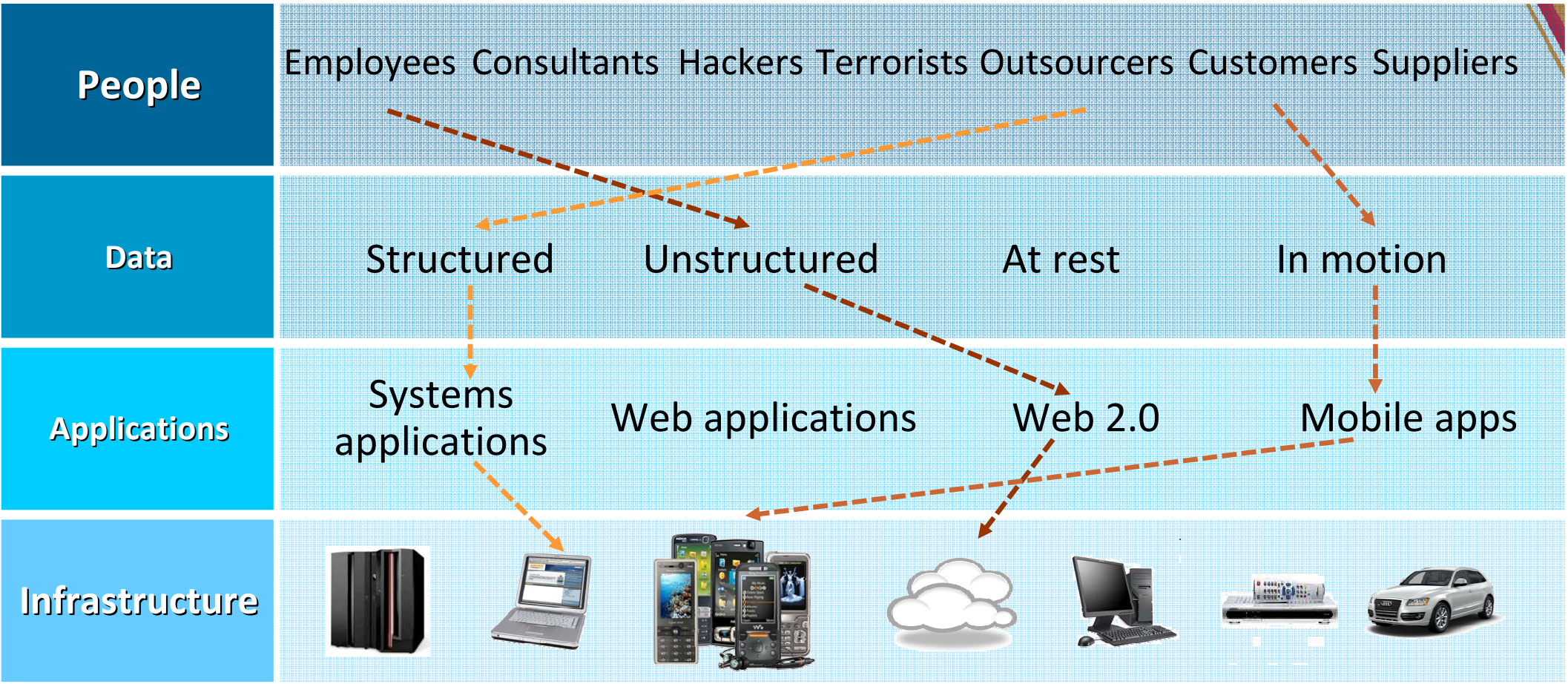
SIEM - Security Intelligence

Alfonso Ponticelli
IBM Security Systems

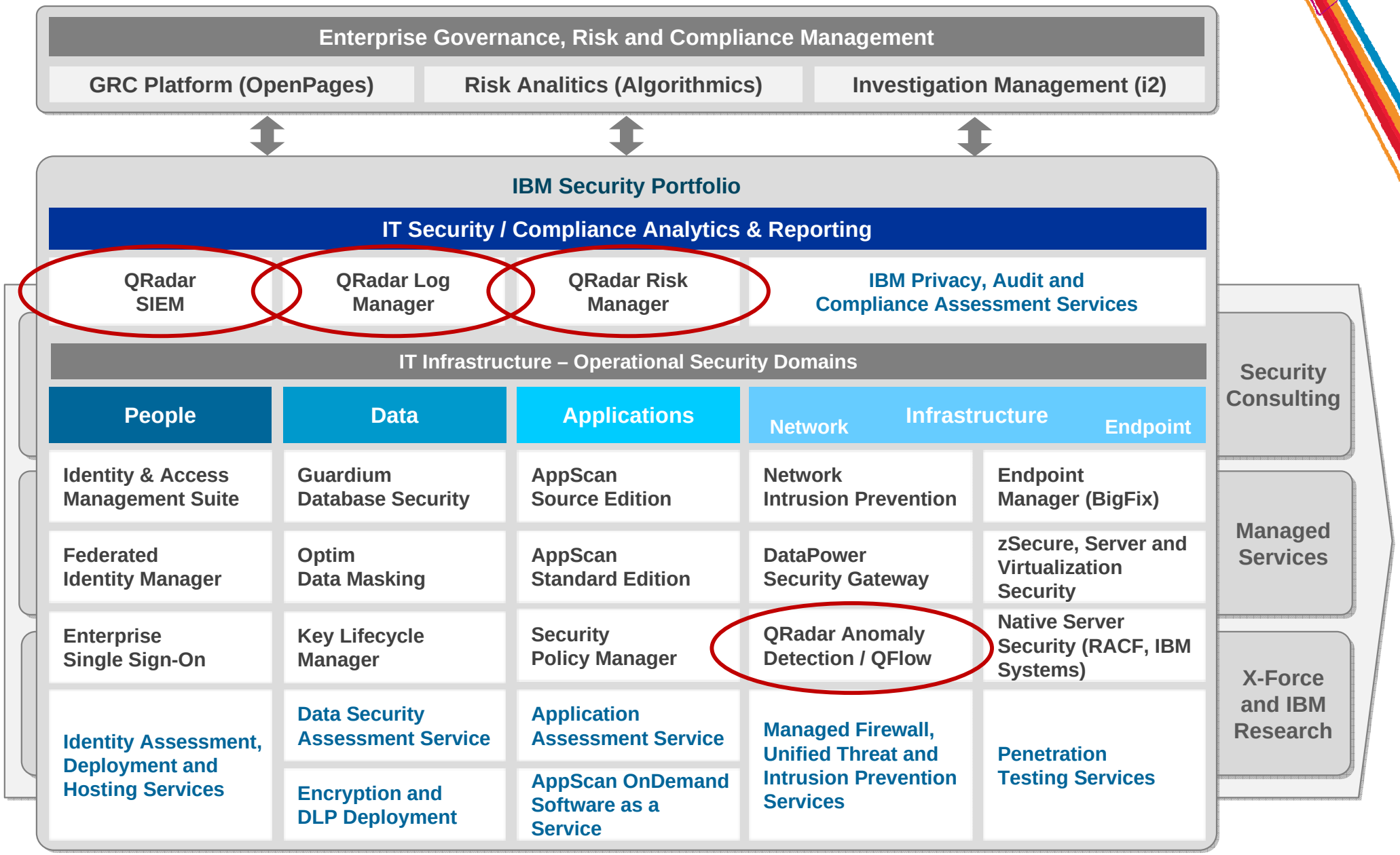
PCTY2012
Pulse Comes to You

Optimizing the World's Infrastructure
[May, 15° Rome]

Security: A complex, four- dimensional puzzle



Total Visibility: Product Portfolio, Services and Research



Products Services

PCTY2012

World's Infrastructure

Q1Labs

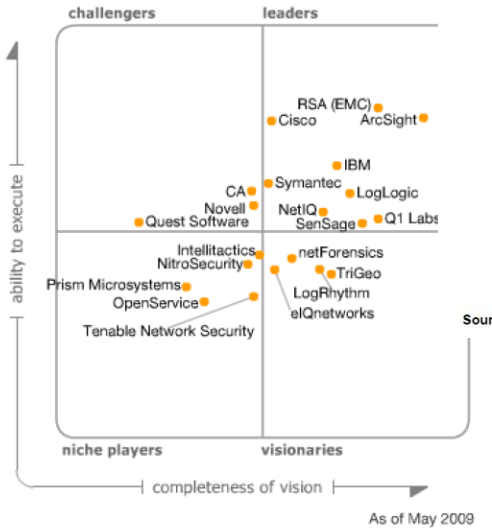
- ✓ **Who they are:**
  - Innovative Security Intelligence software company
  - Largest independent SIEM vendor
  - Leader in Gartner 2010 and 2009 Magic Quadrants

- ✓ **Award winning solutions:**
  - Family of next-generation Risk Management, Log Management, SIEM, security intelligence solutions

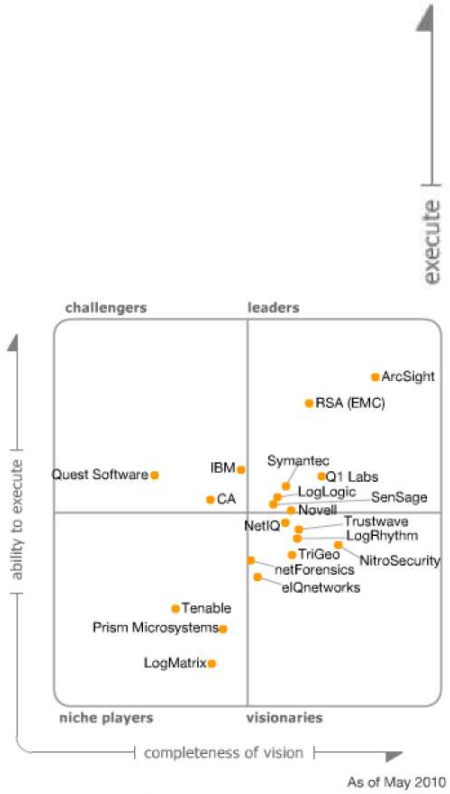
- ✓ **Executing, growing rapidly:**
  - +1600 customers worldwide
  - Five-year average revenue growth +70%
  - North America, EMEA and Asia Pacific

Consistent Leadership Progress

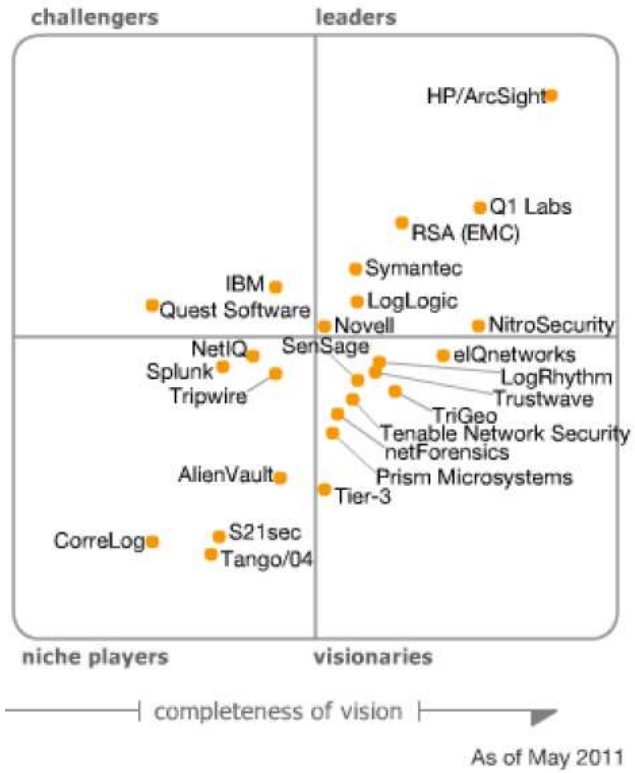
Source: Gartner (May 2008)



Source: Gartner (May 2009)

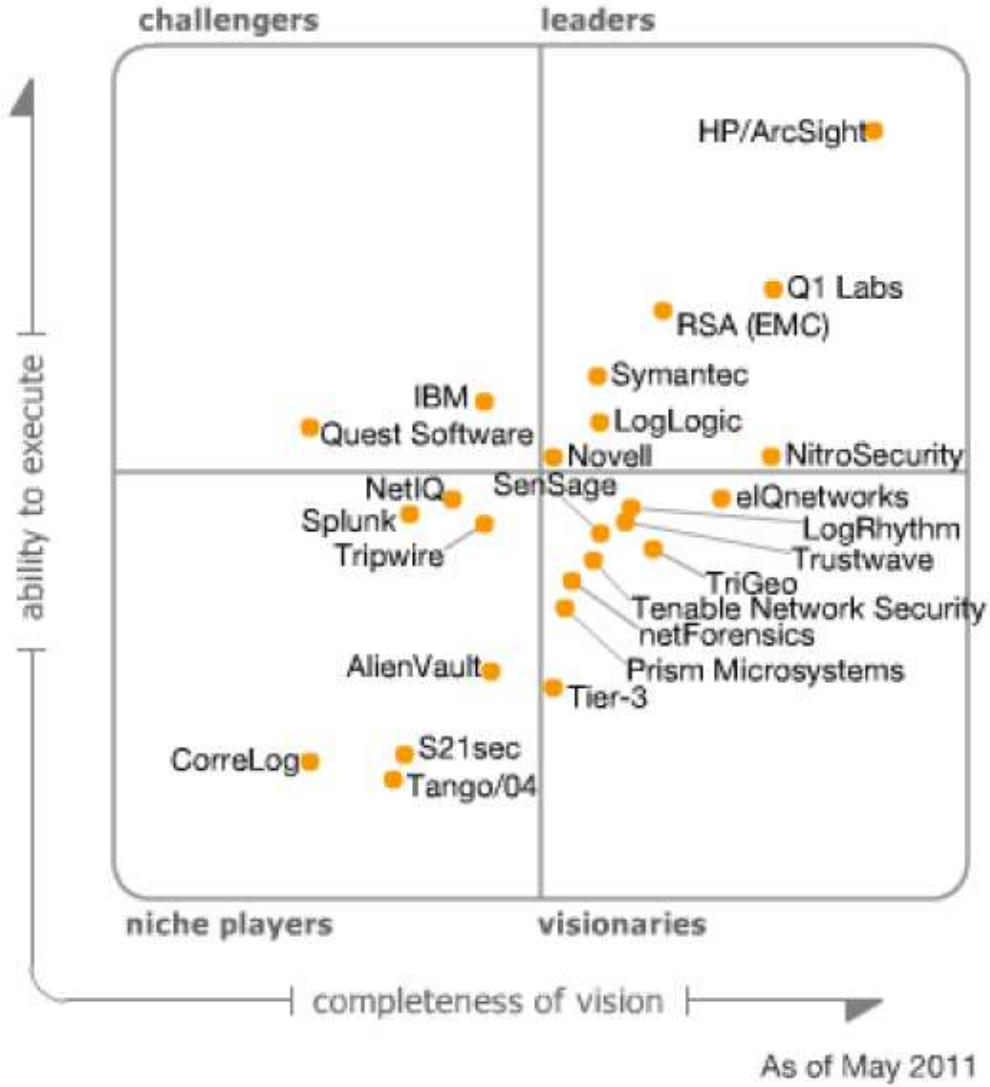


Source: Gartner (May 2010)



Clear Leadership 2011 SIEM MQ

Figure 1. Magic Quadrant for Security Information and Event Management



Solving Customer Business Pains that Point Products Can't Address

Detecting threats others miss

- Arm yourself with total security intelligence

Consolidating data silos

- Collect, correlate and report on data in one integrated solution

Detecting insider fraud

- Next generation SIEM with identity correlation

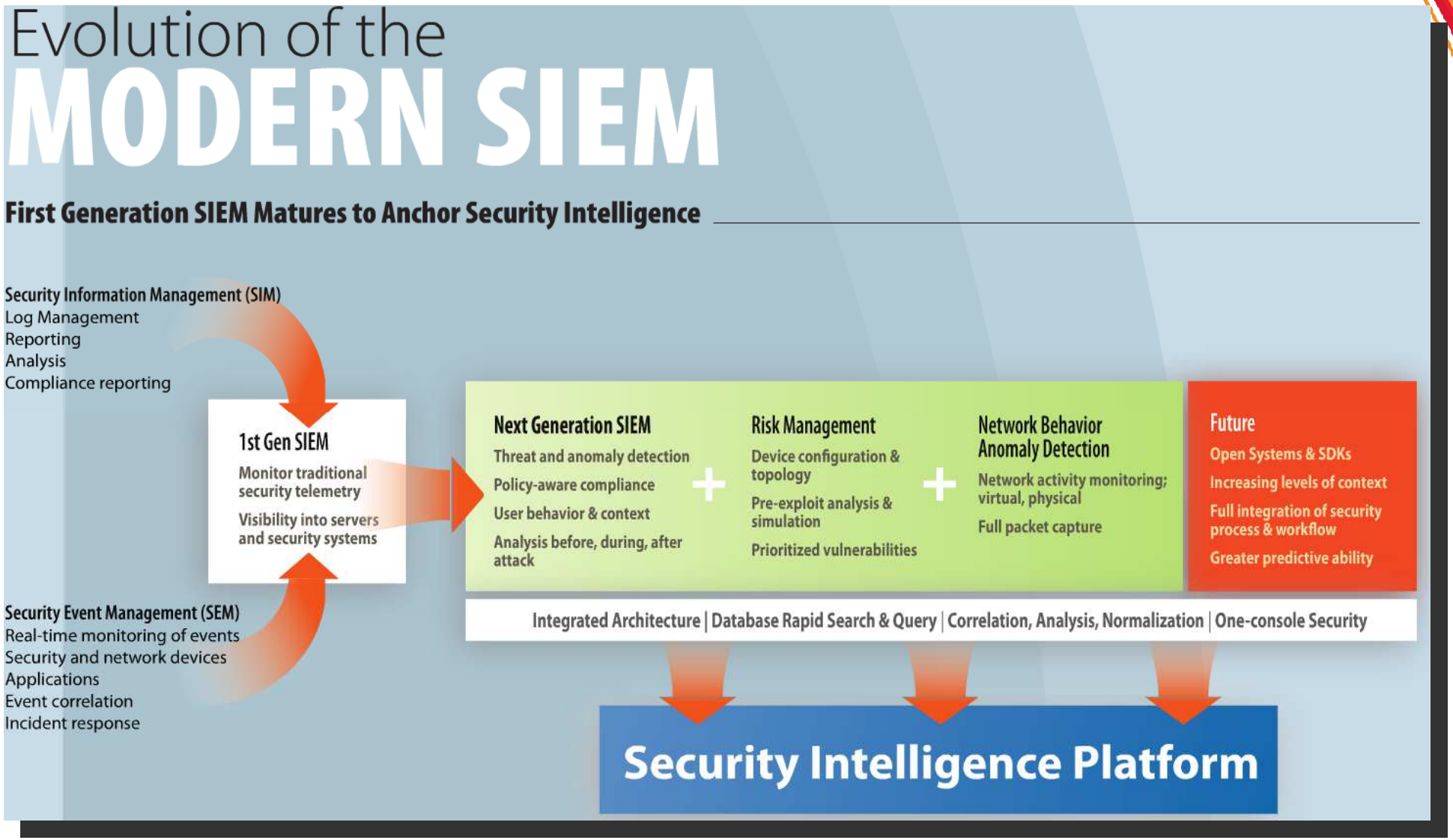
Predicting risks to your business

- Full life cycle of compliance and risk management for network and security infrastructures

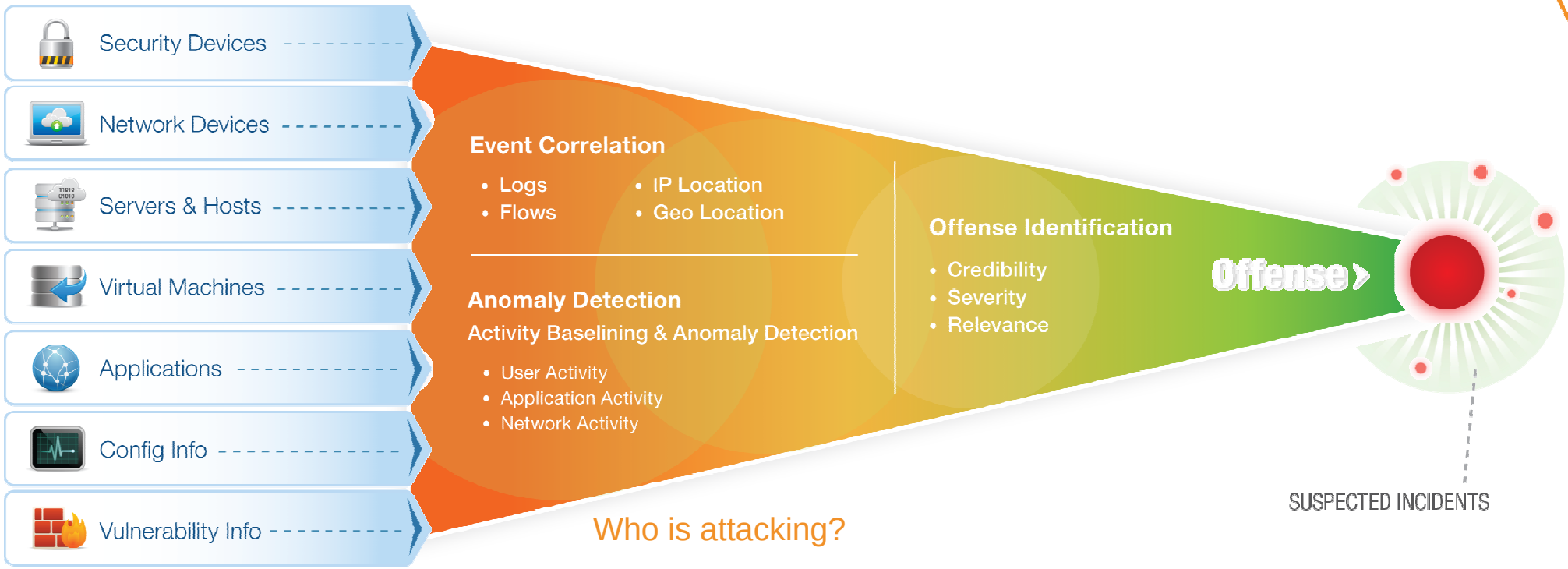
Exceeding regulation mandates

- Automated data collection and configuration audits

QRadar – SIEM 2st Generation



QRadar Security Intelligence Platform: helps provide security teams with the intelligence they need to act



Who is attacking?

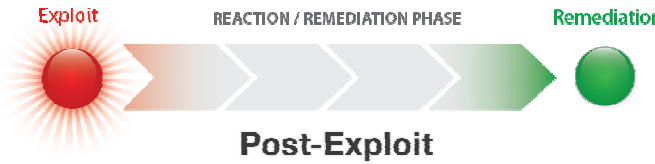
What is being attacked?

What is the business impact?

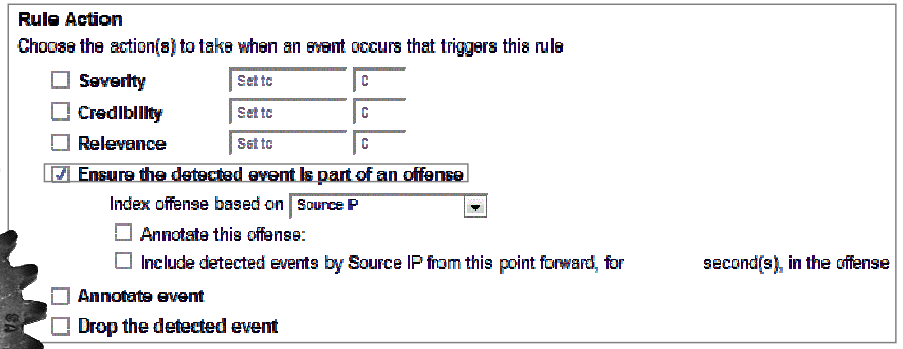
Where do I investigate?

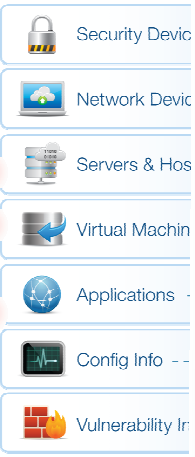
Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Offenses are Real-Time



Post-Exploit





Event Correlation

- Logs
- Flows
- IP Location
- Geo Location

Anomaly Detection

Activity Baselining & Anomaly Detection

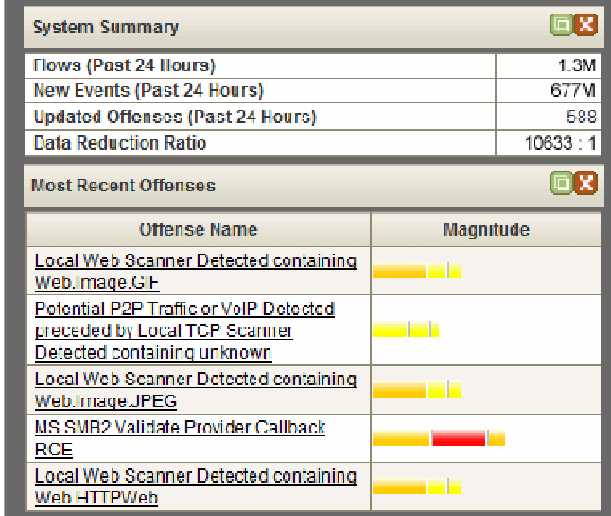
- User Activity
- Application Activity
- Network Activity

Rules Engine

Offenses

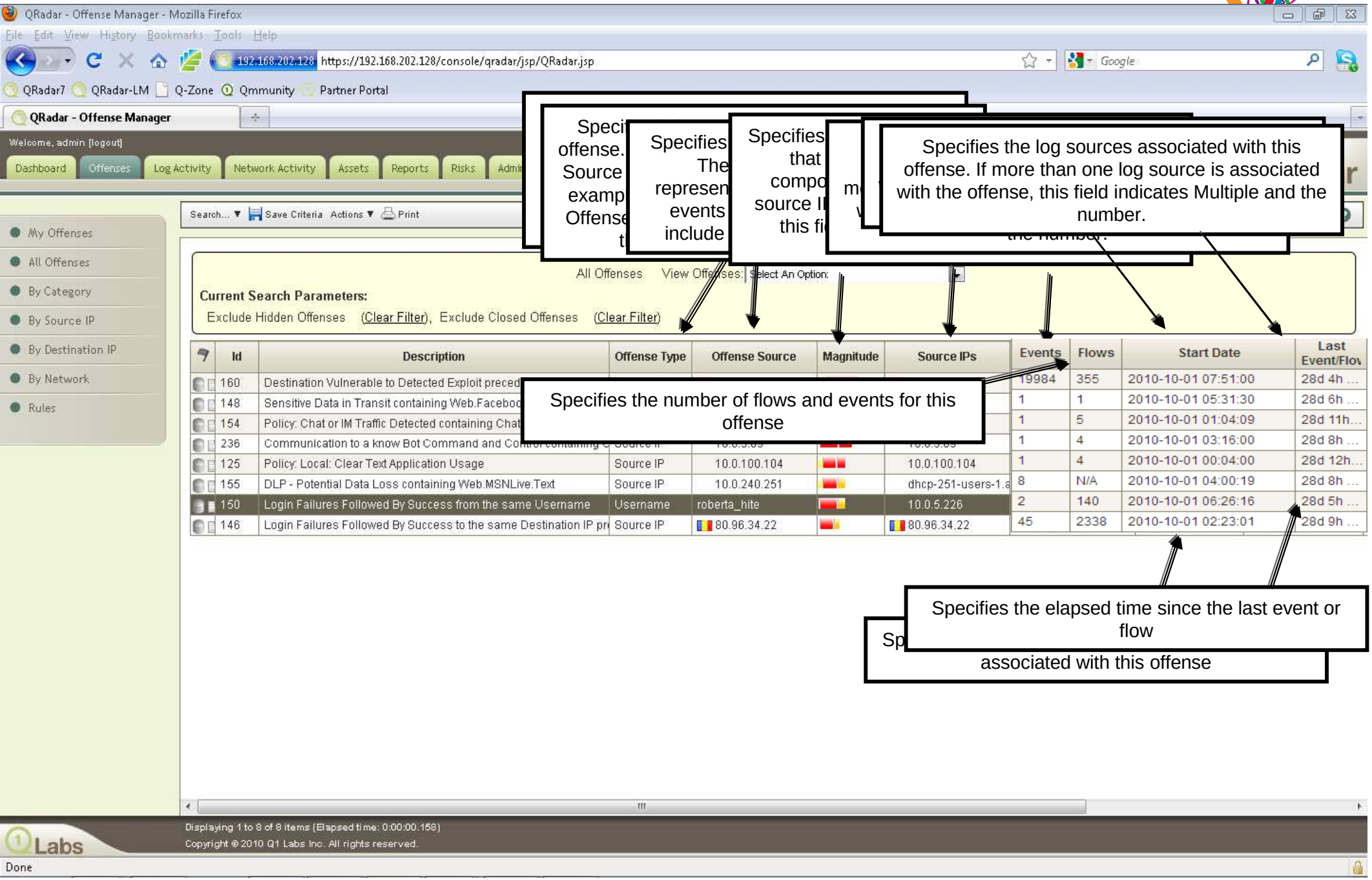
ID	Description	Attacker(s)/Src	Magnitude	Target(s)/Dest
001	Remote FTP Scanner detected, Excessive Firewall Denies	217.64.100.162	8	Multiple (99)
002	Excessive Login Faliures, Login Success	81.240.89.210	9	10.100.50.81

The Key to Data Management:

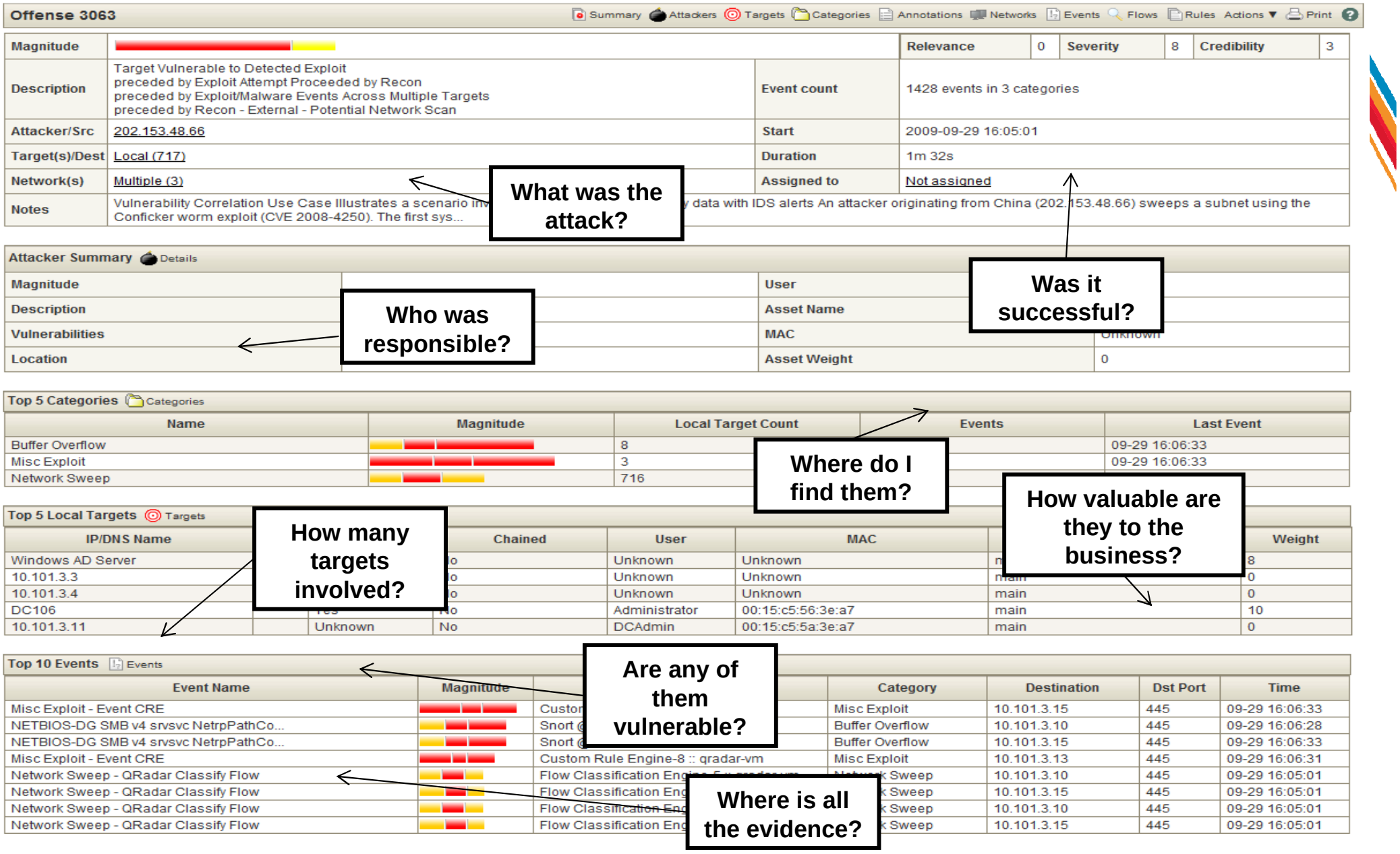


Reduction and Prioritization

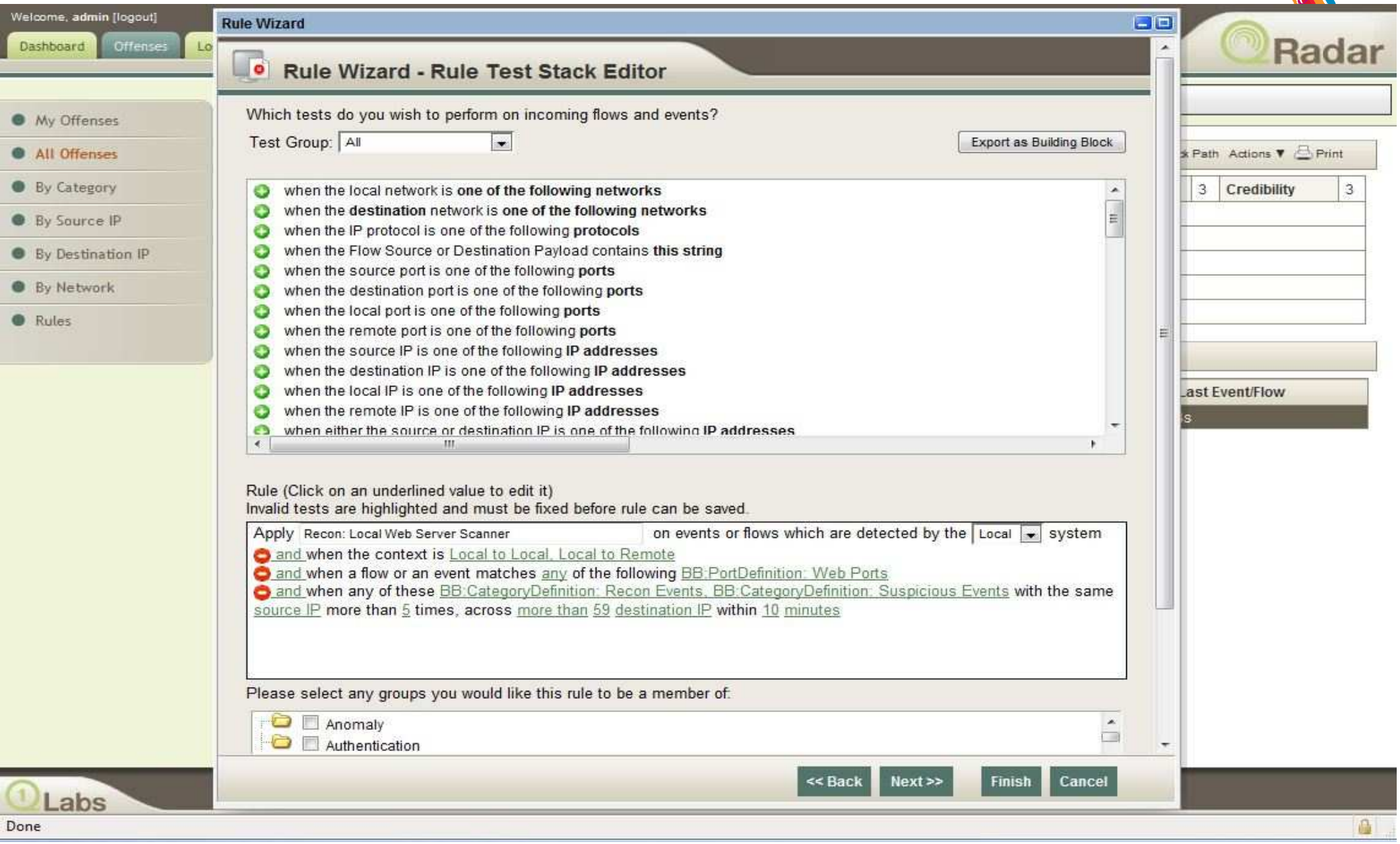
QRadar Offense Management



QRadar Offense Management



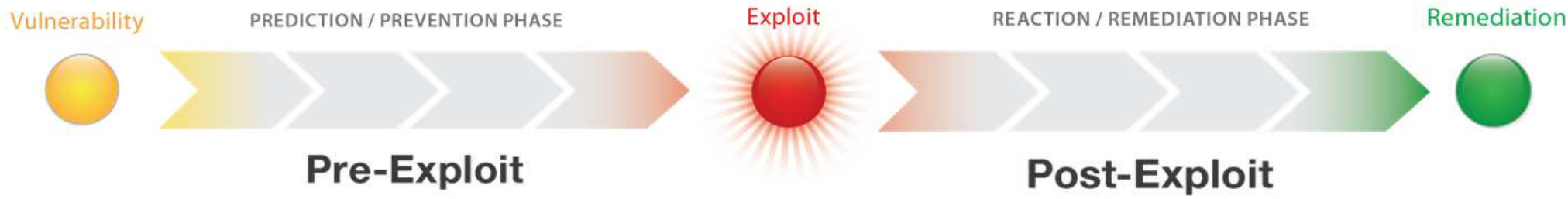
Rule Modification - Editor



Attack Sophistication

IBM is helping clients combat advanced threats with pre- and post-exploit intelligence and action

- What are the external and internal threats?
- Are we configured to protect against these threats?
- What is happening right now?
- What was the impact?



Prediction & Prevention

Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

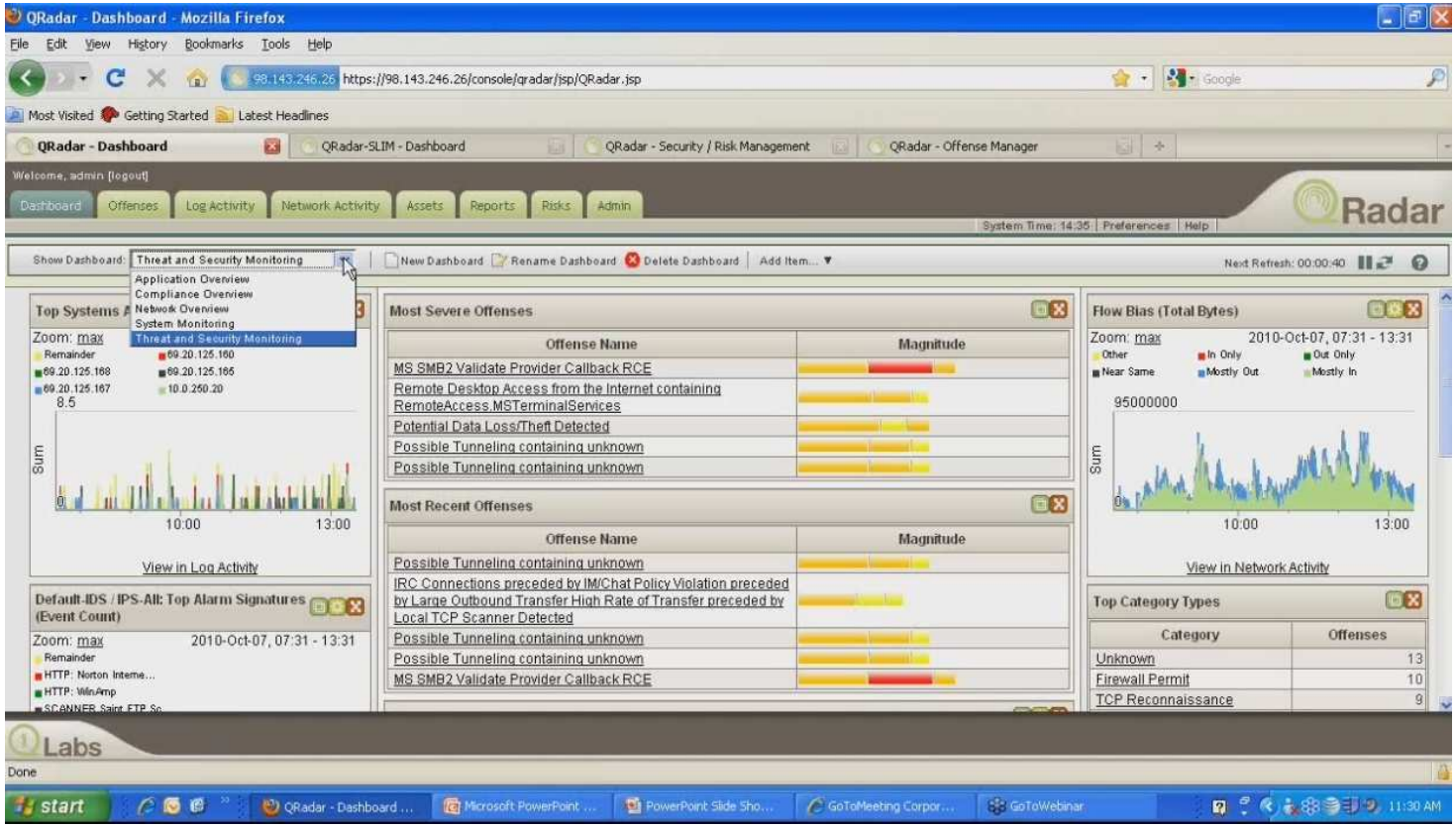
Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

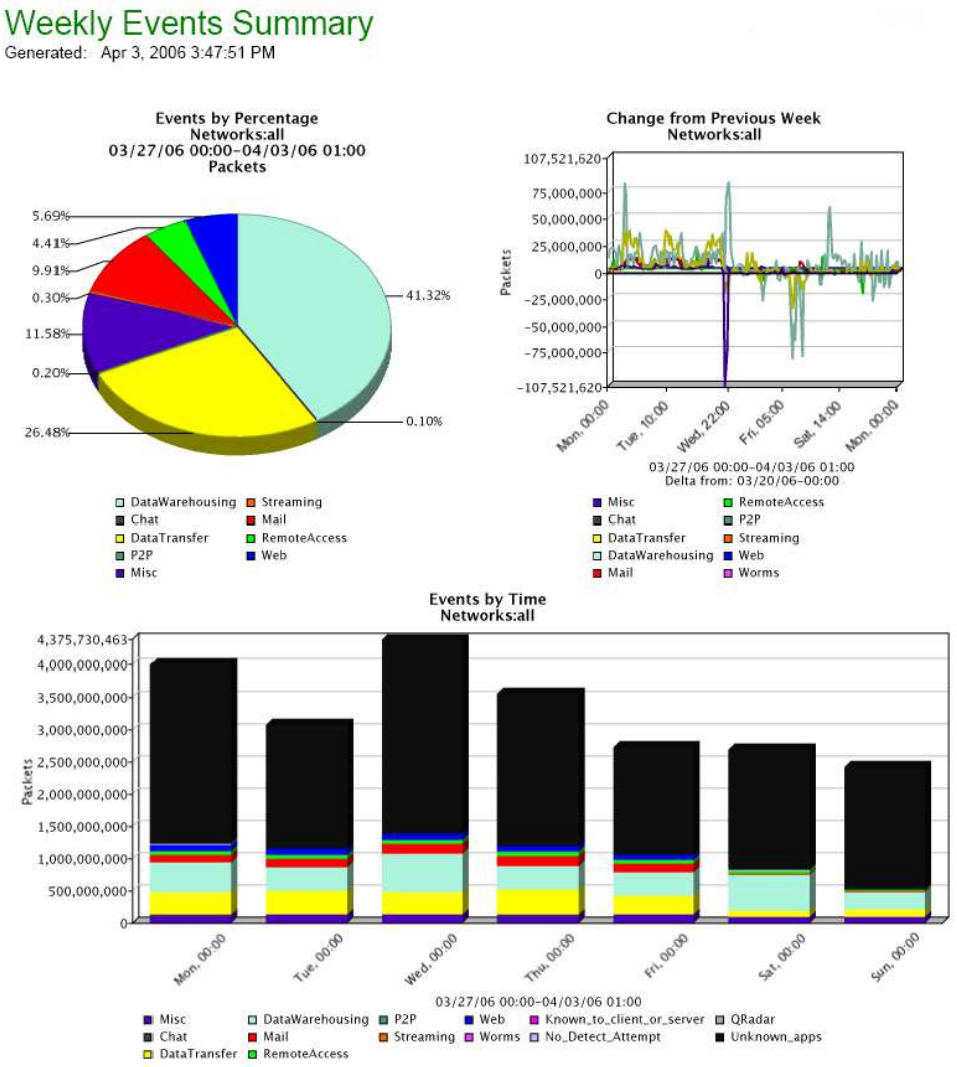
The QRadar Security Intelligence Solutions Deploy, Expand at Your Pace

- Log Management
- SIEM/SEM
- Risk Management
- Scale
- Visibility/ Network Activity

One Console Security



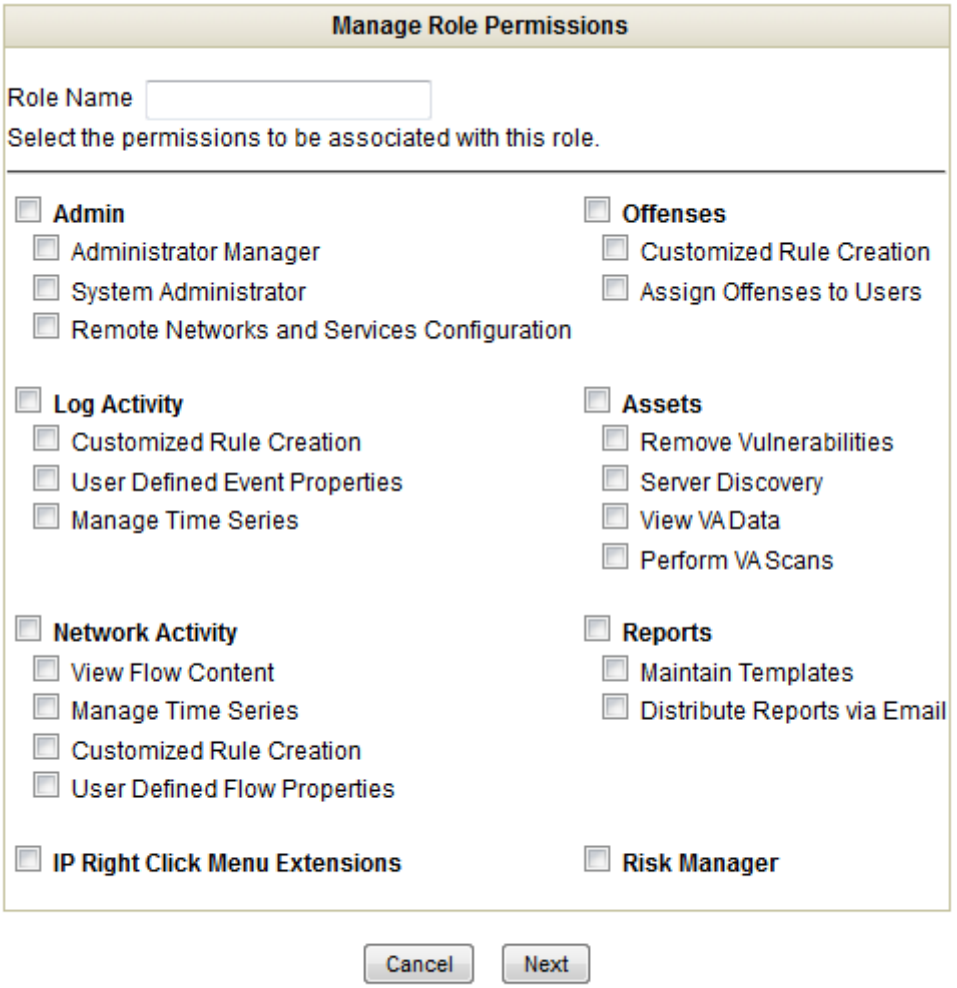
Reporting



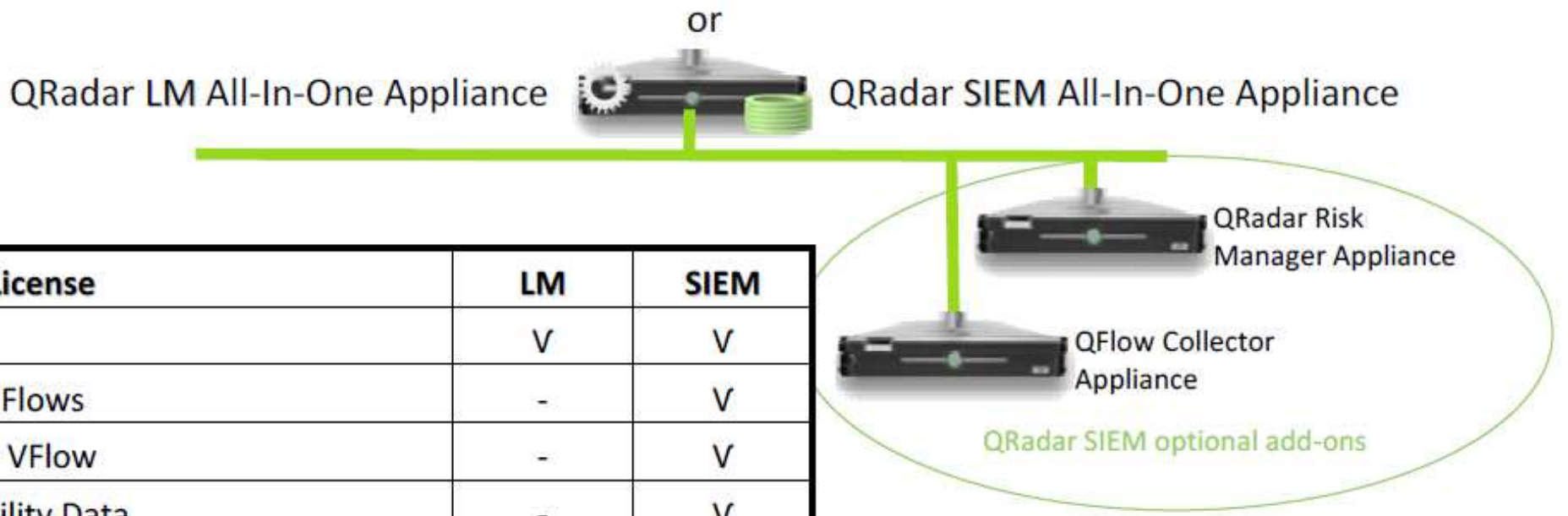
- ✓ All information collected is available for reports
- ✓ Thousands out-of-the-box report templates for compliance and device reporting
- ✓ Fully customizable reporting engine: creating, branding and scheduling delivery of reports
- ✓ Compliance reporting packages for PCI, SOX, FISMA, GLBA, and HIPAA
- ✓ Reports based on control frameworks: NIST, ISO, and CoBIT

Manage User Roles Function

- ✓ Best Practice: Create roles before users
- ✓ Roles must be created for user accounts that will not have full administrative access
- ✓ To create a role, use the Manage User Roles function in the Administration Console
- ✓ Select the check boxes for the functionality you want
- ✓ You can have an unlimited number of roles

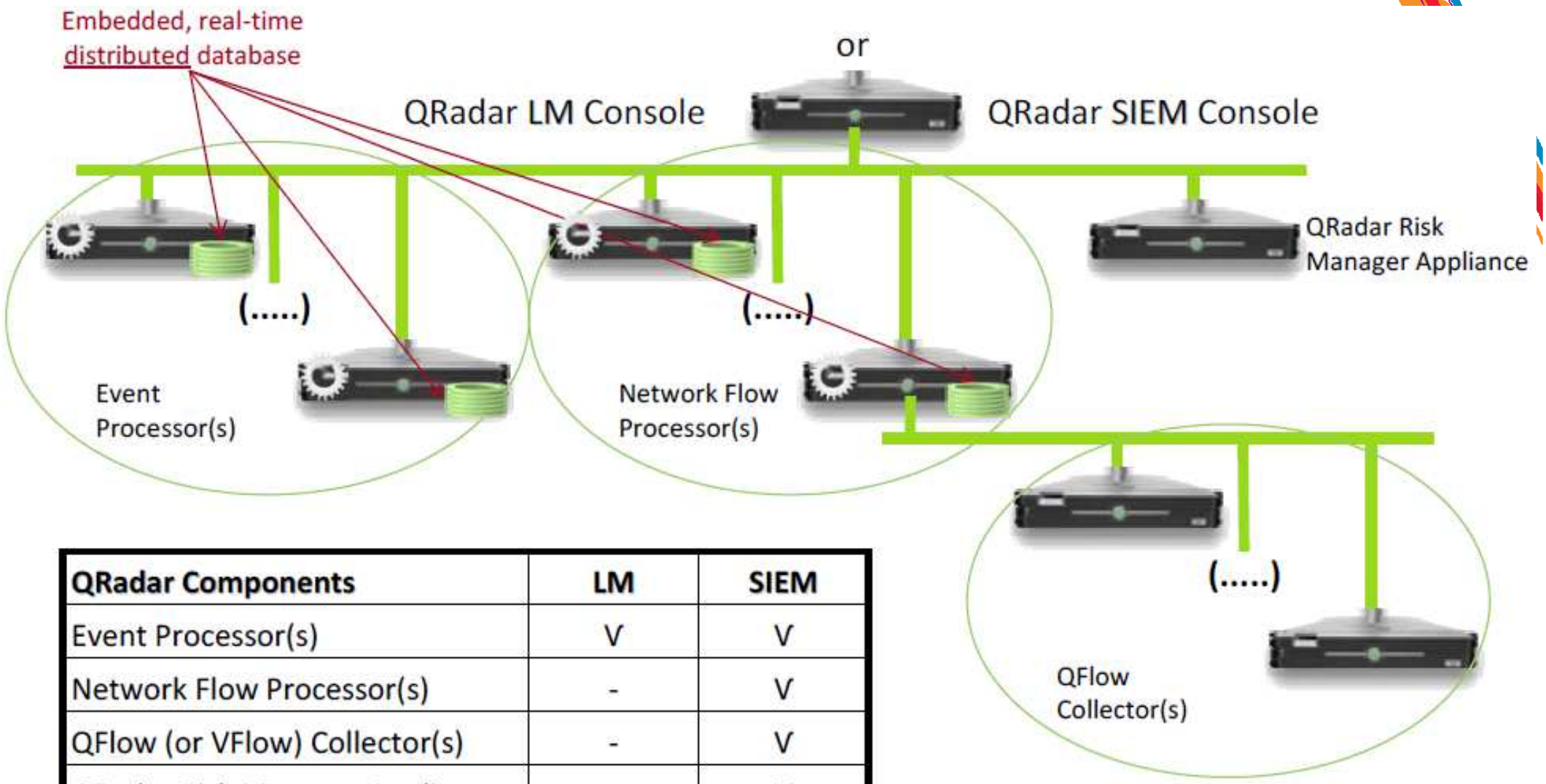


QRadar Architecture – “All In One”



QRadar License	LM	SIEM
Events	V	V
Network Flows	-	V
QFlow or VFlow	-	V
Vulnerability Data	-	V
Log Management	V	V
Correlation Engine	V	V
Offenses	-	V
Risk Manager Option	-	V
Upgradable to SIEM	V	N/A
Migration to Distributed Architecture	V	V
Max EPS	5,000	5,000
Max FPI	N/A	200,000

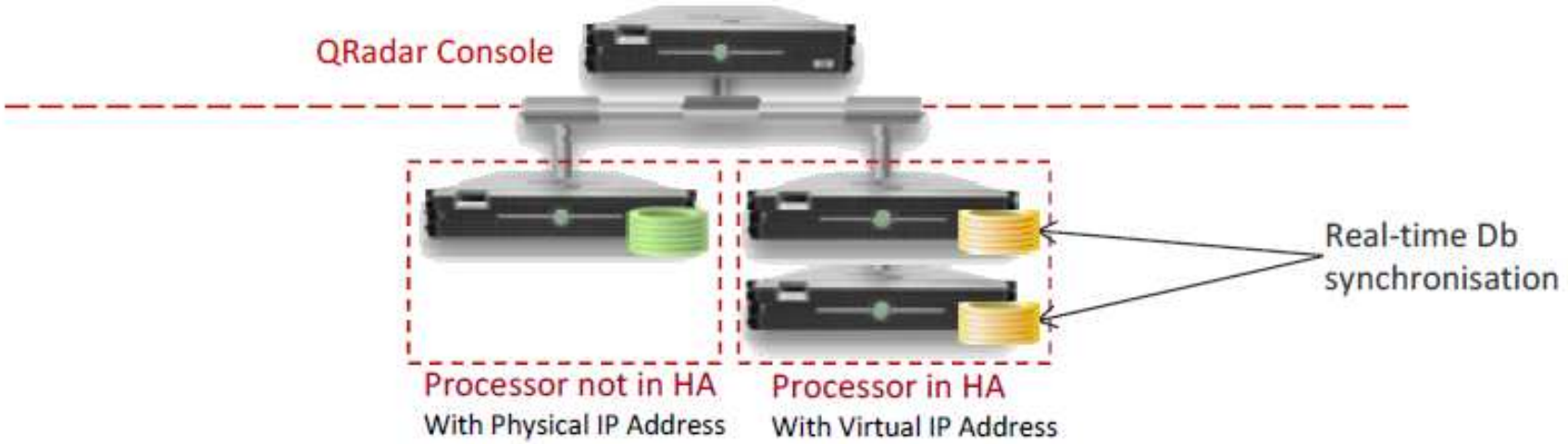
QRadar Architecture – Distributed Architecture



QRadar Components	LM	SIEM
Event Processor(s)	V	V
Network Flow Processor(s)	-	V
QFlow (or VFlow) Collector(s)	-	V
QRadar Risk Manager Appliance	-	V
Max EPS	Unlimited*	Unlimited*
Max FPI	N/A	Unlimited*

* Unlimited as long as enough processors are deployed to support the required volume of events/flows.

QRadar Architecture – High Availability



E x a m p l e : Distributed Architecture
with 1 Processor and 2 Processors in HA

Appliance Specifications Matrix

All in One and Console Appliances

	2000	2100	3100/Console	LM/Console	3105	3124
Dimensions	1U:30.4" D x 16.7" W x	2U:26.8" D x 17.44" W x 3.4" H			2U:26.7" D x 17.2" W x 3.4" H	2U:26.7" D x 17.2" W x 3.4" H
CPU	Quad Core Xeon with 8MB Cache, 2.4GHz, 5.86 GT/s QPI, TurboHT	2 Quad Core Xeon 2.4GHz 8M Cache, Turbo, HT, 1066MHz Max Mem			2 Quad Core Xeon with 2.4GHz 8M Cache, Turbo, HT, 1056MHz Max Mem	2 Intel Xeon X5670, 2.93Ghz, 12M Cache,Turbo, HT, 1333MHz Max Mem
Memory	12GB	24GB	24GB		24GB	64GB
Storage	2x500GB SATA II Drives/RAID 1 (500GB)	6x500GB SATA II Drives/RAID10 (1.5TB)	6x1 TB SATA II Drives/RAID10 (3 TB)		8x1TB SATA II Drives/RAID 5 (6.2 TB)	12x2TB SATA II Drives/RAID 5 (16 TB)
Network Interfaces	4x10/100/1000 CX				2x10/100/1000 CX	2x10/100/1000 CX
Power	Dual Redundant Auto Sensing 110/220 Volt Power Supply (670 Watt)	Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)			Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)	Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)
	Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 175.5 watts 598.9 btu/hTotal Input Current: 1.6 ampsSound Power Level: 6.2 bels *Airflow Rate: 11.2 l/s 23.7 CFMTotal Weight: 17.7 kg 39.0 lbs	Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 377.6 watts 1288.4 btu/hTotal Input Current: 3.5 ampsSound Power Level: 6.1 bels *Airflow Rate: 17.6 l/s 37.4 CFMTotal Weight: 26.1 kg 57.5 lbs			Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 354.8 watts 1210.7 btu/hTotal Input Current: 3.3 ampsSound Power Level: 0.0 bels * Total Weight: 34.5 kg 76.1 lbs	Configuration Totals for 110 AC Input Voltage and 77°F, Total Input Power: 477 watts 1627.6 btu/h, Total Input Current: 4.4 amps, Sound Power Level: 4.4 bels * Total Weight: 34.5 kg 76.1 lbs
QFlow Traffic Rate	50Mbps	50Mbps	NA	NA	NA	NA
EPS Sustained	200	1000	5000/NA	5000/NA	5000	5000
EPS Burst	50,000				50,000	50,000
Flows Per Interval	15,000	up to 50,000	up to 200,000	NA	up to 200,000	up to 200,000
Event Storage	*3 Weeks	*5 Weeks	*6 Weeks/NA	Up to 41 Wks @ 1000 Avg. EPS	*10 weeks	*10 weeks
Flow Storage	*7 Days			NA	*14 days	*14 days
Views Storage	*6 Weeks			NA	NA on 7.0	NA on 7.0
Network Objects	100	100	1000	1000	1000	1000

Appliance Specifications Matrix

Processor Appliances

	1701	1601/SLIM	1801	1802	1805	1624	1724
Dimensions	2U:26.8" D x 17.44" W x 3.4" H				2U:26.8" D x 17.44" W x 3.4" H	2U:26.7" D x 17.2" W x 3.4" H	
CPU	2 Quad Core Xeon with 2.4GHz 8M Cache, Turbo, HT, 1066MHz Max Mem					2 Intel Xeon X5670, 2.93Ghz, 12M Cache,Turbo, HT, 1333MHz Max Mem	
Memory	12GB			24GB	12GB	64GB	
Storage	6x1TB SATA II Drives/RAID10 (3 TB)		6x500GB SATA II Drives/RAID10 (1.5TB)	6x1 TB SATA II Drives/RAID10 (3 TB)	8x1TB SATA II Drives/RAID 5 (6.2 TB)	12x2TB SATA II Drives/RAID 5 (16 TB)	
Network Interfaces	4x10/100/1000 CX				2x10/100/1000 CX	2x10/100/1000 CX	
Power	Dual Redundant Auto Sensing 110/220 Volt Power Supply (750 Watt)						
	Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 377.6 watts 1288.4 btu/hTotal Input Current: 3.5 ampsSound Power Level: 6.1 bels * Total Weight: 26.1 kg 57.5 lbs				Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 354.8 watts 1210.7 btu/hTotal Input Current: 3.3 ampsSound Power Level: 0.0 bels * Total Weight: 34.5 kg 76.1 lbs	Configuration Totals for 110 AC Input Voltage and 77°F, Total Input Power: 477 watts 1627.6 btu/h, Total Input Current: 4.4 amps, Sound Power Level: 4.4 bels * Total Weight: 34.5 kg 76.1 lbs	
EPS Sustained	NA	Up to 10000*	1000*	5,000	Up to 20,000*	Up to 20,000*	N/A
EPS Burst	NA	75000*	50000*	50000*	75000*	75000*	N/A
Flows Per Interval	Up to 600,000	NA	Up to 50,000	Up to 200,000	NA	N/A	Up to 1.2M*
Event Storage	NA	Up to 16 Weeks @ 2500 EPS	*5 Weeks	10 Weeks @ 1000eps	Up to 90 days @ 10,000 sustained EPS*	Up to 260 days at 10,000 EPS*	
Flow Storage	*3 Weeks	NA	*7 Days	14 Days @ 50,000fpl		Up to 130 days at 1.2M Flows*	
Network Objects	NA	NA	NA	NA	NA	NA	

QFlow Collector Appliances

	1101	1201	1202	1301	1302	1310
Dimensions	1U: Dimensions: 21.5" D x 17.6" W x 1.68" H	1U: Dimensions: 30.4" D x 16.7" W x 1.67" H				
CPU	Quad Core Xeon 2x4MB Cache, 2.40GHz, 1066MHz FSB	Quad Core Xeon with 8MB Cache, 2.4GHz, 5.86 GT/s QPI, TurboHT				
Memory	2GB	6GB				
Storage	NA	NA	NA	NA	NA	NA
Network Interfaces	2x10/100/1000 CX	4x10/100/1000 CX	1x10/100/1000 CX Mngt 4x1000 CX Monitor (Napatech NIC)	1x10/100/1000 CX Mngt 4x1000 SX Monitor (Napatech NIC)	1x10/100/1000 CX Mngt 2x1000 SX Monitor	1x10/100/1000 CX Mngt 2x10GB SR - 850nm or LR - 1310nm (Napatech)
Power	Single power supply (345W)	Dual Redundant Auto Sensing 110/220 Volt Power Supply (670 Watt)				
		Configuration Totals for 110 AC Input Voltage and 77°FTotal Input Power: 185.8 watts 633.9 btu/hTotal Input Current: 1.7 ampsSound Power Level: 6.2 bels *Airflow Rate: 11.2 l/s 23.7 CFMTotal Weight: 17.7 kg 39.0 lbs				
Traffic Rate	50Mbps	200Mbps	2Gbps*	2Gbps*	200Mbps	2Gbps*

questions?