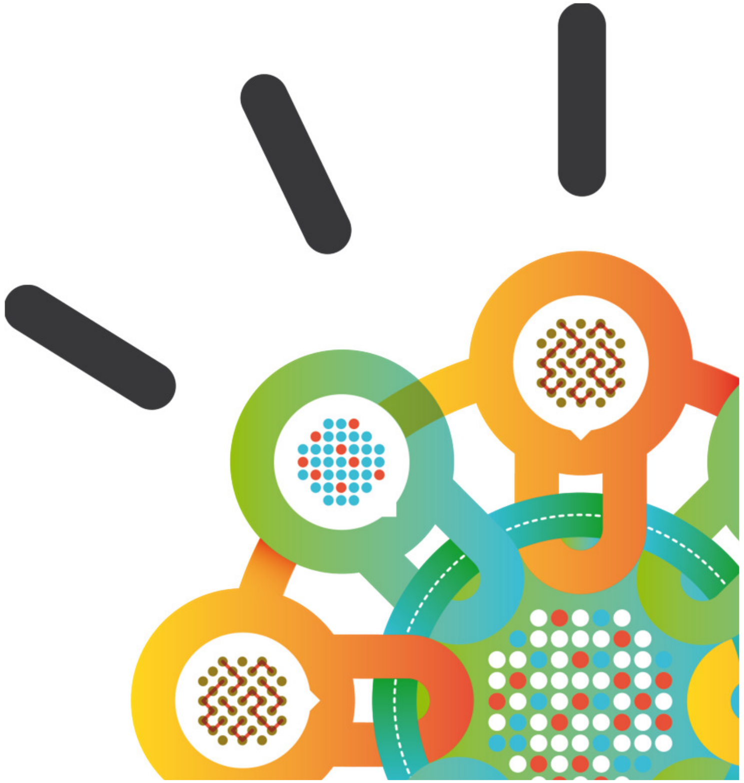
Security Intelligence.
Think Integrated.

Qradar Security Intelligence

Filip Schepers

Technical Security Architect
Security Intelligence & Forensics
fschepers@be.ibm.com

July 3, 2014



We are in an era of continuous breaches

Operational Sophistication

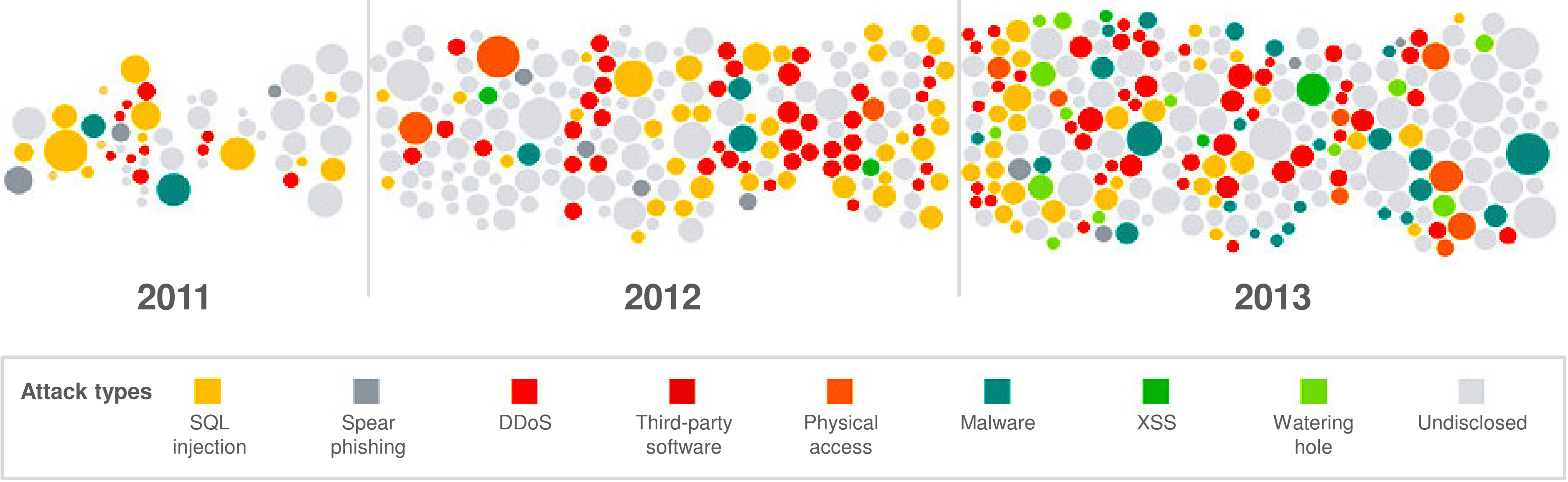
IBM X-Force® declared **Year of the Security Breach**

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records were leaked, while the future shows no sign of change

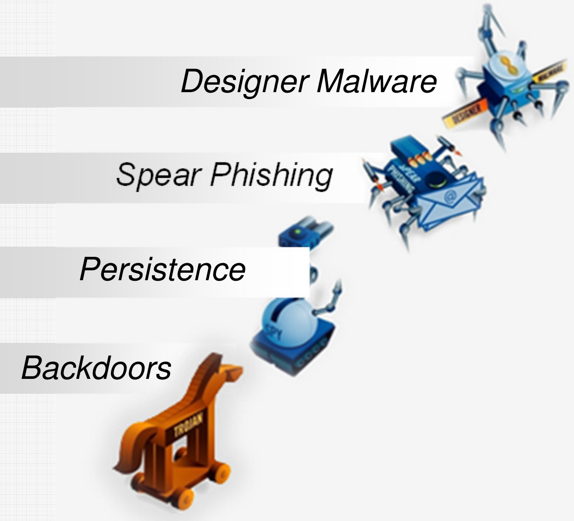


Note: Size of circle estimates relative impact of incident in terms of cost to business.

Source: IBM X-Force® Research 2013 Trend and Risk Report

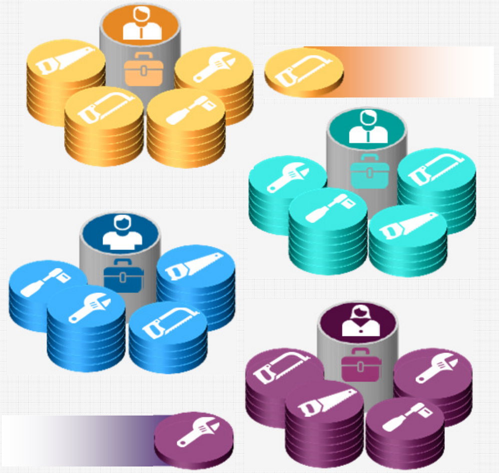
Today’s challenges

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

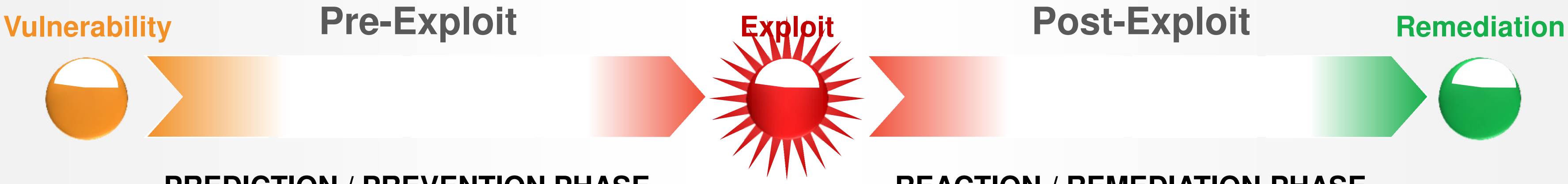
Ask the right questions

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?



Vulnerability

Pre-Exploit

Exploit

Post-Exploit

Remediation

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

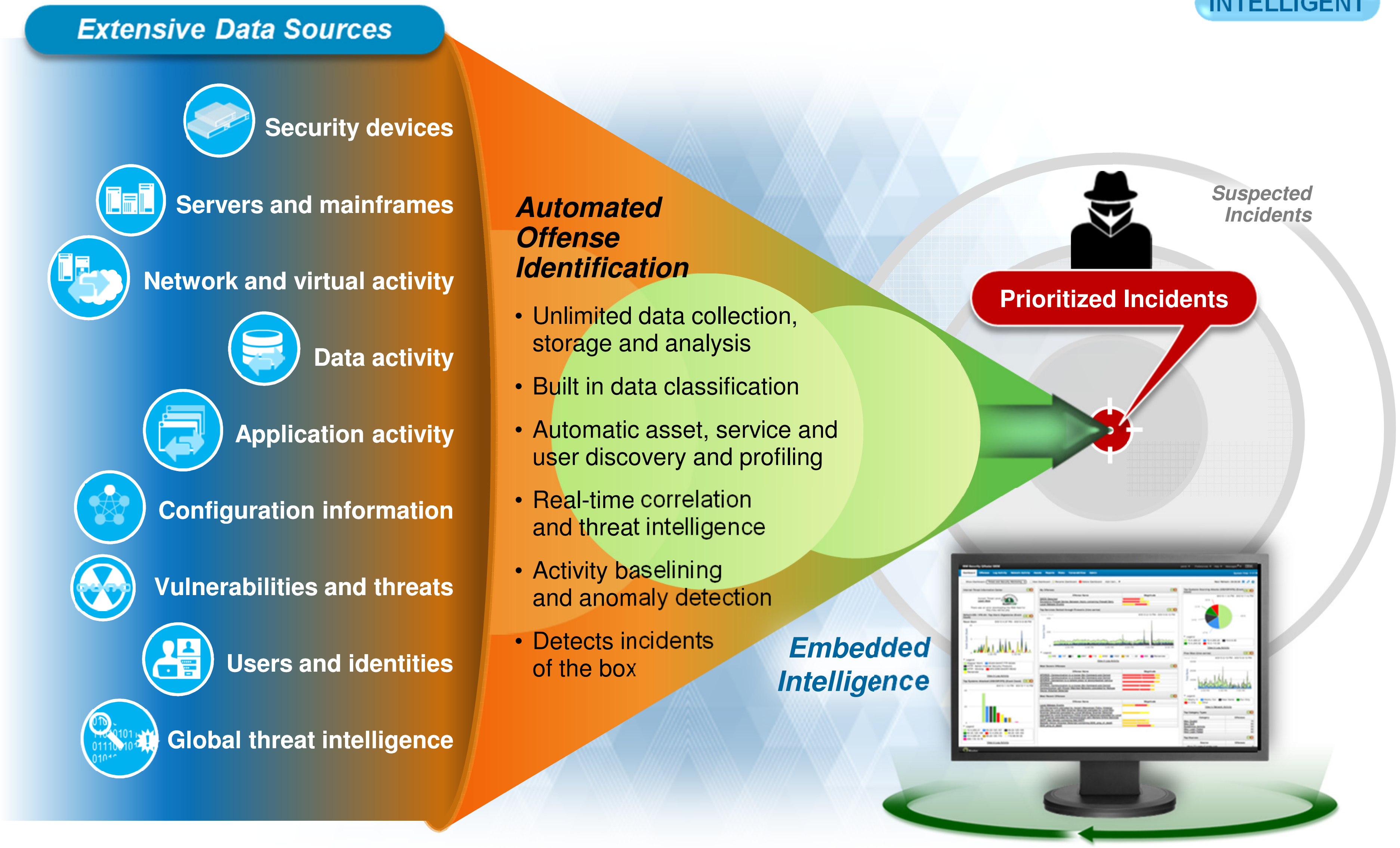
IBM QRadar Security Intelligence Platform

INTEGRATED

Unified architecture delivered in a single console

Embedded intelligence offers automated offense identification

INTELLIGENT



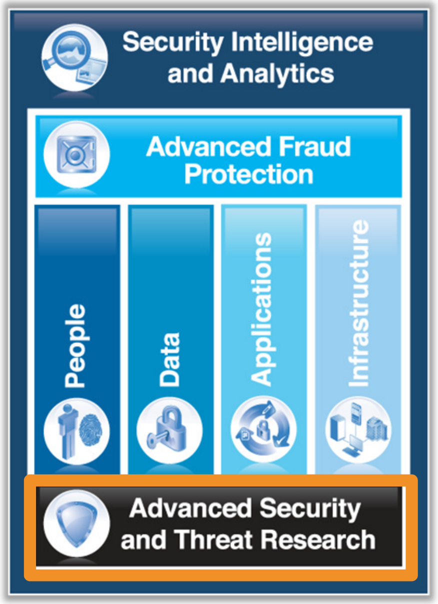
Extensive Data Sources

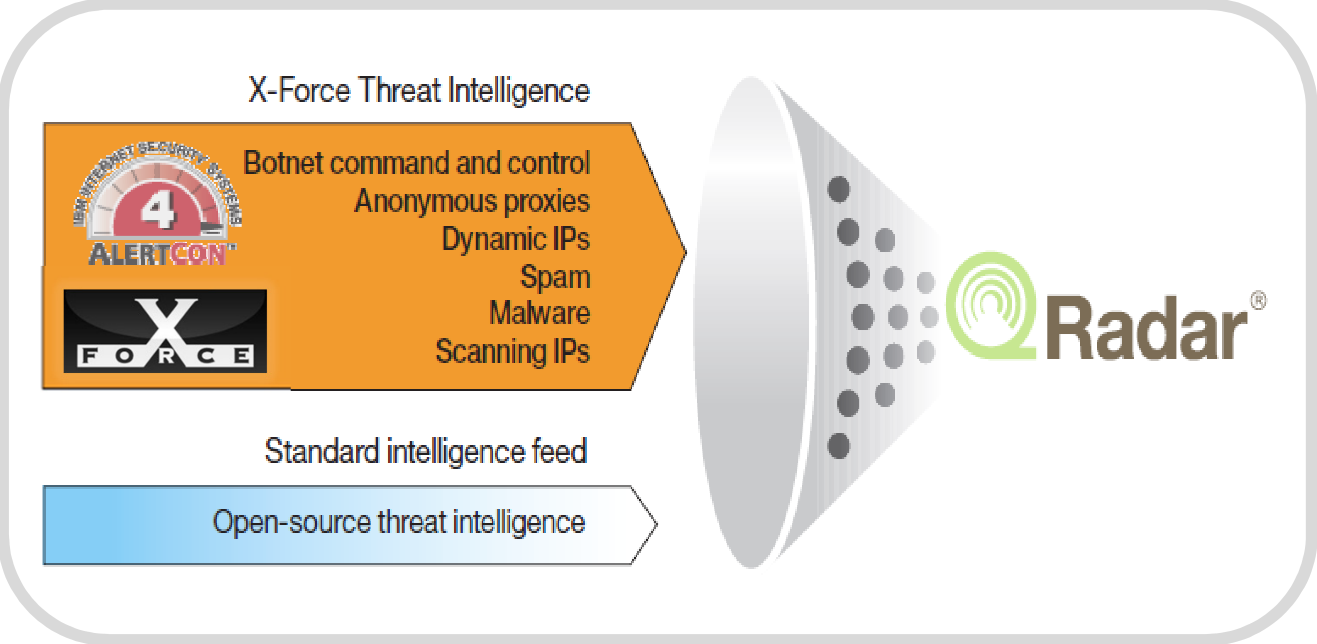
Security devices
Servers and mainframes
Network and virtual activity
Data activity
Application activity
Configuration information
Vulnerabilities and threats
Users and identities
Global threat intelligence

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

X-Force Threat Intelligence adds additional value to the standard feeds that are part of QRadar


Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

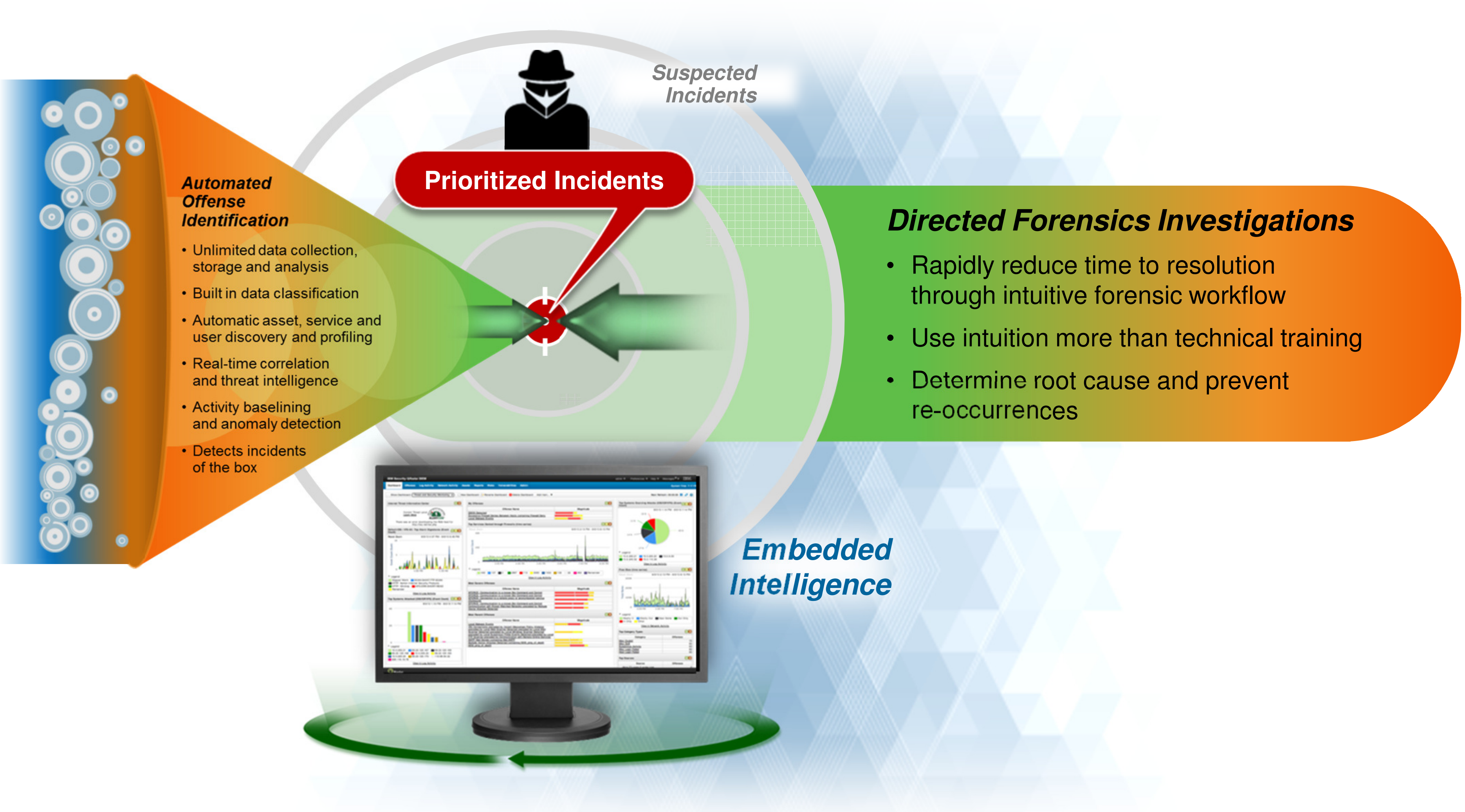

X-Force Threat Intelligence
Botnet command and control
Anonymous proxies
Dynamic IPs
Spam
Malware
Scanning IPs
IBM INTERNET SECURITY SYSTEMS
4
ALERTCON
X FORCE
Standard intelligence feed
Open-source threat intelligence
QRadar

X-Force Threat Intelligence adds

Frequent updates	In-house analytics	Confidence rank	Comprehensive coverage

Extend clarity around incidents with in-depth forensics data

INTELLIGENT



Suspected Incidents

Prioritized Incidents

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

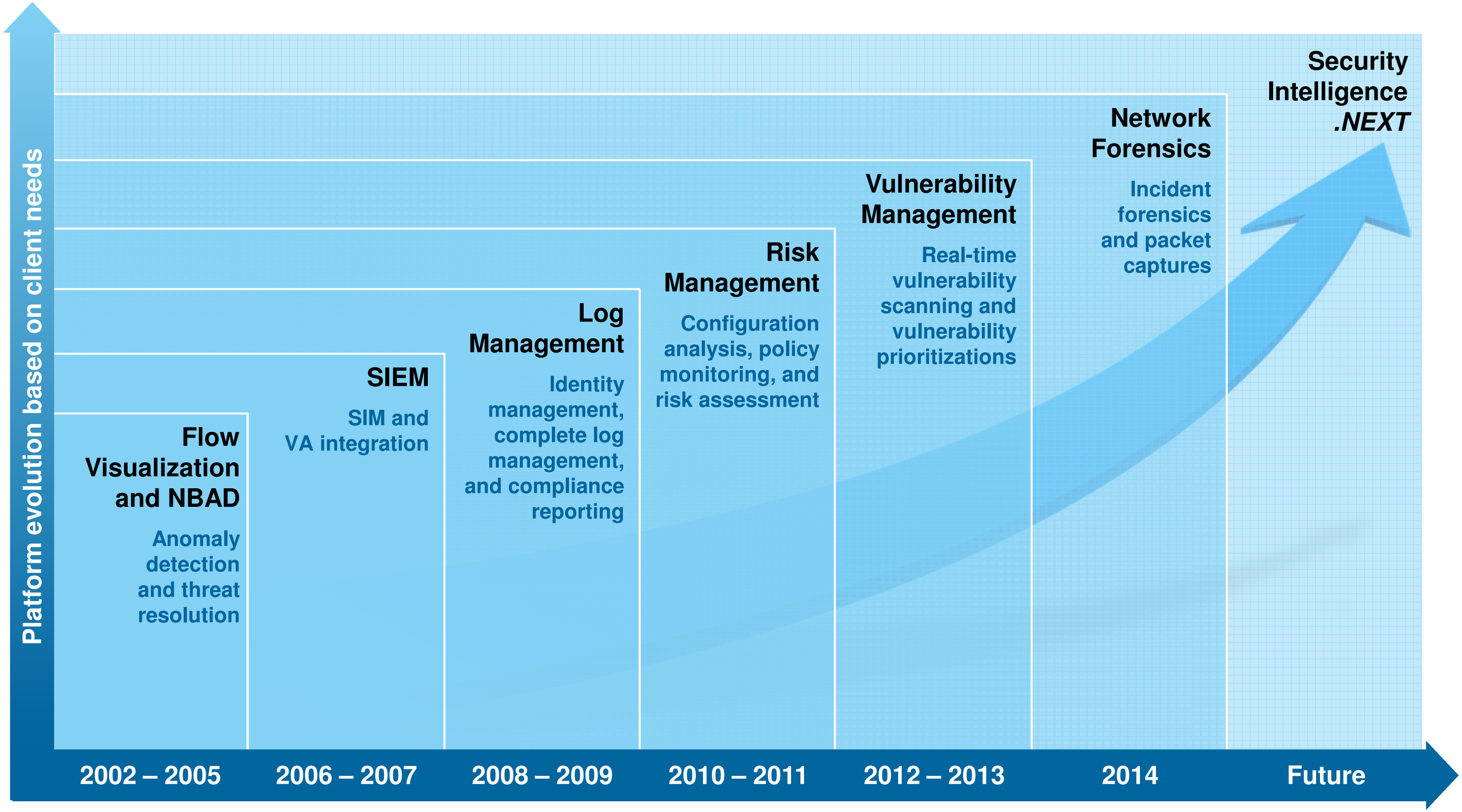
Directed Forensics Investigations

- Rapidly reduce time to resolution through intuitive forensic workflow
- Use intuition more than technical training
- Determine root cause and prevent re-occurrences

Embedded Intelligence

Evolving the IBM Security Intelligence strategy based on client needs

INTELLIGENT



Platform evolution based on client needs
Flow Visualization and NBAD
Anomaly detection and threat resolution
SIEM
SIM and VA integration
Log Management
Identity management, complete log management, and compliance reporting
Risk Management
Configuration analysis, policy monitoring, and risk assessment
Vulnerability Management
Real-time vulnerability scanning and vulnerability prioritizations
Network Forensics
Incident forensics and packet captures
Security Intelligence .NEXT
2002 – 2005
2006 – 2007
2008 – 2009
2010 – 2011
2012 – 2013
2014
Future

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

INTEGRATED

Log Management

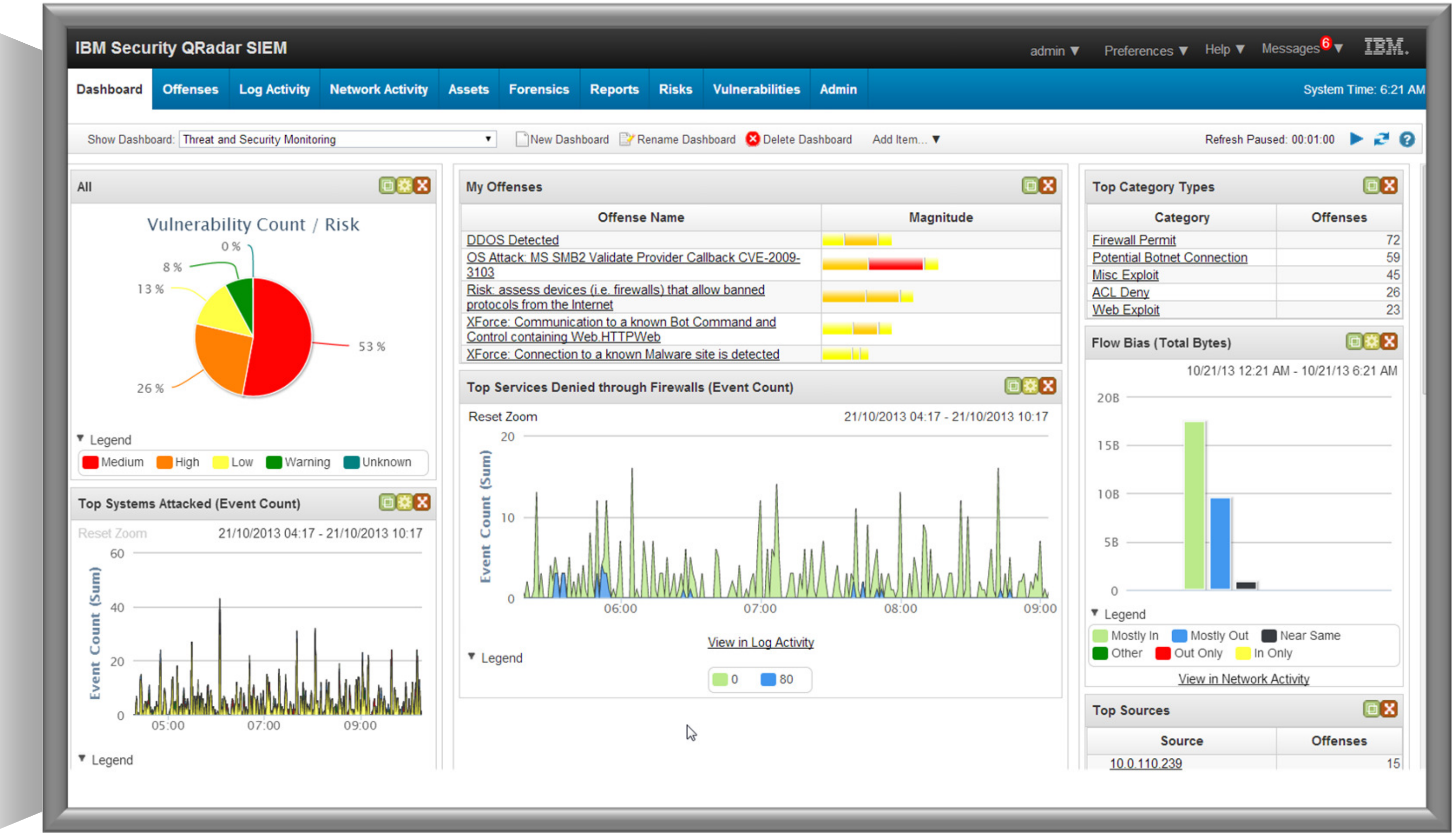
Security Intelligence

Network Activity Monitoring

Risk Management

Vulnerability Management

Network Forensics



IBM Security QRadar SIEM

admin ▼ Preferences ▼ Help ▼ Messages 6 ▼ IBM.

Dashboard | Offenses | Log Activity | Network Activity | Assets | Forensics | Reports | Risks | Vulnerabilities | Admin

System Time: 6:21 AM

Show Dashboard: Threat and Security Monitoring ▼ New Dashboard Rename Dashboard Delete Dashboard Add Item... ▼

Refresh Paused: 00:01:00

All

My Offenses

Offense Name	Magnitude
DDOS Detected	
OS Attack: MS SMB2 Validate Provider Callback CVE-2009-3103	
Risk: assess devices (i.e. firewalls) that allow banned protocols from the Internet	
XForce: Communication to a known Bot Command and Control containing Web.HTTPWeb	
XForce: Connection to a known Malware site is detected	

Top Category Types

Category	Offenses
Firewall Permit	72
Potential Botnet Connection	59
Misc Exploit	45
ACL Deny	26
Web Exploit	23

Top Services Denied through Firewalls (Event Count)

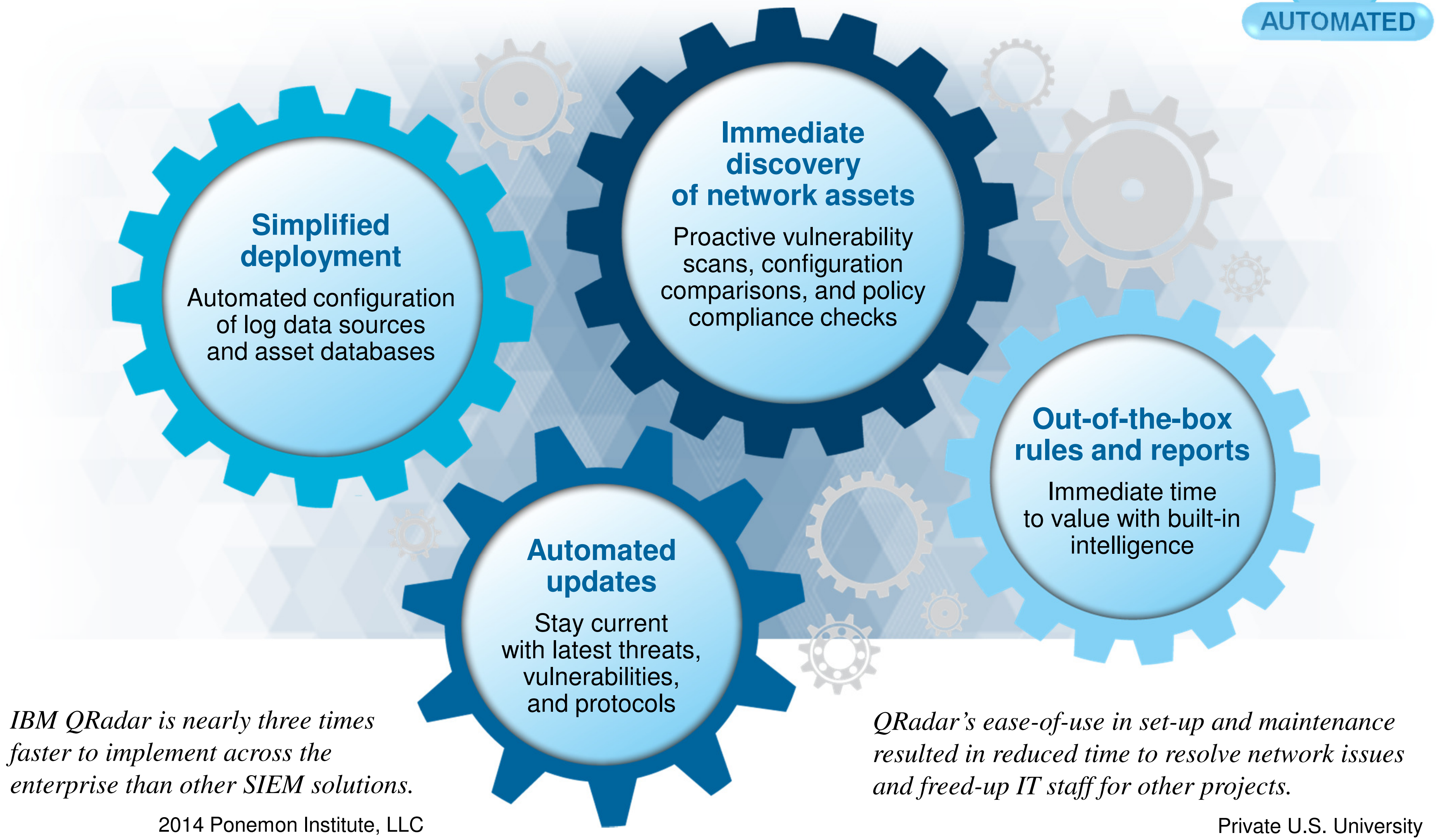
Flow Bias (Total Bytes)

Top Systems Attacked (Event Count)

Top Sources

Source	Offenses
10.0.110.239	15

Driving simplicity and accelerated time to value



AUTOMATED

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

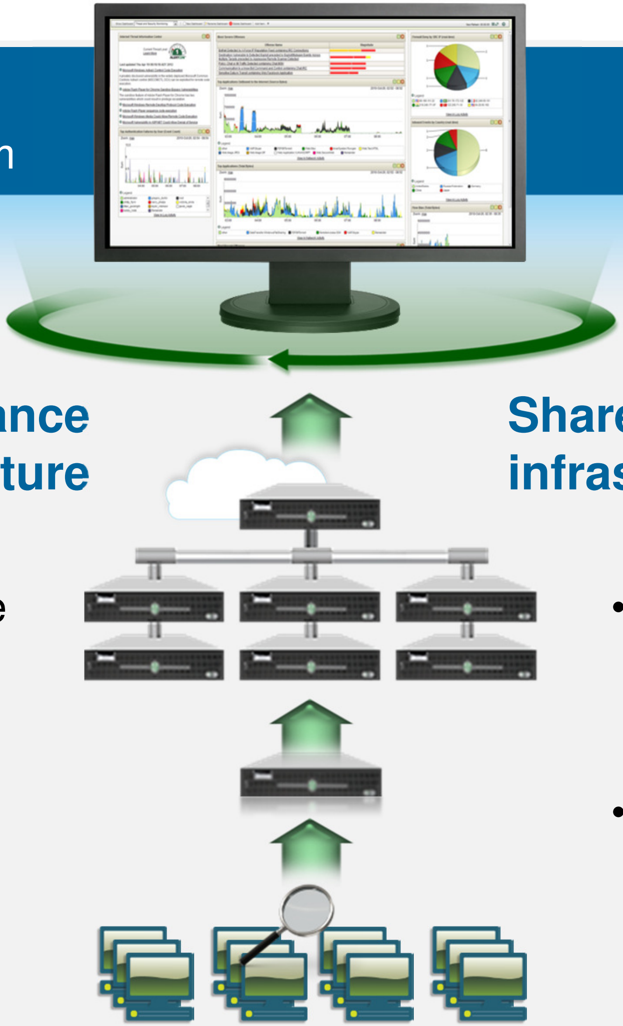
QRadar's ease-of-use in set-up and maintenance resulted in reduced time to resolve network issues and freed-up IT staff for other projects.

Private U.S. University
with large online education community

Optimized appliance and software architecture for high performance and rapid deployment

IBM QRadar

Security Intelligence Platform



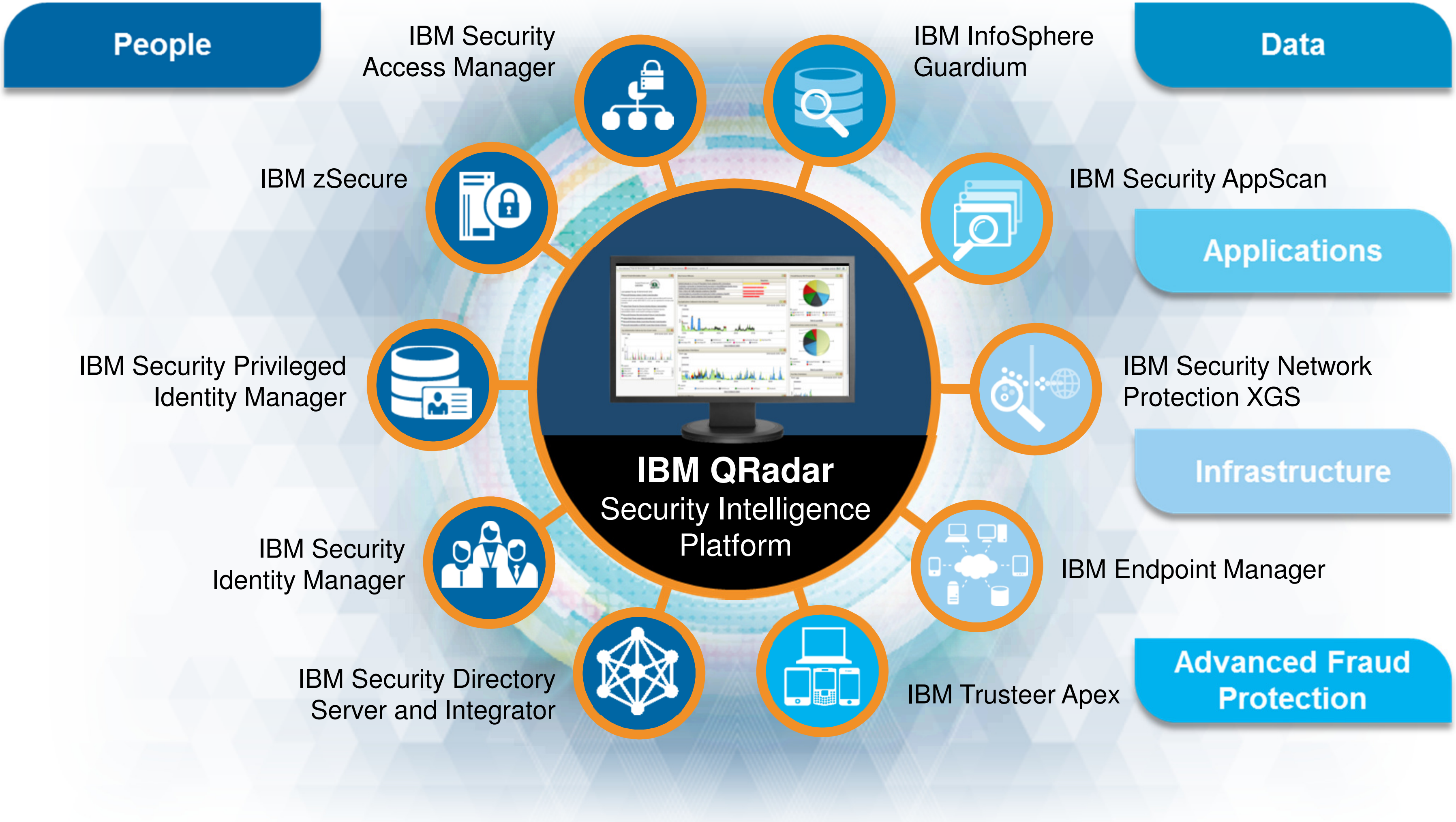
Scalable appliance architecture

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

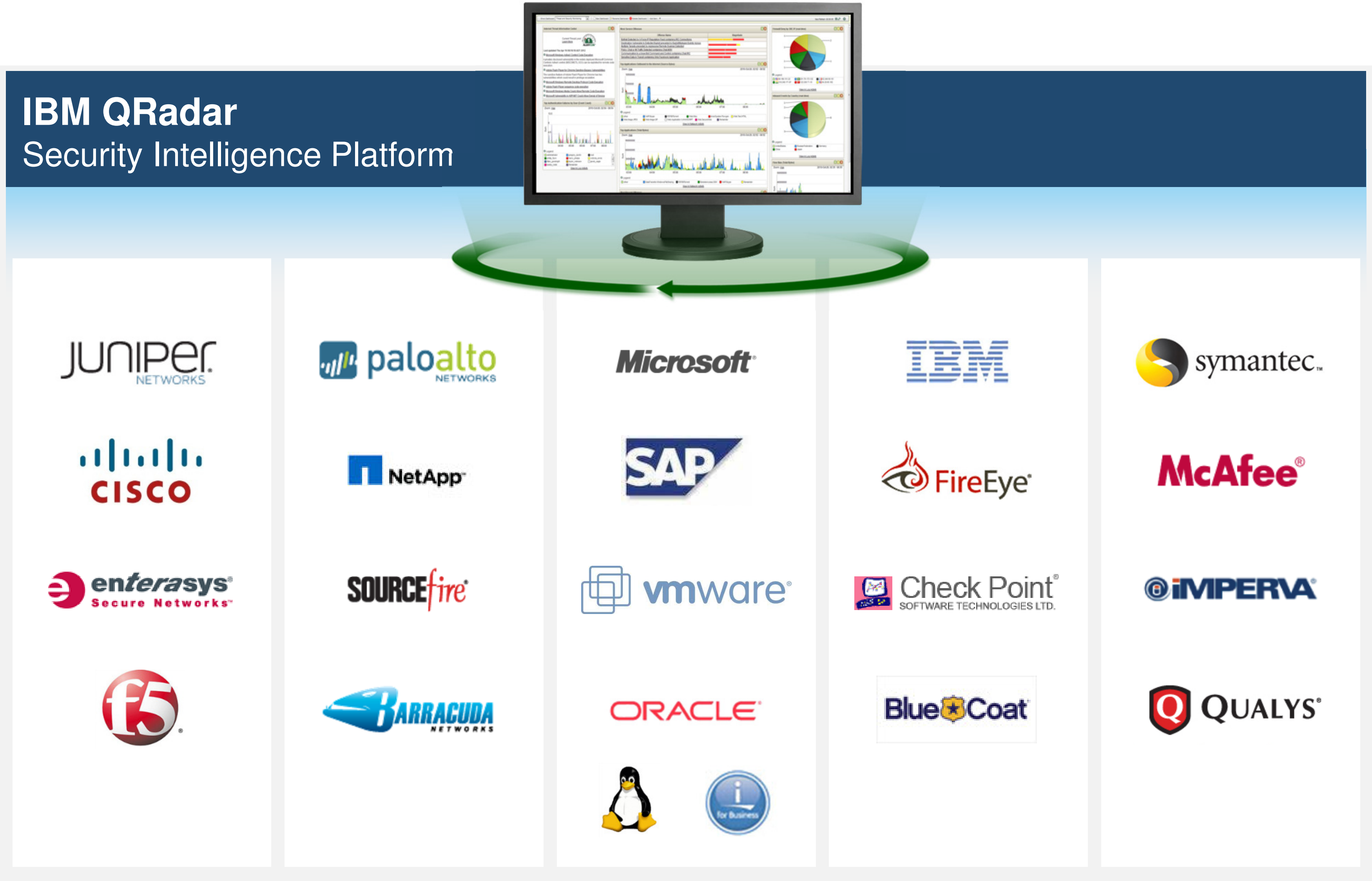
Shared modular infrastructure

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

IBM QRadar is the centerpiece of IBM security integration


People
IBM Security Access Manager
IBM zSecure
IBM Security Privileged Identity Manager
IBM Security Identity Manager
IBM Security Directory Server and Integrator
IBM QRadar
Security Intelligence Platform
IBM InfoSphere Guardium
Data
IBM Security AppScan
Applications
IBM Security Network Protection XGS
Infrastructure
IBM Endpoint Manager
IBM Trusteer Apex
Advanced Fraud Protection

IBM QRadar supports hundreds of third-party products



IBM QRadar
Security Intelligence Platform

Analyst recognition

IBM Security Intelligence

- **Leader in the Gartner Magic Quadrant since 2009**
  Security Information and Event Management (SIEM)
- **IBM QRadar rated #1 by Gartner in the following categories:**
  - Ability to execute
  - Analytics and behavior profiling
  - Compliance use cases
  - SIEM use case, product rating, and overall use case

- **#1 IDC Security Vulnerability Management** (including SIEM)
- **Champion / Leading Product by InfoTech**
- **2013 Global SIEM/LM Customer Value Leadership Award by Frost and Sullivan**

Client example: A large European banking company gained superior threat detection and a richer view of enterprise activities

Detect, analyze, and prioritize threats

1 million:1

Reduction in security events

99 percent

Decreased investigation time with **immediate** detection and notification of anomalies

Business challenge

- Integrate data from disparate systems and application sources in order to better detect and respond to threats.

IBM Security Intelligence and Compliance Analytics solutions

Gained superior threat detection and a richer view of enterprise activities, realizing a 1 million:1 reduction in security events, 99 percent decrease in investigation time, and immediate detection and notification of anomalies.

Client example: An international energy company reduces billions of events per day to find those that should be investigated

Optimize threat analysis

An international energy firm analyzes

2 billion

events per day to find

20-25

potential offenses to investigate

Business challenge

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

IBM Security Solutions (QRadar SIEM, QFlow, Risk Manager)

Combined analysis of historical data with real-time alerts to gain a ‘big picture’ view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

Client example: A financial information provider hardens defenses against threats and fraud

Optimize risk management

financial information provider tracks

250 activity baselines

and saved

50-80%

on staffing versus alternative solutions

Business challenge

- Detect wide range of security threats affecting public-facing Web applications
- Help identify subtle changes in user behavior that could indicate fraud or misuse
- Exceed ISO 27001 standard

IBM Security Solutions (QRadar SIEM, QFlow, X-Force, Network IPS)

Combine analysis of historical data with real-time alerts to gain a ‘big picture’ view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

Intelligence, integration, automation to stay ahead of the threat

New Dashboard | Rename Dashboard | Delete Dashboard | Add Item... ▼

Current Threat Level 1 ALERTCON
Learn More

Last updated Thu Apr 19 09:16:18 ADT 2012

- Microsoft Windows ActiveX Control Code Execution

  A privately disclosed vulnerability in the widely deployed Microsoft Common Controls ActiveX control (MSCOMCTL.OCX) can be exploited for remote code execution.

- Adobe Flash Player for Chrome Sandbox Bypass Vulnerabilities

  The sandbox feature of Adobe Flash Player for Chrome has two vulnerabilities which could result in privilege escalation.

- Microsoft Windows Remote Desktop Protocol Code Execution
- Adobe Flash Player sequence code execution
- Microsoft Windows Media Could Allow Remote Code Execution
- Microsoft Vulnerability in ASP.NET Could Allow Denial of Service

Most Severe Offenses

Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Across Multiple Targets preceded by Aggressive Remote Scanner Detected	
Policy: Chat or IM Traffic Detected containing Chat.MSN	
Communication to a know Bot Command and Control containing Chat.IRC	
Sensitive Data in Transit containing Web.Facebook.Application	

Top Applications Outbound to the Internet (Source Bytes)

Zoom: max 2010-Oct-26, 02:52 - 08:52

View in Network Activity

Top Authentication Failures by User (Event Count)

Zoom: max 2010-Oct-26, 02:54 - 08:54

Top Applications (Total Bytes)

Zoom: max 2010-Oct-26

View in Network Activity

View in Log Activity

Flow Bias (Total Bytes)

Most Recent Offenses

Identify and quickly remediate

Deploy comprehensive security intelligence and incident forensics

Address regulation mandates

Automate data collection and configuration audits

Detect insider fraud

Adopt next-generation SIEM with identity correlation

Consolidate data silos

Collect, correlate and report on data in one integrated solution

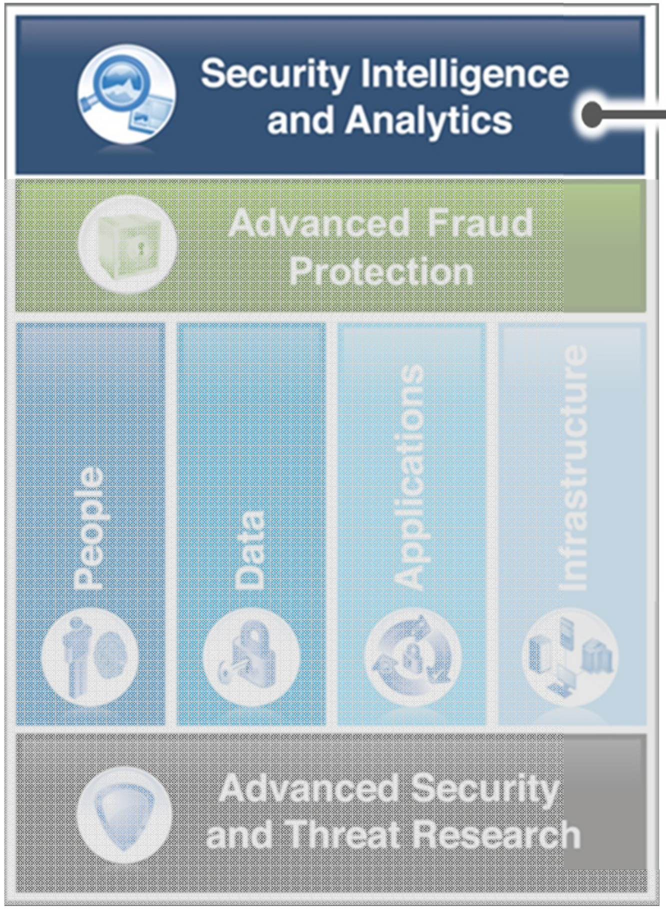
Better predict business risks

Engage entire lifecycle of risk management for network and security infrastructures

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


Security Intelligence and Analytics
Advanced Fraud Protection
People
Data
Applications
Infrastructure
Advanced Security and Threat Research

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

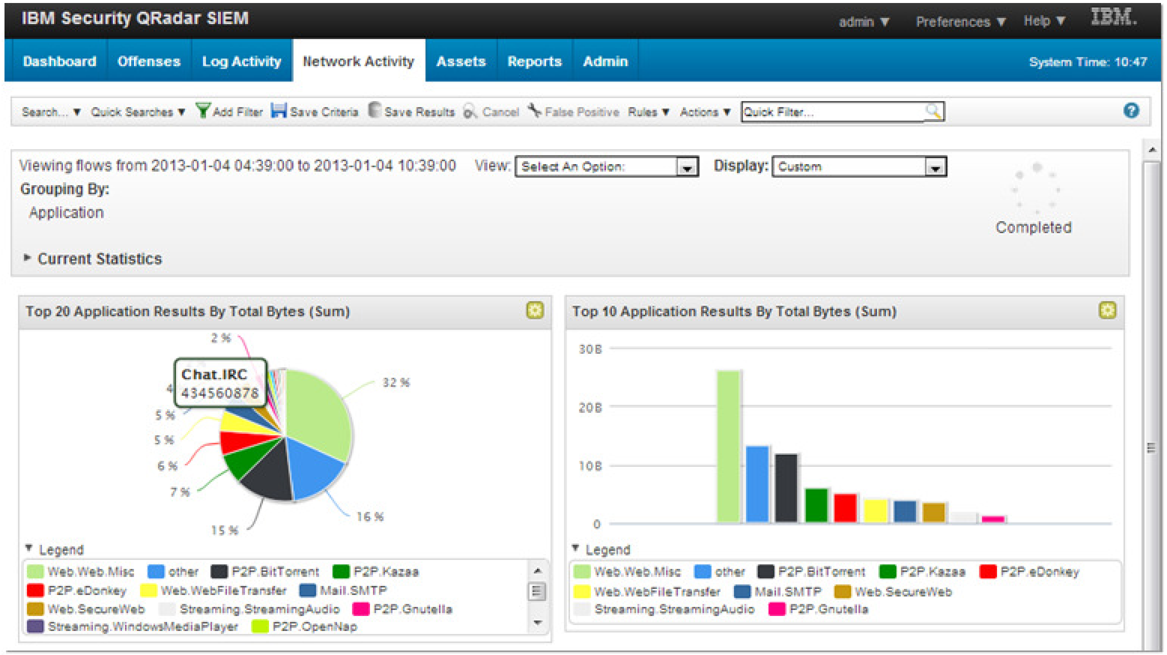
- Integrated Network Scanning & Workflow
- Leverage SIEM, Threat, Risk to prioritize vulnerabilities

QRadar Incident Forensics

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

QRadar SIEM: Command console for Security Intelligence

- Provides full visibility and actionable insight to protect against advanced threats
- Adds network flow capture and analysis for deep application insight
- Employs sophisticated correlation of events, flows, assets, topologies, vulnerabilities and external data to identify and prioritize threats



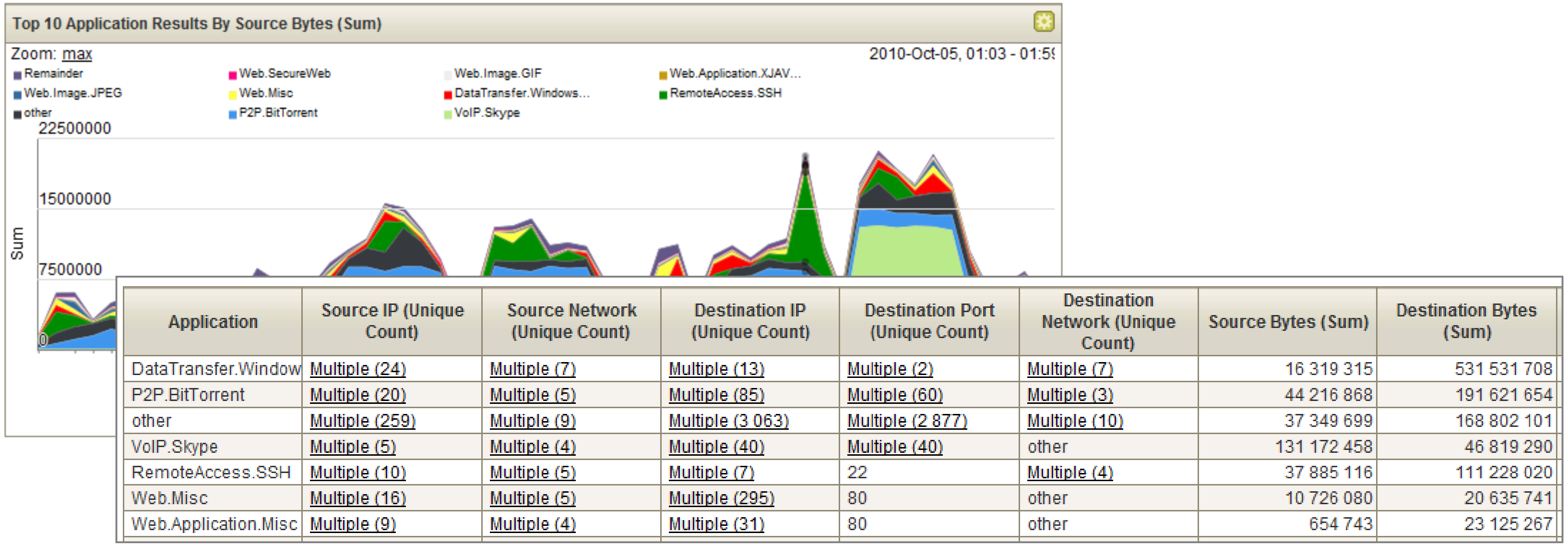
Viewing flows from 2013-01-04 04:39:00 to 2013-01-04 10:39:00 View: Select An Option: Display: Custom

Grouping By:
Application

- Contains workflow management to fully track threats and ensure resolution
- Uses scalable hardware, software and virtual appliance architecture to support the largest deployments

Differentiated by 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 get missed
- Enables visibility into attacker communications



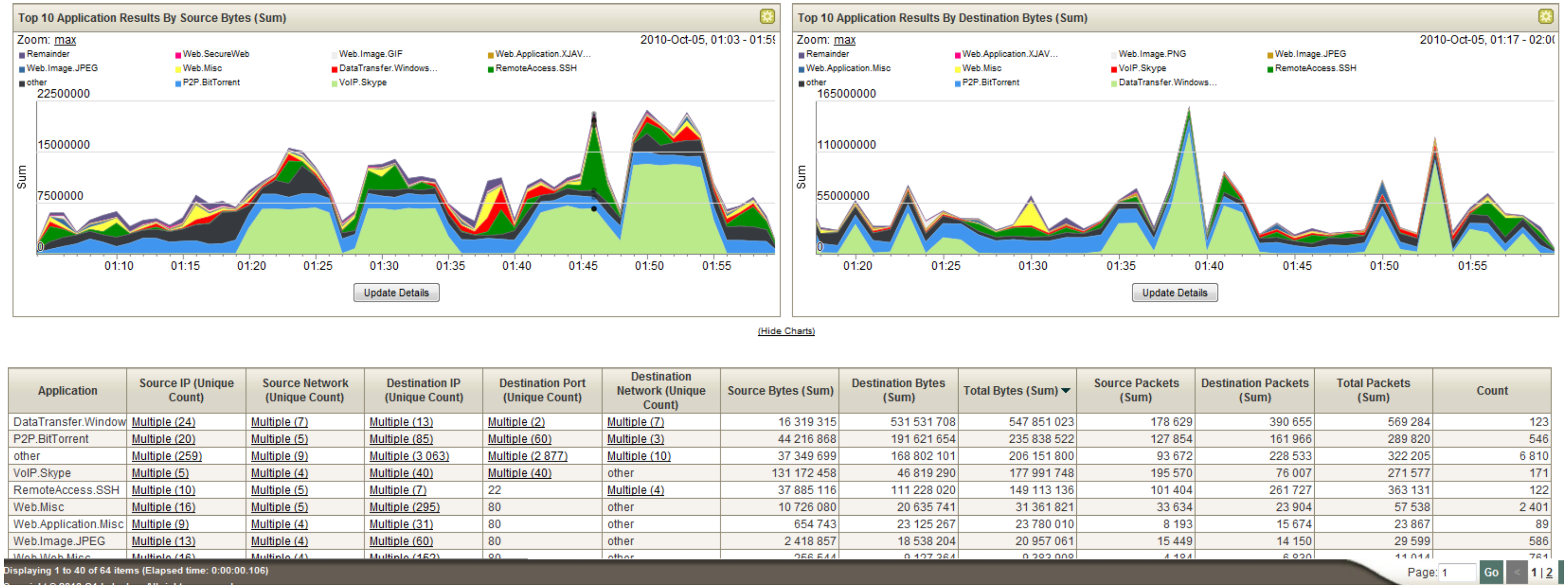
Top 10 Application Results By Source Bytes (Sum)

Zoom: max

2010-Oct-05, 01:03 - 01:5

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

Flows provide context for true network intelligence



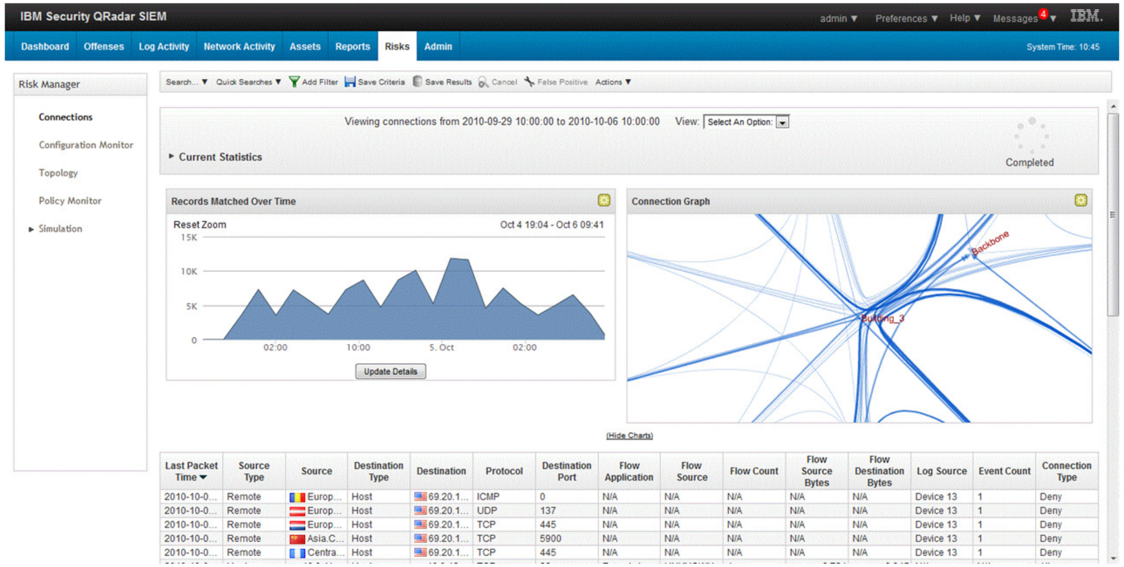
Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum) ▼	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	Multiple (24)	Multiple (7)	Multiple (13)	Multiple (2)	Multiple (7)	16 319 315	531 531 708	547 851 023	178 629	390 655	569 284	123
P2P.BitTorrent	Multiple (20)	Multiple (5)	Multiple (85)	Multiple (60)	Multiple (3)	44 216 868	191 621 654	235 838 522	127 854	161 966	289 820	546
other	Multiple (259)	Multiple (9)	Multiple (3 063)	Multiple (2 877)	Multiple (10)	37 349 699	168 802 101	206 151 800	93 672	228 533	322 205	6 810
VoIP.Skype	Multiple (5)	Multiple (4)	Multiple (40)	Multiple (40)	other	131 172 458	46 819 290	177 991 748	195 570	76 007	271 577	171
RemoteAccess.SSH	Multiple (10)	Multiple (5)	Multiple (7)	22	Multiple (4)	37 885 116	111 228 020	149 113 136	101 404	261 727	363 131	122
Web.Misc	Multiple (16)	Multiple (5)	Multiple (295)	80	other	10 726 080	20 635 741	31 361 821	33 634	23 904	57 538	2 401
Web.Application.Misc	Multiple (9)	Multiple (4)	Multiple (31)	80	other	654 743	23 125 267	23 780 010	8 193	15 674	23 867	89
Web.Image.JPEG	Multiple (13)	Multiple (4)	Multiple (60)	80	other	2 418 857	18 538 204	20 957 061	15 449	14 150	29 599	586
Web.Web.Misc	Multiple (16)	Multiple (4)	Multiple (152)	80	other	256 544	9 127 364	9 383 908	4 184	6 830	11 014	761

Displaying 1 to 40 of 64 items (Elapsed time: 0:00:00.106)

- Helps detect zero-day attacks that have no signature
- Enables policy monitoring and rogue server identification
- Supports risk prioritization
- Provides visibility into all attacker communications
- Uses passive monitoring to build asset profiles and classify hosts
- Improves network visibility and helps resolve traffic problems

QRadar Risk Manager: **Visualize** network, configurations and risks

- Depicts network topology views and helps visualize current and alternative network traffic patterns
- Identifies active attack paths and assets at risk of exploit
- Collects network device configuration data to assess vulnerabilities and facilitate analysis and reporting



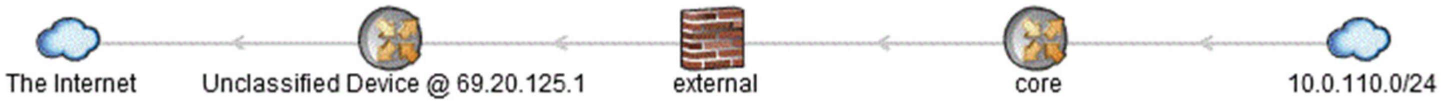
Viewing connections from 2010-09-29 10:00:00 to 2010-10-06 10:00:00 View: Select An Option:

Last Packet Time ▼	Source Type	Source	Destination Type	Destination	Protocol	Destination Port	Flow Application	Flow Source	Flow Count	Flow Source Bytes	Flow Destination Bytes	Log Source	Event Count	Connection Type
2010-10-0...	Remote	Europ...	Host	69.20.1...	ICMP	0	N/A	N/A	N/A	N/A	N/A	Device 13	1	Deny
2010-10-0...	Remote	Europ...	Host	69.20.1...	UDP	137	N/A	N/A	N/A	N/A	N/A	Device 13	1	Deny
2010-10-0...	Remote	Europ...	Host	69.20.1...	TCP	445	N/A	N/A	N/A	N/A	N/A	Device 13	1	Deny
2010-10-0...	Remote	Asia.C...	Host	69.20.1...	TCP	5900	N/A	N/A	N/A	N/A	N/A	Device 13	1	Deny
2010-10-0...	Remote	Centra...	Host	69.20.1...	TCP	445	N/A	N/A	N/A	N/A	N/A	Device 13	1	Deny

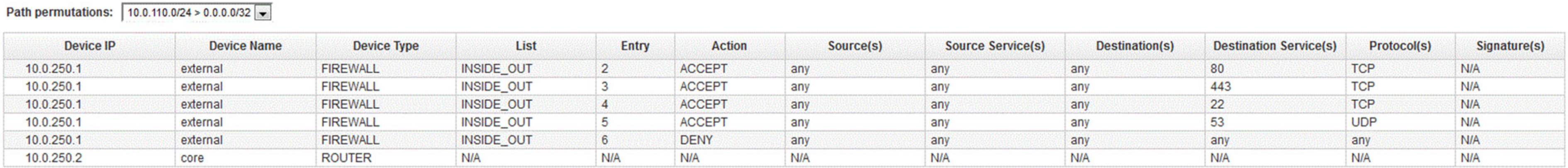
- Discovers firewall configuration errors and improves performance by eliminating ineffective rules
- Analyzes policy compliance for network traffic, topology and vulnerability exposures

QRadar® Risk Manager

Investigating offense attack path



- Clicking ‘attack path’ button for an offense performs search showing precise path (and all permutations) between involved source and destination IPs
- Firewall rules enabling the attack path can then be quickly analyzed to understand the exposure



Path permutations: 10.0.110.0/24 > 0.0.0.0/32

Device IP	Device Name	Device Type	List	Entry	Action	Source(s)	Source Service(s)	Destination(s)	Destination Service(s)	Protocol(s)	Signature(s)
10.0.250.1	external	FIREWALL	INSIDE_OUT	2	ACCEPT	any	any	any	80	TCP	N/A
10.0.250.1	external	FIREWALL	INSIDE_OUT	3	ACCEPT	any	any	any	443	TCP	N/A
10.0.250.1	external	FIREWALL	INSIDE_OUT	4	ACCEPT	any	any	any	22	TCP	N/A
10.0.250.1	external	FIREWALL	INSIDE_OUT	5	ACCEPT	any	any	any	53	UDP	N/A
10.0.250.1	external	FIREWALL	INSIDE_OUT	6	DENY	any	any	any	any	any	N/A
10.0.250.2	core	ROUTER	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

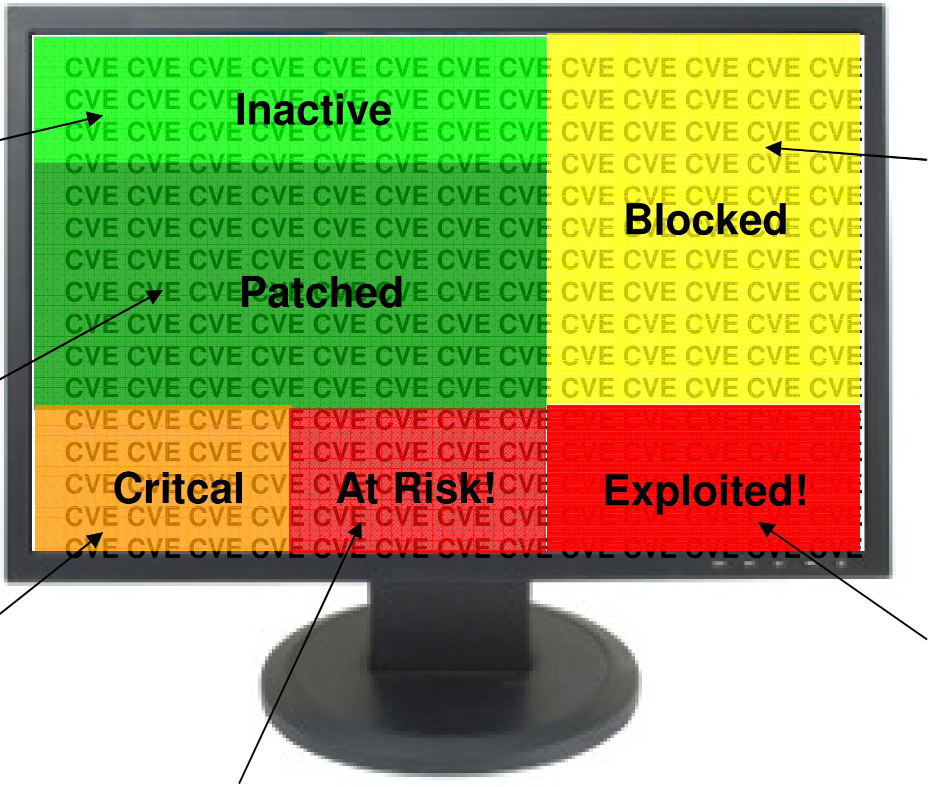
- Allows “virtual patch” to be applied by quickly showing which firewall rules may be changed to immediately shut down attack path—before patching or other configuration changes can typically be implemented

QVM enables customers to interpret ‘sea’ of vulnerabilities

Inactive: QFlow Collector data helps QRadar Vulnerability Manager sense application activity

Patched: IBM Endpoint Manager helps QVM understand which vulnerabilities will be patched

Critical: Vulnerability knowledge base, remediation flow and QRM policies inform QVM about business critical vulnerabilities



Blocked: QRadar Risk Manager helps QVM understand which vulnerabilities are blocked by firewalls and IPSs

Exploited: SIEM correlation and IPS data help QVM reveal which vulnerabilities have been exploited

At Risk: X-Force Threat and SIEM security incident data, coupled with QFlow network traffic visibility, help QVM see assets communicating with potential threats

Expandable and scalable QRadar platform solutions

Log Management

Radar®
Log Manager

- Turn-key log management and reporting
- SME to Enterprise
- Upgradeable to enterprise SIEM

SIEM

Radar®
SIEM

- Log, flow, vulnerability & identity correlation
- Sophisticated asset profiling
- Offense management and workflow

Network and Application Visibility

Radar
QFlow

Radar
VFlow

- Layer 7 application monitoring
- Content capture for deep insight & forensics
- Physical and virtual environments

Risk & Vulnerability Management

Radar®
Risk Manager

Radar
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

Radar
Incident Forensics

- Reconstructs network sessions from PCAPs
- Data pivoting and visualization tools
- Accelerated clarity around who, what, when

Fully integrated architecture and interface

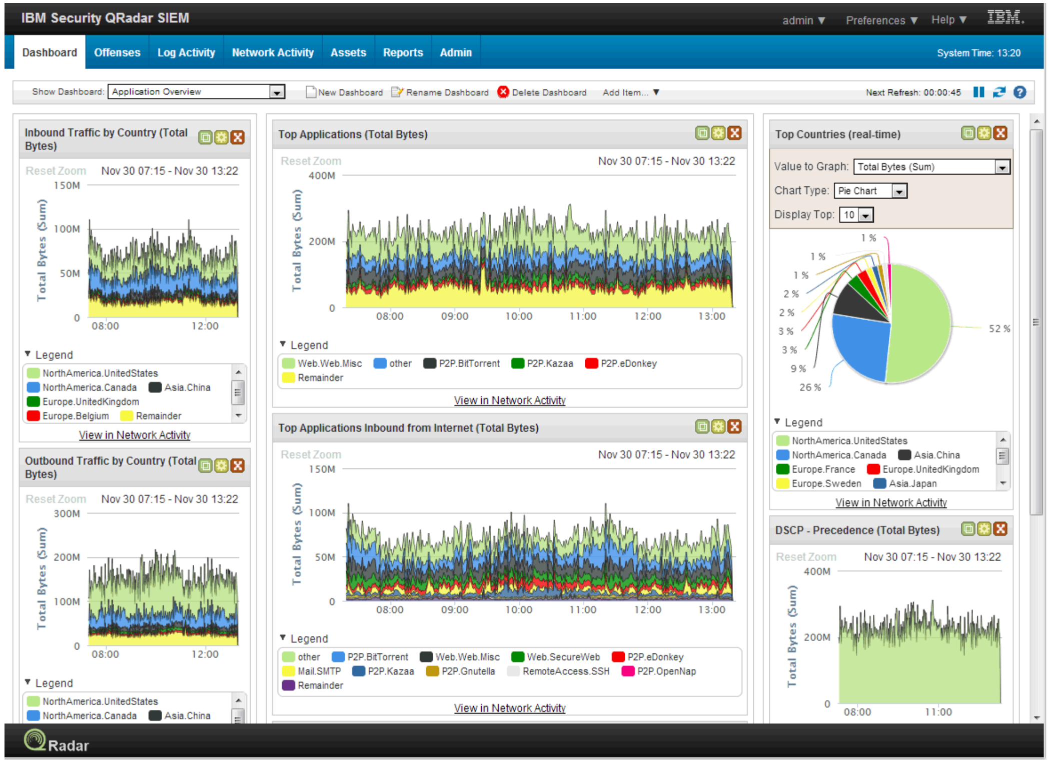
Log Management

SIEM

Risk & Vulnerability Management

Network and Application Visibility

One Console Security


IBM Security QRadar SIEM
admin ▼ Preferences ▼ Help ▼ IBM.
Dashboard Offenses Log Activity Network Activity Assets Reports Admin
System Time: 13:20
New Dashboard Rename Dashboard Delete Dashboard Add Item... ▼
Next Refresh: 00:00:45
Inbound Traffic by Country (Total Bytes)
Reset Zoom Nov 30 07:15 - Nov 30 13:22
150M 100M 50M 0 08:00 12:00
Total Bytes (Sum)
Legend
NorthAmerica.UnitedStates NorthAmerica.Canada Asia.China Europe.UnitedKingdom Europe.Belgium Remainder
View in Network Activity
Outbound Traffic by Country (Total Bytes)
Reset Zoom Nov 30 07:15 - Nov 30 13:22
300M 200M 100M 0 08:00 12:00
Legend
NorthAmerica.UnitedStates NorthAmerica.Canada Asia.China
Top Applications (Total Bytes)
Reset Zoom Nov 30 07:15 - Nov 30 13:22
400M 200M 0 08:00 09:00 10:00 11:00 12:00 13:00
Legend
Web.Web.Misc other P2P.BitTorrent P2P.Kazaa P2P.eDonkey Remainder
View in Network Activity
Top Applications Inbound from Internet (Total Bytes)
Reset Zoom Nov 30 07:15 - Nov 30 13:22
150M 100M 50M 0 08:00 09:00 10:00 11:00 12:00 13:00
Legend
other P2P.BitTorrent Web.Web.Misc Web.SecureWeb P2P.eDonkey Mail.SMTP P2P.Kazaa P2P.Gnutella RemoteAccess.SSH P2P.OpenNap Remainder
View in Network Activity
Top Countries (real-time)
1 % 1 % 1 % 2 % 2 % 3 % 3 % 9 % 26 % 52 %
Legend
NorthAmerica.UnitedStates NorthAmerica.Canada Asia.China Europe.France Europe.UnitedKingdom Europe.Sweden Asia.Japan
View in Network Activity
DSCP - Precedence (Total Bytes)
Reset Zoom Nov 30 07:15 - Nov 30 13:22
400M 200M 0 08:00 11:00
Radar

Show Dashboard: Application Overview

Value to Graph: Total Bytes (Sum)

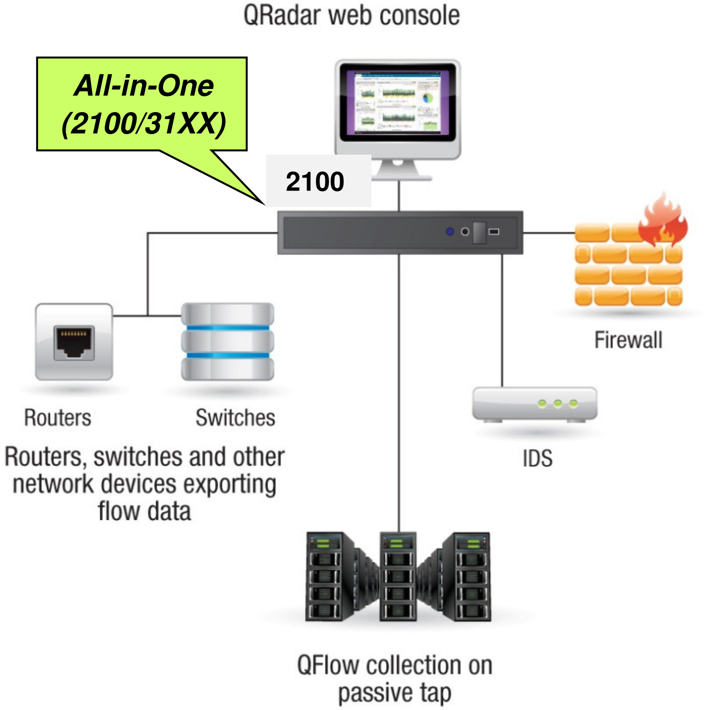
Chart Type: Pie Chart

Display Top: 10

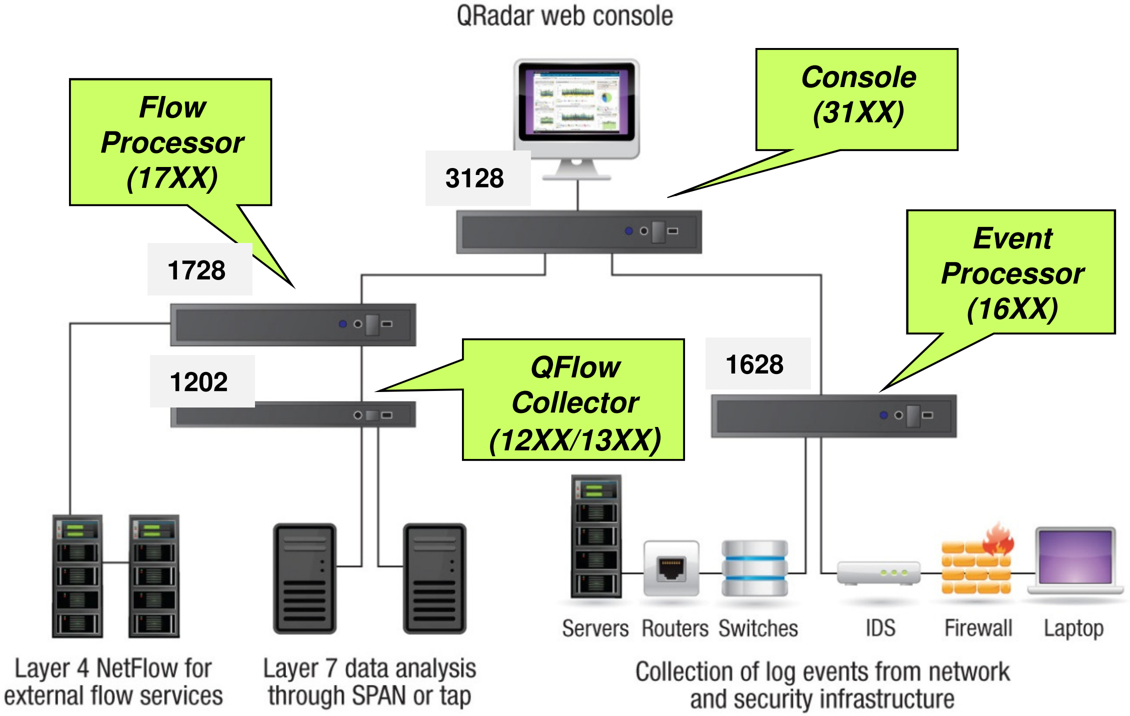
Built on a Single Data Architecture

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

Sample IBM Security QRadar SIEM 2100 all-in-one deployment


QRadar web console
All-in-One (2100/31XX)
2100
Firewall
Routers
Switches
Routers, switches and other network devices exporting flow data
IDS
QFlow collection on passive tap

Sample IBM Security QRadar SIEM 3124 distributed deployment


QRadar web console
Flow Processor (17XX)
Console (31XX)
3128
1728
Event Processor (16XX)
1202
QFlow Collector (12XX/13XX)
1628
Servers
Routers
Switches
IDS
Firewall
Laptop
Layer 4 NetFlow for external flow services
Layer 7 data analysis through SPAN or tap
Collection of log events from network and security infrastructure

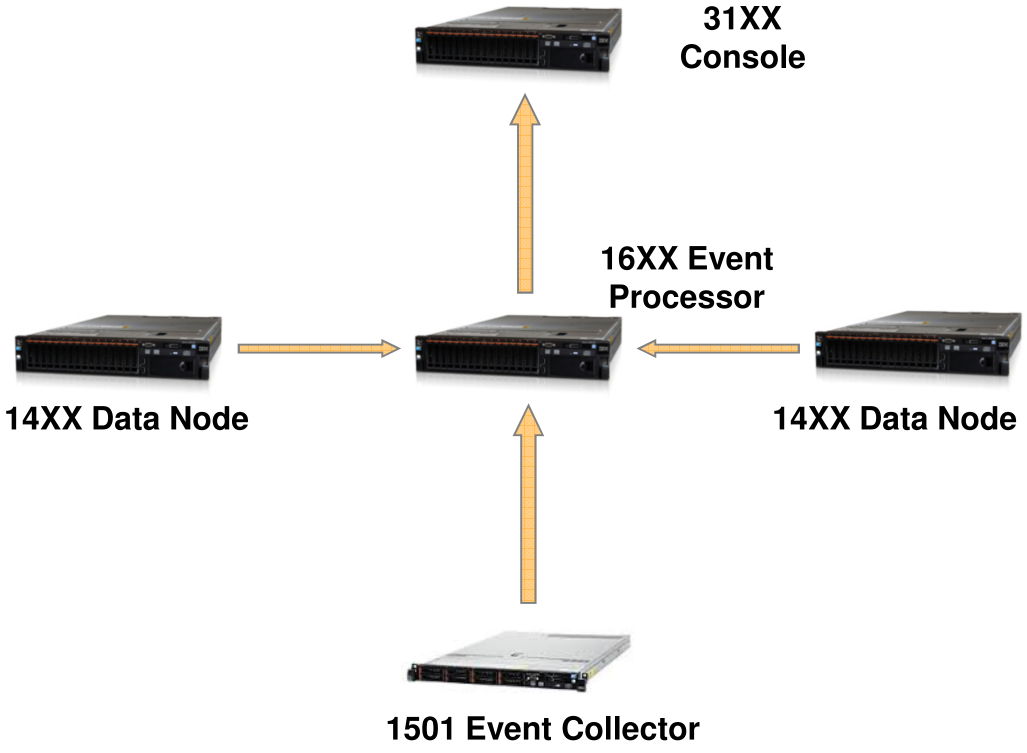
All-in-One is a single appliance used to collect both events and flow data from various security and network devices, perform data correlation and rule matching, report alerts/threats, and provide all admin functions through a Web browser.

A Distributed deployment consists of multiple appliances for different purposes:

- **Event Processor** to collect, process and store log events
- **Flow Processor** to collect, process and store several kinds of flow data generated from network device. Optional **QFlow Collector** is used to collect layer 7 application data.
- **Console** to correlate data from managed processors, generate alerts/reports, and provide all admin functions.

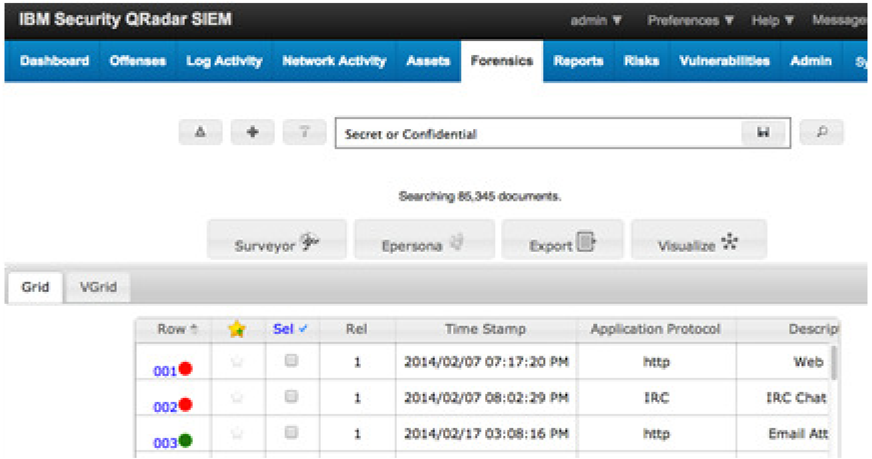
Data Node effectively addresses limited storage and search performance concerns

- Data Node is designed to be attached to an existing QRadar product to provide scalable data storage and search performance.
- Multiple Data Nodes can be attached to a product. Collected/processed data is distributed to the attached Data Nodes so data storage can be linearly increased. Search performance can also be significantly increased.
- Can be added to a new or existing deployment.



QRadar® Incident Forensics

Intuitive investigation of security incidents



Secret or Confidential

Searching 85,345 documents.

Row	★	Sel ✓	Rel	Time Stamp	Application Protocol	Descrip
001 ●	☆	□	1	2014/02/07 07:17:20 PM	http	Web
002 ●	☆	□	1	2014/02/07 08:02:29 PM	IRC	IRC Chat
003 ●	☆	□	1	2014/02/17 03:08:16 PM	http	Email Att

Features:

- Employs Internet search engine technology closing security team skill gaps
- Creates rich 'digital impression' visualizations of related content
- Adds full packet captures to complement SIEM security data collection and analytics

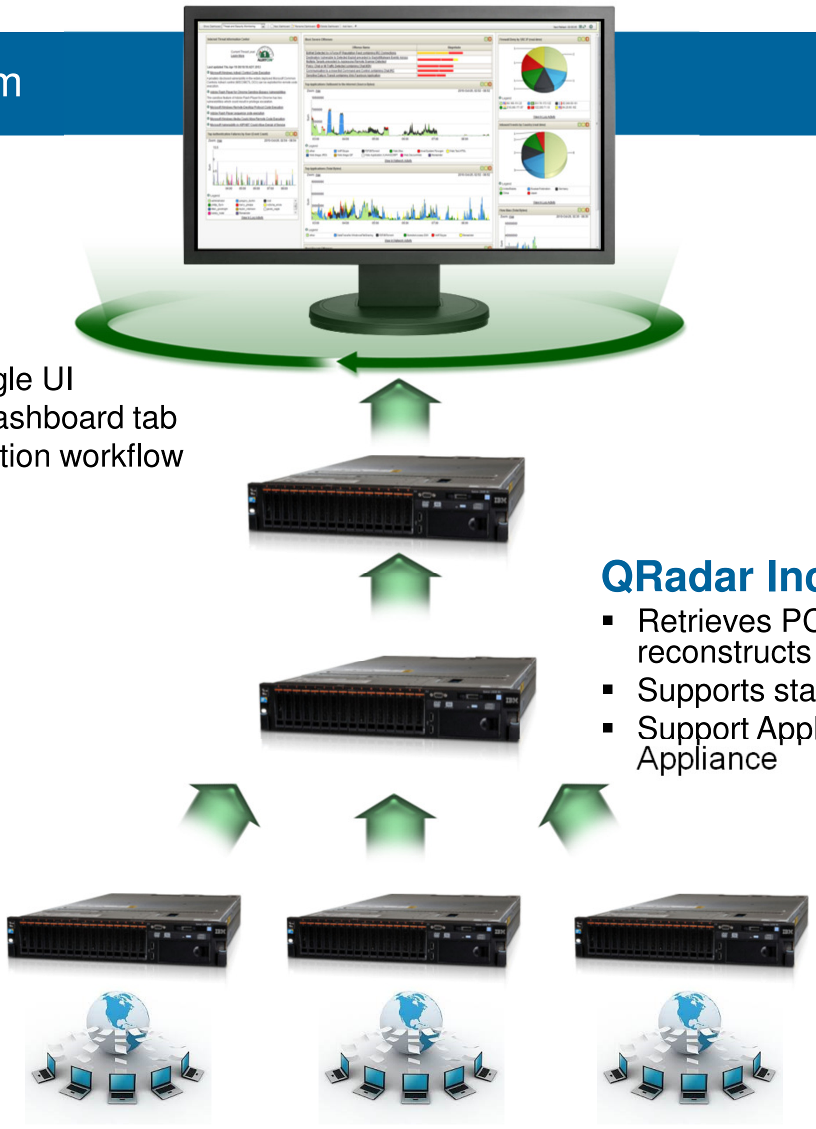
Benefits:

- Reduces incident investigation periods from days or hours to minutes
- Helps determine root cause of successful breaches helping prevent recurrences
- Compiles evidence against malicious entities breaching secure systems and deleting or stealing sensitive data

Wins the race against time

QRadar Packet Capture and Incident Forensics

Security Intelligence Platform



QRadar Console

- Seamlessly integrated, single UI
- Includes new ‘Forensics’ dashboard tab
- Supports incident investigation workflow

QRadar Incident Forensics

- Retrieves PCAPs for an incident and reconstructs sessions for forensics
- Supports standard PCAP format
- Support Appliance, Software, Virtual Appliance

QRadar Packet Capture

- Performs Full Packet Capture
- Optimized appliance solution
- Scalable storage
- Appliance only

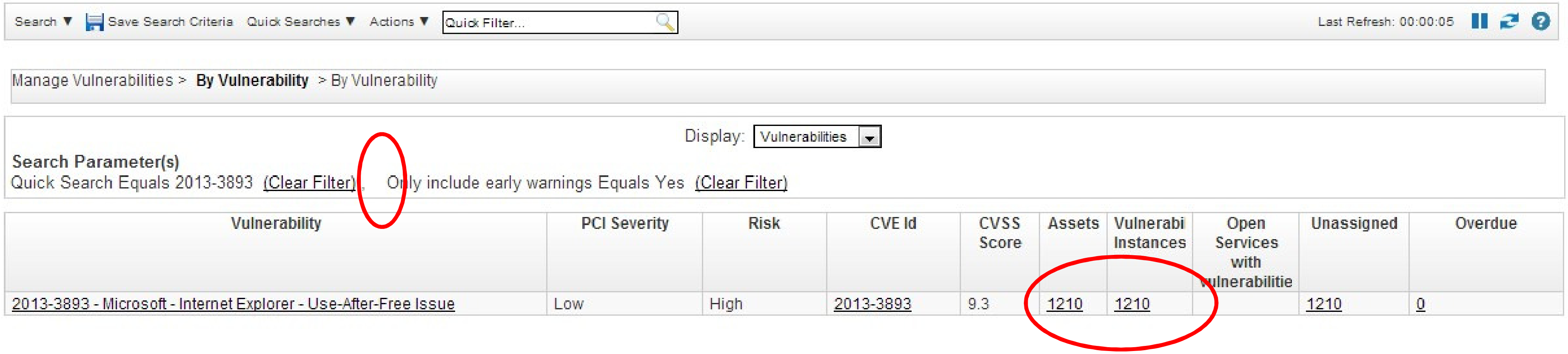
USE CASE: IE 0-DAY VULNERABILITY

IE Zero day announced !

- Real example, from a real customer
- The background
  - 2014-3893 Use-after-free vulnerability
  - Most versions of IE are affected
  - Exploits are available and have been active on the internet at malicious web sites for a week
  - Metasploit release an exploit kit within 1 week
- The Challenge
  - 10000’s of windows assets in the enterprise
  - What ones are vulnerable ?
    - Re scan the network – how long will that take ?
    - Need answers now !
  - Length of time to patch
    - Must prioritise
    - What ones do I patch first ?

How did QVM and Security Intelligence help – Stage 1

- No need to re-scan
- QVM’s early alerts correlated data from the last scan with the zero data vulnerability information to immediately create early warning vulnerabilities



Manage Vulnerabilities > **By Vulnerability** > By Vulnerability

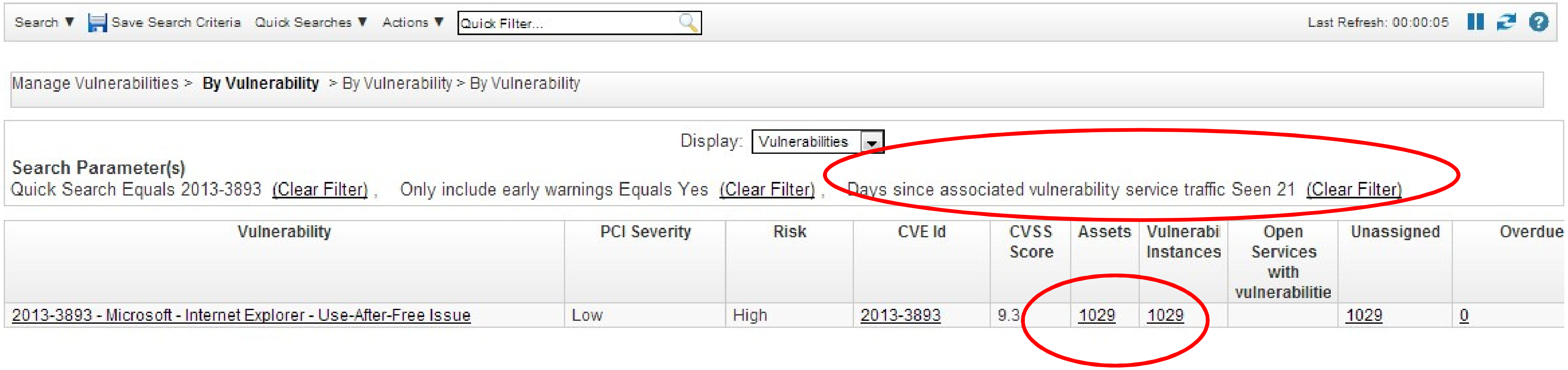
Search Parameter(s)
Quick Search Equals 2013-3893 (Clear Filter), Only include early warnings Equals Yes (Clear Filter)

Vulnerability	PCI Severity	Risk	CVE Id	CVSS Score	Assets	Vulnerabi Instances	Open Services with vulnerabilitie	Unassigned	Overdue
2013-3893 - Microsoft - Internet Explorer - Use-After-Free Issue	Low	High	2013-3893	9.3	1210	1210		1210	0

- Time saved 1-2 days in scanning time

How did QVM and Security Intelligence help – Stage 2

- Patch them all ?
- Not yet. Prioritize – don’t patch assets were there has been no web traffic in the last 30 days
- QVM correlates QFlow Layer 7 traffic with vulnerabilities on assets to remove those without associated traffic



Manage Vulnerabilities > **By Vulnerability** > By Vulnerability > By Vulnerability

Display: Vulnerabilities

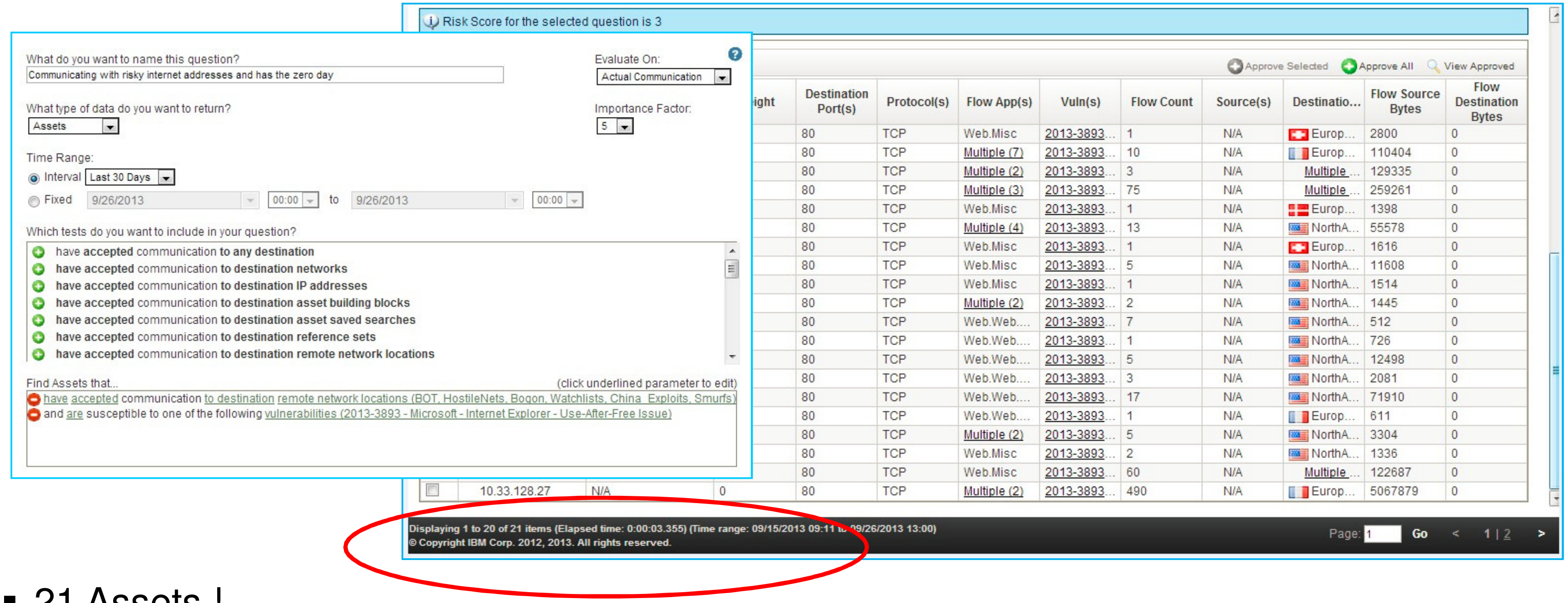
Search Parameter(s)
Quick Search Equals 2013-3893 (Clear Filter) , Only include early warnings Equals Yes (Clear Filter) , Days since associated vulnerability service traffic Seen 21 (Clear Filter)

Vulnerability	PCI Severity	Risk	CVE Id	CVSS Score	Assets	Vulnerabi Instances	Open Services with vulnerabilitie	Unassigned	Overdue
2013-3893 - Microsoft - Internet Explorer - Use-After-Free Issue	Low	High	2013-3893	9.3	1029	1029		1029	0

- Time saved 15%-20% reduction in patching time
- Not wasting time and effort on patching assets where there has been no web traffic

How did QVM and Security Intelligence help – Stage 3

- Patch the remainder ?
- Not yet... Exploits of this vulnerability live in malicious web sites.
- QVM and QRM and the QRadar Threat Intelligence feed can highlight those assets with the vulnerability that have visited potentially malicious web sites in the last month



Risk Score for the selected question is 3

What do you want to name this question?
Communicating with risky internet addresses and has the zero day

Evaluate On: Actual Communication

What type of data do you want to return?
Assets

Importance Factor: 5

Time Range:
● Interval Last 30 Days
○ Fixed 9/26/2013 00:00 to 9/26/2013 00:00

Which tests do you want to include in your question?
- have **accepted** communication **to any destination**
- **have accepted** communication **to destination networks**
- **have accepted** communication **to destination IP addresses**
- **have accepted** communication **to destination asset building blocks**
- **have accepted** communication **to destination asset saved searches**
- **have accepted** communication **to destination reference sets**
- **have accepted** communication **to destination remote network locations**

Find Assets that... (click underlined parameter to edit)
- have accepted communication to destination remote network locations (BOT, HostileNets, Bogon, Watchlists, China_Exploits, Smurfs)
- and are susceptible to one of the following vulnerabilities (2013-3893 - Microsoft - Internet Explorer - Use-After-Free Issue)

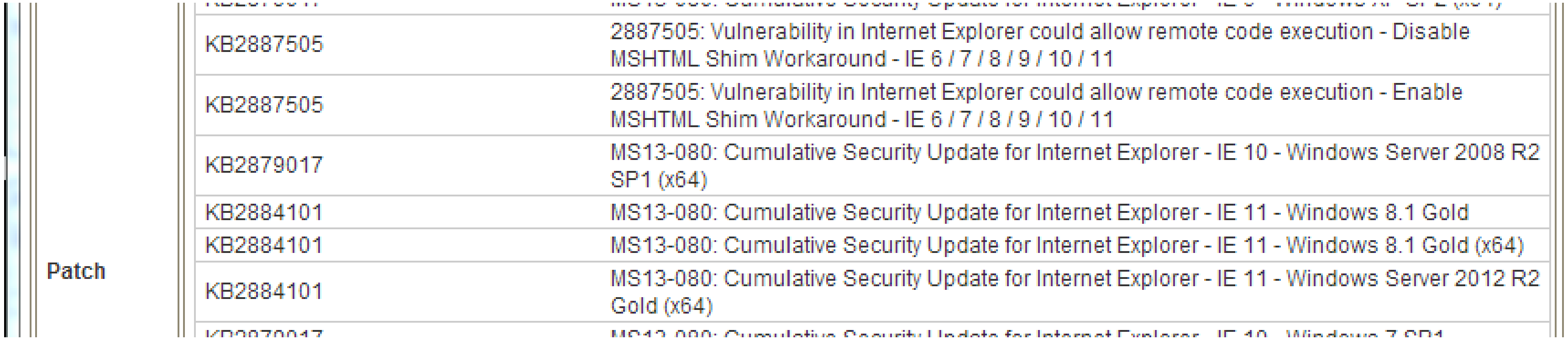
			ight	Destination Port(s)	Protocol(s)	Flow App(s)	Vuln(s)	Flow Count	Source(s)	Destinatio...	Flow Source Bytes	Flow Destination Bytes
				80	TCP	Web.Misc	2013-3893...	1	N/A	Europ...	2800	0
				80	TCP	Multiple (7)	2013-3893...	10	N/A	Europ...	110404	0
				80	TCP	Multiple (2)	2013-3893...	3	N/A	Multiple ...	129335	0
				80	TCP	Multiple (3)	2013-3893...	75	N/A	Multiple ...	259261	0
				80	TCP	Web.Misc	2013-3893...	1	N/A	Europ...	1398	0
				80	TCP	Multiple (4)	2013-3893...	13	N/A	NorthA...	55578	0
				80	TCP	Web.Misc	2013-3893...	1	N/A	Europ...	1616	0
				80	TCP	Web.Misc	2013-3893...	5	N/A	NorthA...	11608	0
				80	TCP	Web.Misc	2013-3893...	1	N/A	NorthA...	1514	0
				80	TCP	Multiple (2)	2013-3893...	2	N/A	NorthA...	1445	0
				80	TCP	Web.Web....	2013-3893...	7	N/A	NorthA...	512	0
				80	TCP	Web.Web....	2013-3893...	1	N/A	NorthA...	726	0
				80	TCP	Web.Web....	2013-3893...	5	N/A	NorthA...	12498	0
				80	TCP	Web.Web....	2013-3893...	3	N/A	NorthA...	2081	0
				80	TCP	Web.Web....	2013-3893...	17	N/A	NorthA...	71910	0
				80	TCP	Web.Web....	2013-3893...	1	N/A	Europ...	611	0
				80	TCP	Multiple (2)	2013-3893...	5	N/A	NorthA...	3304	0
				80	TCP	Web.Misc	2013-3893...	2	N/A	NorthA...	1336	0
				80	TCP	Web.Misc	2013-3893...	60	N/A	Multiple ...	122687	0
☐	10.33.128.27	N/A	0	80	TCP	Multiple (2)	2013-3893...	490	N/A	Europ...	5067879	0

Displaying 1 to 20 of 21 items (Elapsed time: 0:00:03.355) (Time range: 09/15/2013 09:11 to 09/26/2013 13:00)
© Copyright IBM Corp. 2012, 2013. All rights reserved.

- 21 Assets !
- Time saved >90% reduction in patching time – ~5 days
- Not wasting time and effort on patching assets where assets have been talking to trusted sites

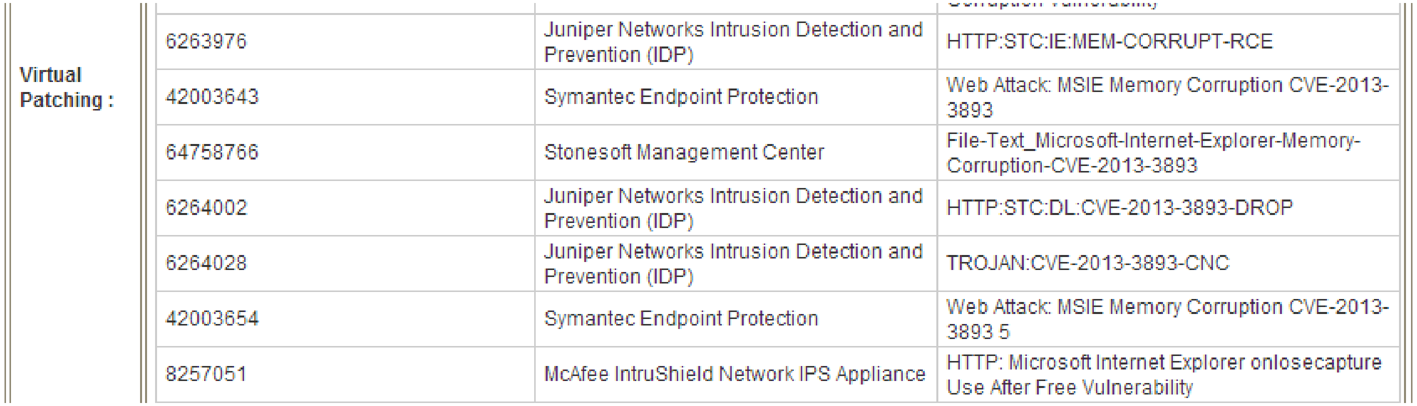
What action to take next ?
Apply virtual patch & vendor patch

- Patch to apply – QVM has the answer



Patch	KB2887505	2887505: Vulnerability in Internet Explorer could allow remote code execution - Disable MSHTML Shim Workaround - IE 6 / 7 / 8 / 9 / 10 / 11
	KB2887505	2887505: Vulnerability in Internet Explorer could allow remote code execution - Enable MSHTML Shim Workaround - IE 6 / 7 / 8 / 9 / 10 / 11
	KB2879017	MS13-080: Cumulative Security Update for Internet Explorer - IE 10 - Windows Server 2008 R2 SP1 (x64)
	KB2884101	MS13-080: Cumulative Security Update for Internet Explorer - IE 11 - Windows 8.1 Gold
	KB2884101	MS13-080: Cumulative Security Update for Internet Explorer - IE 11 - Windows 8.1 Gold (x64)
	KB2884101	MS13-080: Cumulative Security Update for Internet Explorer - IE 11 - Windows Server 2012 R2 Gold (x64)
	KB2879017	MS13-080: Cumulative Security Update for Internet Explorer - IE 10 - Windows 7 SP1

- IPS signature to enable – QVM has the answer



Virtual Patching :	6263976	Juniper Networks Intrusion Detection and Prevention (IDP)	HTTP:STC:IE:MEM-CORRUPT-RCE
	42003643	Symantec Endpoint Protection	Web Attack: MSIE Memory Corruption CVE-2013-3893
	64758766	Stonesoft Management Center	File-Text_Microsoft-Internet-Explorer-Memory-Corruption-CVE-2013-3893
	6264002	Juniper Networks Intrusion Detection and Prevention (IDP)	HTTP:STC:DL:CVE-2013-3893-DROP
	6264028	Juniper Networks Intrusion Detection and Prevention (IDP)	TROJAN:CVE-2013-3893-CNC
	42003654	Symantec Endpoint Protection	Web Attack: MSIE Memory Corruption CVE-2013-3893 5
	8257051	McAfee IntruShield Network IPS Appliance	HTTP: Microsoft Internet Explorer onlosecapture Use After Free Vulnerability

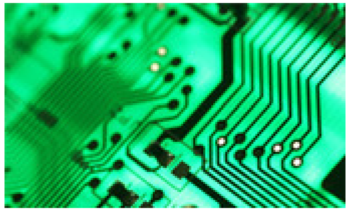
Learn more about IBM Security Intelligence and Analytics

Visit the
IBM Security Intelligence Website

Watch the videos on the
IBM Security Intelligence YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity



Built in. Not bolted on.

Smarter security solutions from IBM

Q&A

IBM Institute for Advanced Security

Where global security leaders go to share intelligence and collaborate

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