

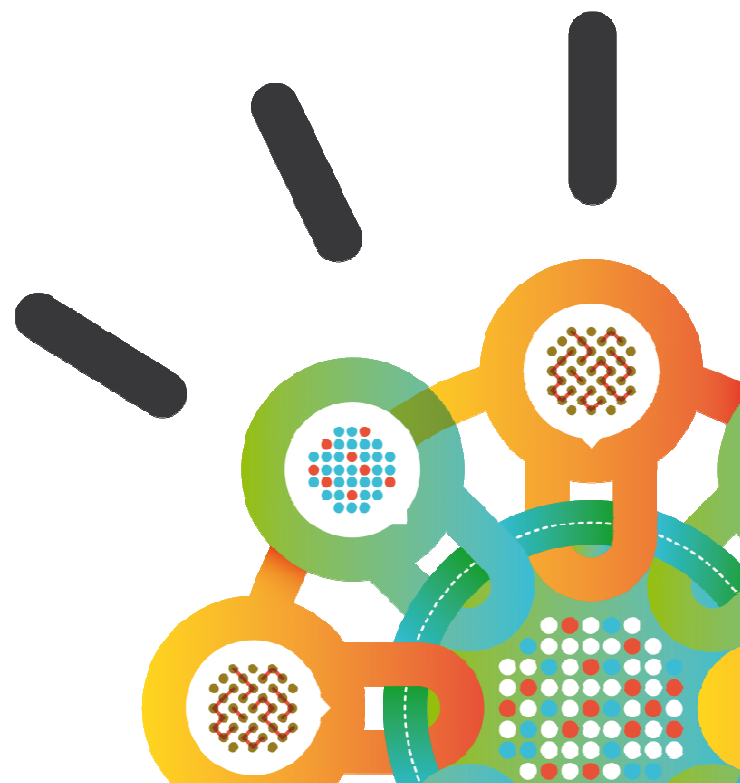
Security Intelligence.
Think Integrated.

QRadar Workshop POT

2014 Rev. 1.002

Introduction & Agenda

Erasmus Volpe
Security Systems



Disclaimer

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

No IBM course material may be reproduced in whole or in part without the prior written permission of IBM.

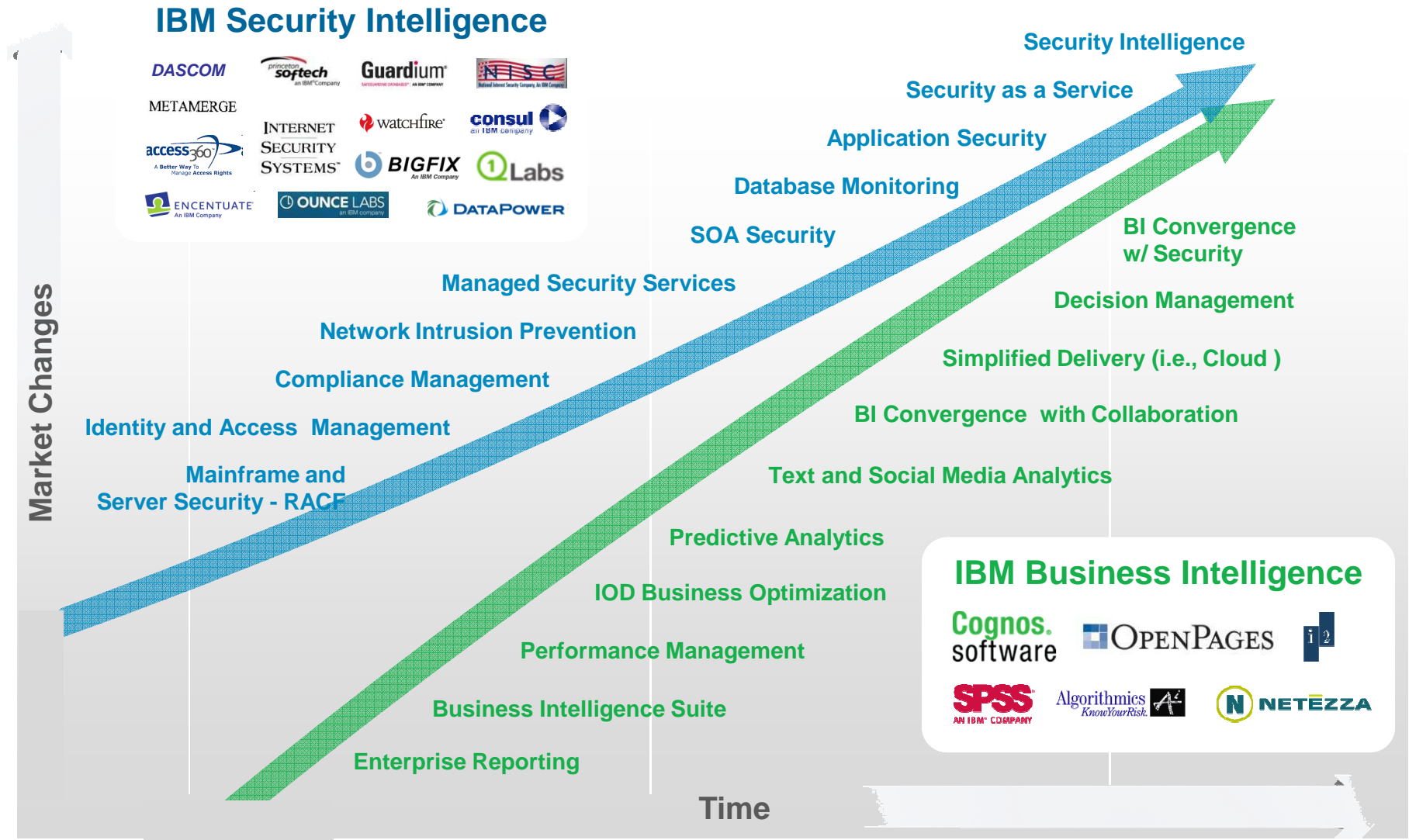
Objectives

When you complete this unit, you should be familiar with the following:

- QRadar Security Intelligence value proposition
- QRadar components, form factors and architecture



Security and Business Intelligence offer insightful parallels



Expertise: Global coverage and security awareness



IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration



14B analyzed Web pages & images
 40M spam & phishing attacks
 54K documented vulnerabilities
 Billions of intrusion attempts daily
 Millions of unique malware samples



World Wide Managed Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 13B+ events managed per day
- 1,000+ security patents
- 133 monitored countries (MSS)

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

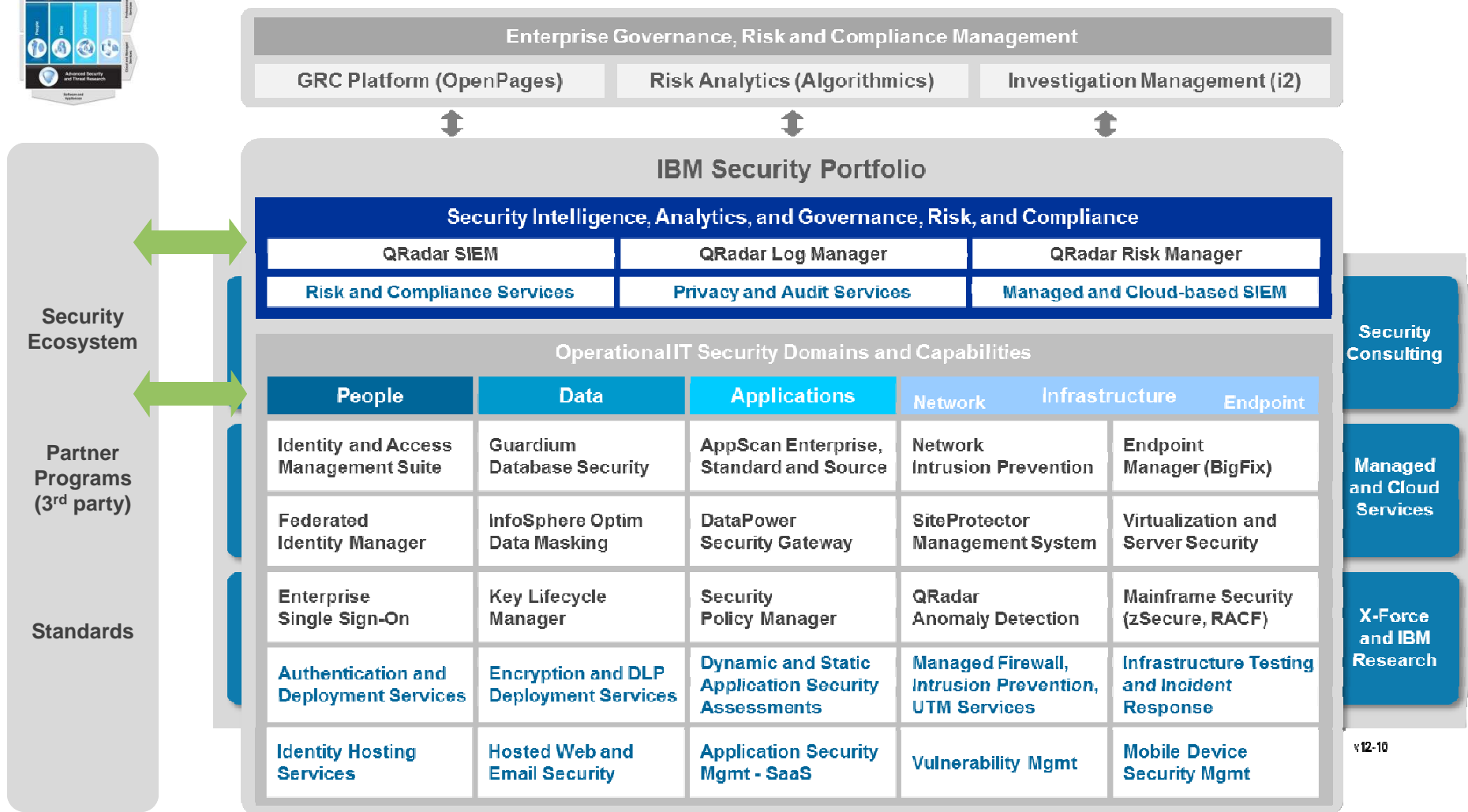
IBM Security Systems

- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- One of the largest vulnerability databases



Intelligence • Integration • Expertise

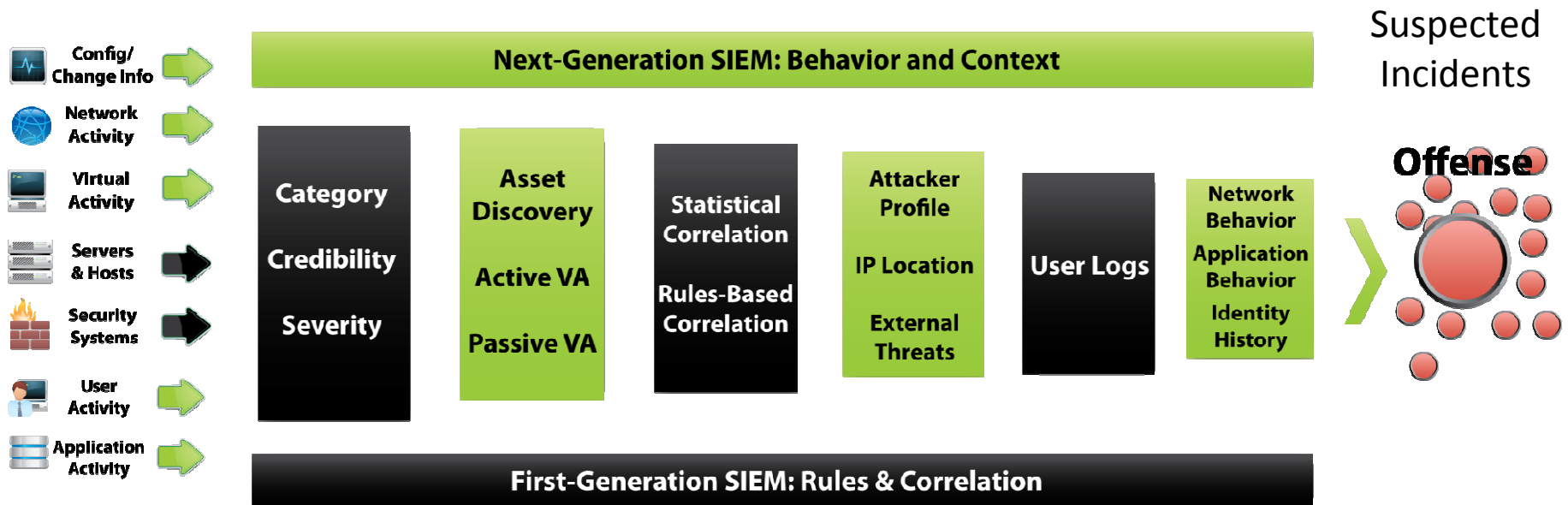
A comprehensive portfolio of products and services across all domains



Products **Services**

v12-10

QRadar Next-Generation SIEM: Total Intelligence



Threats and Fraud Detected That Others Miss

User correlation and application forensics enabled fraud detection prior to exploit completion

Liz claborne®

Massive Data Reduction

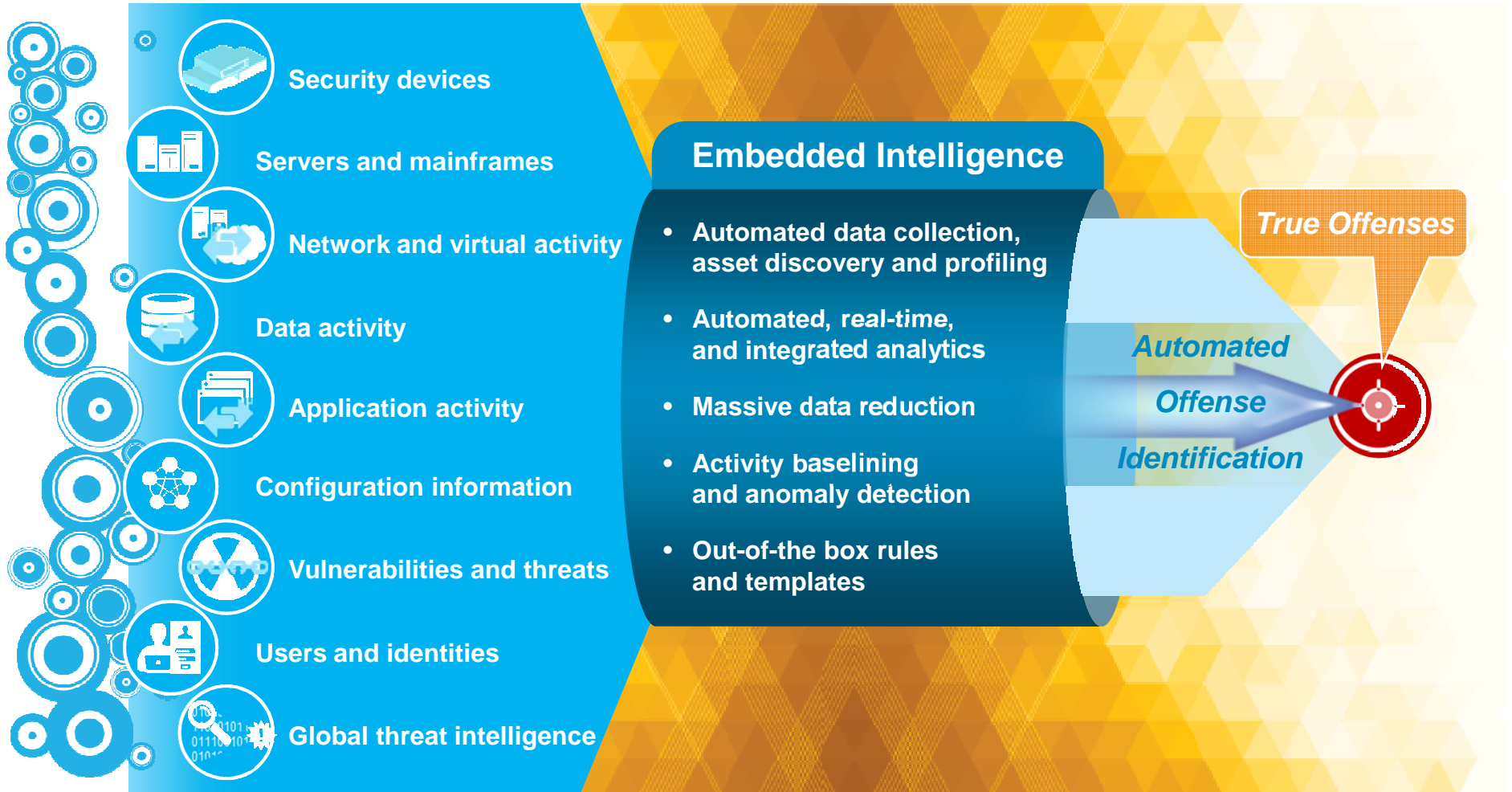
2Bn log and event records a day reduced to 25 high priority



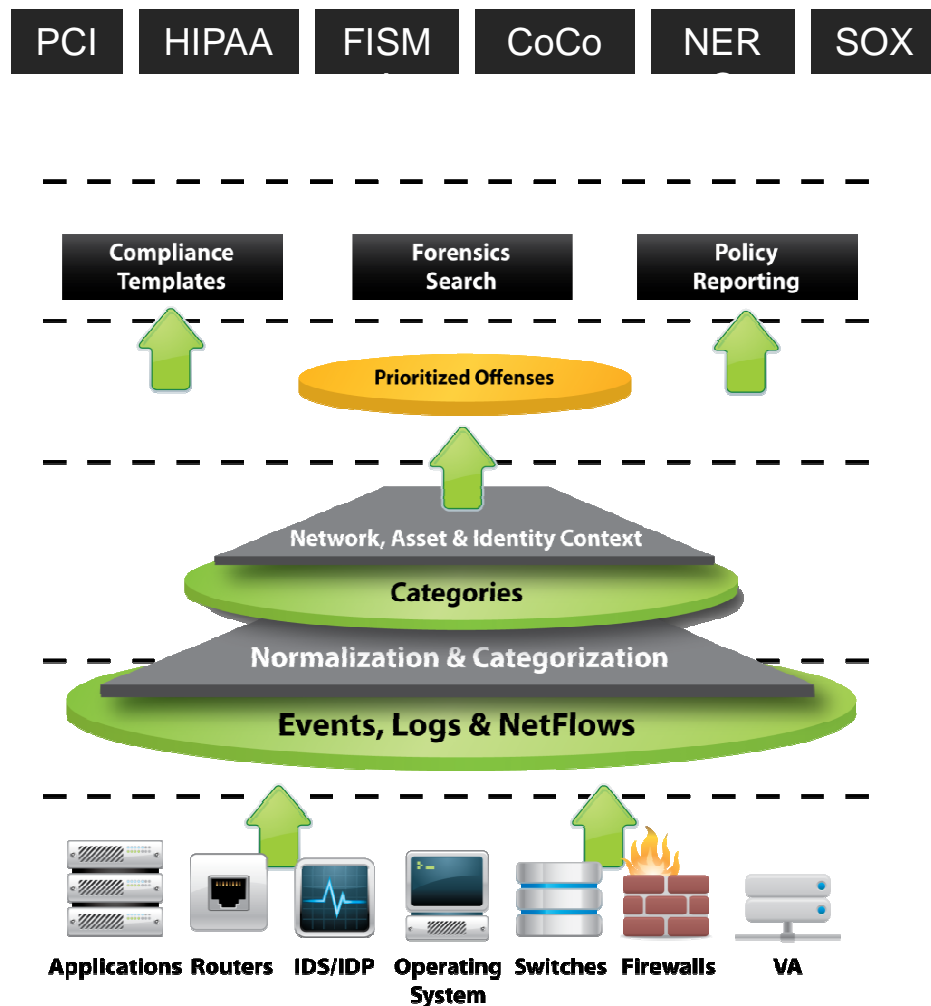
Intelligence: Embedded intelligence to find true offenses

Extensive Data Sources

...Suspected Incidents

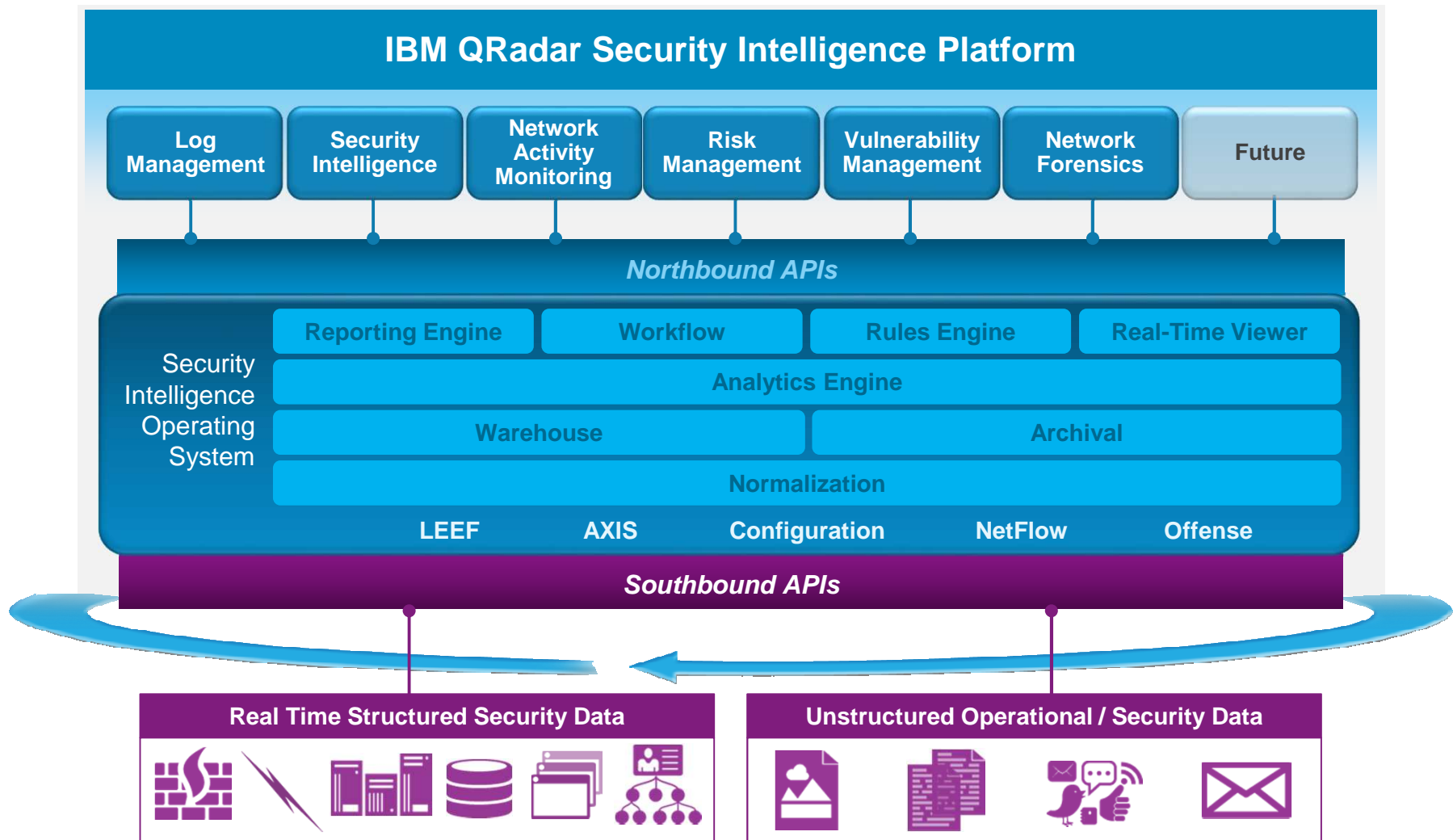


Compliance and Management Security

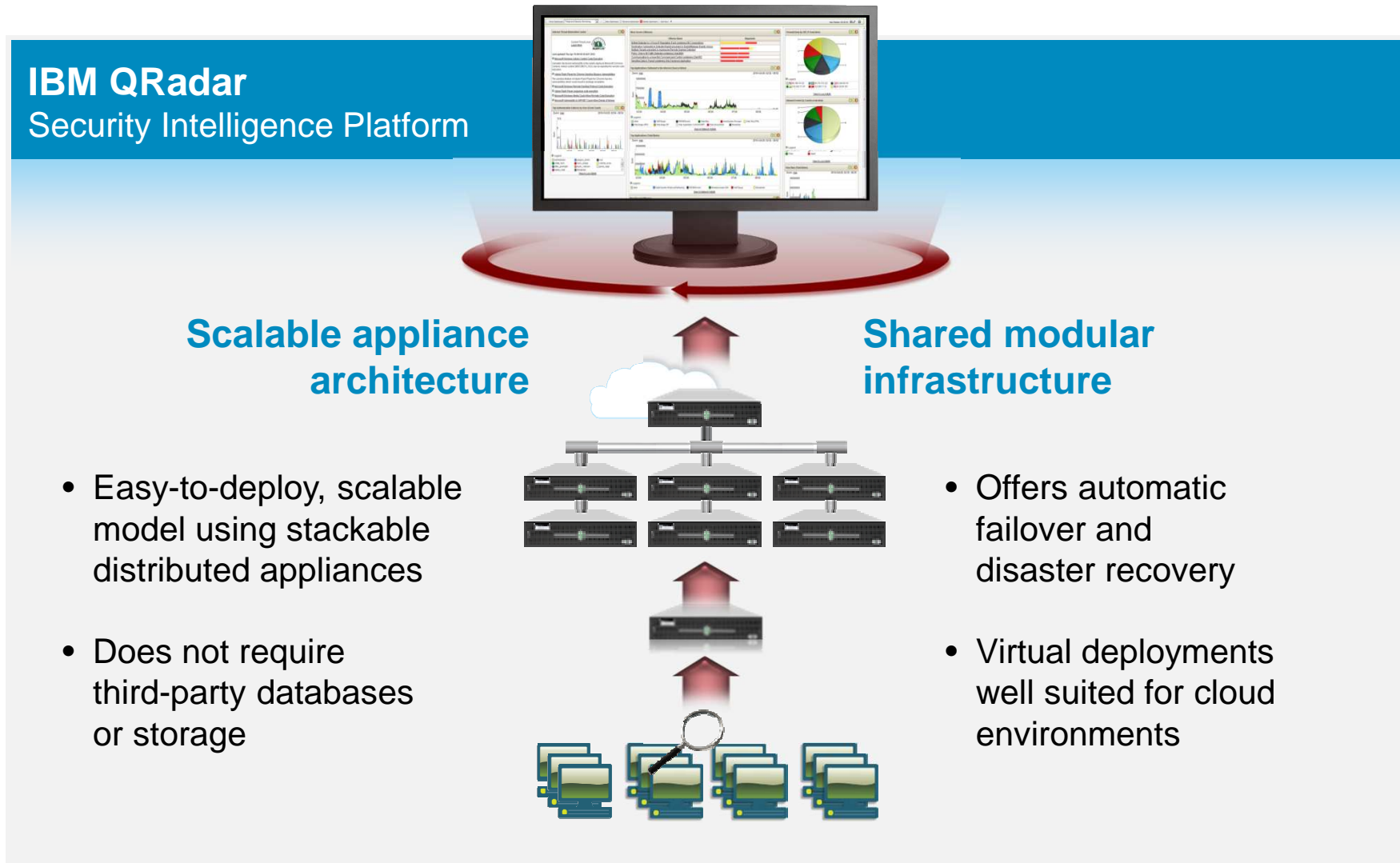


- ◆ Compliance validation and security response improvement in the same solution
- ◆ Out of the box content to swiftly meet PCI, NERC, SOX, HIPAA, GLBA, CoCo, ISO 27001 etc.
- ◆ Flexibility to meet new compliance standards as they evolve

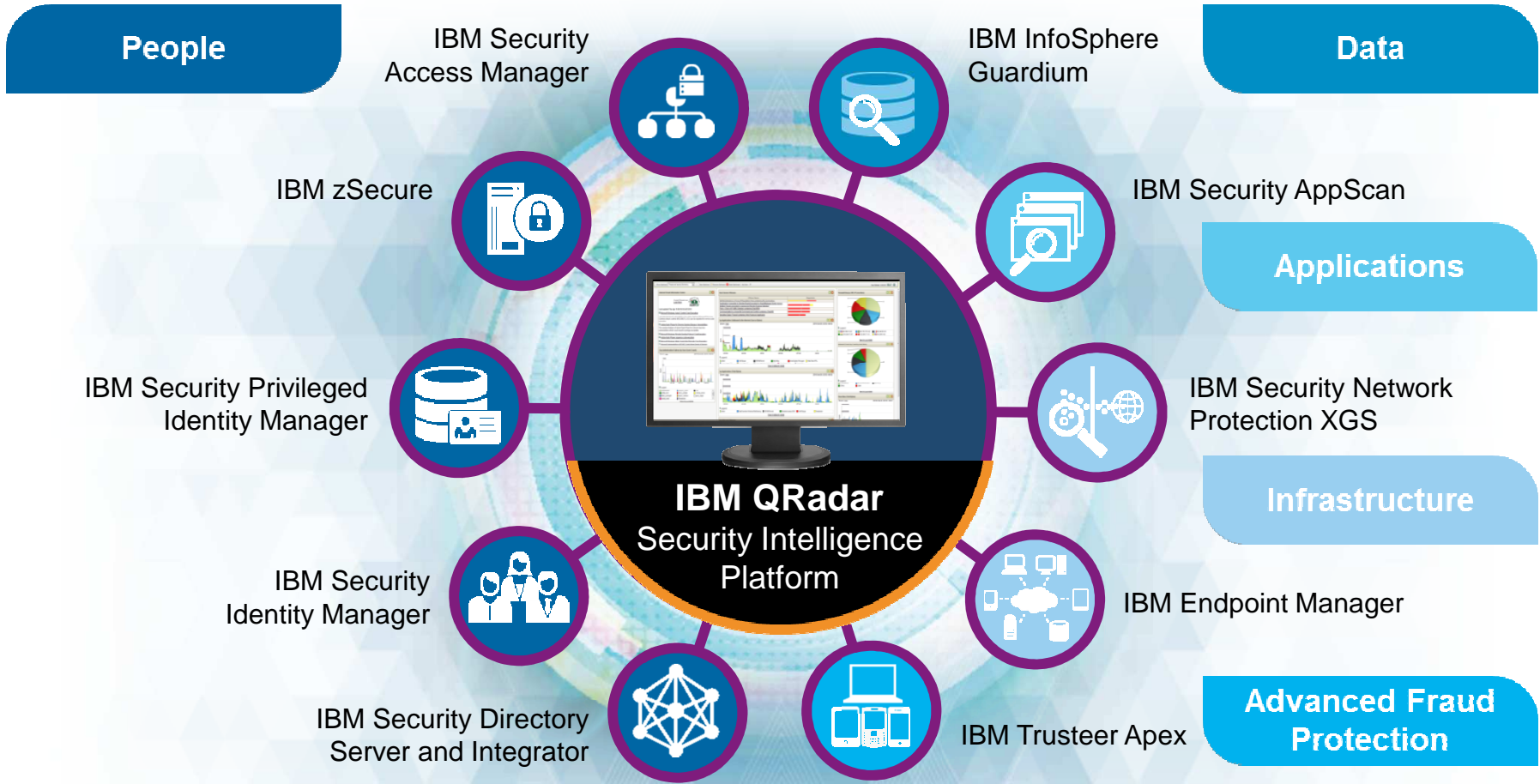
Delivering multiple security capabilities through a purpose-built, extensible platform



Optimized appliance and software architecture for high performance and rapid deployment









IBM QRadar is the centerpiece of IBM security integration



IBM QRadar supports hundreds of third-party products

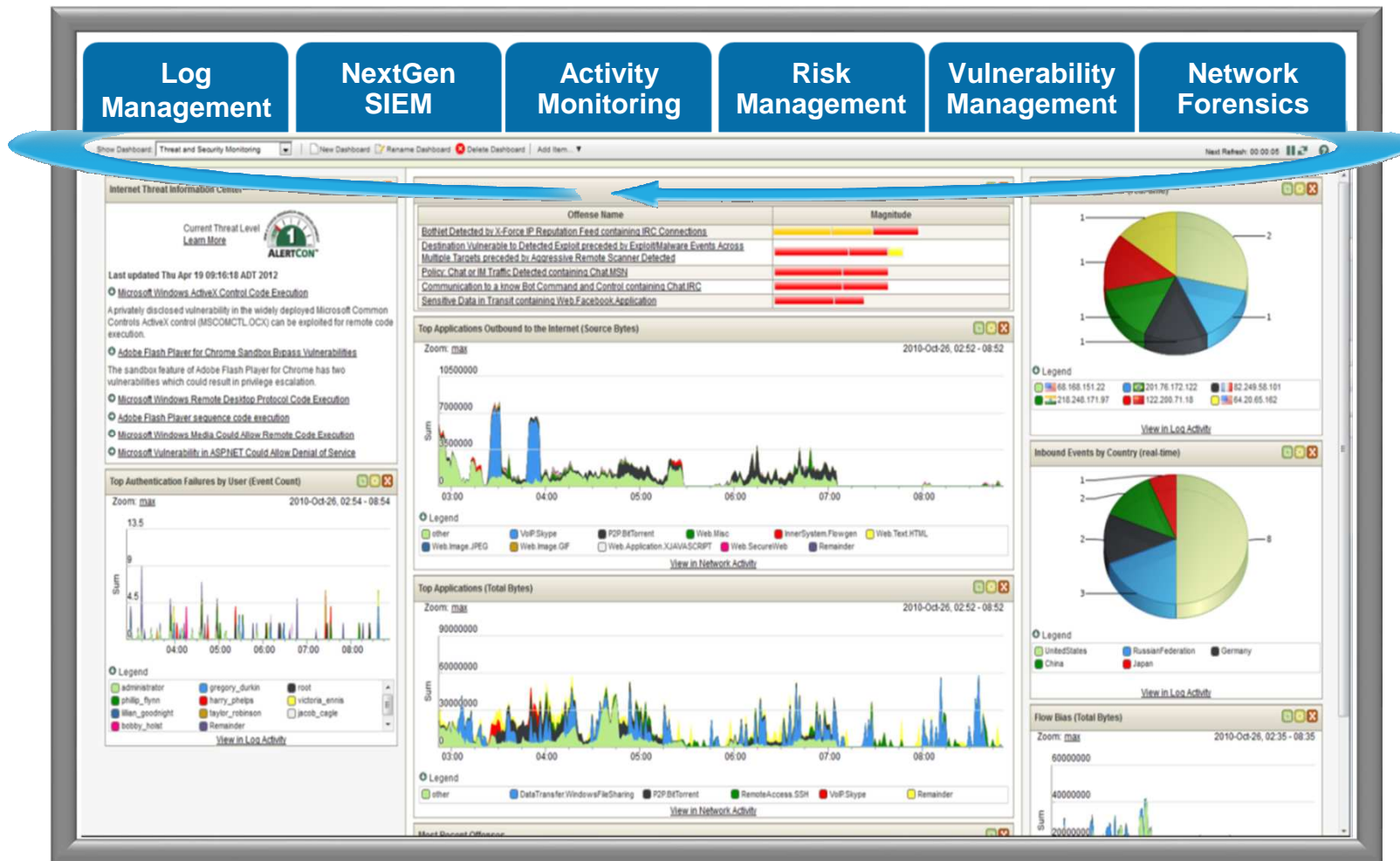
IBM QRadar
Security Intelligence Platform

Expandable and scalable QRadar platform solutions

<p>Log Management</p>		<ul style="list-style-type: none"> • Turn-key log management and reporting • SME to Enterprise • Upgradeable to enterprise SIEM
<p>SIEM</p>		<ul style="list-style-type: none"> • Log, flow, vulnerability & identity correlation • Sophisticated asset profiling • Offense management and workflow
<p>Network and Application Visibility</p>		<ul style="list-style-type: none"> • Layer 7 application monitoring • Content capture for deep insight & forensics • Physical and virtual environments
<p>Risk & Vulnerability Management</p>		<ul style="list-style-type: none"> • Network security configuration monitoring • Vulnerability scanning & prioritization • Predictive threat modeling & simulation
<p>Scalability</p>		<ul style="list-style-type: none"> • Event Processors for remote site • High Availability & Disaster Recovery • Data Node to increase storage & performance
<p>Network Forensics</p>		<ul style="list-style-type: none"> • Reconstructs network sessions from PCAPs • Data pivoting and visualization tools • Accelerated clarity around who, what, when

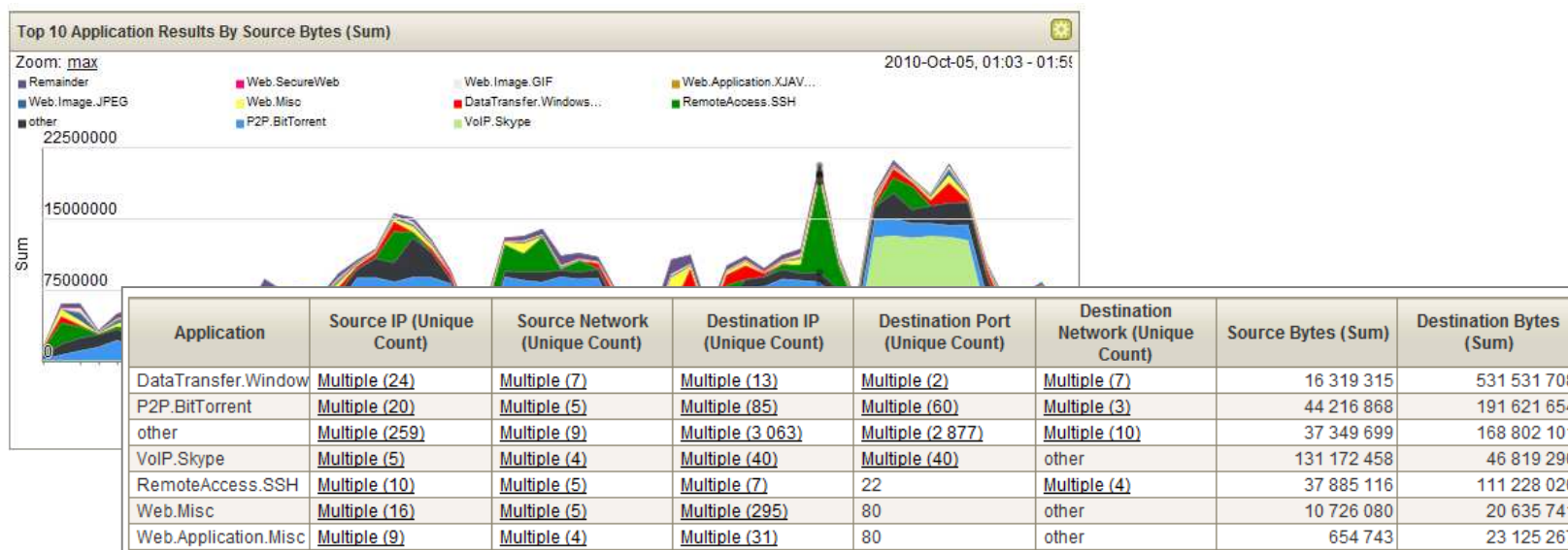


Integration: A unified architecture delivered in a single console



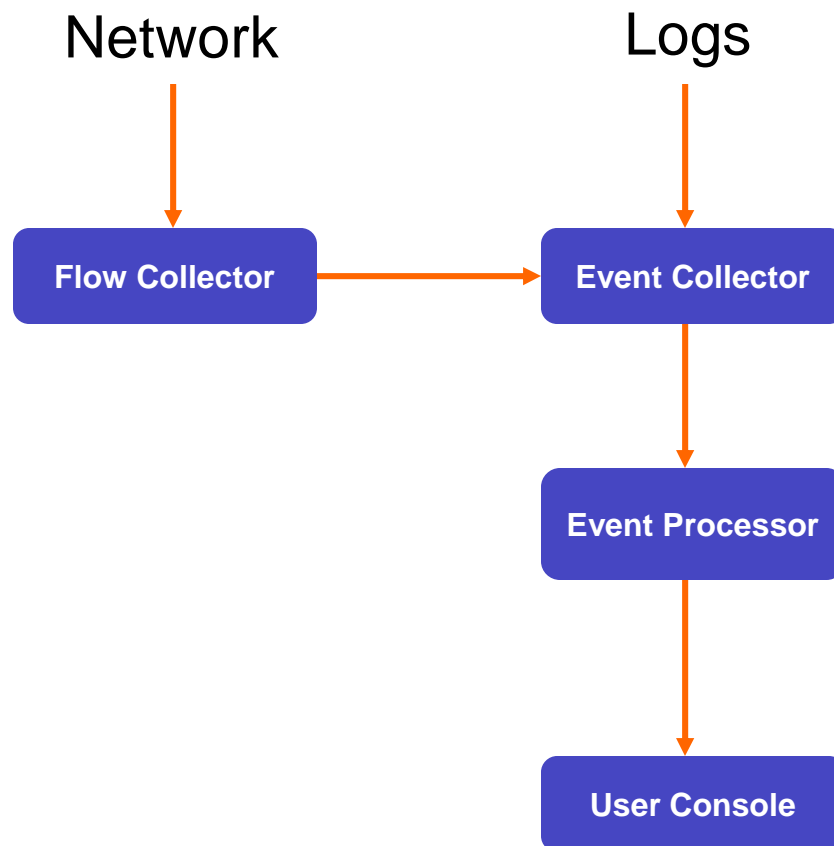
Differentiated by network flow analytics

- **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



QRadar components

QRadar software components and data flow

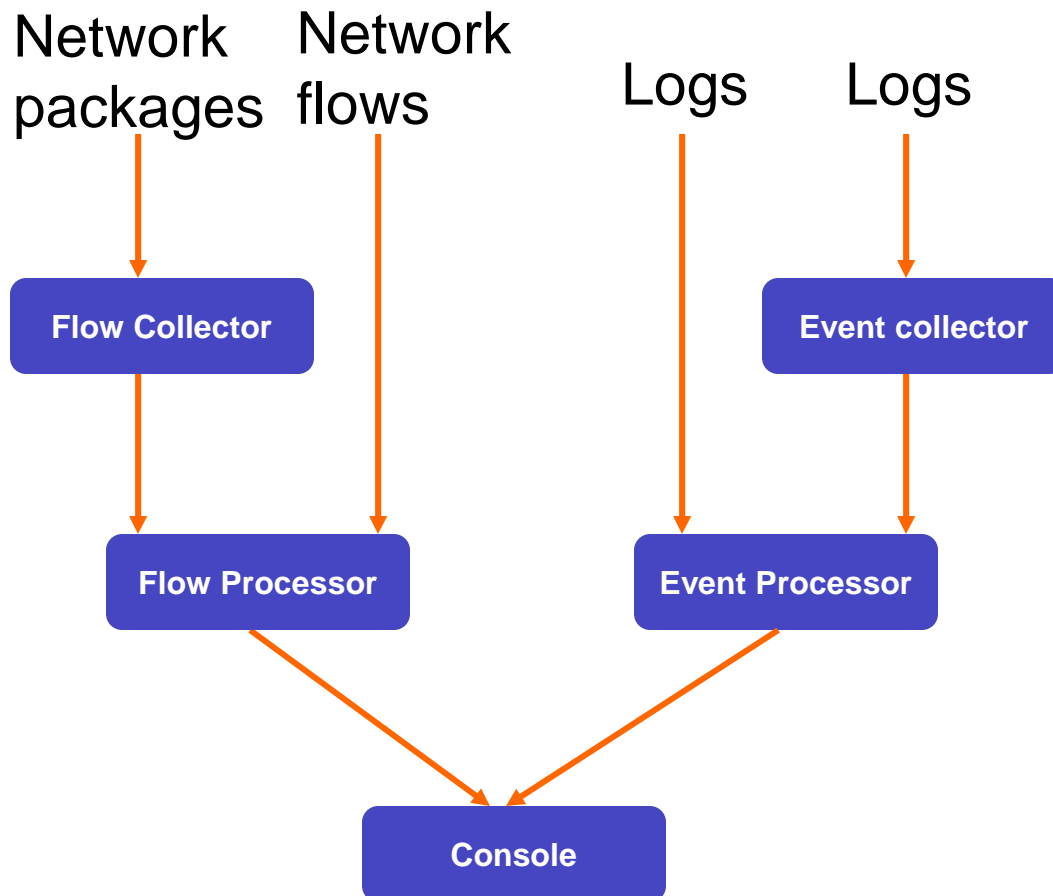


- Network information collected from 3rd party network flows, and from onboard network card interfaces.
- Logs collected from devices, applications, databases, or operating systems.

QRadar software components

- **Central User Console**
 - Magistrate (manages offense creation and magnitude)
 - Global correlation across flow and event processors
 - Offense management
 - Assets and identity management
- **Event Processor**
 - Rule Processor
 - Storage for events, accumulated meta data
 - Storage for flows, accumulated meta data
- **Event Collector**
 - Log event collection, coalescing, and normalization
 - 3rd party Flow collection J-Flow, NetFlow, S-Flow, deduplication, and recombination
- **Flow Collector**
 - QFlow and Superflow creation, and application detection

QRadar appliance components and data flow



- Network flows preferably are processed by a separate flow processor appliance
- Event logs preferably are processed by a separate event processor appliance
- A flow collector is required if layer 7 data analysis is required.
- An event collector is used where bandwidth between log sources and log storage is

QRadar appliance types

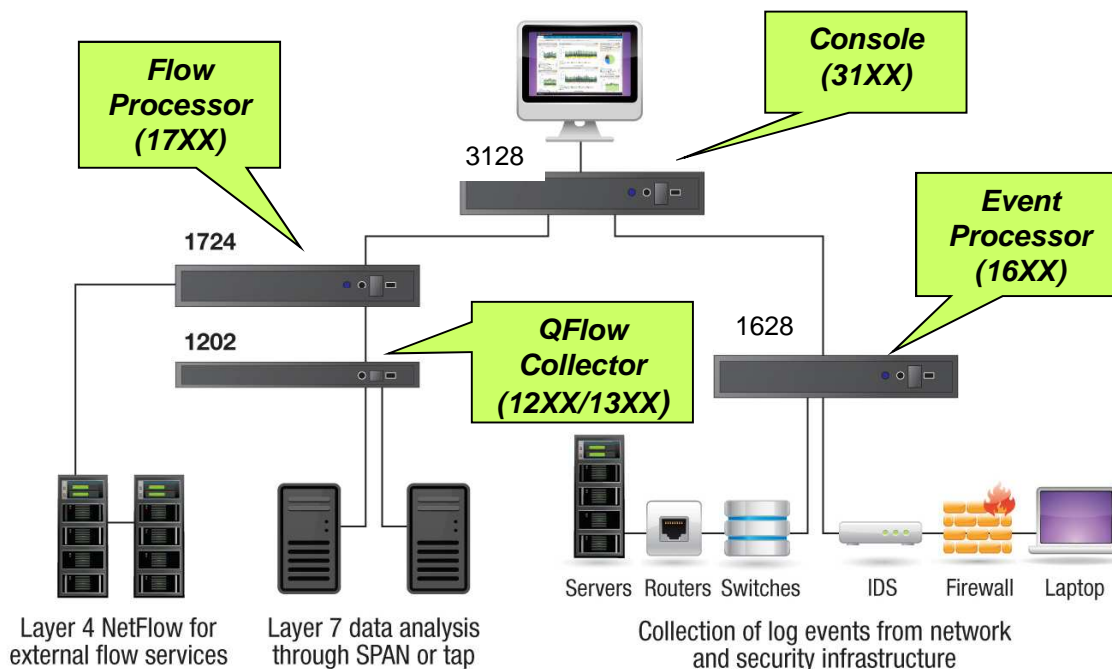
- Console only. Must be combined with event or flow processors, and flow collectors.
- Server. For medium and enterprise environments. Combines a flow processor and event processor in one
- Event Processor . Processes and stores event logs.
- Flow Processor. Processes 3rd party network flows, QFlow and stores flows.
- Flow Collector. Receives 3rd party network flows and packages. Normalizes and forwards them as QFlows.
- Event Collector. Receives log records, normalizes and forwards them to an event processor. Temporary storage of normalized log events and payload.

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

Sample IBM Security QRadar SIEM all-in-one deployment
QRadar web console



Sample IBM Security QRadar SIEM 3124 distributed deployment
QRadar web console

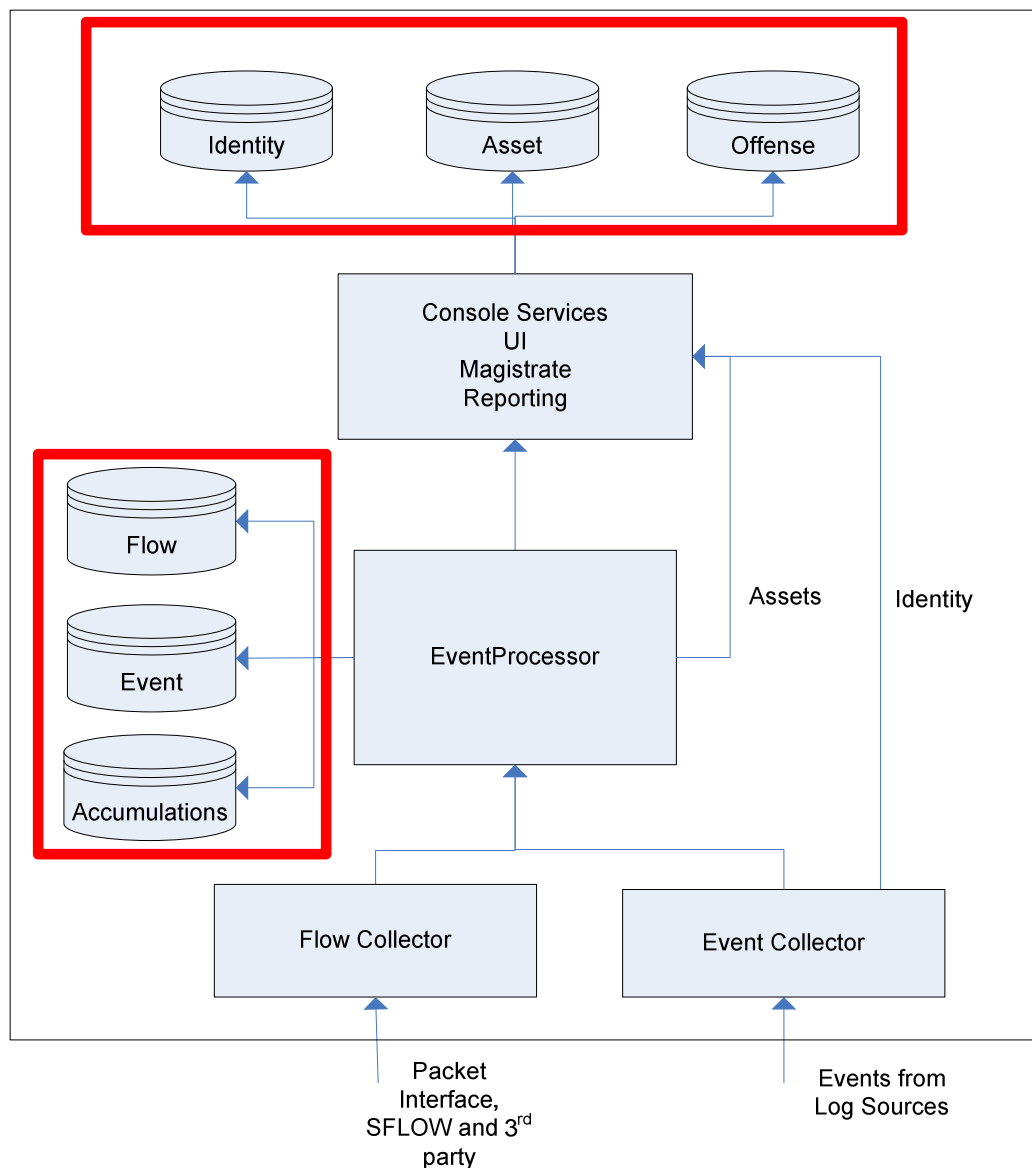


All-in-One is a single appliance used to collect both events and flow data from various security and network devices, perform data correlation and rule matching, report alerts/threats, and provide all admin functions through a Web browser.

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.

High Level architecture

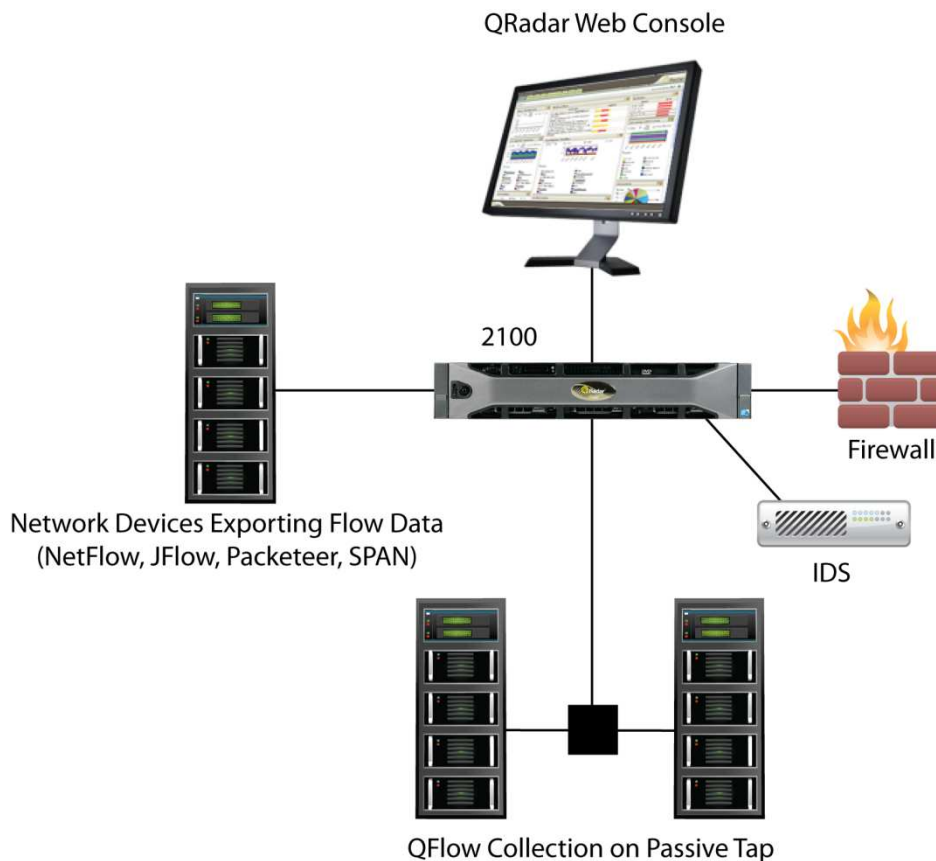


- Flow and event data is stored on the Ariel datastorage on the processors. If accumulation is required, then accumulated data will be stored in the accumulation database
- Offenses, asset, and identity information is stored in the master PostgreSQL database on the console.
- SSH between appliances in a distributed environment is supported.

Deployment Examples

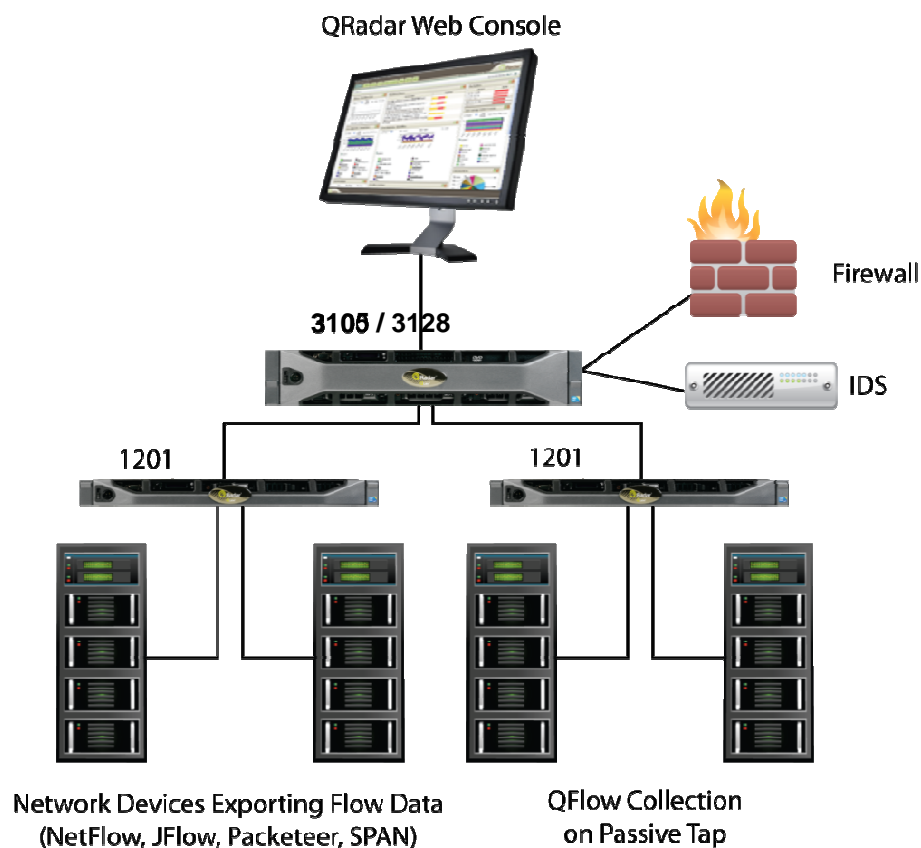
SIEM All-in-One 2100 Appliance

- **Positioning**
 - Single box for centralized deployment in a small/medium enterprise
- **Characteristics and Capacity**
 - 1000 EPS, 50K Flows, 750 Log Sources, 100 network objects
 - Onboard 250Mbps QFlow for SPAN or TAP
 - Includes QFlow Collector for layer 7 network activity monitoring
 - 1.5TB of storage for QRadar
- **Upgradability**
 - No EPS upgrade
 - Flows upgradable to 50K
 - No deployment upgrade
- **HA / DR available**



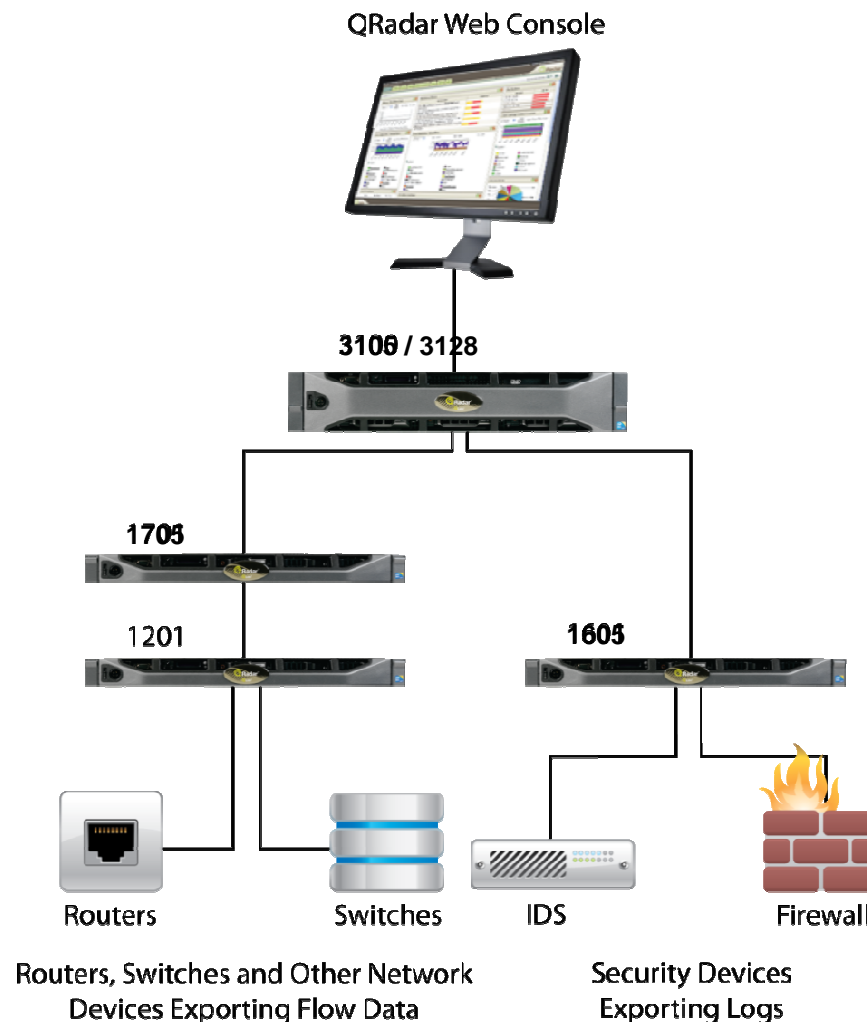
SIEM All-in-One 3105 and 3128 Appliances

- **Positioning**
 - QRadar appliance for centralized deployment in a medium/large enterprise
 - Contains event & flow processing capabilities
- **Characteristics and Capacity**
 - 1000 EPS, 25K Flows, 750 Log Sources, 1000 network objects
 - Requires external QFlow Collectors for layer 7 network activity monitoring
 - Dedicated storage for QRadar
 - 3105: 6.2TB of storage
 - 3128: 40TB of storage
- **Upgradability**
 - 3105: EPS upgradable to 5000. Flows upgradable to 200K.
 - 3128: EPS upgradable to 15,000. Flows upgradable to 300K.
 - Upgradable to 31XX Console for distributed deployment with events/flows transferred to new 16XX, 17XX, or 18XX appliance.
- **HA / DR available**



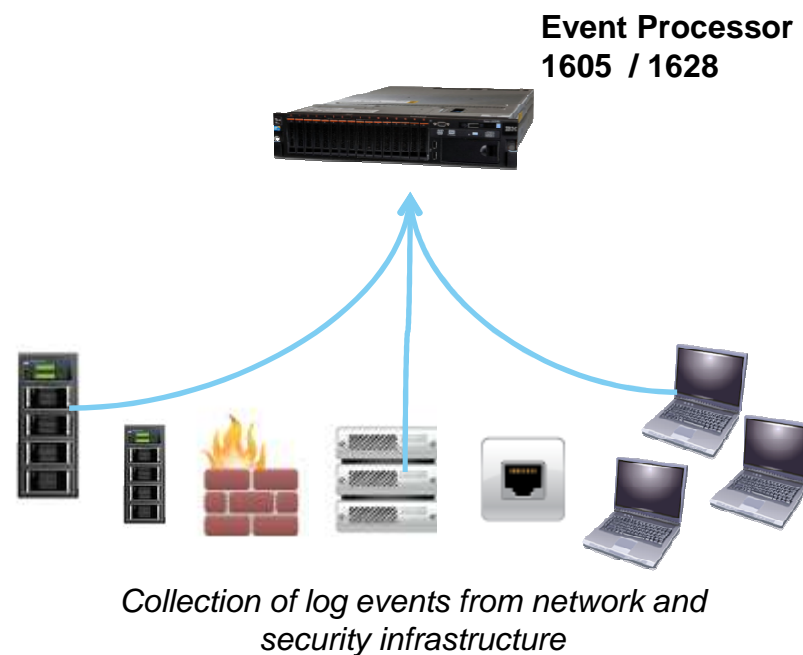
SIEM Console 3105 and 3128 Appliances

- **Positioning**
 - Console dedicated to management of distributed deployment in a large enterprise
 - Manages distributed event/flow processors
- **Characteristics and Capacity**
 - Focuses on processing and analysis of offenses, generating views and reports
 - Requires 16XX to collect log events or 17XX to collect flows (or 18XX for both)
 - Requires external QFlow Collectors for layer 7 network activity monitoring
 - Dedicated storage for QRadar
 - 3105: 6.2TB of storage
 - 3128: 40TB of storage
- **Upgradability**
 - No upgrade available
- **HA / DR available**



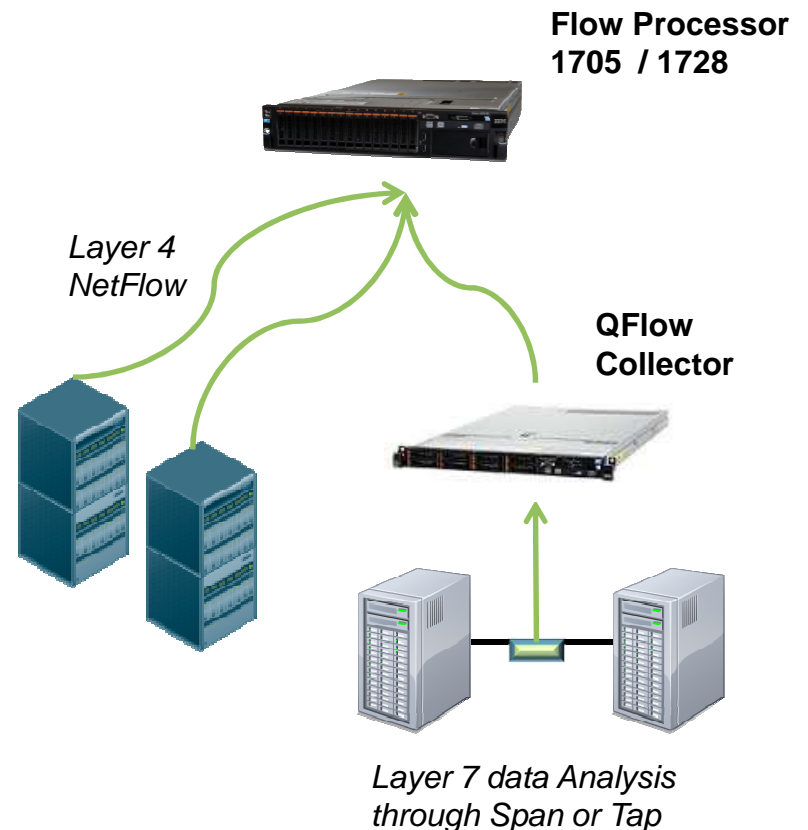
SIEM Event Processor 1605 and 1628 Appliances

- **Positioning**
 - High capacity and scalable event collection for distributed deployment in a large enterprise
- **Characteristics and Capacity**
 - Collect logs from network devices, security devices, operating systems and applications
 - 2500 EPS
 - Requires Console 31XX
 - Dedicated storage for QRadar
 - 1605: 6.2TB of storage
 - 1628: 40TB of storage
- **Upgradability**
 - 1605 upgradeable to 20,000 EPS
 - 1628 upgradeable to 40,000 EPS
- **HA / DR available**



SIEM Flow Processor 1705 and 1728 Appliances

- Positioning
 - High capacity and scalable flow collection for distributed deployment in a large enterprise
- Characteristics and Capacity
 - Receives flows from external flow sources (e.g. NetFlow) or QFlow Collectors for layer 7 network activity monitoring
 - 100K Flows/minute
 - Requires Console 31XX
 - Dedicated storage for QRadar
 - 1705: 6.2TB of storage
 - 1728: 40TB of storage
- Upgradability
 - 1705 upgradable to 600K Flows
 - 1728 upgradable to 1.2M Flows.
- HA / DR available



SIEM Combined Event/Flow Processor 1805 and 1828 Appliances

Positioning

- High capacity and scalable event & flow collection for distributed deployment in a large enterprise

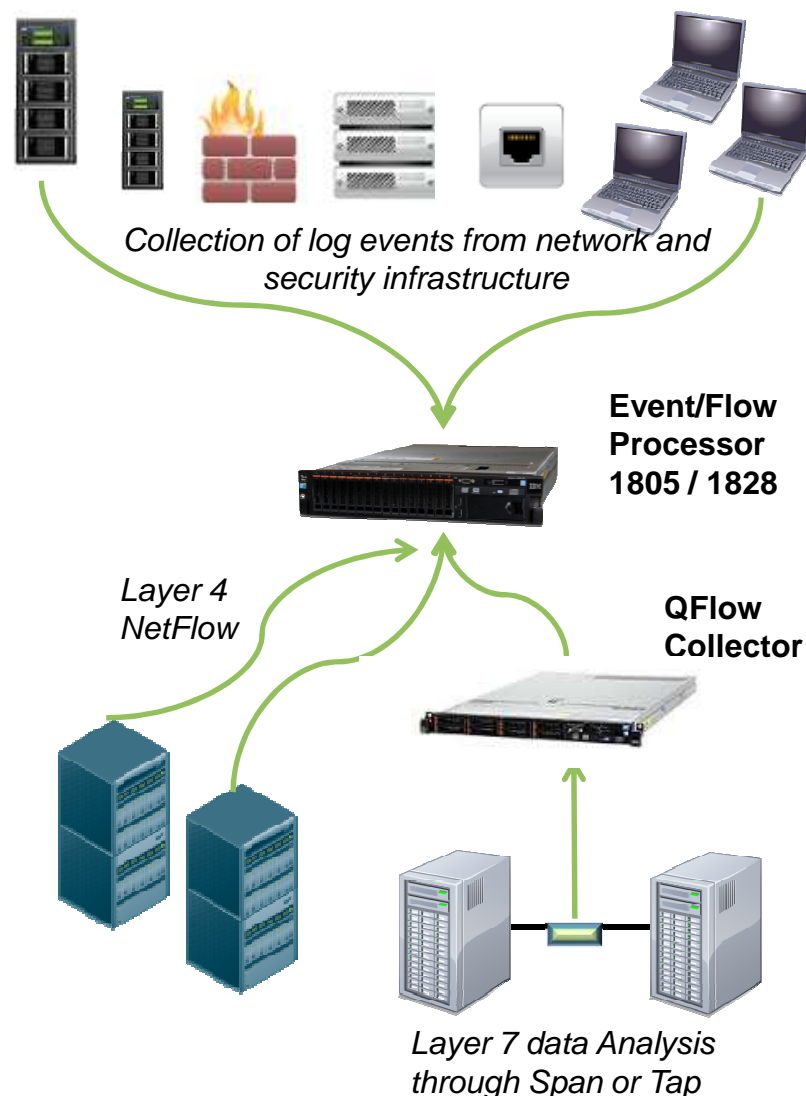
Characteristics and Capacity

- Collect logs from network devices, security devices, operating systems and applications
- Receives flows from external flow sources (e.g. NetFlow) or QFlow Collectors for layer 7 network activity monitoring
- 1000 EPS, 25K Flows/minute
- Requires Console 31XX
- Dedicated storage for QRadar
 - 1805: 6.2TB of storage
 - 1828: 40TB of storage

Upgradability

- 1805: EPS upgradable to 5000. Flows upgradable to 200K.
- 1828: EPS upgradable to 15,000. Flows upgradable to 300K.

HA / DR available



Event Collector 1501 Appliance

Positioning

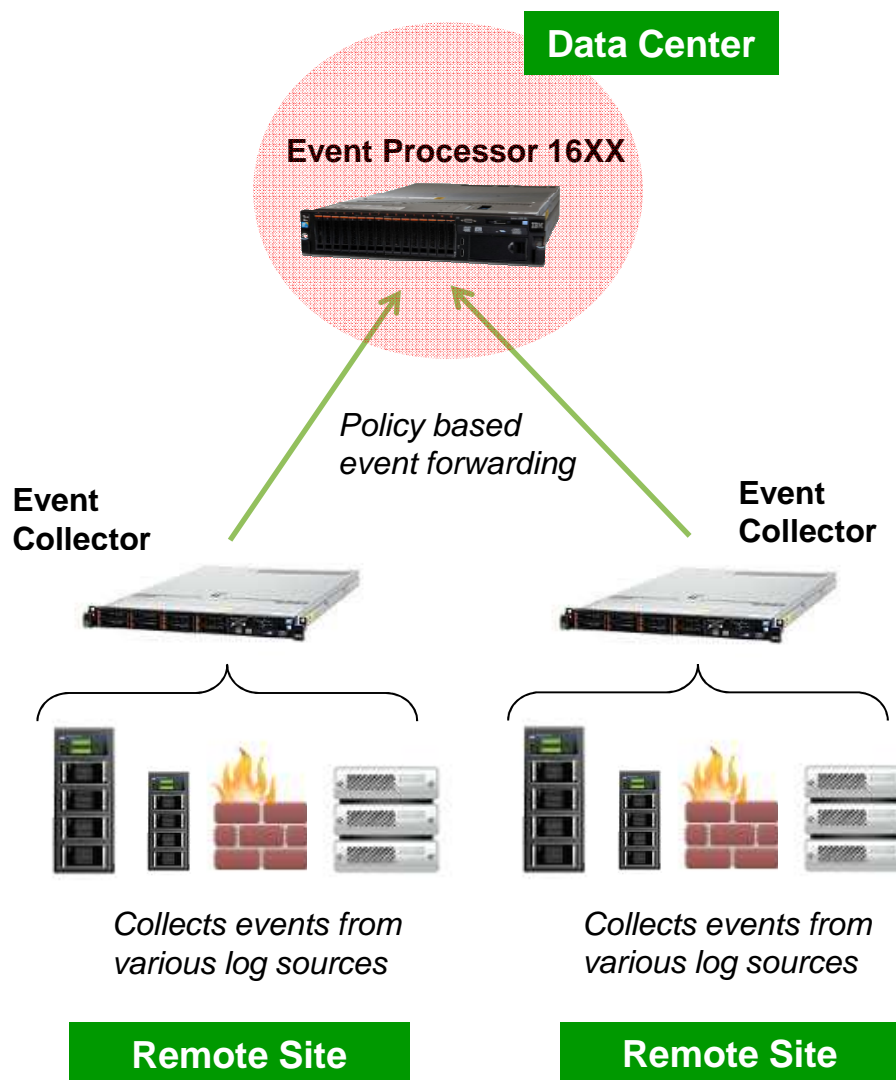
- Intended for customers with remote sites that have unreliable connectivity or constrained bandwidth, but still require reliable event collection, such as retail store/office, cruise ships, Naval vessels
- Collects and parses events on a remote site, stores events temporarily, and forwards events (based on a policy) to an upstream Event Processor 16XX or All-in-1 31XX for analysis, correlation, and storage.

Characteristics and Capacity

- EC appliance based on 1201 hardware configuration
- Supports up to 2500 EPS but no license associated. EPS enforced by the license at the upstream Event Processor.

Upgradability

- No upgrade available



QFlow Collector 1201, 1202, 1301, and 1310 Appliances

Positioning

- High capacity and scalable layer 7 application data collection for distributed deployment in a large/medium enterprise

Characteristics and Capacity

- Collect QFlow data through Span or Tap
- Requires Flow Processor 17XX or Console 31XX
- Performance depends on models:
 - 1201 – 1 Gbps
 - 1202 – 3 Gpbs
 - 1301 – 3 Gpbs
 - 1310 SR/LR – 3 Gpbs

Upgradability

- No upgrade available

QFlow Collector can send collected layer 7 application data to a Flow Processor or a Console directly.

Flow Processor 17XX



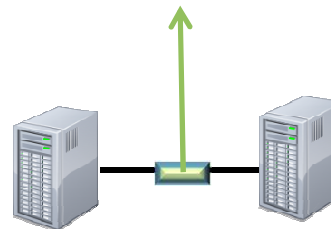
Console 31XX



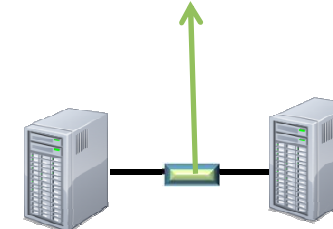
QFlow Collector



QFlow Collector



Layer 7 data Analysis through Span or Tap



Layer 7 data Analysis through Span or Tap

QRadar Risk Manager (QRM) Appliance

Positioning

– QRM expands the QRadar SIEM solution to proactive security management by providing multi-vendor network configuration monitoring and audit, risk and policy compliance assessment, and predictive threat modeling and simulation.

Characteristics and Capacity

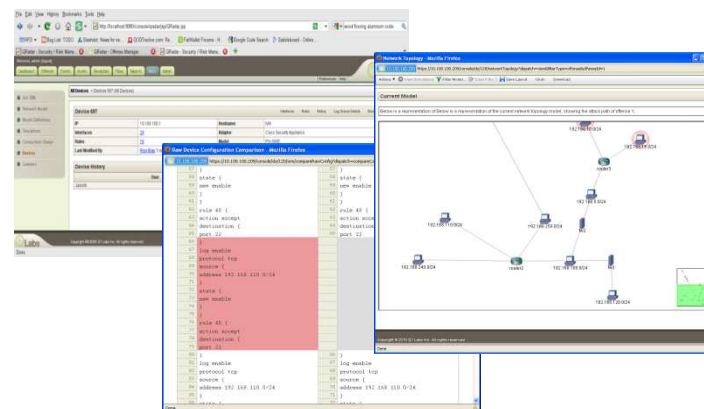
- Based on QRadar Core Appliance xx05
- Requires QRadar Console for configuration, policy, and risk management and simulation tasks
- Licensed based on Configuration Sources

- Standard configuration sources (firewalls, routers, IDS/IPS devices)
- Remote/branch configuration sources (1U/2U security devices located at remote locations)

– Includes support for 50 standard configuration sources

Upgradability

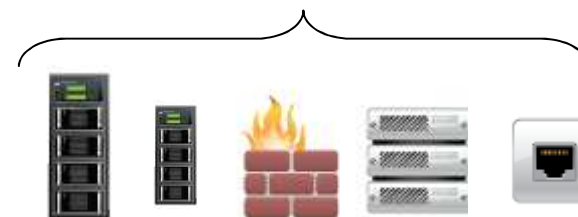
– More configuration sources can be added as needed



QRadar Console



QRM



Supports various network and security devices

QRadar Vulnerability Manager (QVM) Appliance

Positioning

- QVM a new QRadar offering that provides seamlessly integrated network vulnerability scanning and reporting with network context aware vulnerability management workflow that is fully integrated with QRadar SIEM.

Characteristics and Capacity

- Based on QRadar Core Appliance xx05
- Works with QRadar Console for a “remote deployment” where there is a QRadar installation
- Can also exist by itself for a “standalone deployment” where there is no QRadar installation
- Licensed based on scanning assets
- Includes support for 255 scanning objects

Upgradability

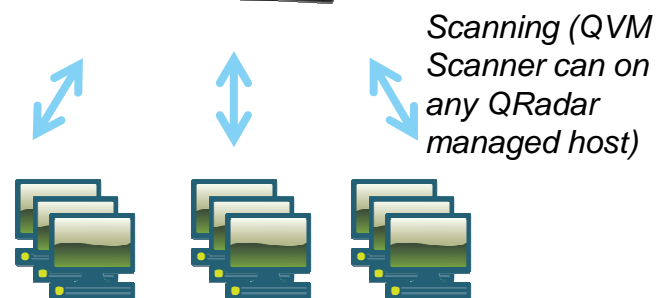
- More scanning objects can be added as needed.



QRadar Console



QVM



Packet Capture and Incident Forensics Appliances

Positioning

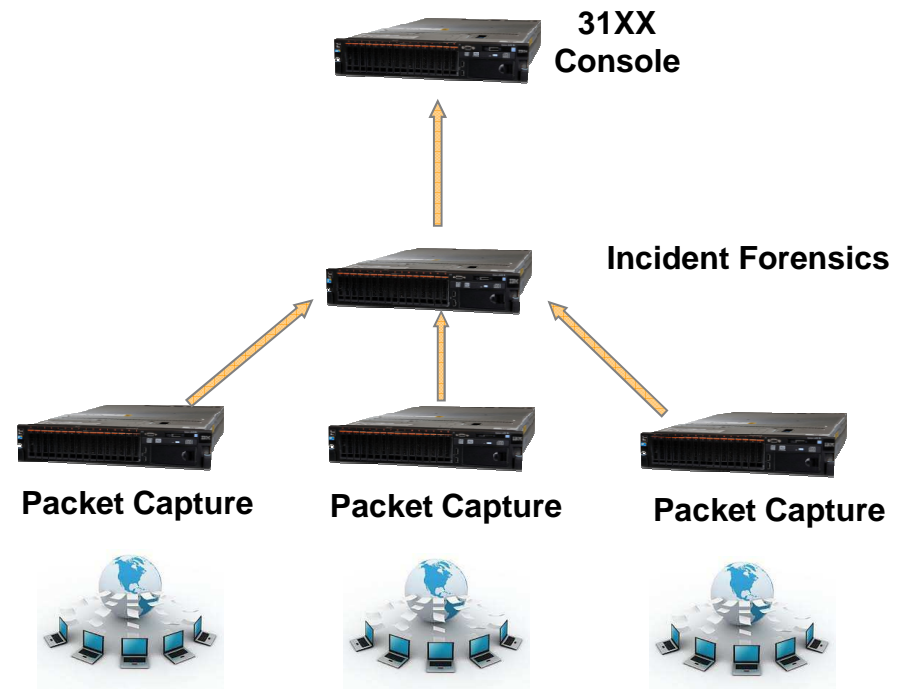
– Packet Capture appliance is to collect and store raw network packets. Incident Forensics appliance is used to reconstruct raw network packets to original format and quickly pinpoint the root cause of security incidents.

Characteristics and Capacity

- Based on the same hardware used for QRadar Core Appliance xx28 (but having different Core Appliance part numbers)
- No additional capacity license.
- Only one Incident Forensics instance can be used in a QRadar deployment (All-in-1 or distributed)
- Multiple Packet Capture appliances can be used with a single Incident Forensics instance. Recommended maximum ratio is 5:1 but a higher ratio is possible.

Upgradability

- No upgrade available



High Availability and Disaster Recovery

High Availability

- HA appliance shares EPS/Flows licenses with Primary (so no additional EPS/Flow increase purchase is needed).
- Data and configuration replicated from Primary appliance to HA appliance near real time.
- Failover to HA whenever Primary becomes unavailable.

Disaster Recovery

- DR appliance provides redundant parallel system
- The same amount of EPS and Flows as Primary needs to be purchased for DR.
- Event and Flow Data from Primary to DR, but configuration is not copied over.

