SolutionsConnect
IBMSoftwareUniverse2013
Meet Possible

Improving security and user productivity with E-SSO

Speaker: Randeep Singh Chhabra

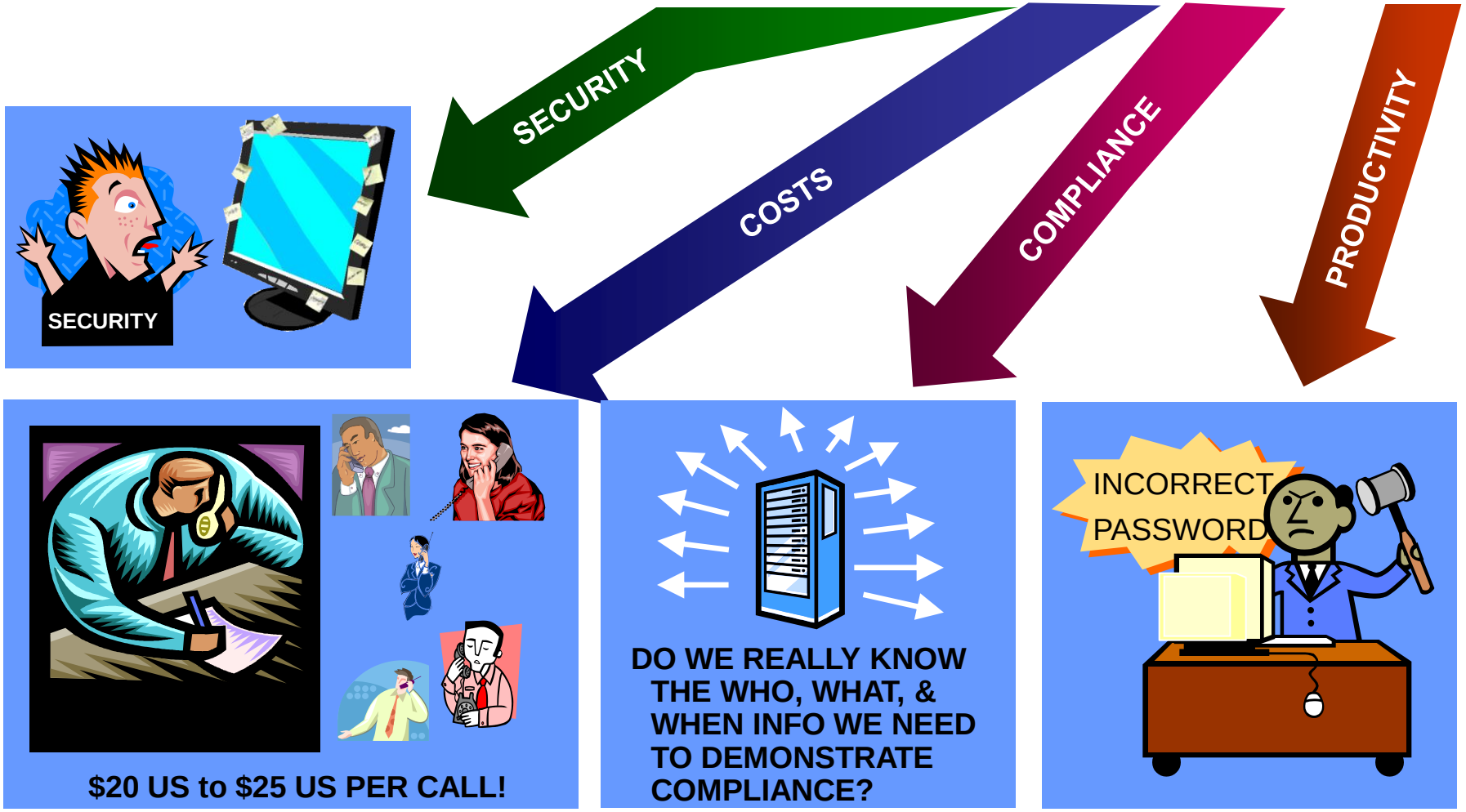
Why Single Sign On?

- Passwords must be:
  - Nontrivial
    - To avoid being guessed
    - Password strength policy rules
    - Problem: hard to guess = hard to remember
  - Changed frequently
    - To avoid brute force attacks
  - Unique
    - To limit risk if compromised

- End User's Solution:

The PC Sunflower

SSO addresses hot buttons for Security Mgrs, CFOs, CCOs and Users



IBM provides complete coverage of SSO needs

Internet: B2C

Extranet: B2E

Managed Desktops
Kiosk

TFIM

TAMeb

Web Services

Federated

SOA

Web SSO Targets

Web Servers

Web Applications

Portals, e.g. WPS

Non-Web Targets

Windows

URL

Java

Citrix/ Term. Svcs.

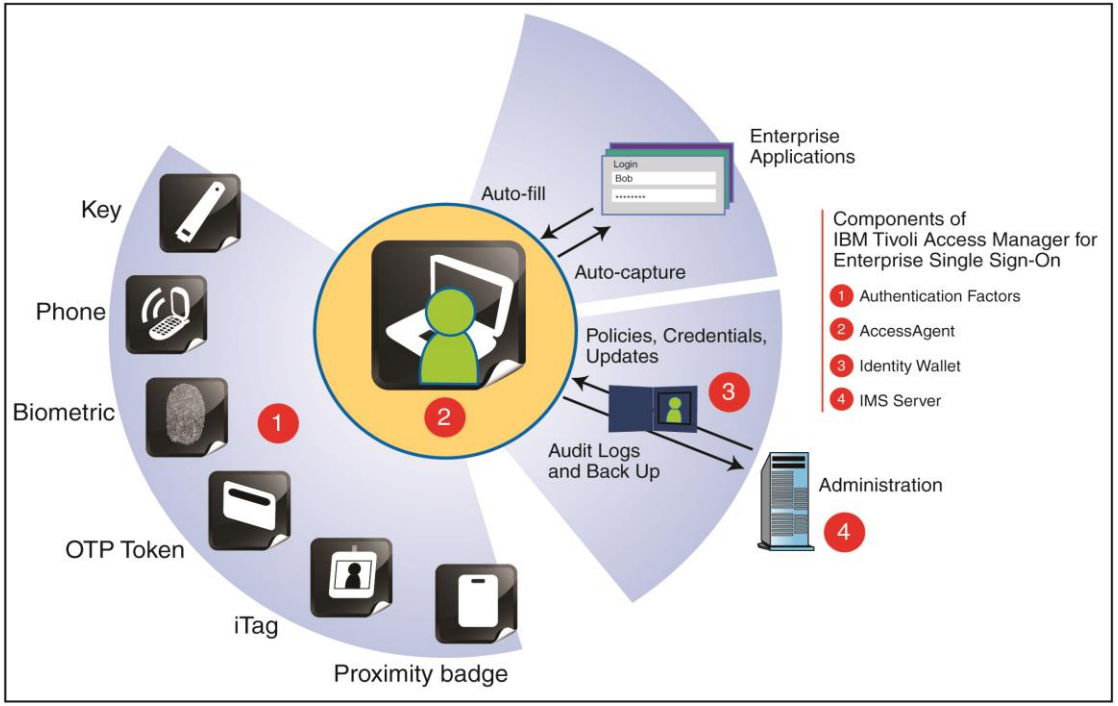
Mainframe

TAM E-SSO v8 Solution Overview

TAM E-SSO provides:

- **Enterprise SSO**
- **Two-Factor Authentication**
- **Access and Security Workflow Automation**
- **Fast user switching**
- **User Access Tracking & Audit**
- **Centralized Identity & Policy Management**

with no change to the infrastructure



TAM E-SSO enables visibility into user activity, control over access to business assets, and automation of the sign-on process in order to drive value for our clients.

Key Differentiation

- *Integrated Strong Auth: "What you know, and what you have, ALREADY"*
- *Comprehensive coverage of access points*
- *Powerful profiling tools: Wizard and Visual Profiling*
- *Complete session management*
- *Integration with IBM Tivoli IAM offerings*

Case Studies

Government Outsourced Service

Company
- Government Agency responsible for central government wide projects
- More than 70,000 users, across ~27 agencies and more than 390 sites

Problem
- Ease password management issue
- Require two-factor authentication for VPN access to central network

Solution
- Implement Encentuate based on USB smartcard token
- Currently deployed to more than 45,000 users

Impact
- Compliance with government policy for secure remote access
- Ease login for users
- Reduce password reset

Integrated Healthcare Network

Company

- Integrated delivery network of 16-facilities in central California
- Privately-held, for-profit organization; over 7,800 employees & doctors

Problem

- Regulatory compliance requirements (HIPAA)
- Securing workstations shared by multiple users
- Strong user resistance to new security policies

Solution

- Implement Encentuate with HID Prox cards
- Fully deployed

Impact

- Immediate compliance to HIPAA regulations
- Dramatic improvement in user acceptance
- Ability to provide user centric access logs to applications

Large Manufacturer

Company
- Fortune 100 company
- $40b in revenue
- 100,000 employees worldwide

Problem
- Reduce keystrokes as part of lean mfg efforts. Users burdened with multiple sign-on credentials for each “tool” interaction.
- Securing workstations from potential “IP leakage” by tools shared by multiple users.
- Improve the accountability of technicians regarding work product and overall productivity
- Improve compliance posture re: SOX

Solution
- Implement Encentuate with roaming sessions
- Encentuate iTag (passive RFID wrist badges) for user authentication

Impact
- Enhanced security
- Improved accountability
- Demonstrated productivity gains for shop floor workers

Large Insurance Provider

Company

- Largest insurance provider worldwide with operations in 10 markets in Asia Pacific (ex Japan)
- Provides Life insurance, wealth management, advice and asset
- management
- APAC regional headquarters have a staff of 4,392 and 9,550 agents

Problem

- Rising operational cost in managing identities in APAC
- Complex heterogeneous environment due to ongoing M&A exacerbates cost of identity admin
- Increased number of new users from emerging markets such as India and China exacerbates cost of identity admin
- Strategic need to establish a centralized shared services within the region

Solution

- Implement the Encentuate IAM Suite

Impact

- End-user productivity enhancement
- Improved compliance and audit
- Established a centralized identity authentication framework
- Manage and reduce operational cost
- Improved overall identity security

Why TAM E-SSO?

User productivity	More than 85% reduction in time-to-information
Security	Improved identity assurance and 100% sign-off
Compliance reporting	More than 75% reduction in audit tracking costs
Helpdesk cost reduction	35-45% reduction in IT helpdesk costs

- **Improve user productivity**
  - Through faster access to information
  - Through better sharing of workstations
- **Enhance security**
  - Through better password security enforcement
  - Through stronger identity assurance
  - Through security policy automation
- **Improve audit and tracking**
  - Through central collation of user-centric logs
  - Through better tracking of user access
- **Reduce help desk cost**
  - Through reduction of password reset calls

IBM Security Intelligence and People Security Solutions

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

DATA EXPLOSION

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

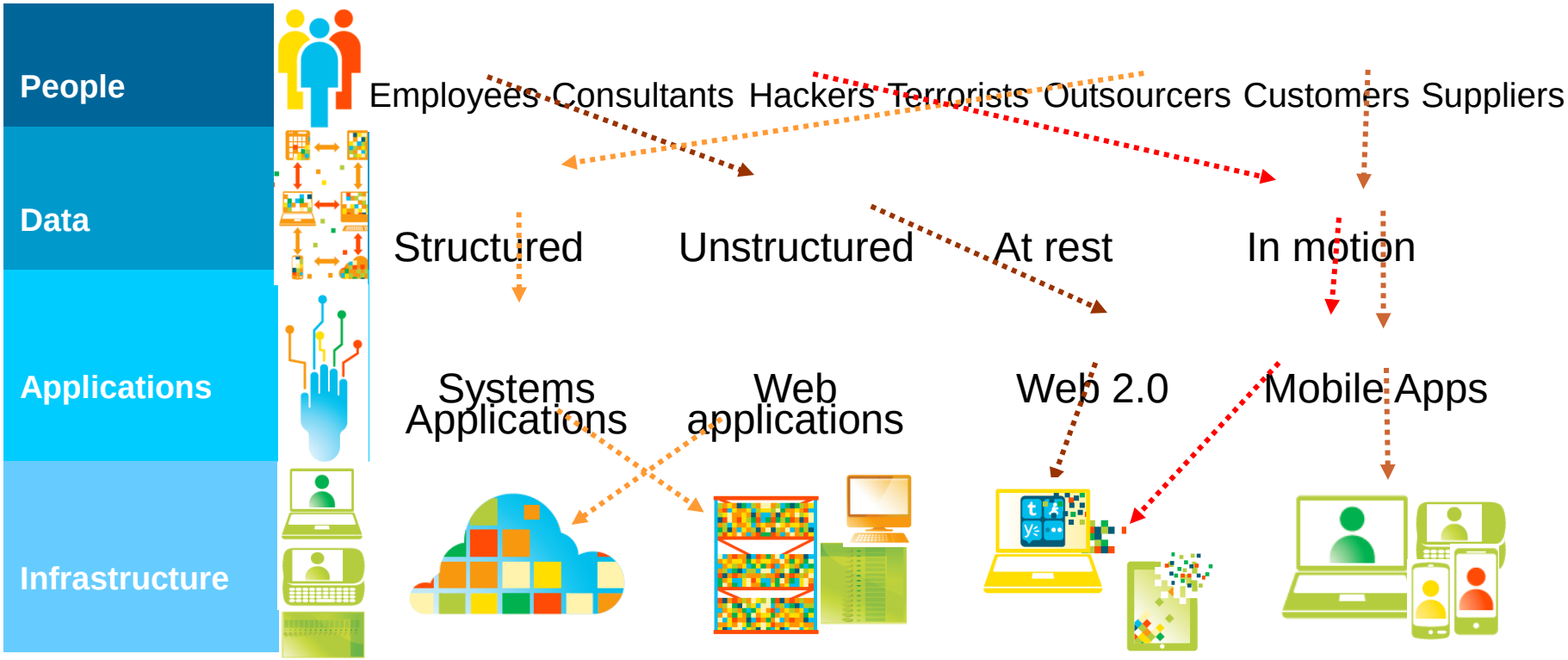
Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more

ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new motivations from cyber crime to state sponsored to terror inspired

…making security a top concern, **from the boardroom down**

Security - within and across domains…



- **77%** of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent
- **75%** felt effectiveness would increase with end-to-end solutions

Source: Ponemon Institute, June 2011

Our customers' pain points:
Security challenges and risks can impact innovation

External threats	Internal threats	Compliance
Sharp rise in external attacks from non-traditional sources	Ongoing risk of careless and malicious insider behavior	Growing need to address an increasing number of mandates
▪ Cyber attacks ▪ Organized crime ▪ Corporate espionage ▪ State-sponsored attacks ▪ Social engineering	▪ Administrative mistakes ▪ Careless inside behavior ▪ Internal breaches ▪ Disgruntled employee actions ▪ Mix of private / corporate data	▪ National regulations ▪ Industry standards ▪ Local mandates ▪ Corporate governance

Impacting innovation

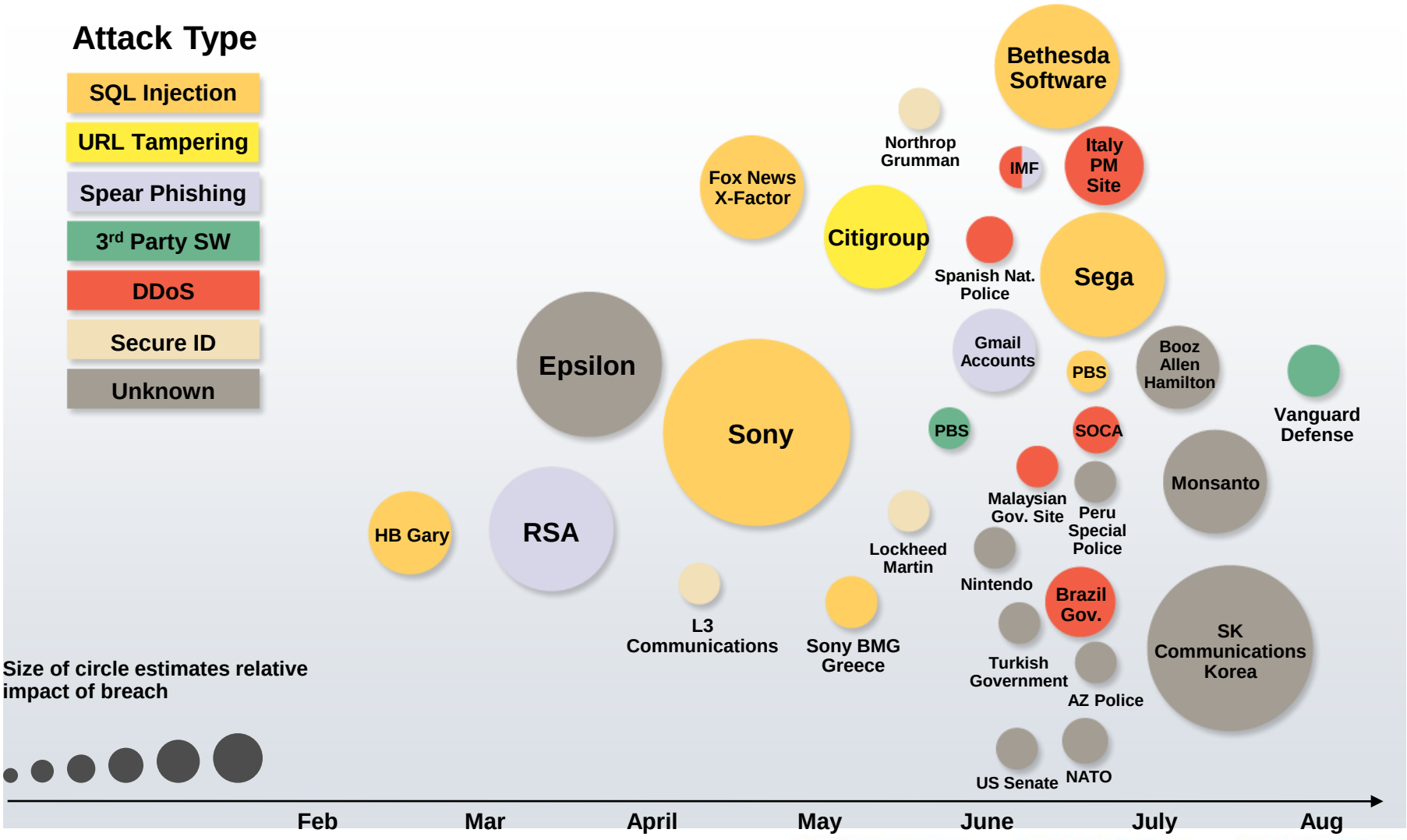
Mobility

Cloud / Virtualization

Social Business

Business Intelligence

2011 – The Year of the Targeted Attack



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

IBM Security Systems

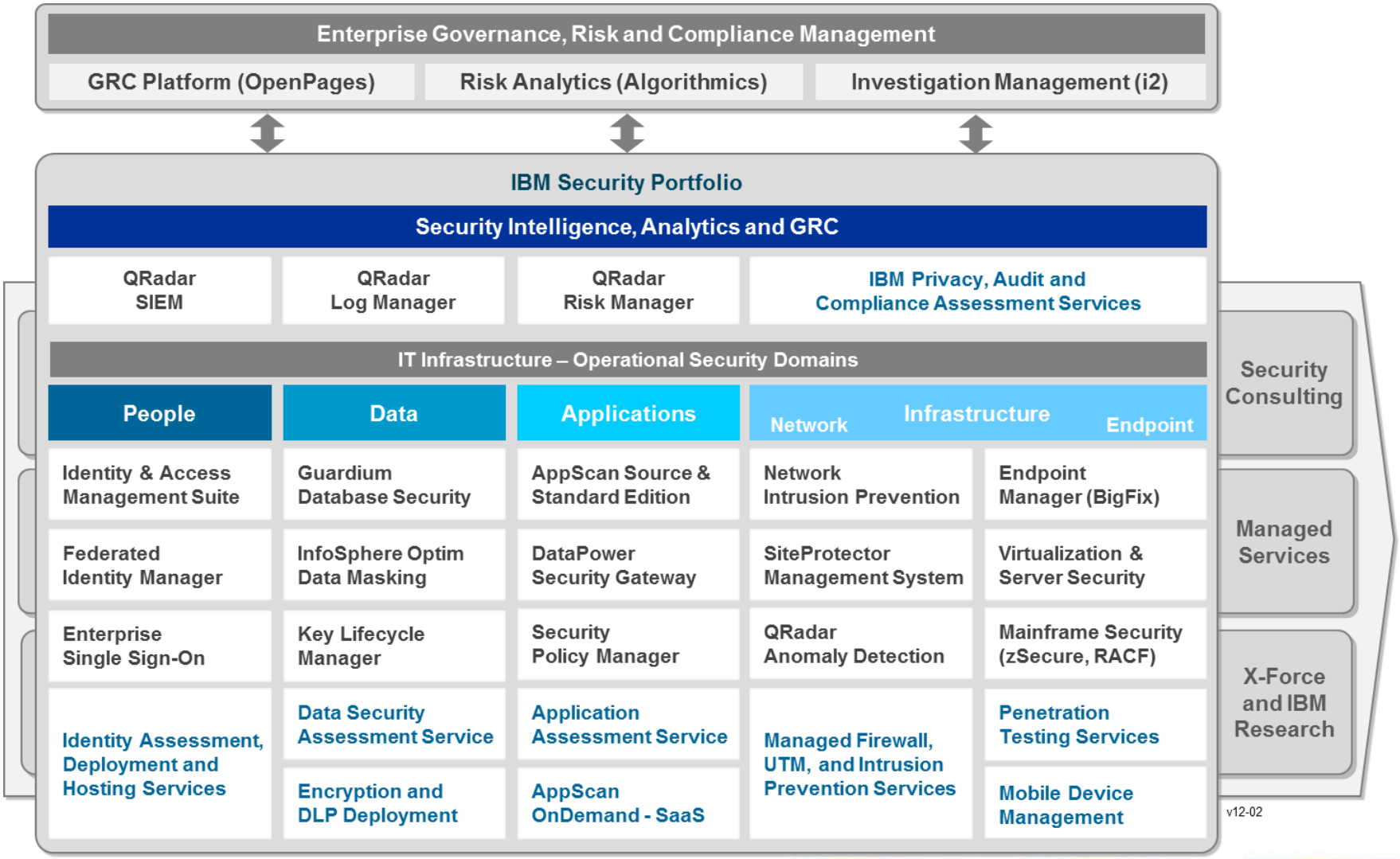
- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence . Integration . Expertise

IBM has security resources that span the globe

- 9 Security operations centers
- 9 Security research centers
- 11 Security solution development labs
- 5500+ Security professionals

Total Visibility: Product Portfolio, Services and Research



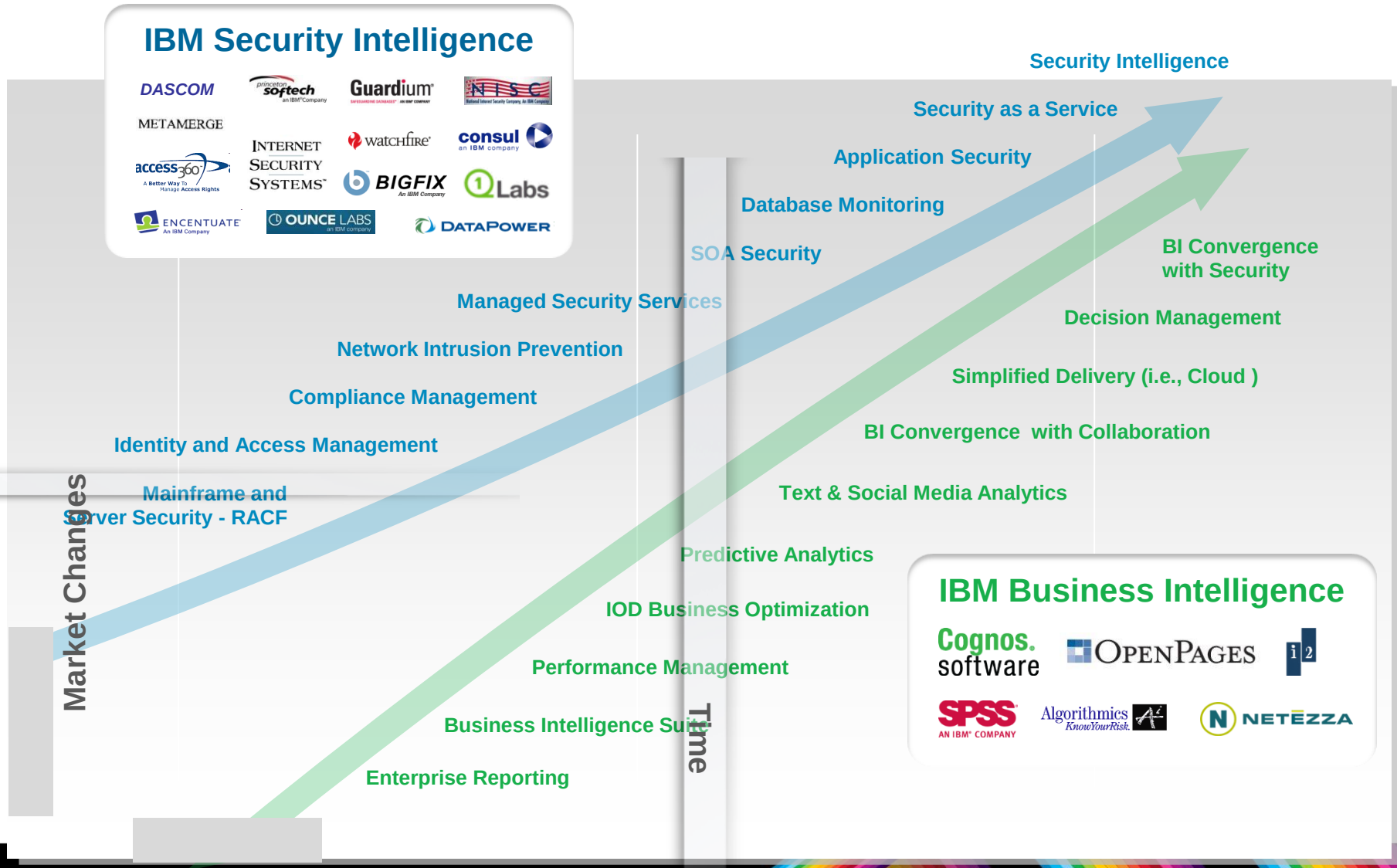
Defense-in-Depth: A Key IBM Differentiator

Unlike competitors, our solutions cover each and every domain of security: *people, applications, data and infrastructure*

This layered approach is analogous to a key security concept: ***defense-in-depth.***

Think of how many security controls you see in a bank, and it's all just protecting the money. *And don't forget the auditors behind the scenes!*

Security and Business Intelligence offer insightful parallels

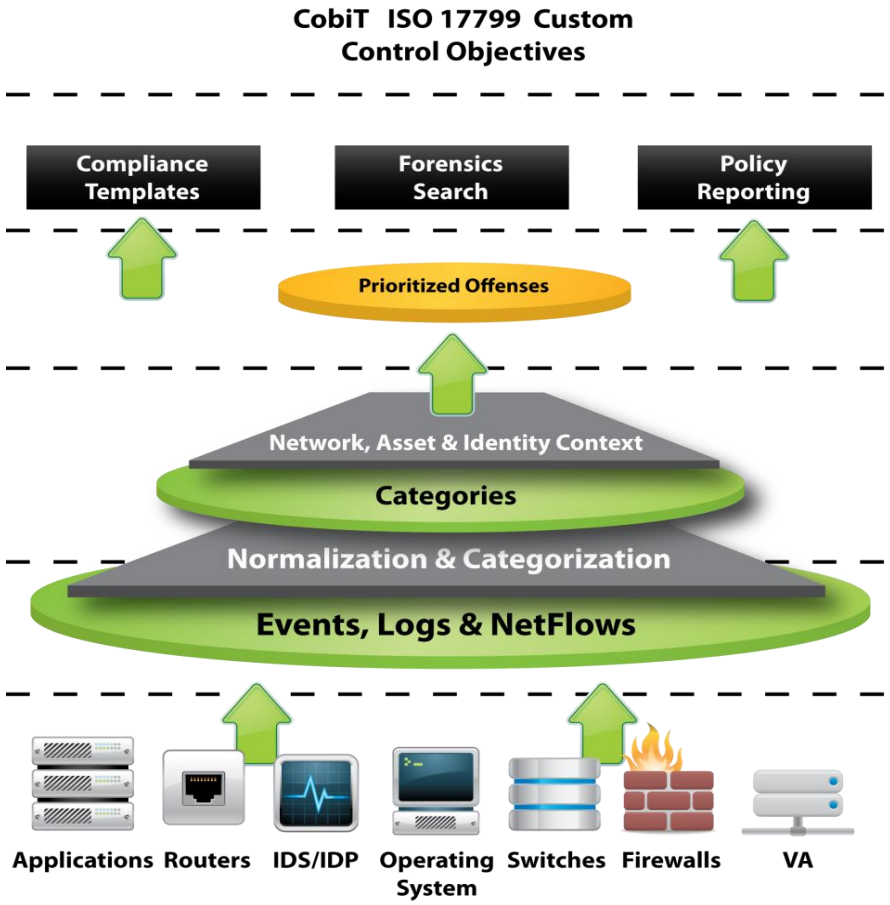


Solving Customer Business Pains that Point Products Can't Address

SRP	DETECTING THREATS OTHERS MISS	Discovered 500 hosts with "Here You Have" virus, which all other security products missed
Chevron	CONSOLIDATING DATA SILOS	2 Billion log events per day reduced to 25 high priority offenses
GUCCI	DETECTING INSIDER FRAUD	Addressed a trusted insider situation involving the stealing and destroying of key data
Cargill	PREDICTING RISKS AGAINST YOUR BUSINESS	Automate the policy monitoring and evaluation process for configuration changes in the infrastructure
WEBB	ADDRESSING REGULATION MANDATES	Real-time monitoring of all network activity, in addition to PCI mandates

QRadar- SOC 2.0

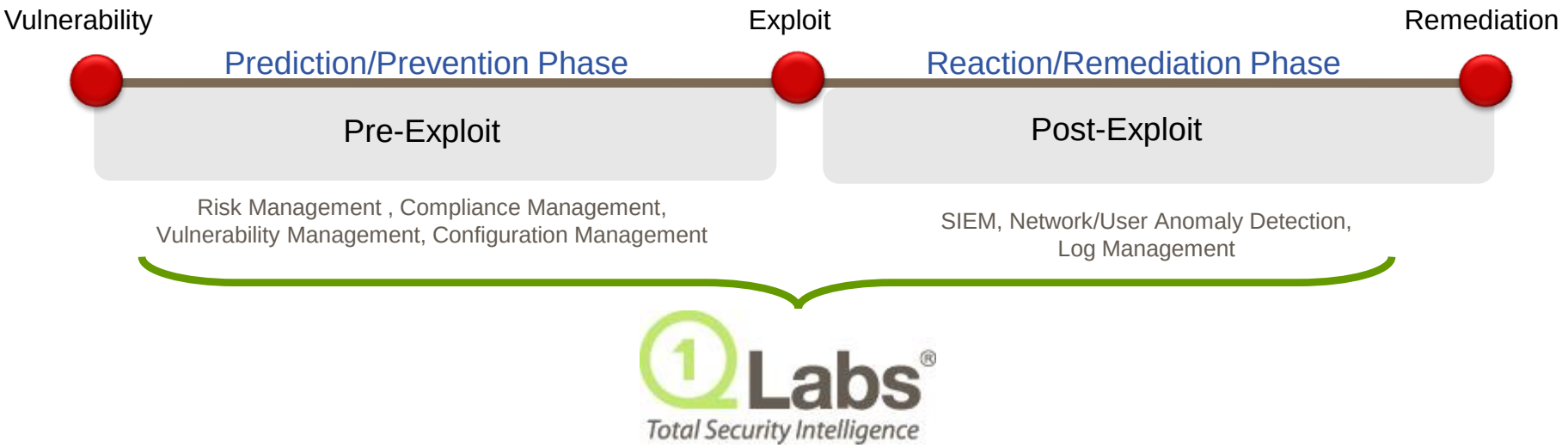
PC | HIPA | FISMA | CoC | NERC | SO



Key Capabilities:

- Sophisticated correlation of events, flows, assets, topologies, vulnerabilities and external data to identify & prioritize threats
- Network flow capture and analysis for deep application insight
- Workflow management to fully track threats and ensure resolution
- Scalable architecture to support the largest deployments

Solutions Across the Entire Compliance and Security Intelligence Lifecycle



- Detecting threats, consolidating data silos, predicting business risk and exceeding regulation mandates require security intelligence
- SIEM is the anchor tenant, collecting and analyzing all telemetry and delivering information in context

"It [enterprise security intelligence] also requires the integration and correlation of security and contextual information to bridge security with business, risk and other key enterprise values, thereby enabling optimal decision making." *--Joseph Feiman, VP and Gartner Fellow*

Gartner

Fully Integrated Security Intelligence

Log Management

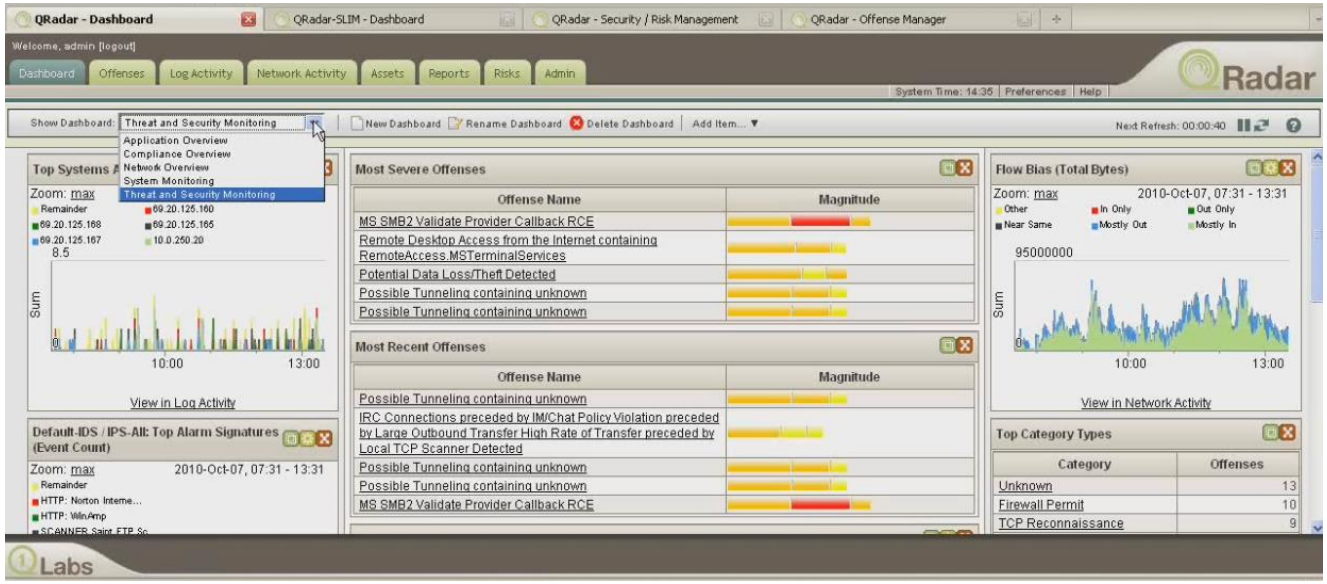
SIEM

Risk Management

Network Activity & Anomaly Detection

Network and Application Visibility

One Console Security

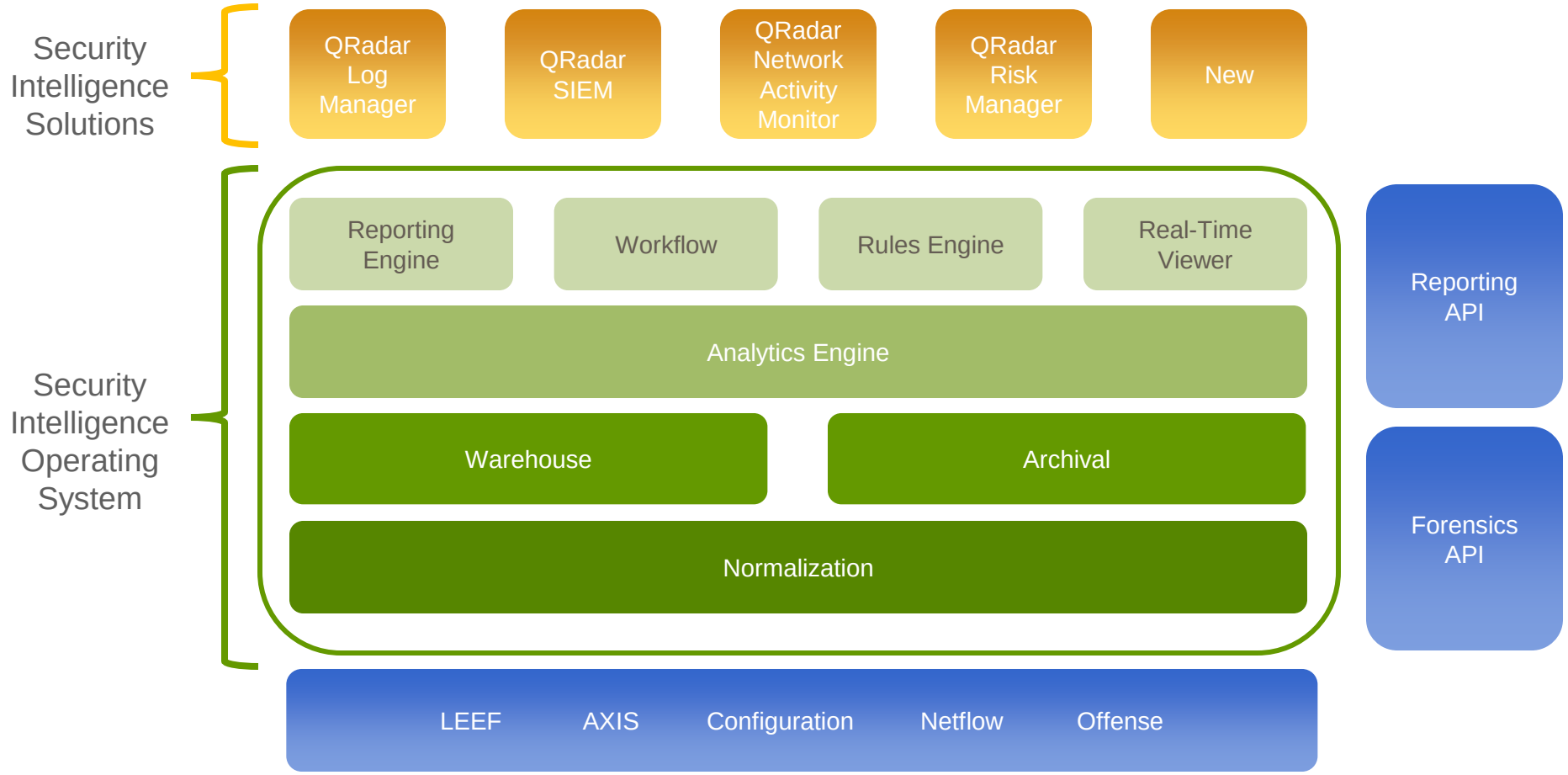


Built on a Single Data Architecture

The QRadar Security Intelligence Solutions Deploy, Expand at Your Pace

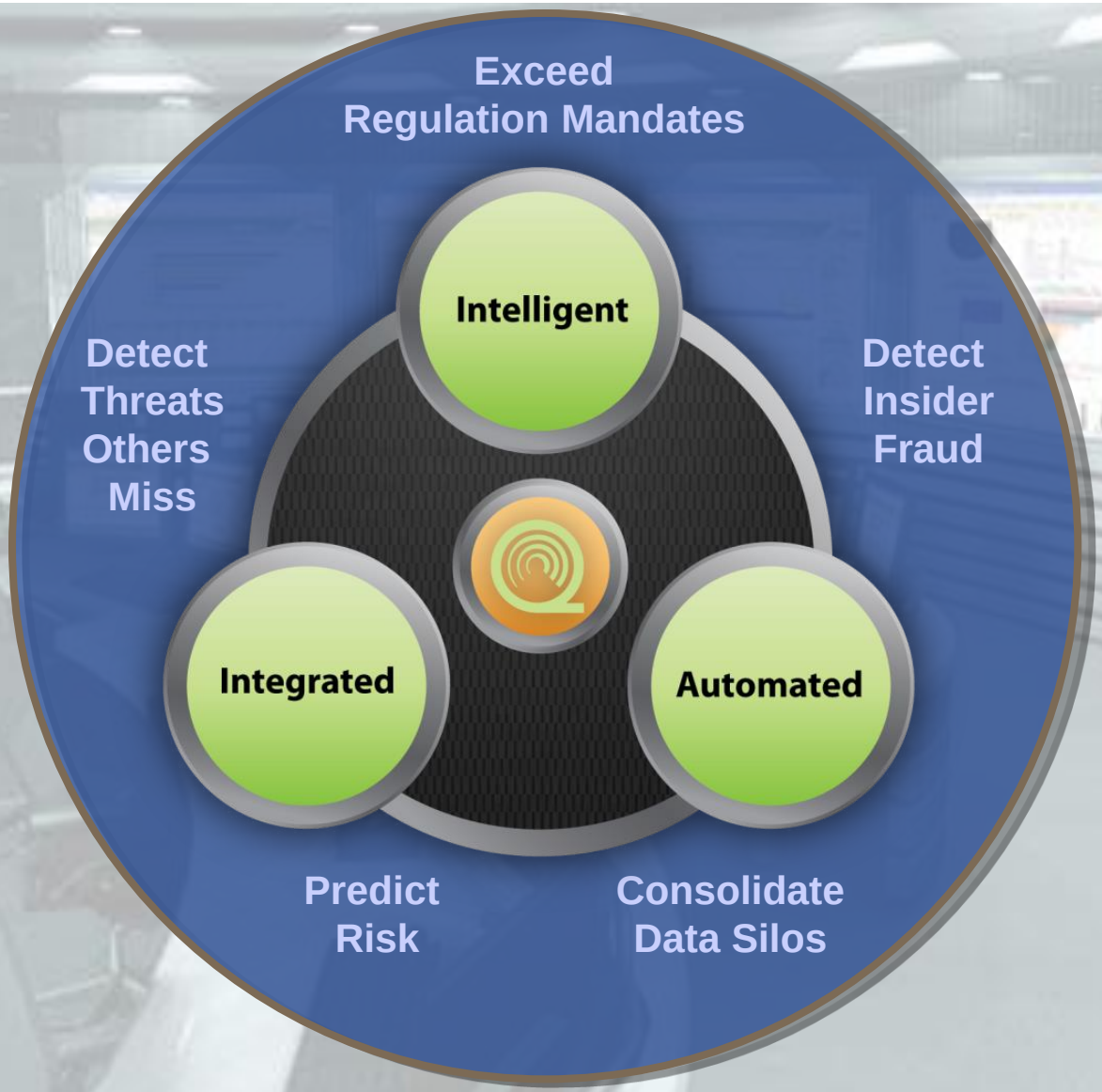
Log Management	QRadar® Log Manager  QRadar® Log Manager Free Edition 	• Turnkey log management • SME to Enterprise • Upgradeable to enterprise SIEM
SIEM/SEM	QRadar® SIEM 	• Integrated log, cyber threat, risk and compliance management • Sophisticated event analytics • Asset profiling and flow analytics
Risk Management	QRadar® Risk Manager 	• Predictive threat modeling & simulation • Scalable configuration monitoring and audit • Advanced threat visualization and impact analysis
Scale	QRadar® High Availability 	• Event Processors • Network Activity Processors • High Availability • Stackable Expansion • Embedded, real-time database
Visibility/ Network Activity	QFlow Collector  VFlow Collector 	• Layer 7 application monitoring • Content capture • Network Analysis

QRadar Product Family
Built On a Common Foundation of QRadar SIOS

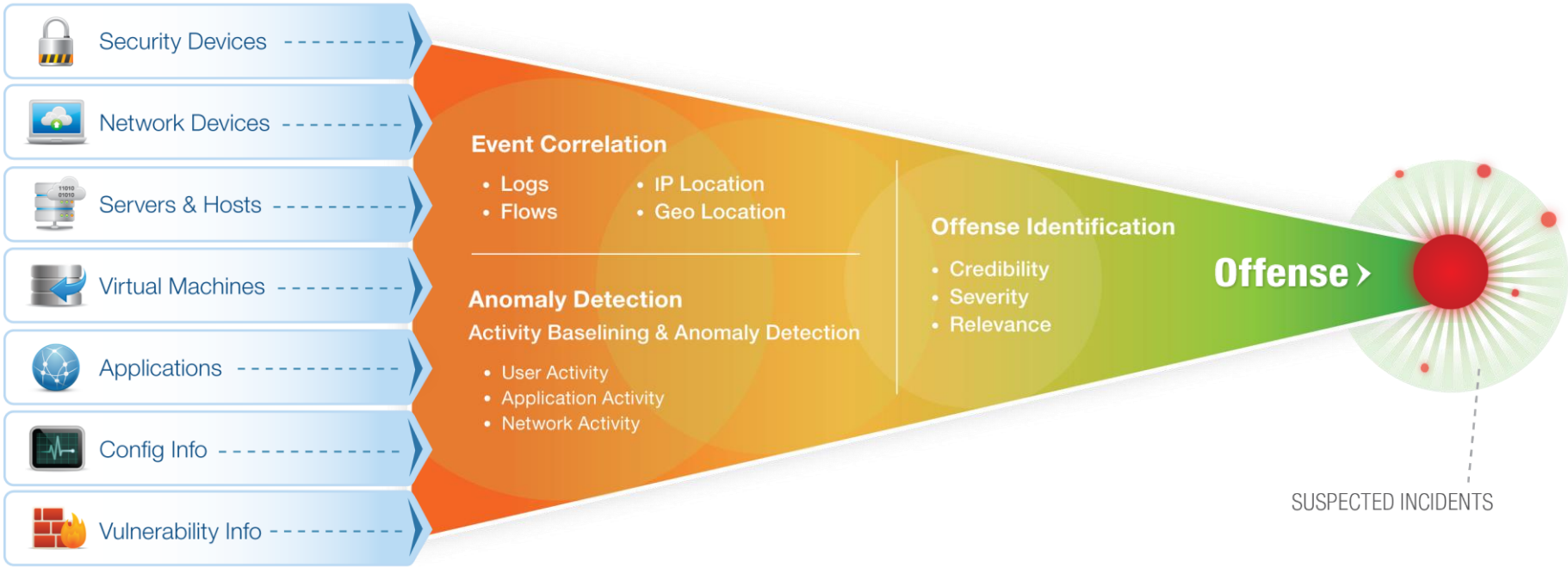


Intelligent Integrated Automated – One Console Security

QRadar: The Most Intelligent, Integrated, Automated Security Intelligence Platform in the Industry

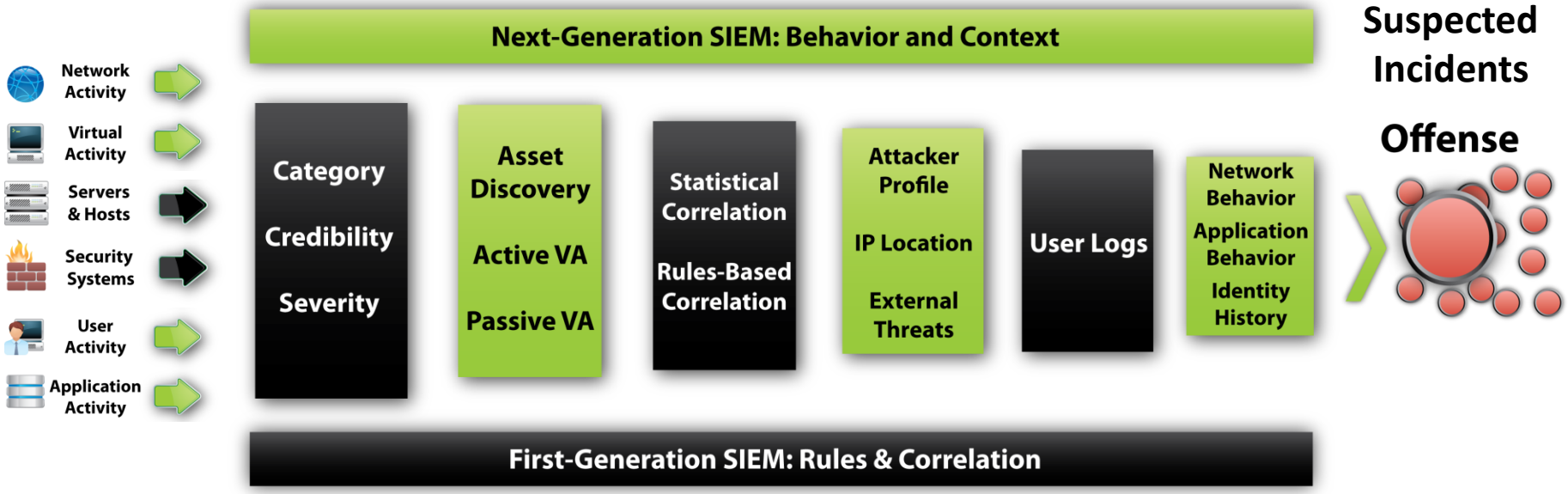


QRadar Security Intelligence Platform: Context and Correlation Drive Deepest Insight



Most Sources + Most Intelligence = Most Accurate & Actionable Insight

Next Generation Intelligence



Threats and Fraud Detected That Others Miss

QRadar's network-wide device integration delivered vastly improved threat detection and compliance reporting.

State Employees' Credit Union

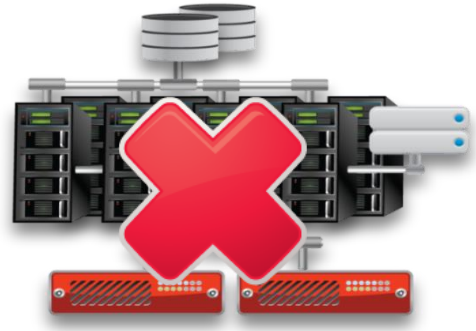
Massive Data Reduction

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

Chevron

QRadar: Integration Eliminates False Choice Between Capability & Simplicity

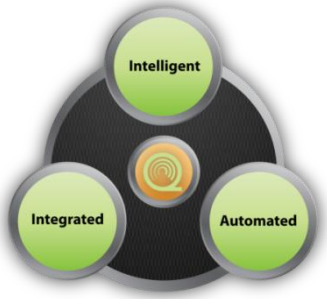
Bolted Together Solution



- Scale problems
- Disparate reporting, searching
- No local decisions
- Complex High Availability
- Multi-product admin and DBA
- Forklift upgrades
- Duplicate log repositories
- Operational bottleneck

QRadar Integrated Solution

- Highly scalable
- Common reporting, searching
- Distributed correlation
- Integrated High Availability
- Unified administration
- Seamless expansion
- Logs stored once
- Total visibility



Unified Administration
Time spent managing security events was reduced by 80% compared to siloed systems

Roto

QRadar: Automation Drives Simplicity and Cost Effectiveness




Monitor

- Auto-discovery of log sources
- Auto-discovery of applications
- Auto-discovery of assets
- Auto-grouping of assets
- Centralized log management
- Automated configuration audits

Analyze

- Auto-tuning
- Auto-detect threats
- Thousands of pre-defined rules
- Easy-to-use event filtering
- Advanced security analytics

Act

- Thousands of predefined reports
- Asset-based prioritization
- Auto-update of threats
- Auto-response
- Directed remediation

Efficient, Immediate, Custom

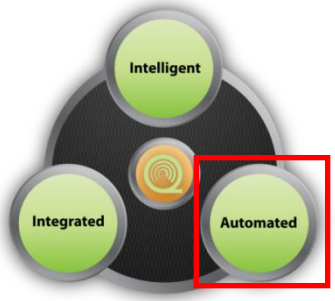
"Where it would take 10 days on our old system to build and test rules, it takes us just 10 minutes in QRadar."

logica

Automation Drives Operations Efficiency

"We were pleased with QRadar being extremely automated, equipped with compliance-driven report templates that were very useful out of the box, which spared us the manpower and resources of having to develop them ourselves."

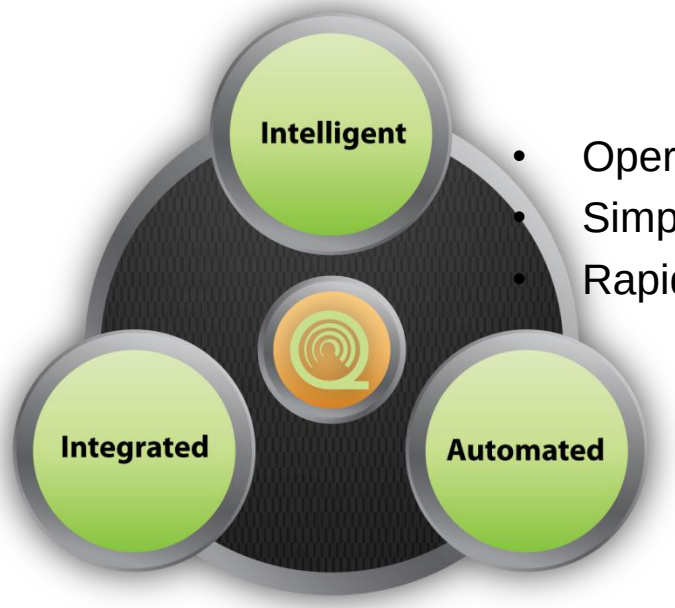
REGULUS



QRadar: The Only Intelligent, Integrated, Automated Security Intelligence Platform in the Industry

- Proactive threat management
- Massive data reduction
- Rapid, complete impact analysis

- Eliminates silos
- Highly scalable
- Flexible, future-proof



- Operational efficiency
- Simple deployment
- Rapid time to value

"We evaluated numerous vendors, including all listed in Gartner's SIEM Magic Quadrant, and Q1 Labs came out on top. Their first-class product support model, superior functionality, and extremely accessible user interface beat the competition"

StateAuto Insurance Companies

"In my 30 years of working with network vendors, Q1 Labs' service is unmatched."
Ron Porritt,
Information security engineer
Gordon Food Service

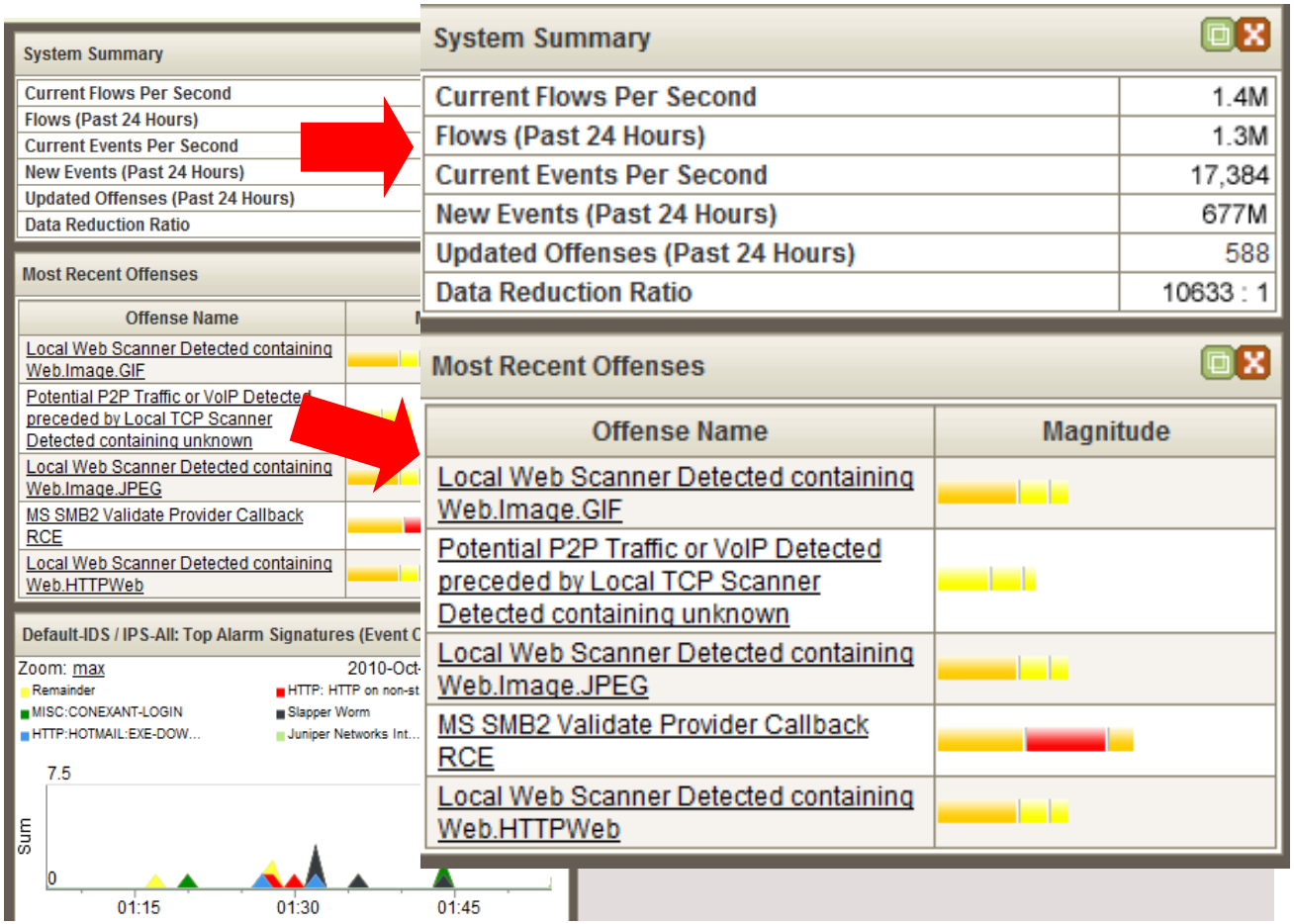
GFS gordon food service

Product Tour: Integrated Console

- Single browser-based UI
- Role-based access to information & functions
- Customizable dashboards (work spaces) per user
- Real-time & historical visibility and reporting

- Advanced data mining and drill down
- Easy to use rules engine with out-of-the-box security intelligence

Product Tour: Data Reduction & Prioritization



Previous 24hr period of network and security activity (2.7M logs)

QRadar correlation & analysis of data creates offenses (129)

Offenses are a complete history of a threat or violation with full context about accompanying network, asset and user identity information

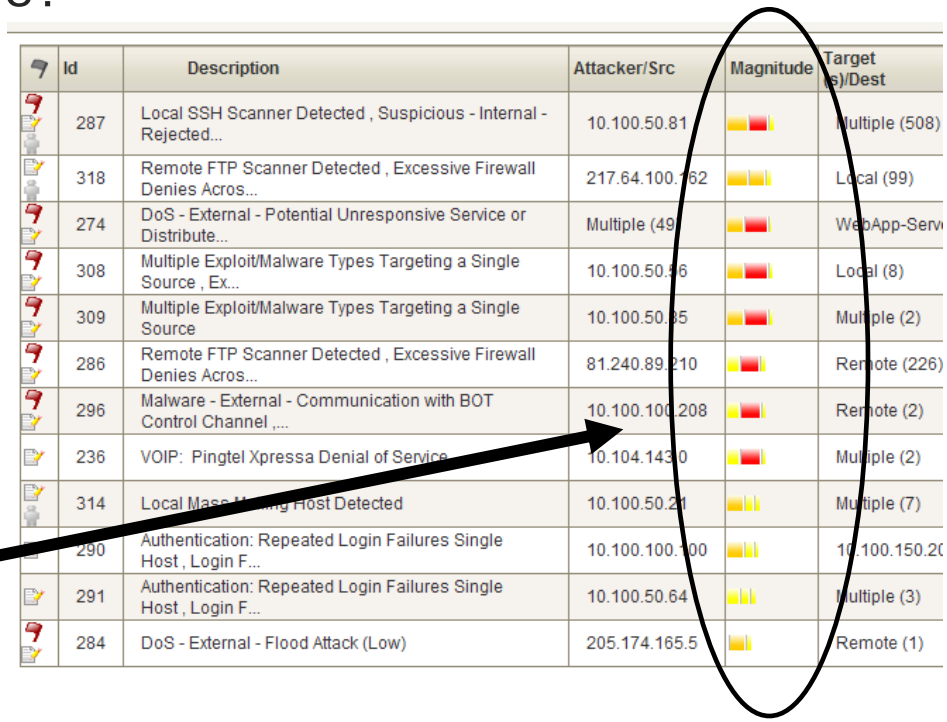
Offenses are further prioritized by business impact

Product Tour: Intelligent Offense Scoring

QRadar judges “magnitude” of offenses:

- *Credibility:*
  A false positive or true positive?
- *Severity:*
  Alarm level contrasted with target vulnerability
- *Relevance:*
  Priority according to asset or network value

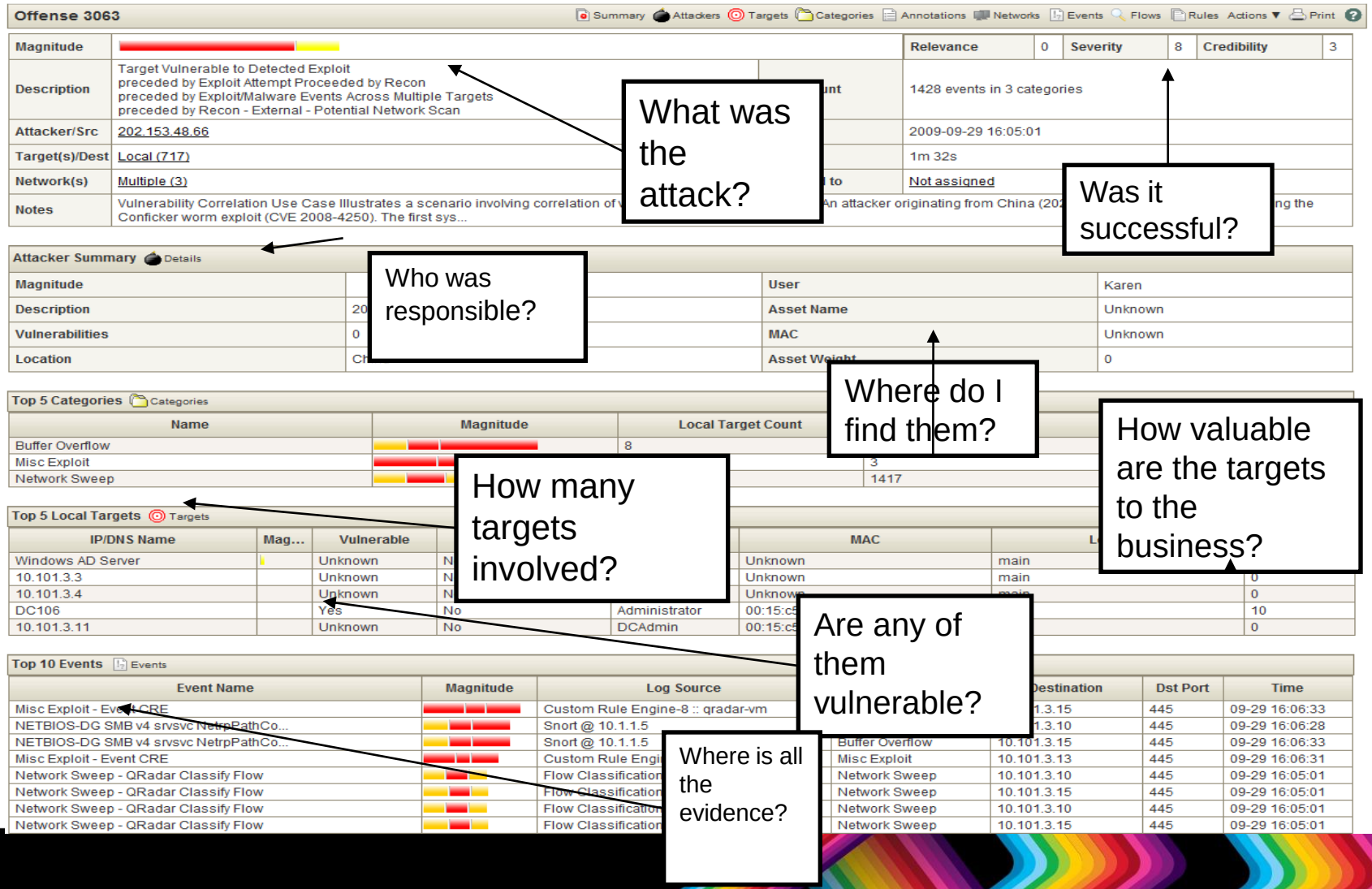
Priorities can change over time based on situational awareness



	Id	Description	Attacker/Src	Magnitude	Target (s)/Dest
	287	Local SSH Scanner Detected , Suspicious - Internal - Rejected...	10.100.50.81		Multiple (508)
	318	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	217.64.100.162		Local (99)
	274	DoS - External - Potential Unresponsive Service or Distribute...	Multiple (49)		WebApp-Serv
	308	Multiple Exploit/Malware Types Targeting a Single Source , Ex...	10.100.50.86		Local (8)
	309	Multiple Exploit/Malware Types Targeting a Single Source	10.100.50.85		Multiple (2)
	286	Remote FTP Scanner Detected , Excessive Firewall Denies Acros...	81.240.89.210		Remote (226)
	296	Malware - External - Communication with BOT Control Channel ,...	10.100.100.208		Remote (2)
	236	VOIP: Pingtel Xpressa Denial of Service	10.104.143.0		Multiple (2)
	314	Local Mass [illegible] Host Detected	10.100.50.21		Multiple (7)
	290	Authentication: Repeated Login Failures Single Host , Login F...	10.100.100.100		10.100.150.20
	291	Authentication: Repeated Login Failures Single Host , Login F...	10.100.50.64		Multiple (3)
	284	DoS - External - Flood Attack (Low)	205.174.165.5		Remote (1)

Product Tour: Offense Management

Clear, concise and comprehensive delivery of relevant information:



Product Tour: Out-of-the-Box Rules & Searches

1000’s of real-time correlation rules and analysis tests

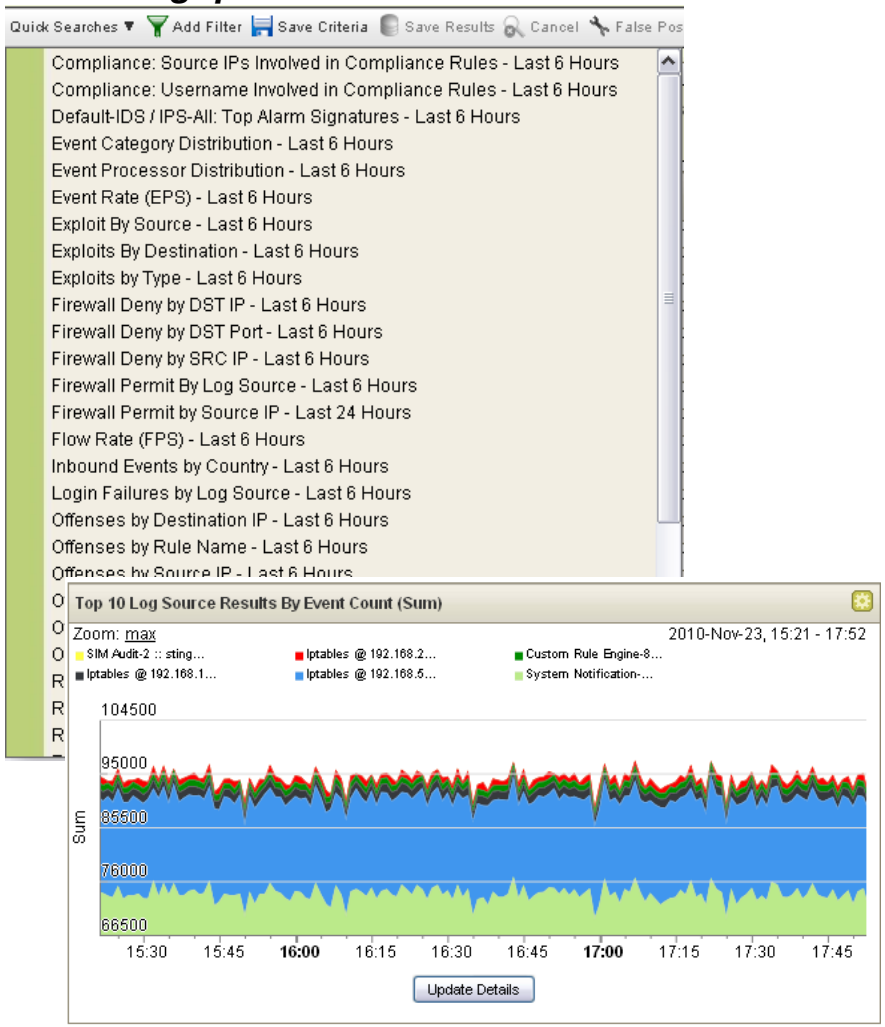
100’s of out-of-the-box searches and views of network activity and log data

- Provides quick access to critical information

Custom log fields

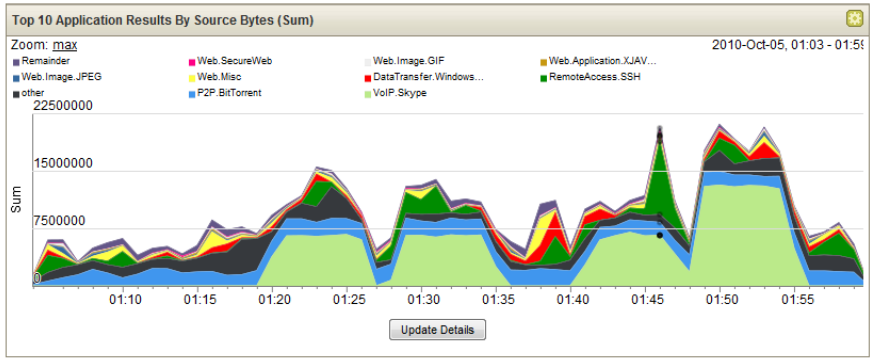
- Provides flexibility to extract log data for searching, reporting and dashboards. Product ships with dozens of pre-defined fields for common devices.

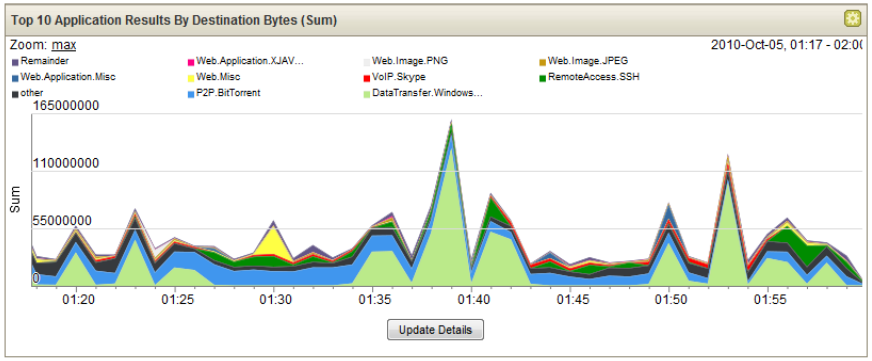
Default log queries/views



Product Tour: Flows for Network Intelligence

- Detection of day-zero attacks that have no signature
- Policy monitoring and rogue server detection
- Visibility into all attacker communication
- Passive flow monitoring builds asset profiles & auto-classifies hosts
- Network visibility and problem solving (not just security related)





(Hide Charts)

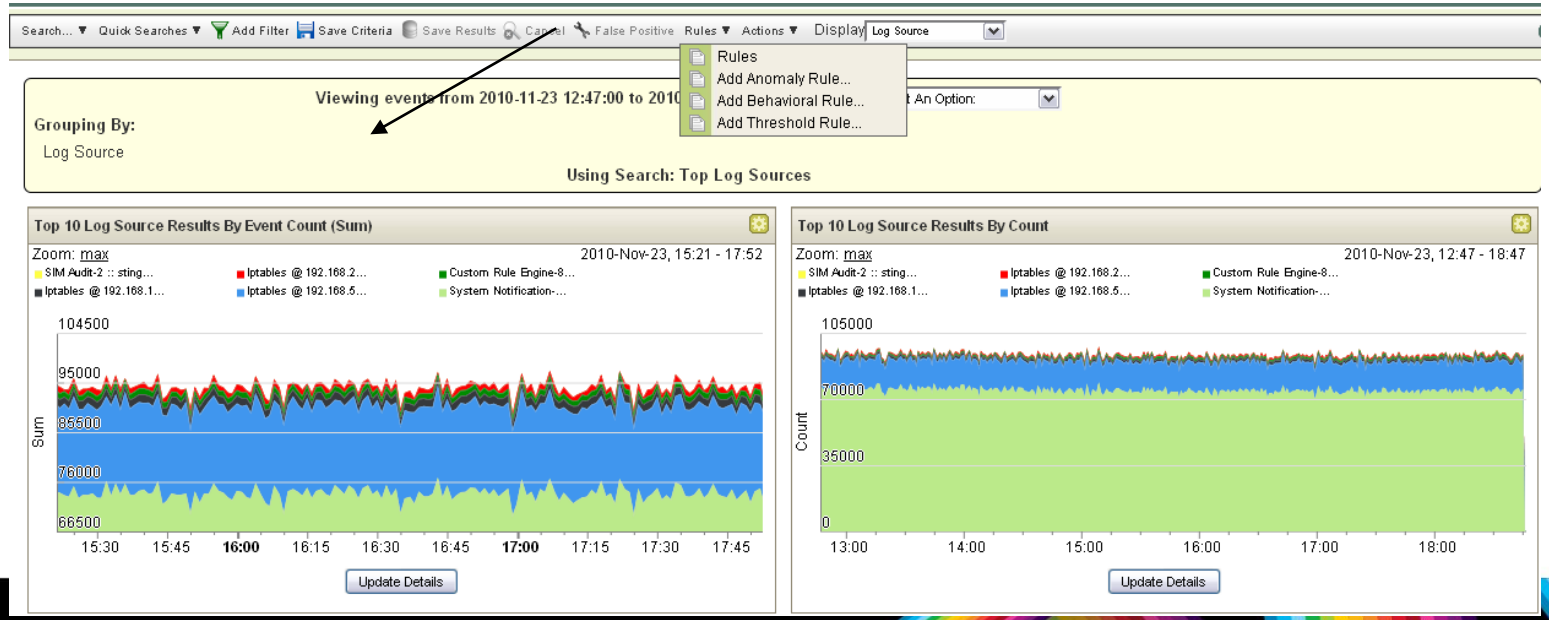
Application	Source IP (Unique Count)	Source Network (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Destination Network (Unique Count)	Source Bytes (Sum)	Destination Bytes (Sum)	Total Bytes (Sum)	Source Packets (Sum)	Destination Packets (Sum)	Total Packets (Sum)	Count
DataTransfer.Window	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	266 544	9 127 364	9 393 908	4 194	6 930	11 014	761

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

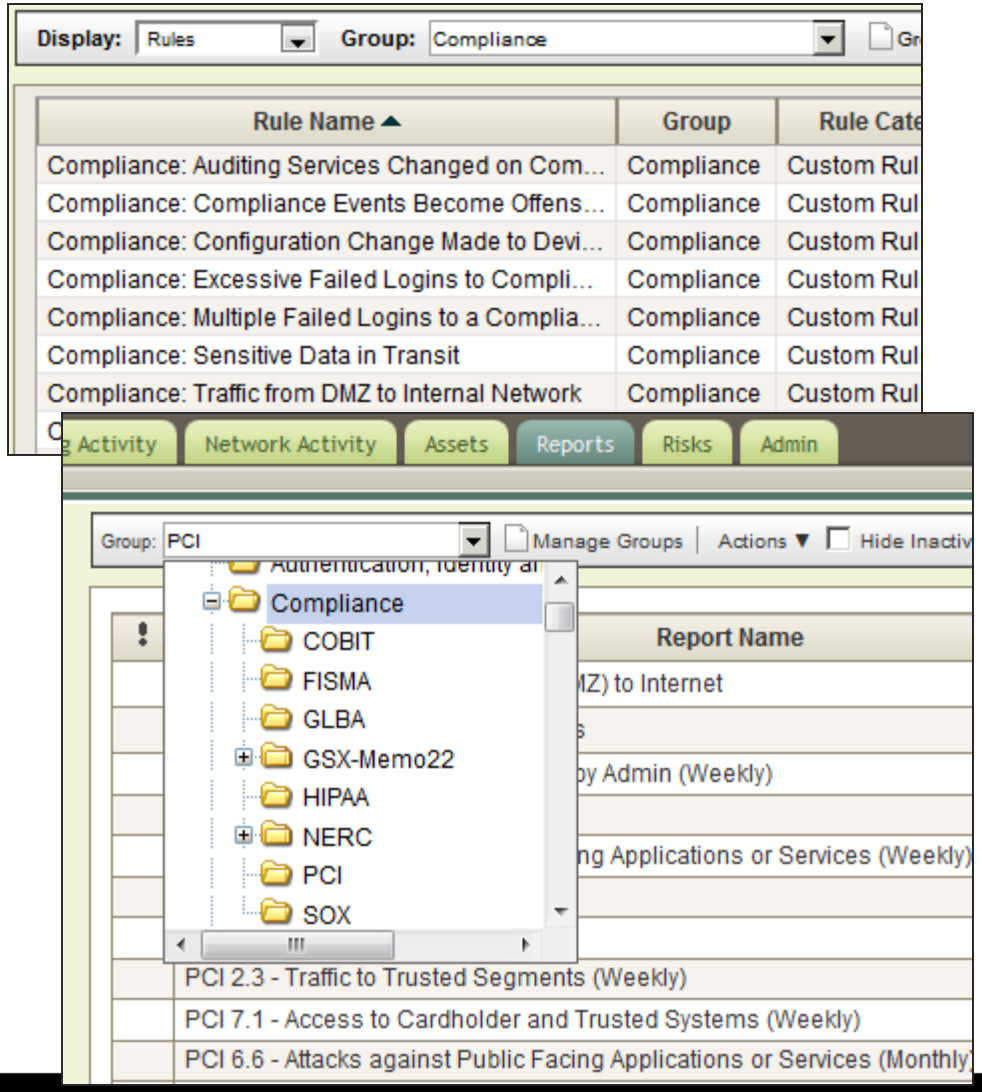
Page: 1 Go < 1 | 2

Product Tour: Flows for Application Visibility

- Flow collection from native infrastructure
- Layer 7 data collection and analysis
- Full pivoting, drill down and data mining on flow sources for advanced detection and forensic examination
- Visibility and alerting according to rule/policy, threshold, behavior or anomaly conditions across network and log activity

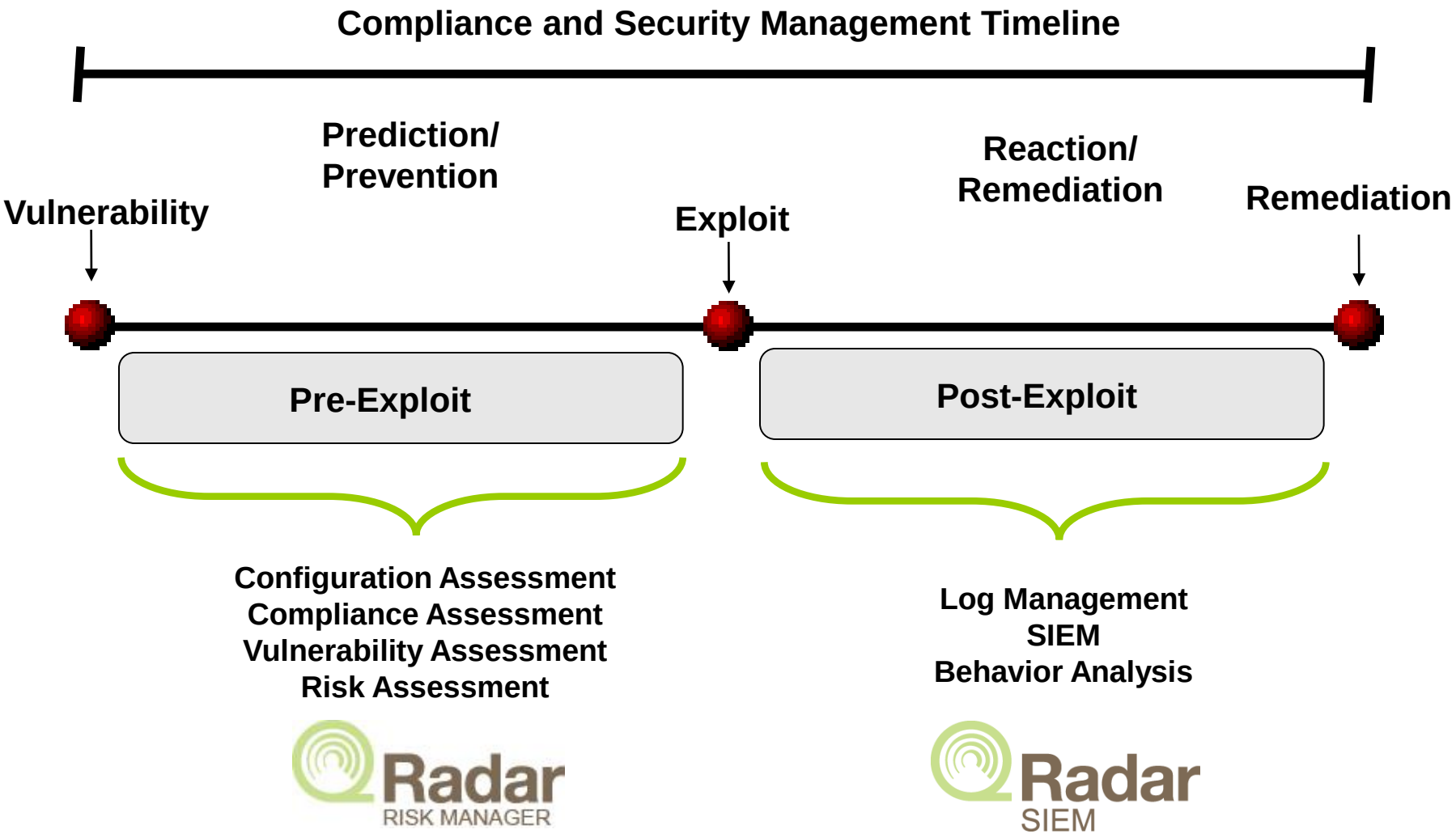


Product Tour: Compliance Rules and Reports



- Out-of-the-box templates for specific regulations and best practices:
  - COBIT, SOX, GLBA, NERC, FISMA, PCI, HIPAA, UK GCSx
- Easily modified to include new definitions
- Extensible to include new regulations and best practices
- Can leverage existing correlation rules

Driver for QRadar Risk Manager (QRM):
Two-Phased Compliance and Security Timeline

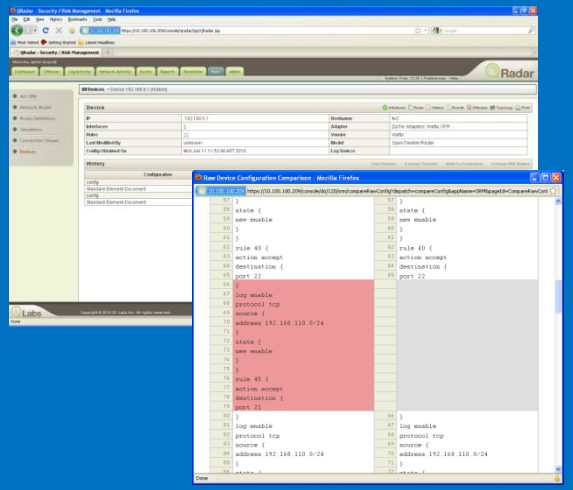


QRadar Risk Manager

Solution At-A-Glance

QRadar Risk Manager moves organizations beyond traditionally reactive security management by delivering:

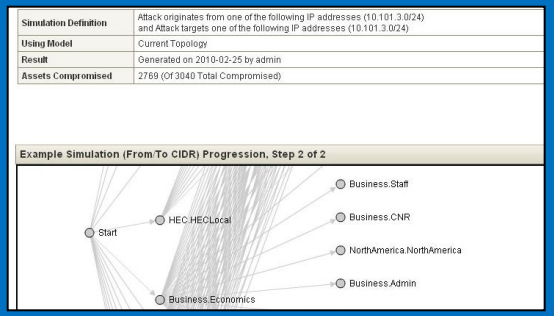
Multi-vendor network configuration monitoring & audit



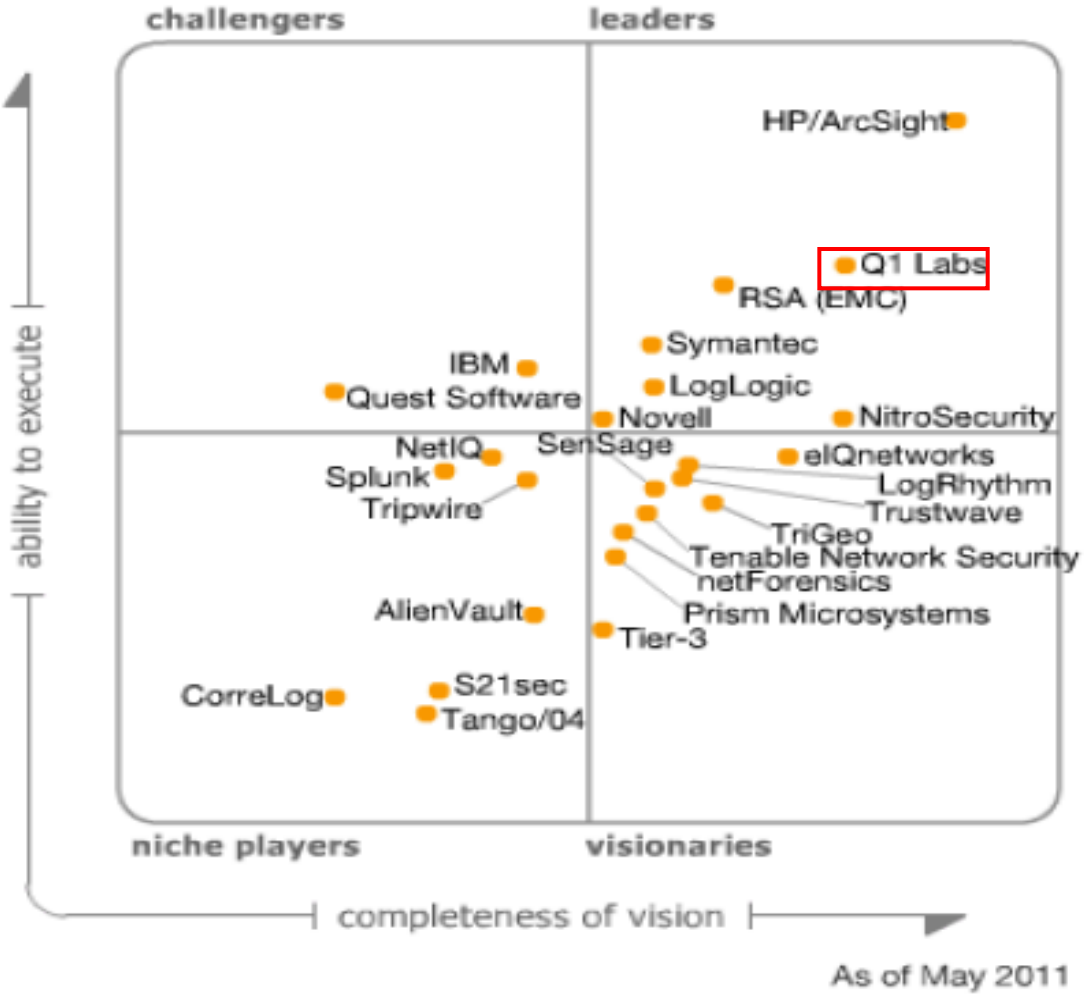
Automated compliance and policy verification

Requirement	
Configuration Audit	✓
Network Activity	✓
Vulnerability Management	✓
Risk Management	✓

Predictive threat modeling & simulation



Analyst View

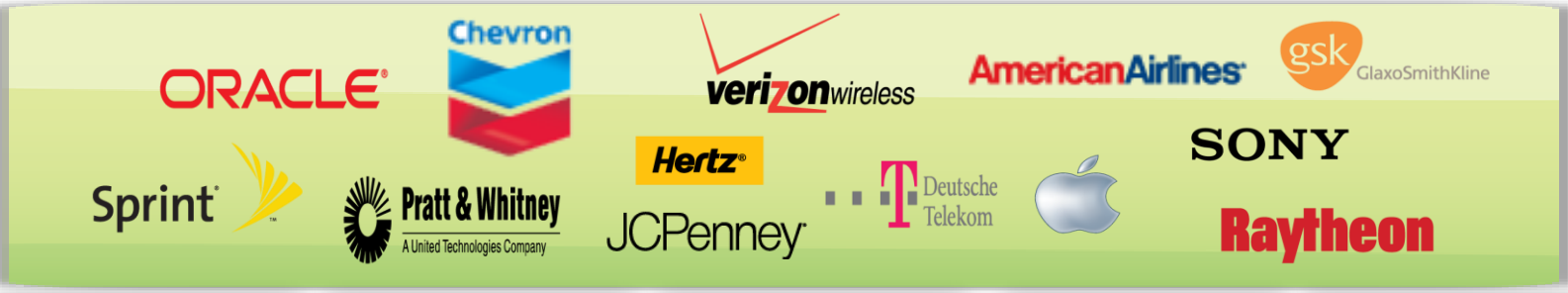


QRadar SIEM Market Success

- “Leader” in Gartner SIEM Magic Quadrant
- Ranked #1 product for Compliance needs by Gartner
- Only SIEM product that incorporates network behavior anomaly detection (NBAD)
- Industry awards include:
  - Global Excellence in Surveillance Award from InfoSecurity Products Guide
  - “Hot Pick” by Information Security magazine
  - GovernmentVAR 5-Star Award

Total Security Intelligence for Any Organization

Security Intelligence for the Total Market



Government

NASA
U.S.ARMY
STATE OF COLORADO 1876
UNITED STATES STRATEGIC COMMAND
GOVERNOR'S OFFICE OF HOMELAND SECURITY STATE OF CALIFORNIA
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
FIRE DEPARTMENT CITY OF NEW YORK

Financial

Hong Leong Bank
Deloitte
PRICEWATERHOUSECOOPERS
GEICO
Scottrade
ABN·AMRO

Energy

FPL
mge
Chesapeake ENERGY
bp
ISO new england

Retail

Yum!
ORVIS
claire's
Lord & Taylor
COACH
AN AMERICAN LEGACY
Liz claiborne
HARVEY NICHOLS

Education

PURDUE
WAYNE STATE UNIVERSITY
McGill
CORNELL UNIVERSITY FOUNDED A.D. 1865

Use Cases

QRadar SIEM excels at the most challenging use cases:

- Complex threat detection
- Malicious activity identification
- User activity monitoring
- Compliance monitoring
- Fraud detection and data loss prevention
- Network and asset discovery

Q&A

Thank You

ISTUTI