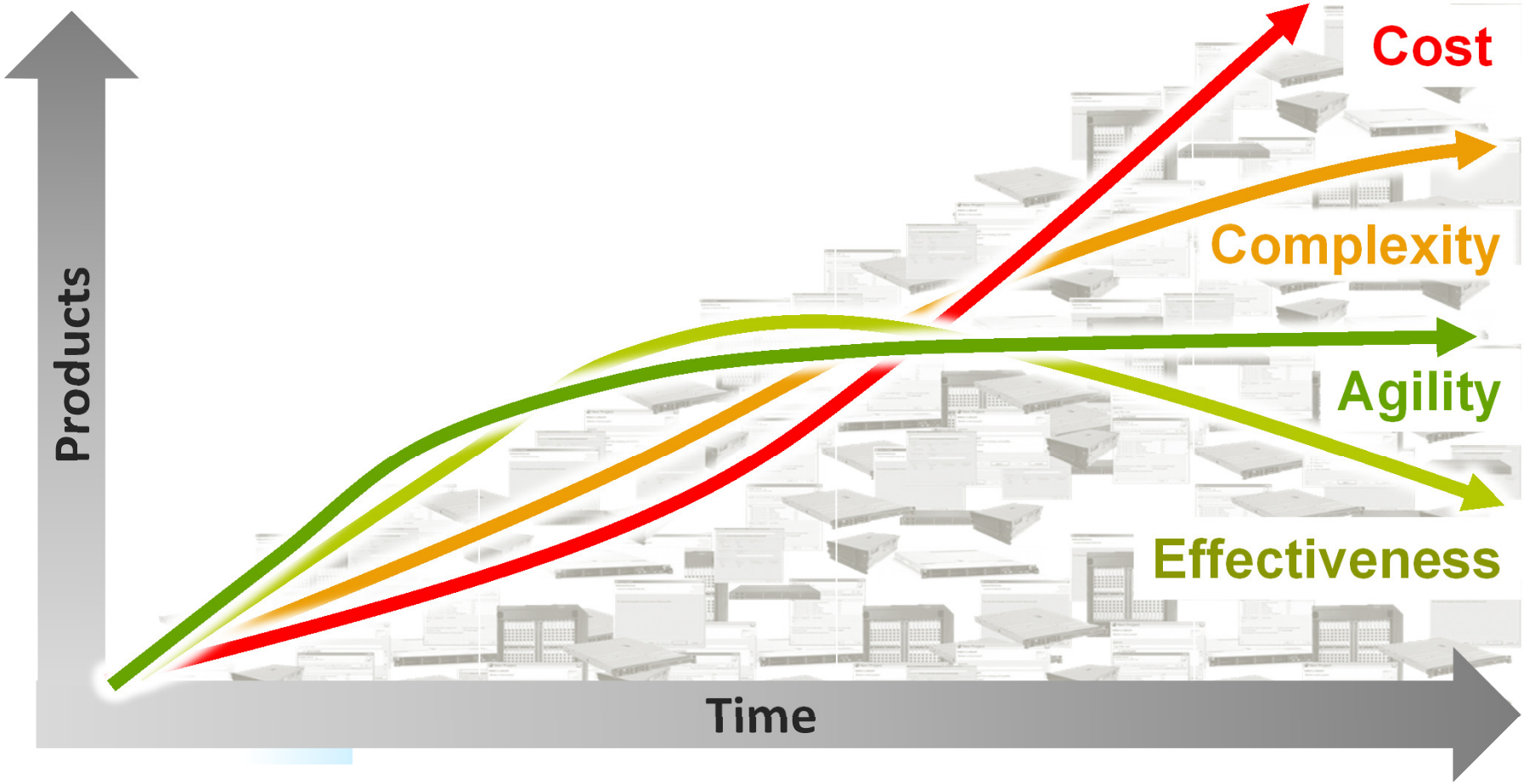


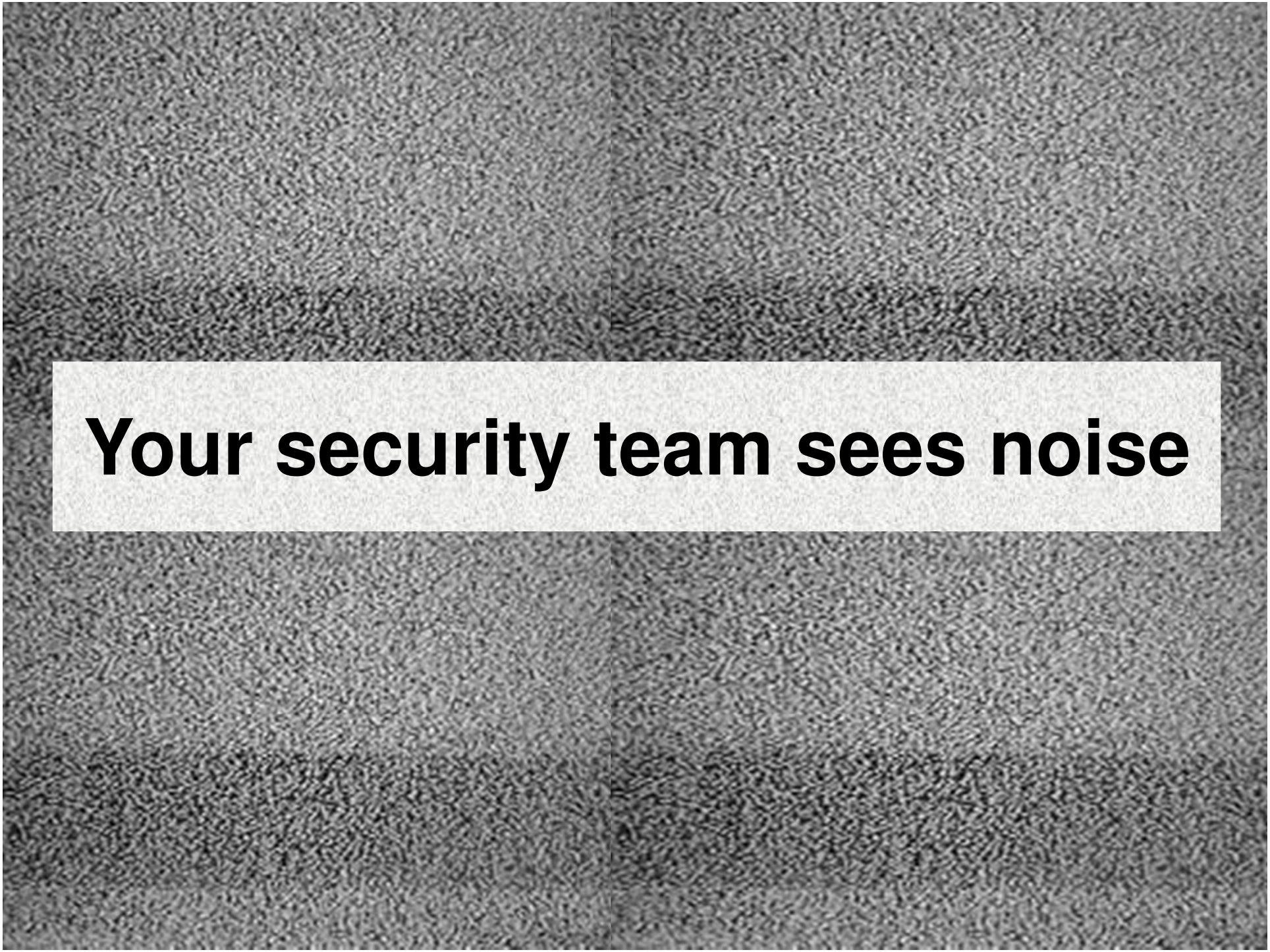
IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.



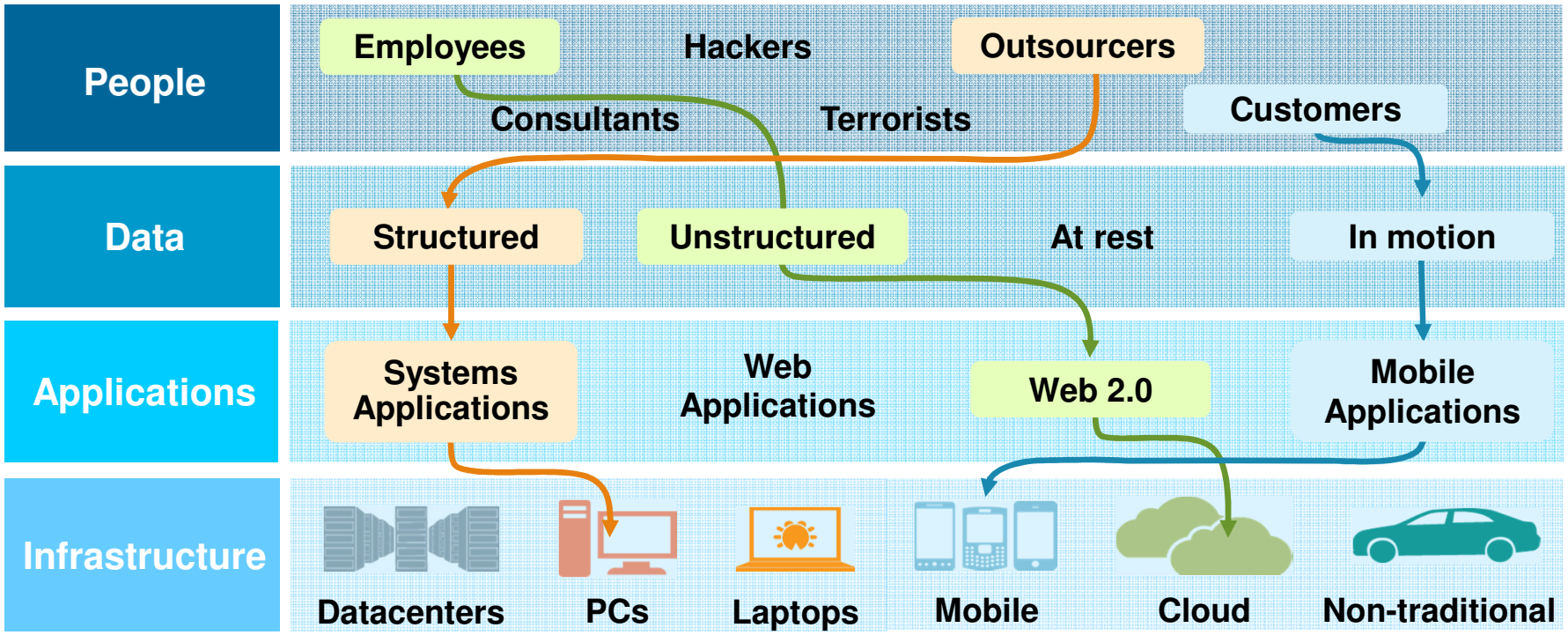
How do we solve this?

Products
Time


Products
Time
Cost
Complexity
Agility
Effectiveness


Your security team sees noise

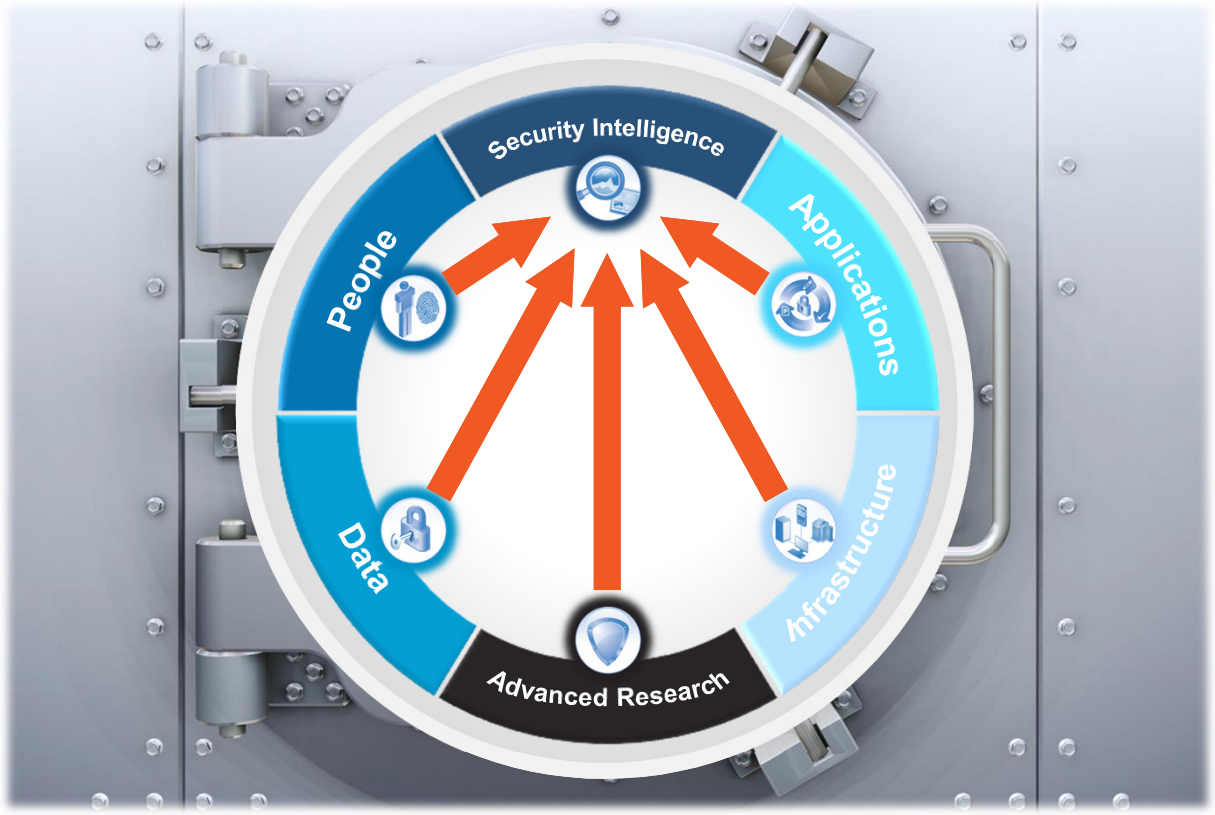
Security challenges are a complex,
four-dimensional puzzle …



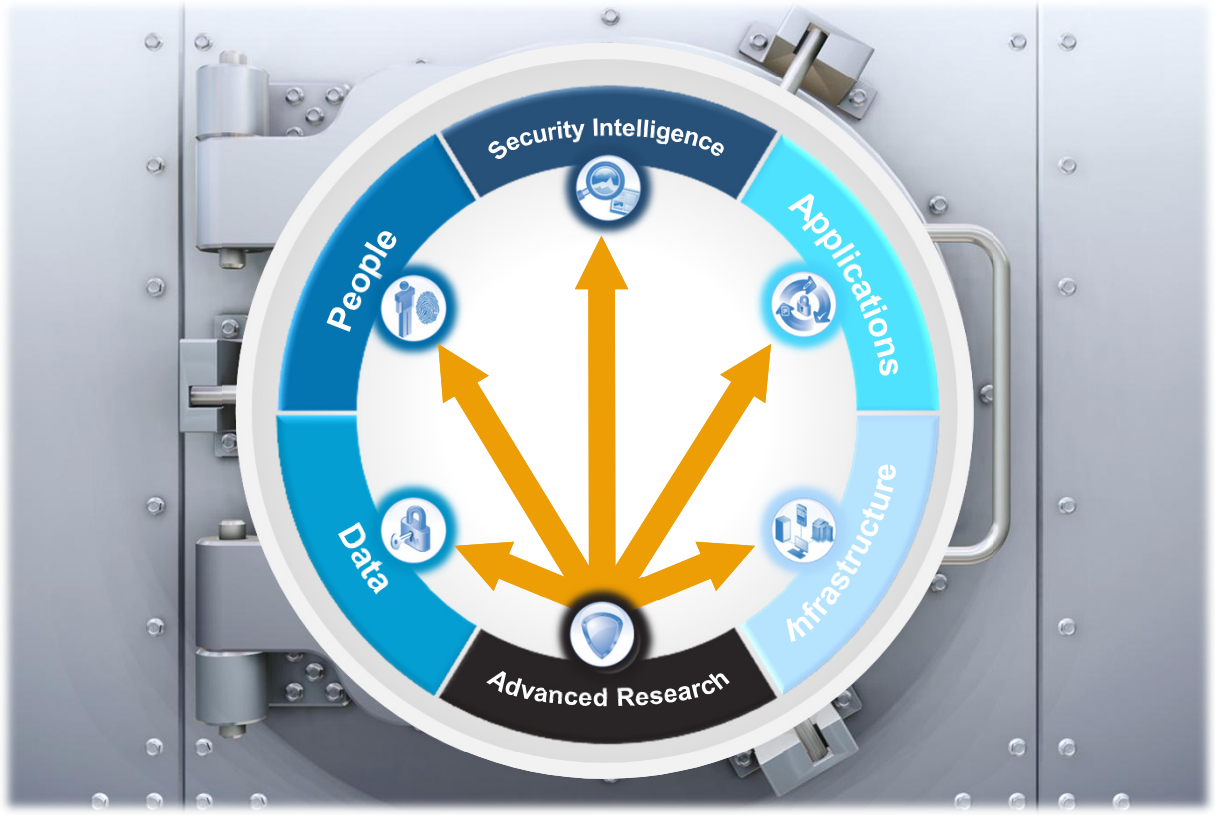
… that requires a new approach

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

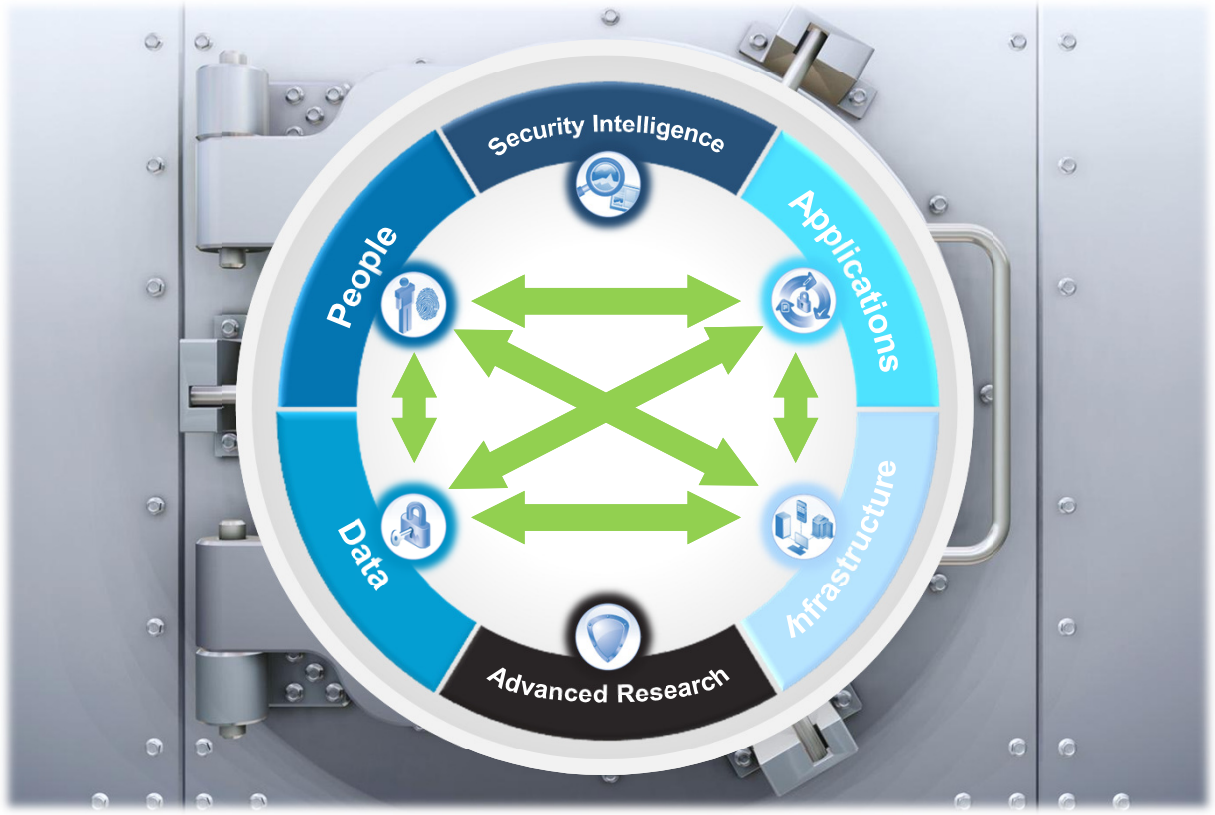
Collect and Analyze Everything



Monitor Everything



Consume Threat Intelligence



Integrate Across Domains

IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

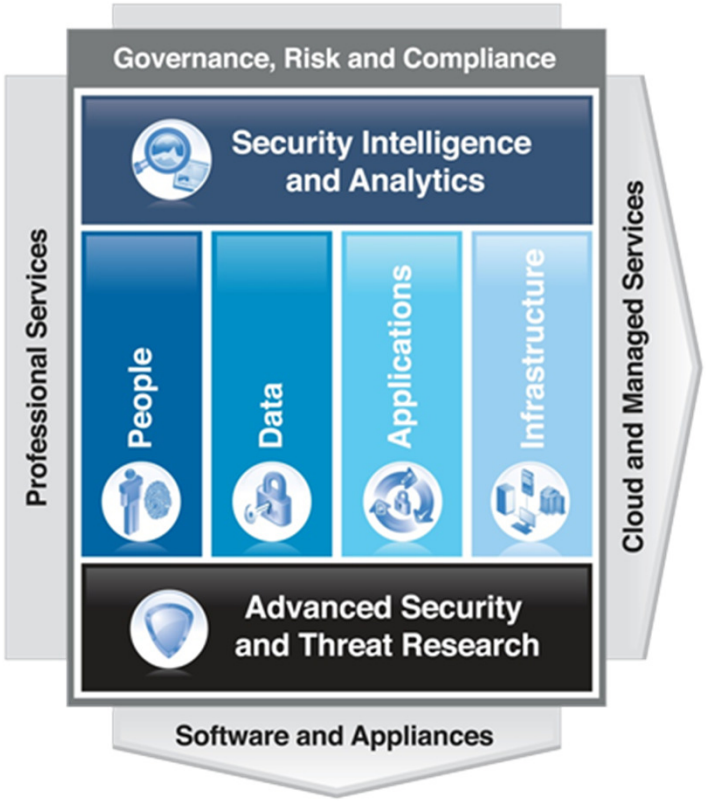
Applying these principles

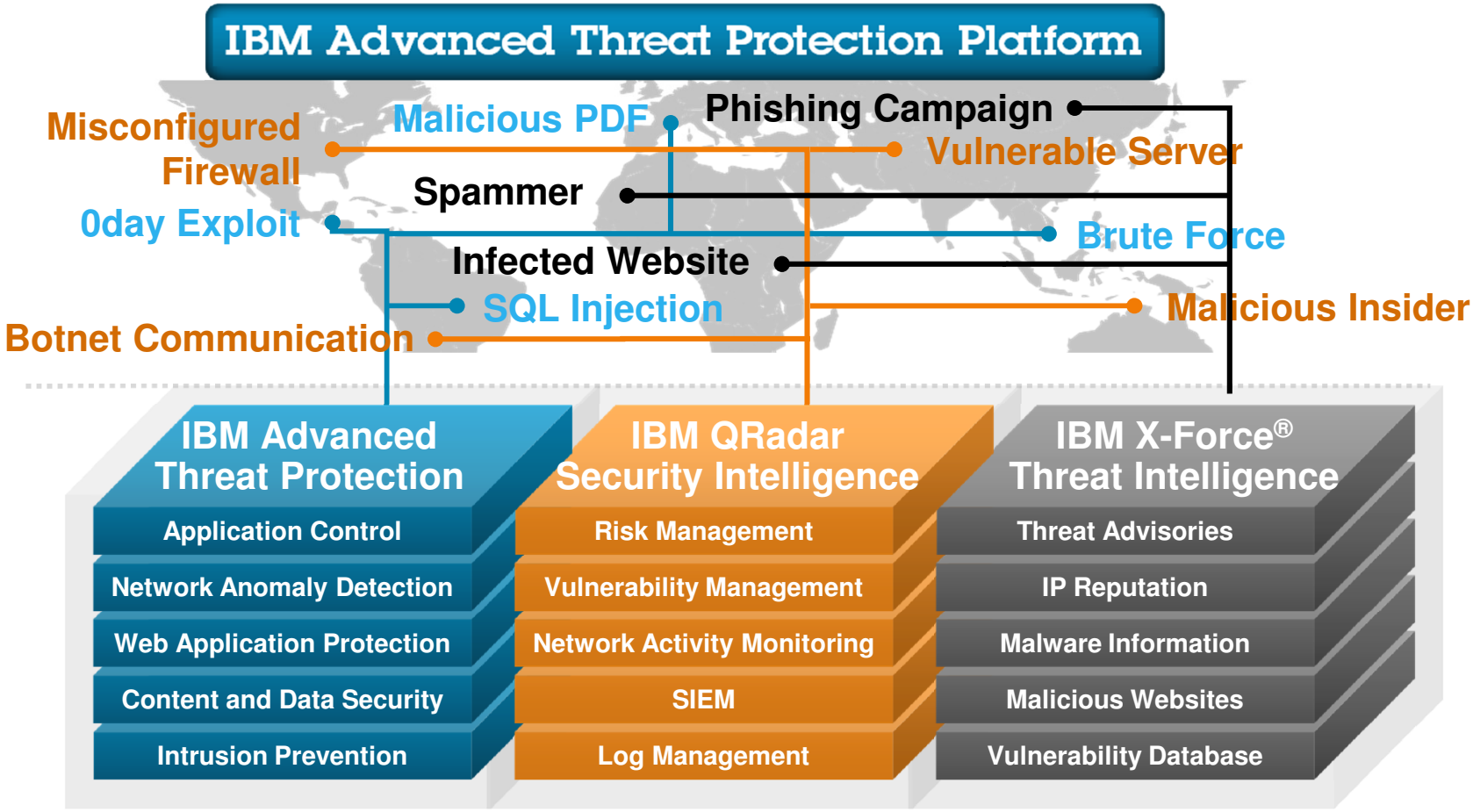
IBM delivers security solutions across a comprehensive framework

Intelligence

Integration

Expertise




IBM Advanced Threat Protection Platform
Misconfigured Firewall
0day Exploit
Botnet Communication
Malicious PDF
Spammer
Infected Website
SQL Injection
Phishing Campaign
Vulnerable Server
Brute Force
Malicious Insider
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 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

In 2013 we will continue to focus on solving the big problems

Advanced Threats

Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence

Advanced Persistent Threats
Stealth Bots Targeted Attacks
Designer Malware Zero-days

Customers

Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed

IBM SmartCloud
Salesforce
vmware

Mobile Computing

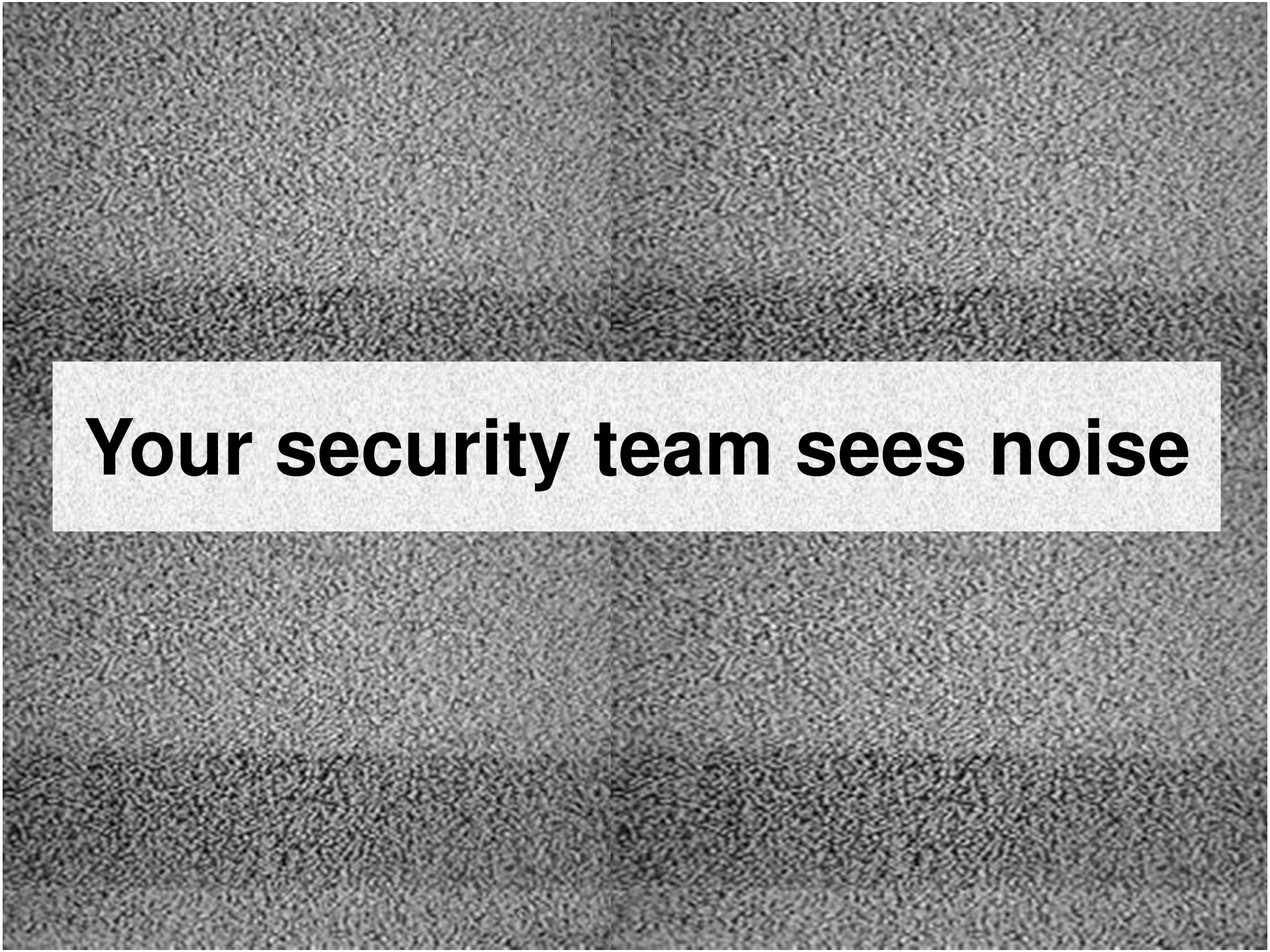
Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility

Windows Phone

Regulation and Compliance

Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures

PCI Security Standards Council
GLBA
FFIEC
Sarbanes-Oxley
Financial and Accounting Disclosure Information

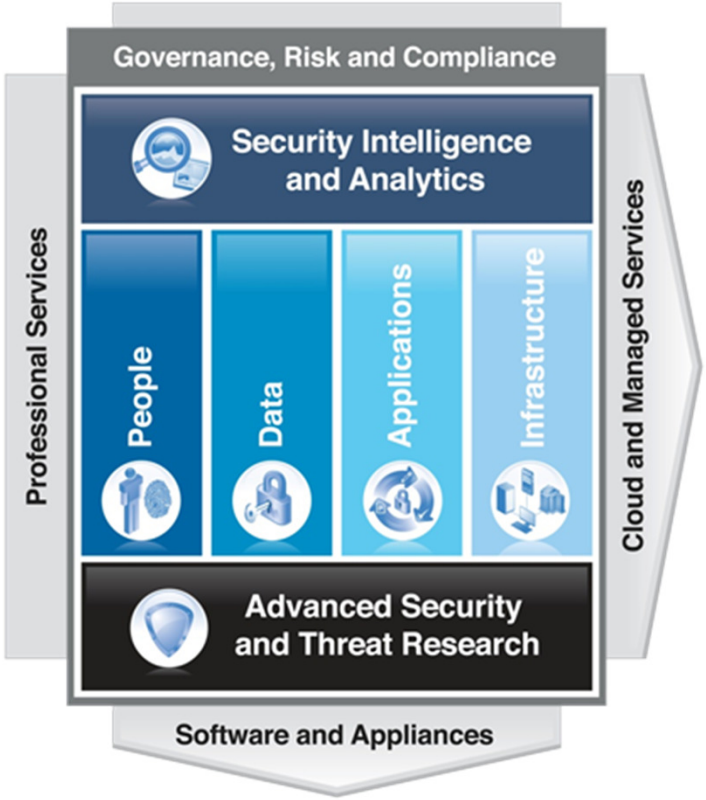

Your security team sees noise

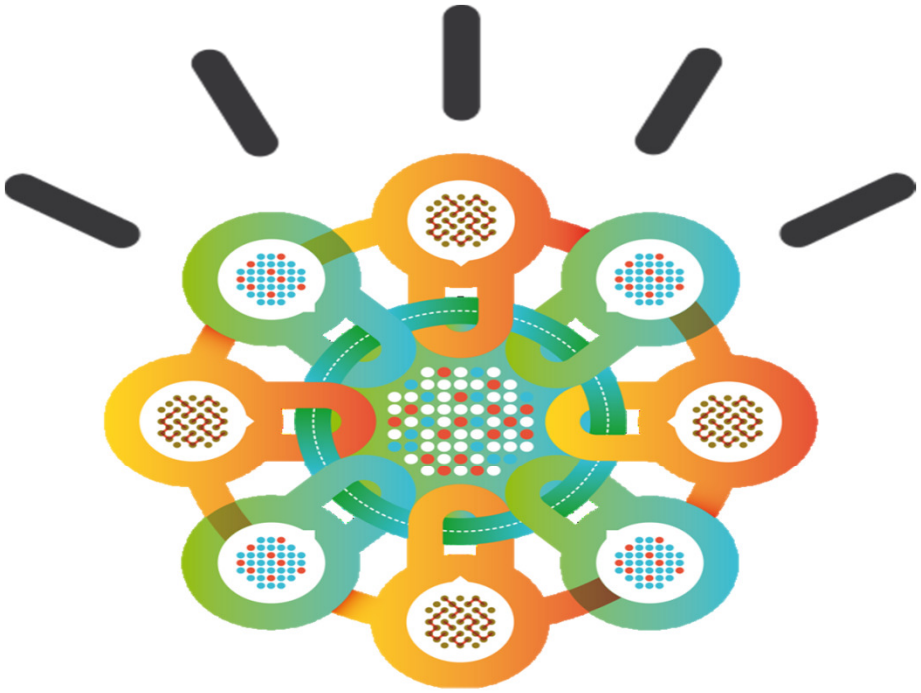
IBM Security Framework

Intelligence

Integration

Expertise





Security Intelligence

ibm.com/security

smartersecurity.nl