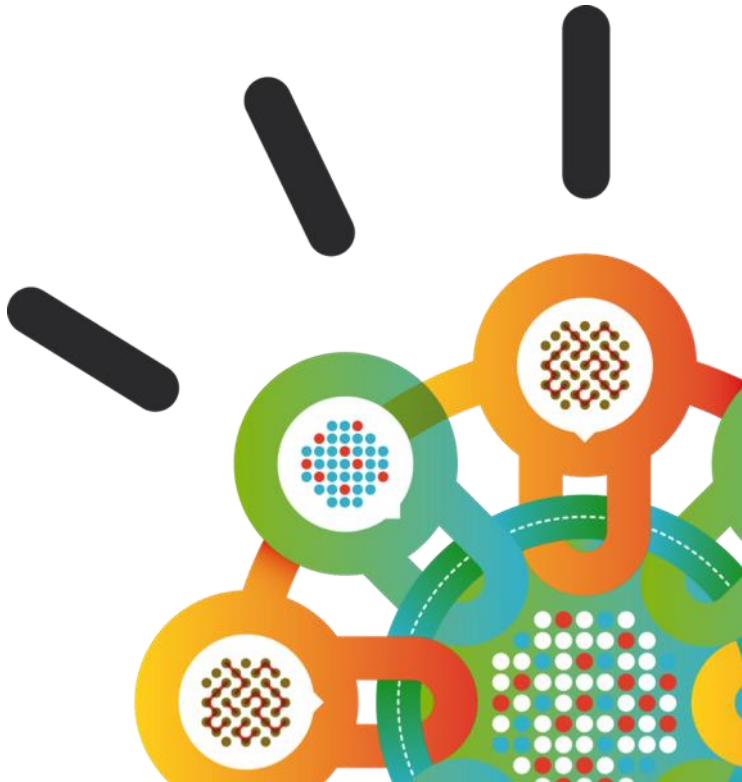
Security Intelligence.
Think Integrated.

Security Intelligence
with IBM Security QRadar solutions

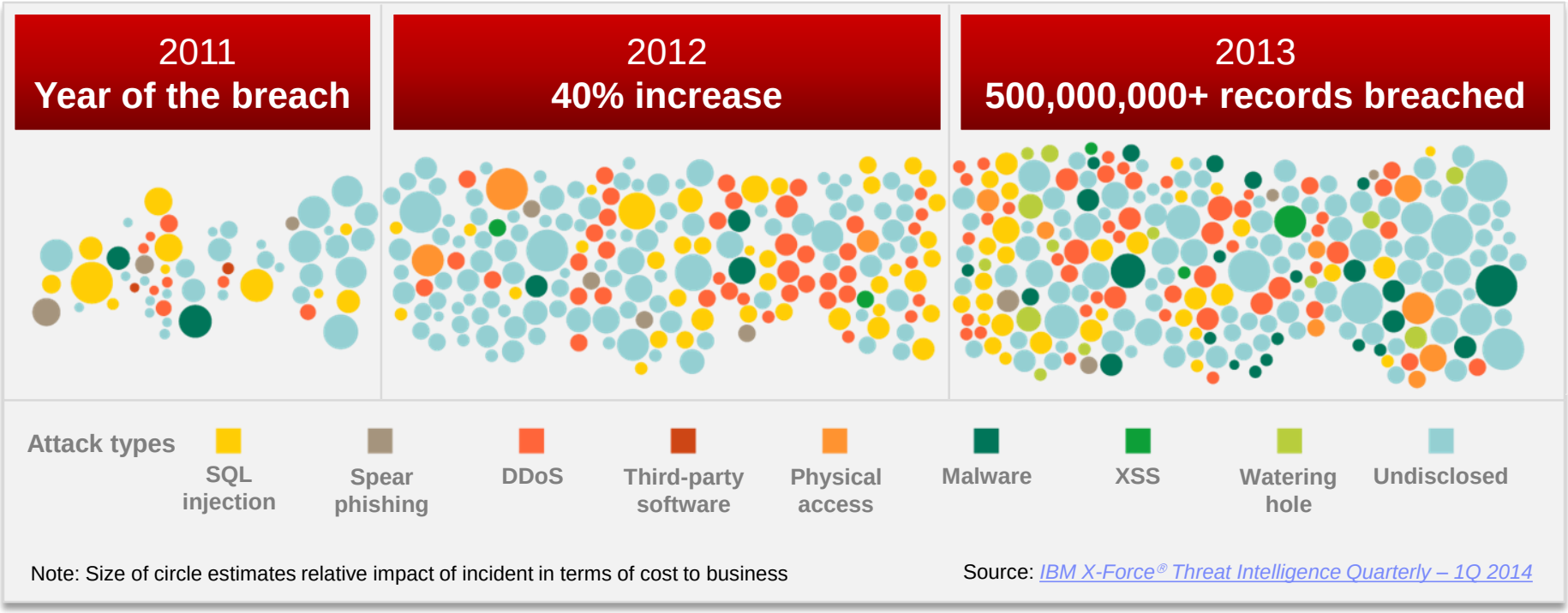


Stanimir Sotirov, Service Centrix Ltd.
stanimir.sotirov@servicecentrix.com
November 2015

Agenda

- **Introduction to Security Intelligence**
  - Customer needs
- **QRadar Security Intelligence Platform**
  - SIEM, Log Manager, Risk Manager, Vulnerability Manager, Incident Forensics and Network/Application Visibility (QFlow/VFlow)

Sophisticated attackers break through safeguards every day



Note: Size of circle estimates relative impact of incident in terms of cost to business

Source: *IBM X-Force® Threat Intelligence Quarterly – 1Q 2014*

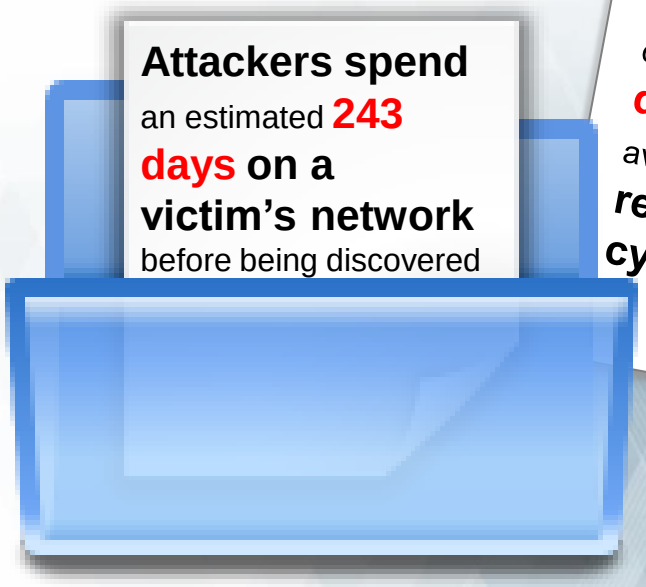
61% of organizations say **data theft and cybercrime** are their greatest threats

2012 IBM Global Reputational Risk & IT Study

$3.5M+ average cost of a **data breach**

2014 Cost of Data Breach, Ponemon Institute

Harsh realities for many enterprise network CISOs



Attackers spend an estimated **243 days on a victim's network** before being discovered

In 2013, it took organizations **32 days** on average **to resolve a cyber-attack**

In 2012, **38%** of targets were **attacked again** once the original incident was remediated.

Annual cost of cyber-crime in the U.S. now stands at **$11.56 million per organization**

63% of victims **made aware** of their breaches **by an external organization**

Has our organization been compromised?

When was our security breached?

How do we identify the attack?

What type of attack is it?

What resources and assets are at risk?

How to avoid becoming a repeat victim?

What is Security Intelligence?

Security Intelligence

Actionable information
derived from the analysis of all security-related data
available to an organization.

Today's challenges

Escalating Attacks

- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity

- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate and ineffective tools

Resource Constraints

- Struggling security teams
- Too much data with limited manpower and skills to manage it all
- Managing and monitoring increasing compliance demands

The security team sees noise

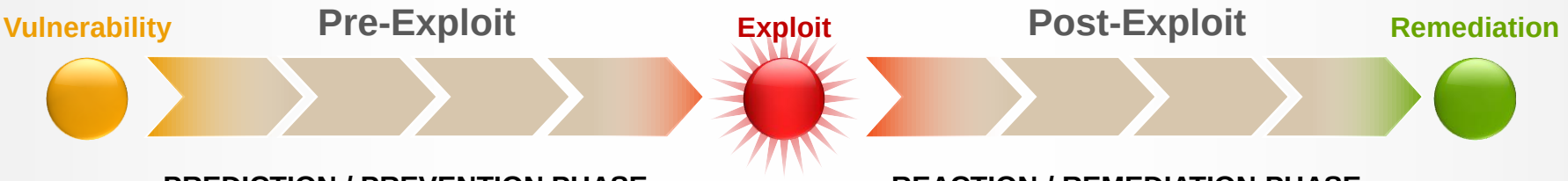
Ask the right questions

What are the major risks and vulnerabilities?

Are we configured to protect against advanced threats?

What security incidents are happening right now?

What was the impact to the organization?



PREDICTION / PREVENTION PHASE

- Gain visibility over the organization's security posture and identity security gaps
- Detect deviations from the norm that indicate early warnings of APTs
- Prioritize vulnerabilities to optimize remediation processes and close critical exposures before exploit

REACTION / REMEDIATION PHASE

- Automatically detect threats with prioritized workflow to quickly analyze impact
- Gather full situational awareness through advanced security analytics
- Perform forensic investigation reducing time to find root-cause; use results to drive faster remediation

Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

IBM QRadar Security Intelligence Platform

Providing actionable intelligence

INTELLIGENT

Correlation, analysis and massive data reduction

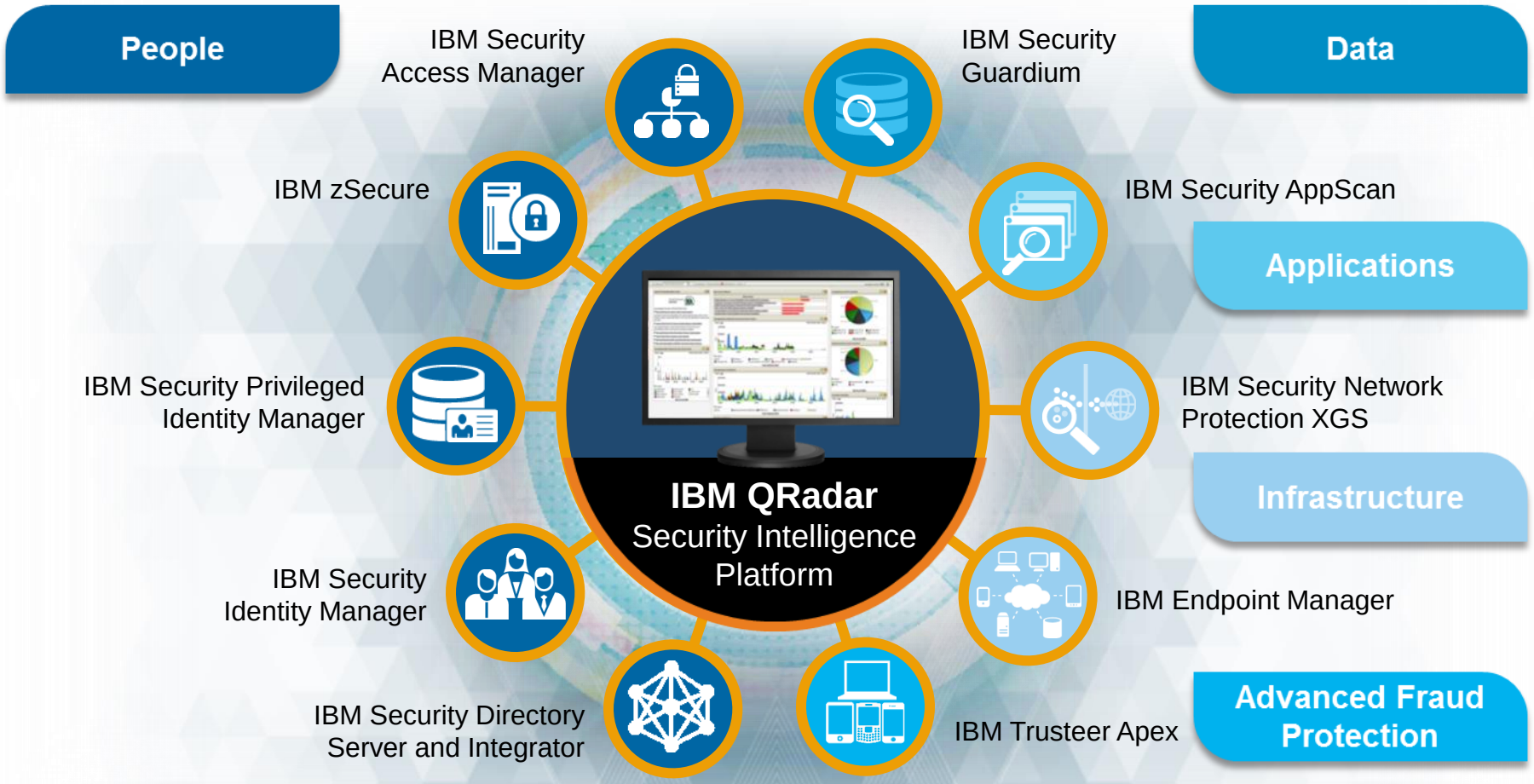
AUTOMATED

Driving simplicity and accelerating time-to-value

INTEGRATED

Unified architecture delivered in a single console

IBM QRadar is the centerpiece of IBM security integration



Embedded intelligence offers automated offense identification

INTELLIGENT

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

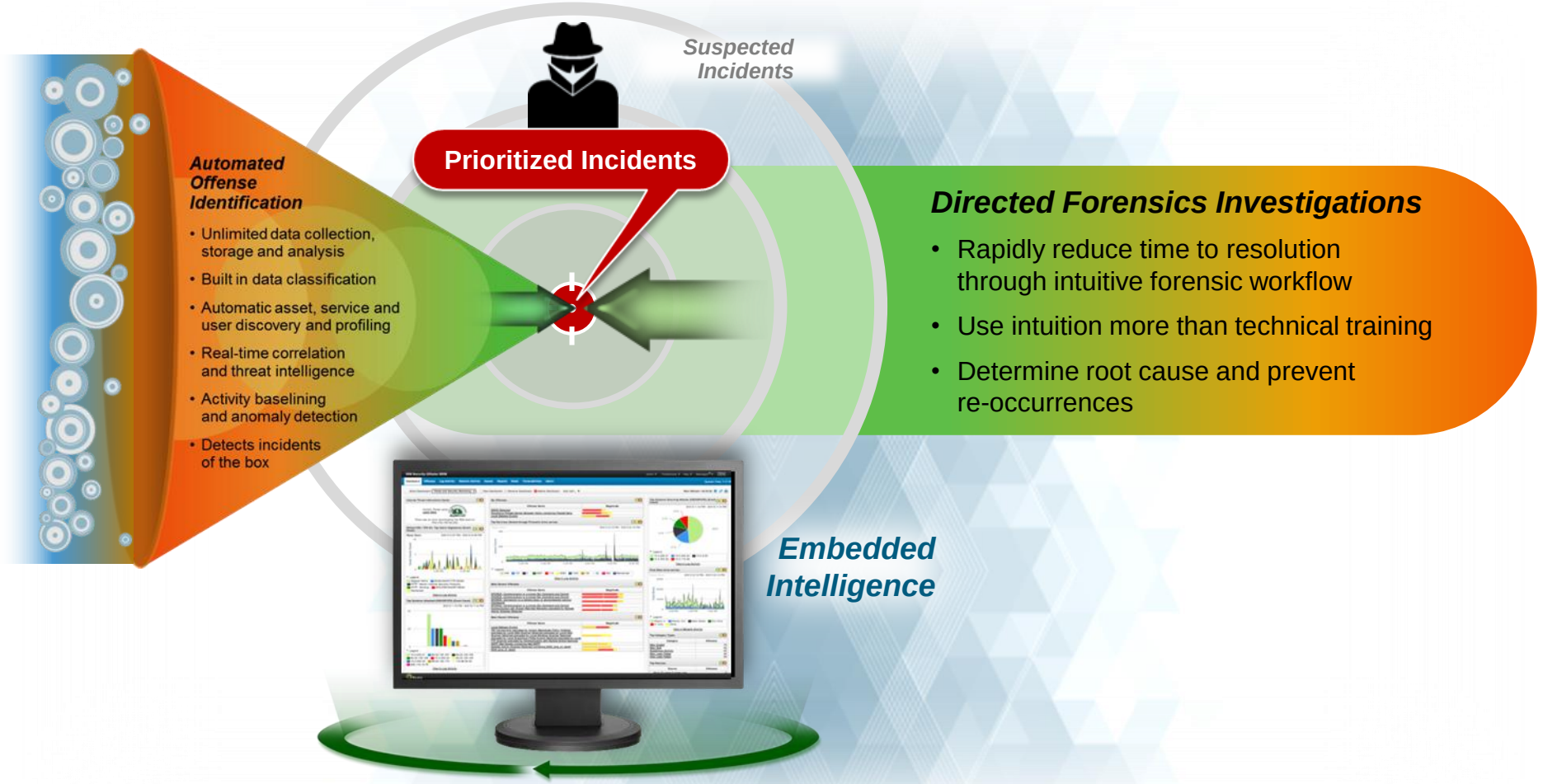
Embedded Intelligence

Suspected Incidents

Prioritized Incidents

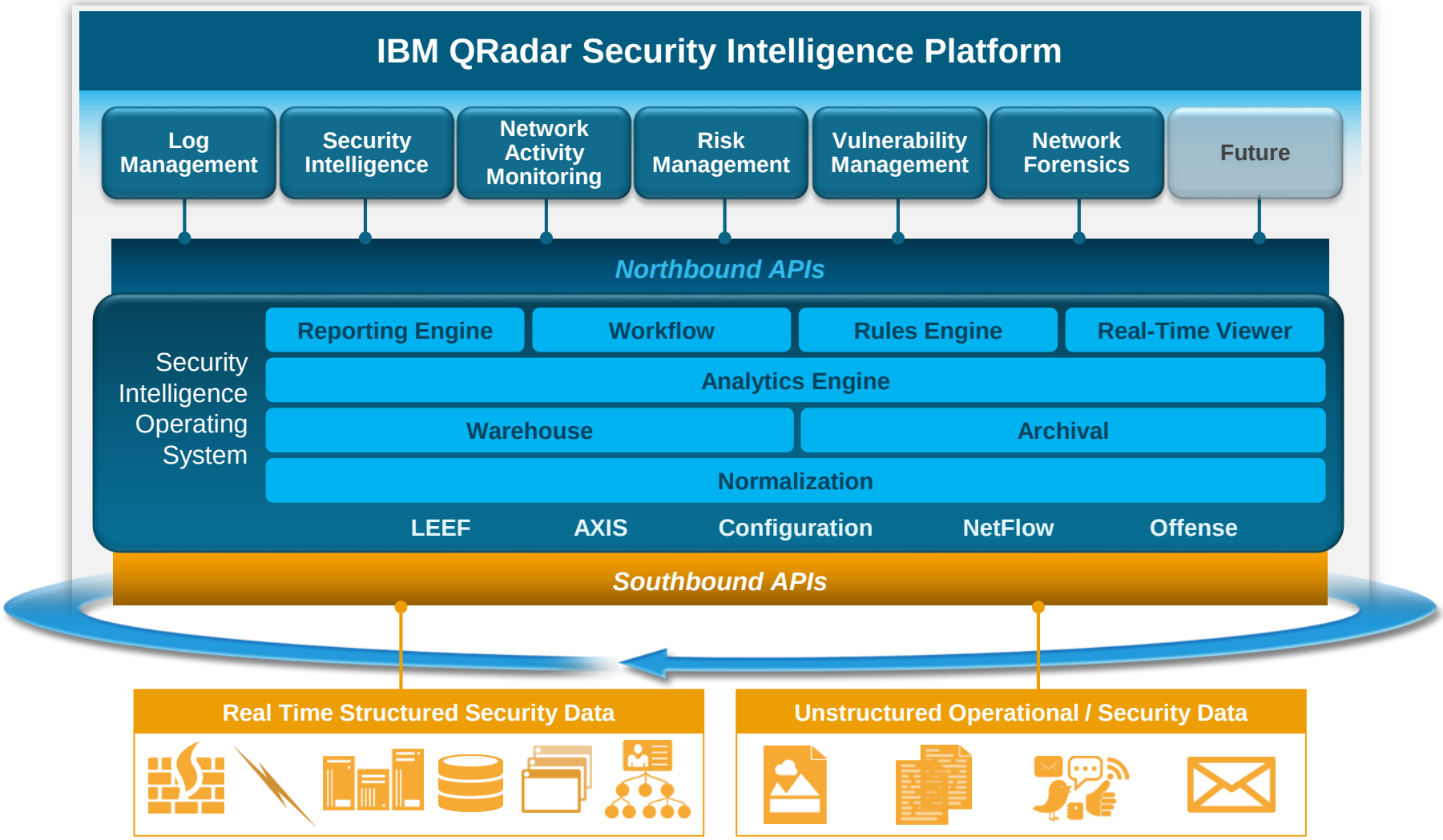
Extend clarity around incidents with in-depth forensics data

INTELLIGENT

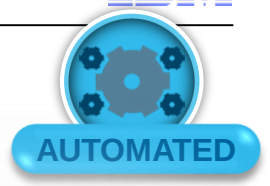


Delivering multiple security capabilities through a purpose-built, extensible platform

AUTOMATED



Driving simplicity and accelerated time to value



Simplified deployment

Automated configuration of log data sources and asset databases

Immediate discovery of network assets

Proactive vulnerability scans, configuration comparisons, and policy compliance checks

Out-of-the-box rules and reports

Immediate time to value with built-in intelligence

Automated updates

Stay current with latest threats, vulnerabilities, and protocols

IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute, LLC
Independent Research Report

QRadar's ease-of-use in set-up and maintenance resulted in reduced time to resolve network issues and freed-up IT staff for other projects.

Private U.S. University
with large online education community

An integrated, unified architecture in a single web-based console

INTEGRATED

- Log Management
- Security Intelligence
- Network Activity Monitoring
- Risk Management
- Vulnerability Management
- Network Forensics

Answering questions to help prevent and remediate attacks

INTEGRATED

What was the attack?

Is the attack credible?

Offense 909

Summary | Display ▼ | Events | Connections | Flows | View Attack Path | Actions ▼ | Print

Magnitude		Status		Relevance	8	Severity	5	Credibility	4
Description	Potential Data Loss	Offense Type	Source IP				
		Event/Flow count	111 events and 1,042 flows in 13 categories				
Source IP(s)	10.0.110.221 (dhcp-221-users-2.acme.com)	Start	Oct 18, 2013 12:28:02 PM				
Destination IP(s)	Local (2) Remote (376)	Duration	4d 10h 42m 57s				
Network(s)	Multiple (3)	Assigned to	admin				

How valuable are the targets to the business?

Offense Source Summary

IP	10.0.110.221	Location	Users.Users-2
Magnitude		Vulnerabilities	0
Username	compliance	MAC Address	00:0E:0C:B4:D8:EE
Host Name	dhcp-221-users-2.acme.com		
Asset Name	dhcp-221-users-2.acme.com	Weight	0
Offenses	8	Events/Flows	15,310

Who was responsible for the attack?

Where are they located?

Last 5 Notes

Notes | Add Note

Notes	Username	Creation Date
Potential data loss detected, forensics case created	admin	Oct 21, 2013 6:39 AM

What was stolen and where is the evidence?

Forensics Reconstructions

Case	Collection	IP	Start	End	Status
DataLoss	DataLoss	10.0.110.221	3/27/2014 3:31:00 PM	3/27/2014 4:31:00 PM	SUCCESS

Top 5 Source IPs

Sources

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
dhc...		Users.Users-2	No	compliance	00:0E:0C:B4:D8:EE	0	8	21	0s	15,310

Are any of the assets vulnerable?

How many targeted assets are involved

QRadar Product Portfolio

Area of Focus

Security Intelligence platform that enables security optimization through advanced threat detection, meet compliance and policy demands and eliminating data silos

Portfolio Overview

QRadar Log Manager
- Turnkey log management for SMB and Enterprises
- Upgradeable to enterprise SIEM

QRadar SIEM
- Integrated log, flow, threat, compliance mgmt
- Asset profiling and flow analytics
- Offense management and workflow

Network Activity Collectors (QFlow)
- Network analytics, behavior and anomaly detection
- Layer 7 application monitoring

QRadar Risk Manager
- Predictive threat modeling & simulation
- Scalable configuration monitoring and audit
- Advanced threat and impact analysis

QRadar Vulnerability Manager
- Integrated Network Scanning & Workflow
- Leverage SIEM, Threat, Risk to prioritize vulnerabilities

QRadar Incident Forensics
- Reconstruct raw network packets to original format
- Determine root cause of security incidents and help prevent recurrences

Fully integrated architecture and interface

Log Management

SIEM

Risk & Vulnerability Management

Network and Application Visibility

One Console Security

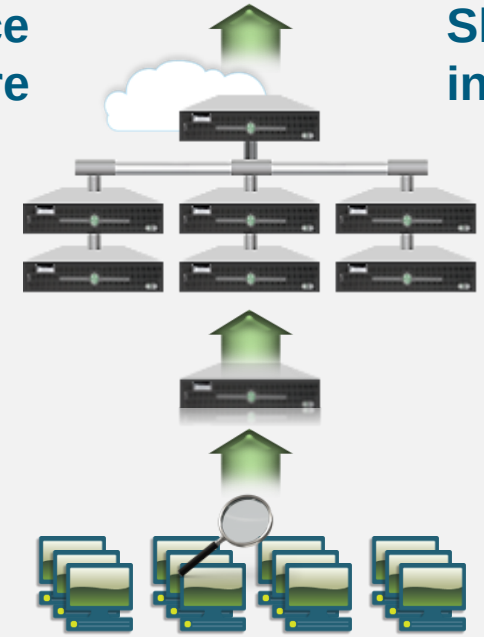
Built on a Single Data Architecture

Optimized appliance and software architecture for high performance and rapid deployment

IBM QRadar
Security Intelligence Platform

Scalable appliance architecture

- Easy-to-deploy, scalable model using stackable distributed appliances
- Does not require third-party databases or storage



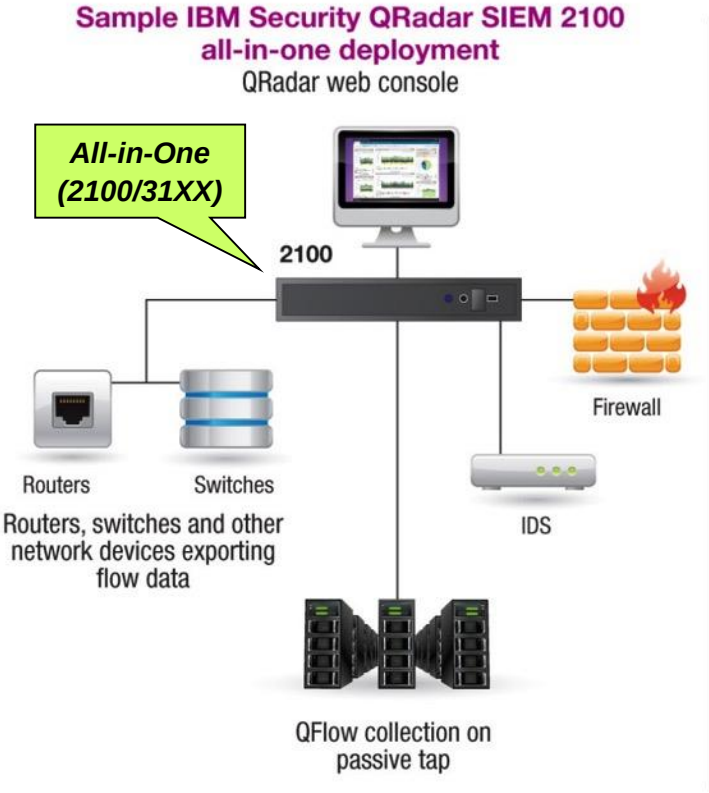
Shared modular infrastructure

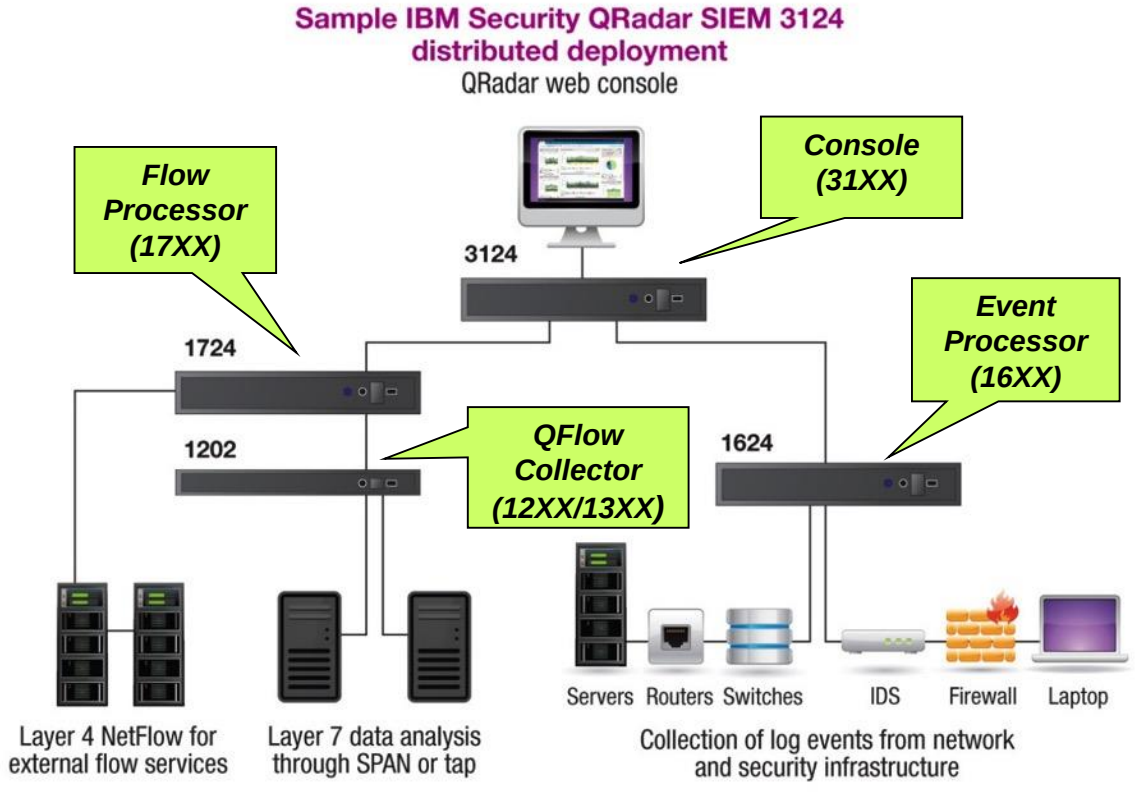
- Offers automatic failover and disaster recovery
- Virtual deployments well suited for cloud environments

Expandable and scalable QRadar platform solutions

Log Management	QRadar Log Manager 	• Turn-key log management and reporting • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM	QRadar SIEM 	• Log, flow, vulnerability & identity correlation • Sophisticated asset profiling • Offense management and workflow
Network and Application Visibility	QRadar QFlow  QRadar VFlow 	• Layer 7 application monitoring • Content capture for deep insight & forensics • Physical and virtual environments
Risk & Vulnerability Management	QRadar Risk Manager QRadar Vulnerability Manager 	• Network security configuration monitoring • Vulnerability scanning & prioritization • Predictive threat modeling & simulation
Scalability		• Event Processors for remote site • High Availability & Disaster Recovery • Data Node to increase storage & performance
Network Forensics	QRadar Incident Forensics 	• Reconstructs network sessions from PCAPs • Data pivoting and visualization tools • Accelerated clarity around who, what, when

QRadar supports two deployment models: All-in-One and Distributed





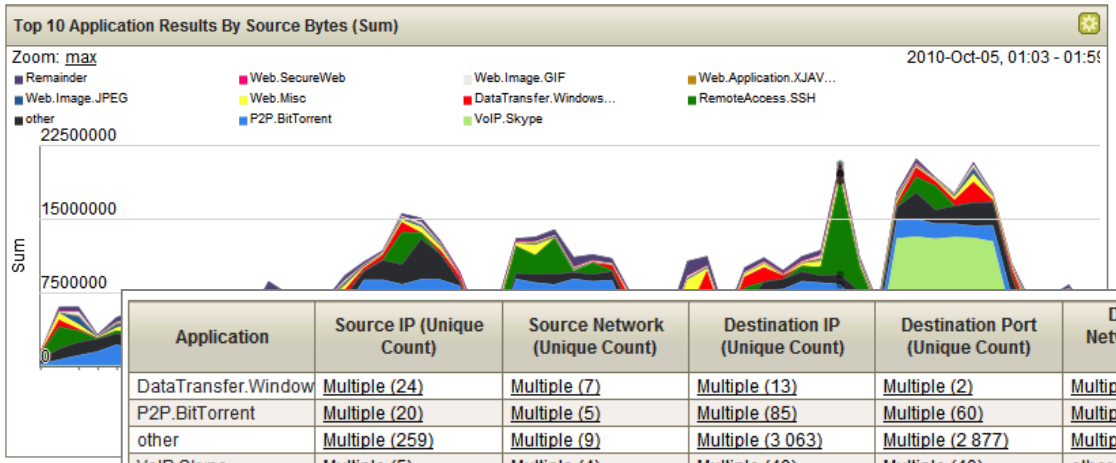
All-in-One (AIO) is a single appliance used to collect both events and flow data from various security and network devices, perform data correlation and rule matching, report alerts/threats, and provide all admin functions through a Web browser.

A distributed deployment provides unlimited scalability by using multiple appliances for different purposes:

- **Event Processors/Collectors** to collect, process and store log events
- **Flow Processors/Collectors** to collect, process and store several kinds of flow data generated from network devices.
- **Console** to correlate data from managed processors, generate alerts/reports, and provide all admin functions.

Key QRadar differentiator: network flow analytics

- **Network traffic doesn't lie.** Attackers can stop logging and erase their tracks, but can't cut off the network (flow data)
  - Deep packet inspection for Layer 7 flow data
  - Pivoting, drill-down and data mining on flow sources for advanced detection and forensics
- Helps detect anomalies that might otherwise be missed
- Enables visibility into attacker communications



Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267

"Managing security without flows is like having one eye closed"

Gartner agrees the IBM strategy is #1

- QRadar has been in Gartner's leadership quadrant since 2009
- QRadar overtook HP Arcsight for the #1 spot in 2014…by a large margin
- And still holds that margin

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