BusinessConnect and SolutionsConnect
It’s time to make bold moves.

Next generation security analytics

Vijay Dheap
Global Product Manager - IBM Master Inventor
Big Data Security Intelligence & Mobile Security
IBM Security Solutions

Please Note:

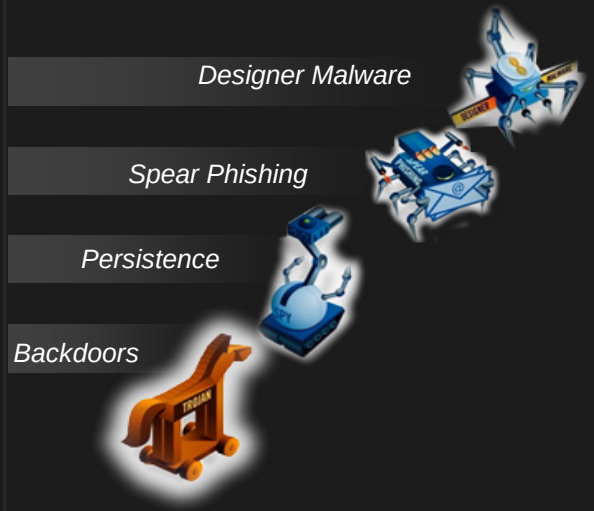
IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.

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.

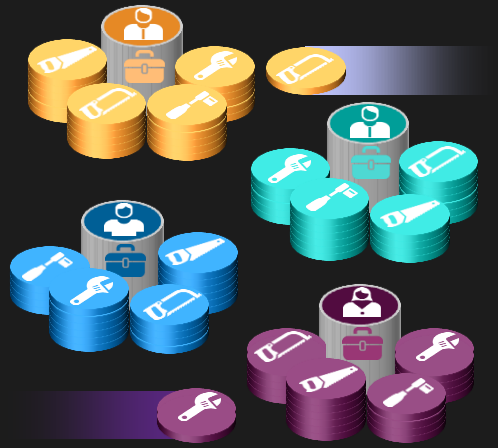
The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features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

Today's challenges

Escalating Attacks



Increasing Complexity



Resource Constraints

ITSecurityJobs.com

Sorry, no applicants found

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

2011 **2012** **2013**

Attack types

- SQL injection
- Spear phishing
- DDoS
- Third-party software
- Physical access
- Malware
- XSS
- Watering hole
- Undisclosed

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

Challenges compounded by volume of data/transactions/issues

200,000+ Facebook, Twitter, Linked-in accesses a day

500+ files uploaded to internet sites a day

2,000+ files a day downloaded from the internet

30% of network use is remote

2 laptops a week go AWOL

20 new IT assets a week

3000+ SPAM and phishing emails a week

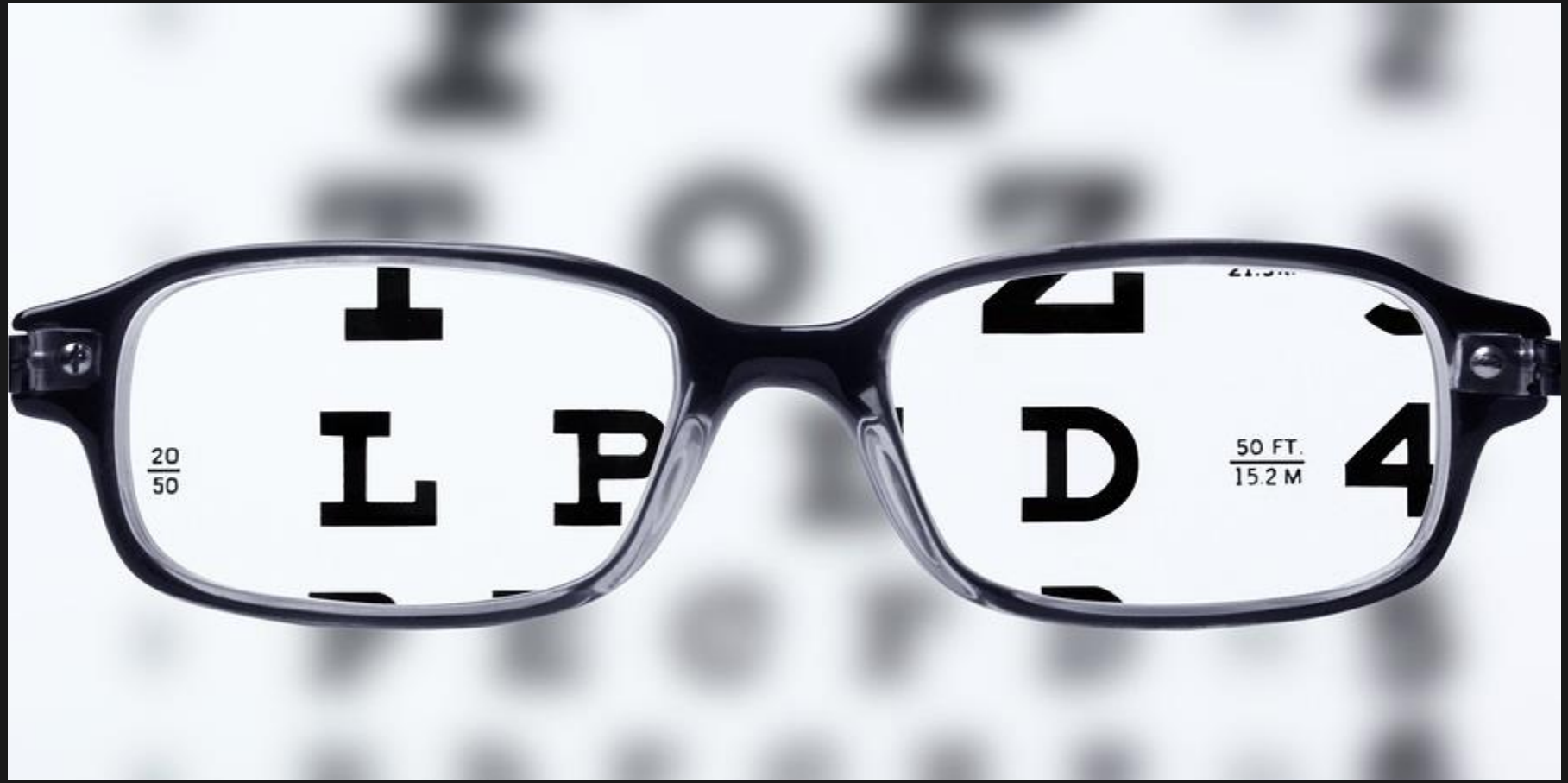
External network scanned 10 times a day

100,000+ vulnerabilities in the network

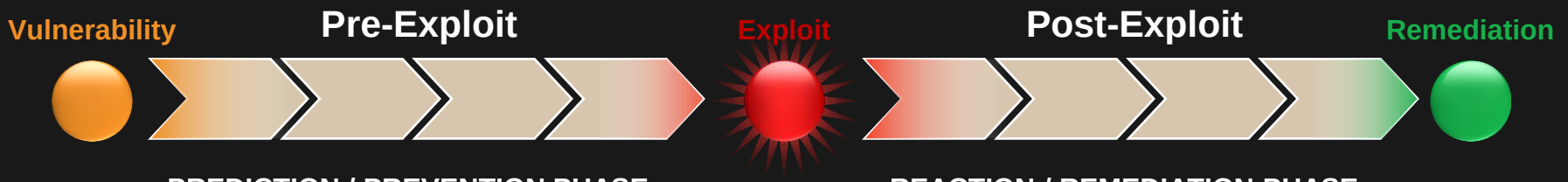
5 network alerts per minute

100+ potentially malicious web site visits per day

20 Network configuration changes a week

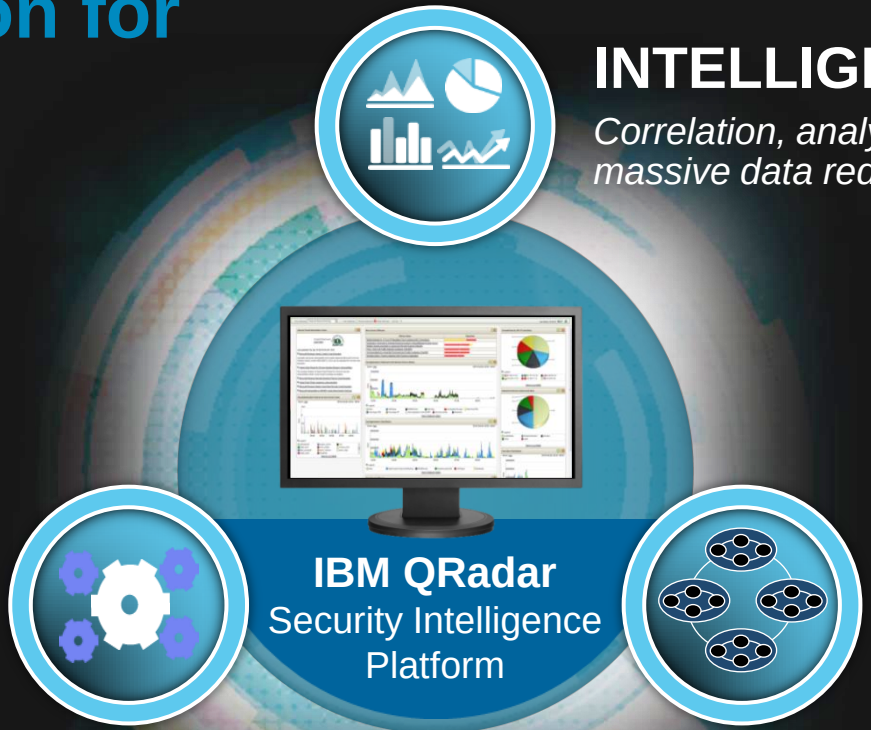


Security Intelligence is asking the right questions, and getting answers



- Gain visibility over gaps
- Detect deviations
- Prioritize vulnerabilities
- Automatically detect threats
- Gather situational awareness
- Quickly investigate incidents

IBM's solution for Security Intelligence



INTELLIGENT

Correlation, analysis and massive data reduction

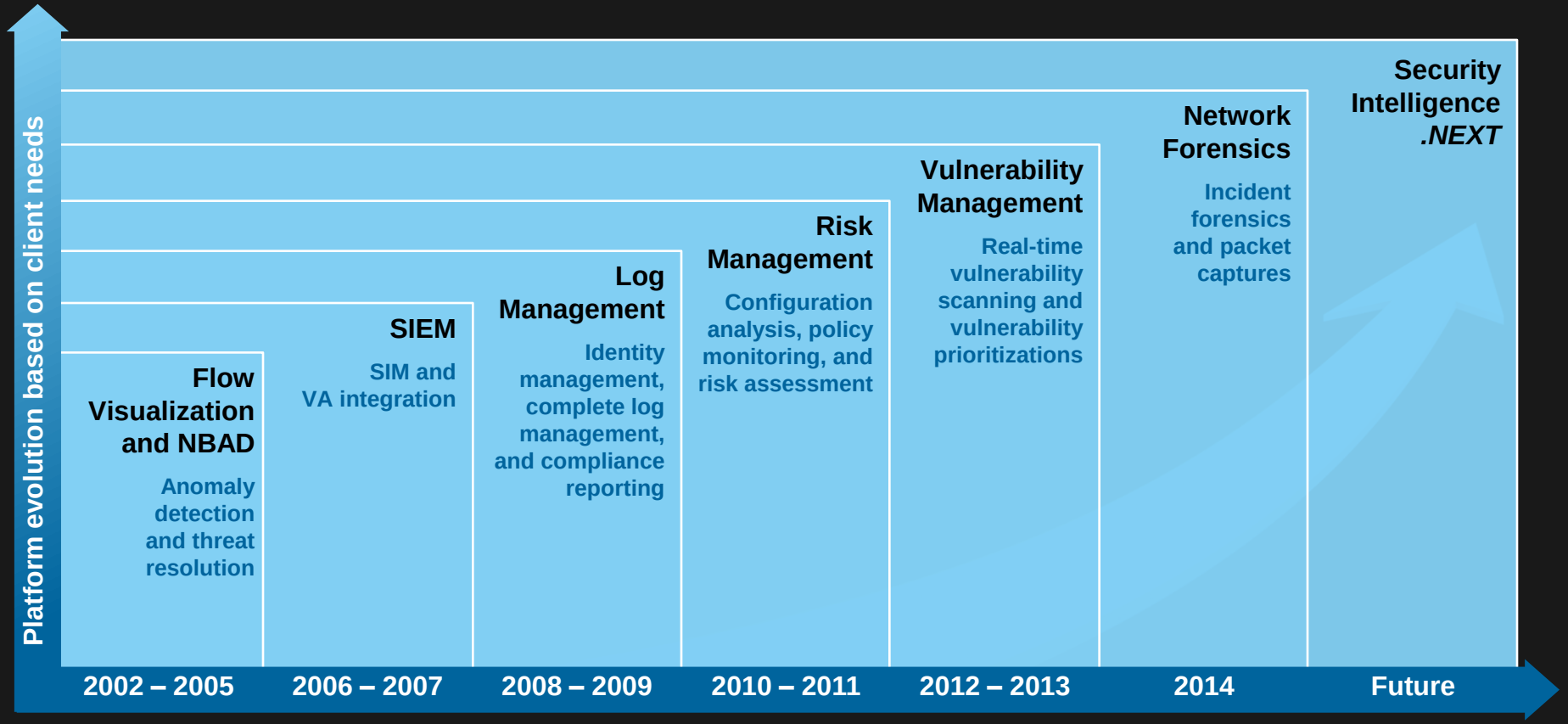
AUTOMATED

Driving simplicity and accelerating time-to-value

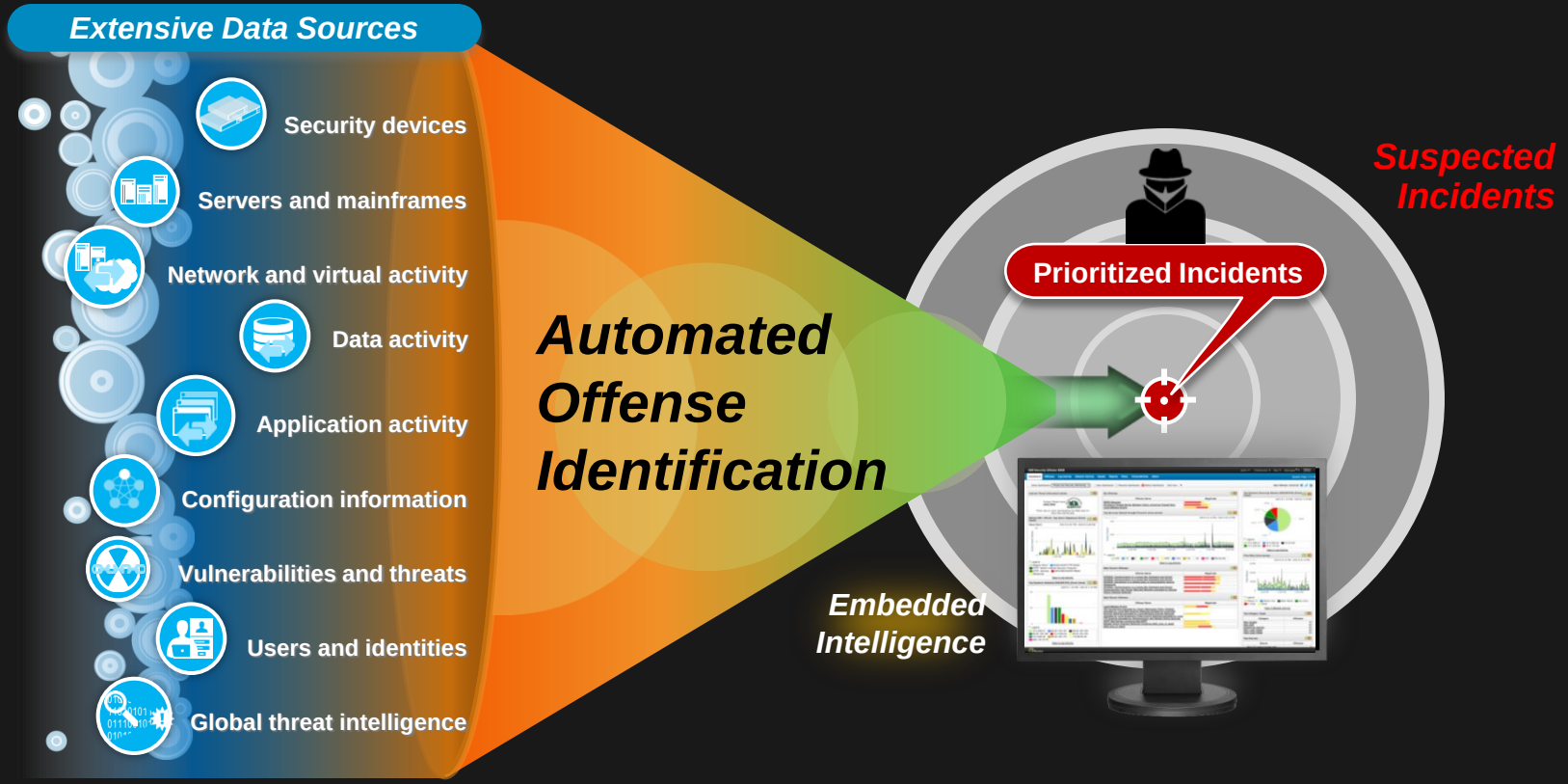
INTEGRATED

Unified architecture delivered in a single console

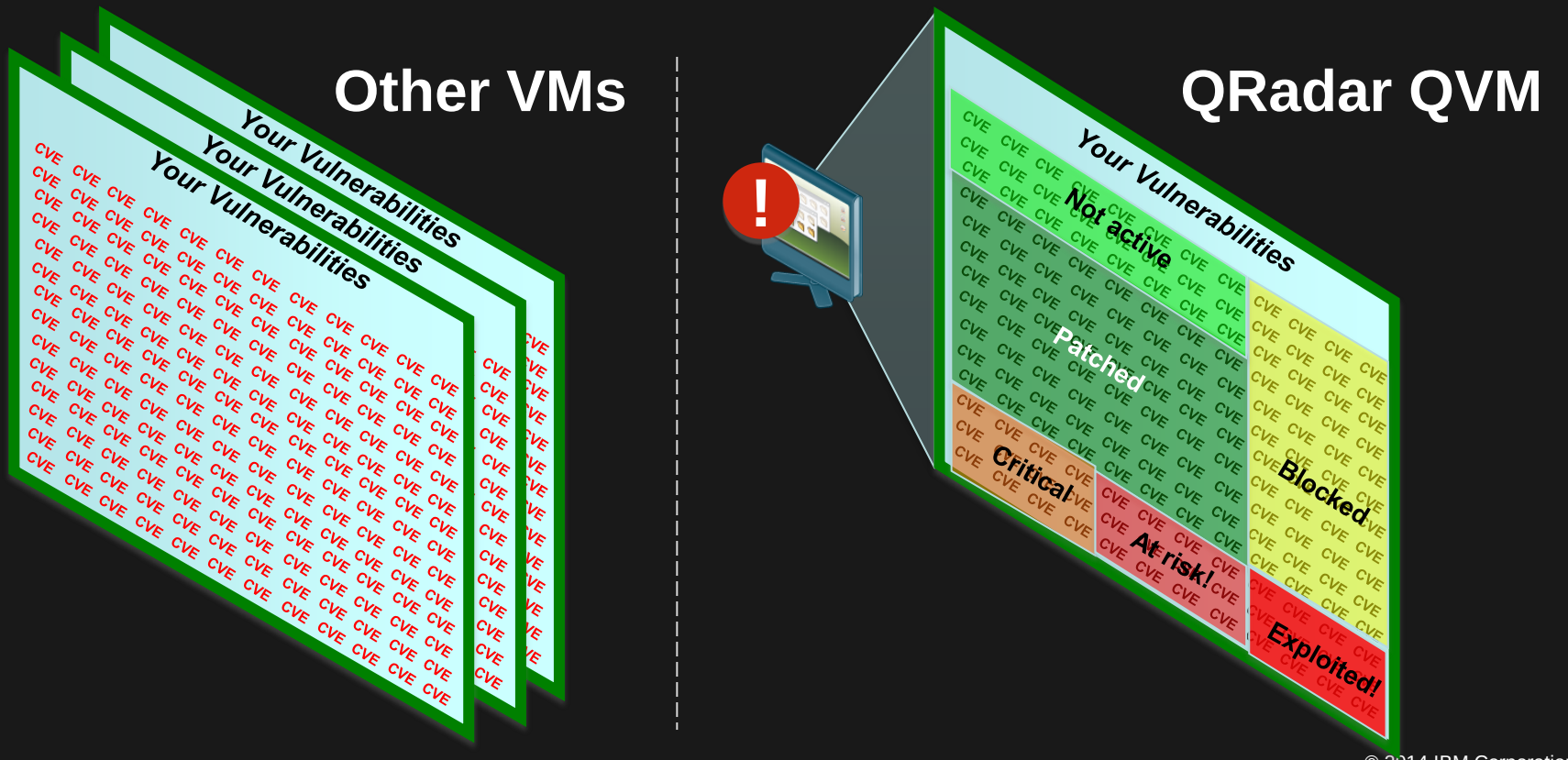
Evolving IBM Security Intelligence strategy based on client needs



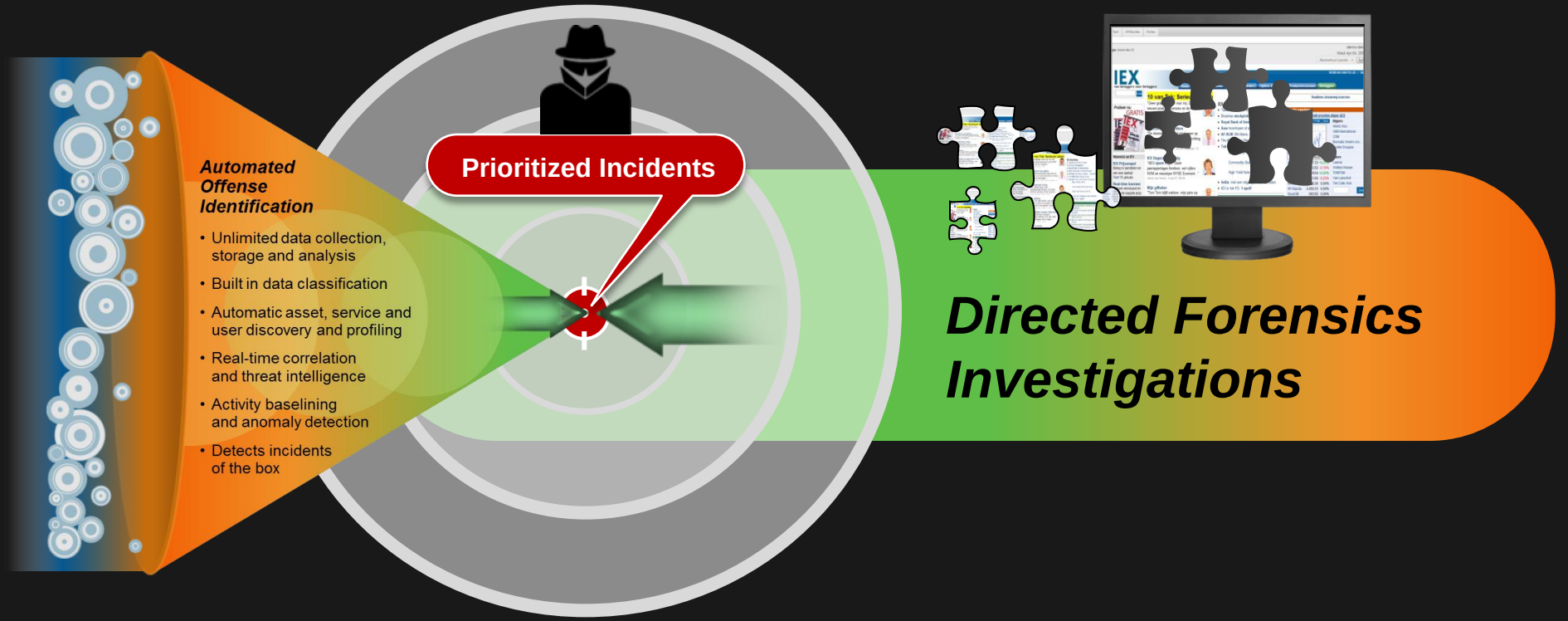
Embedded intelligence offers automated offense identification



Strengthened by integrated vulnerability insights

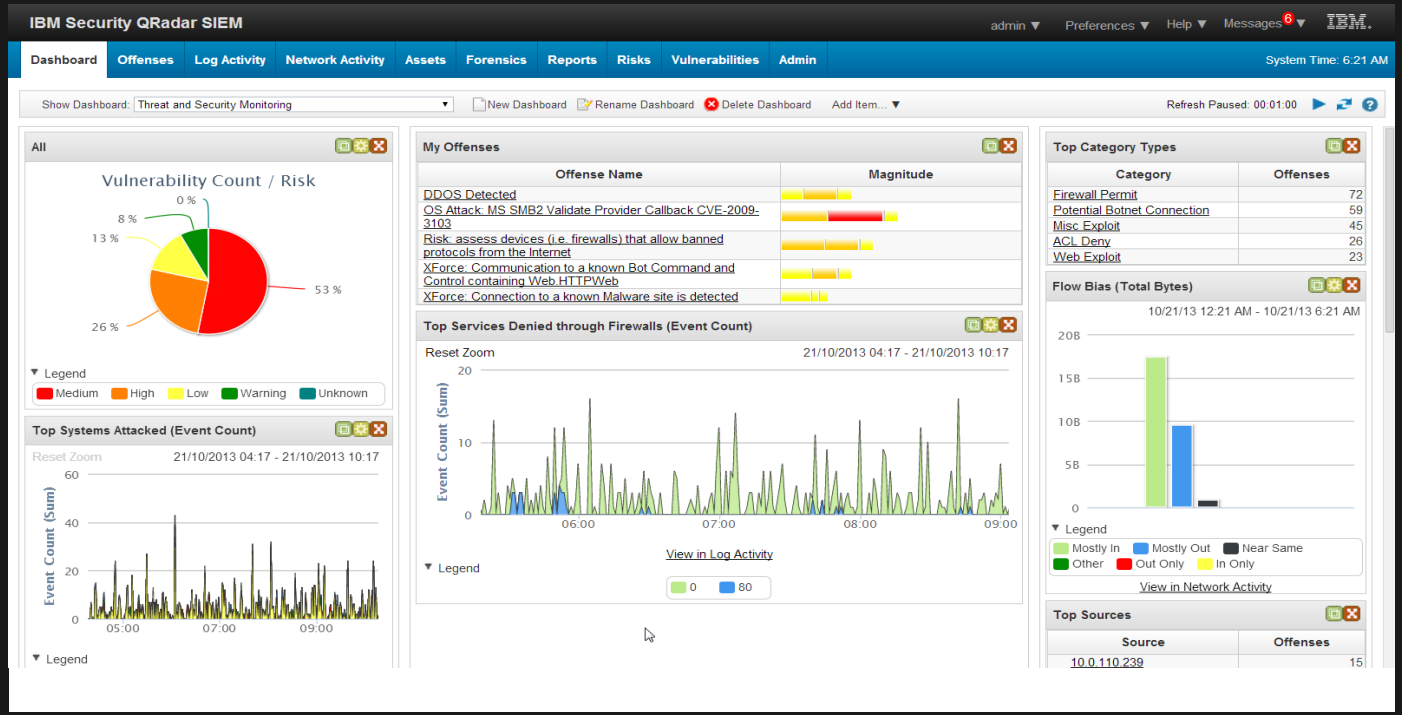


And giving high-fidelity evidence beyond just detecting an incident

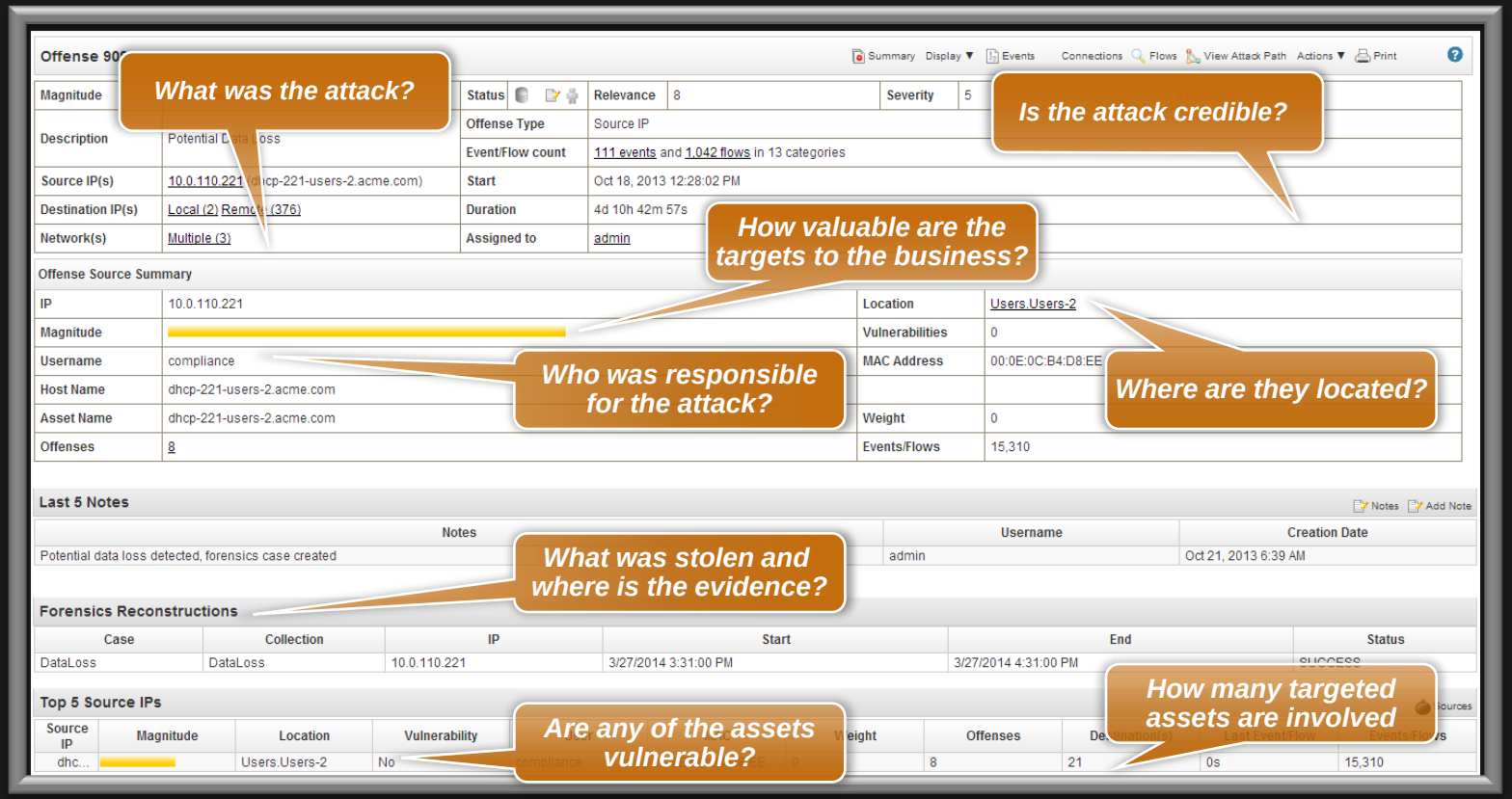


An integrated, unified architecture in a single web-based console

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



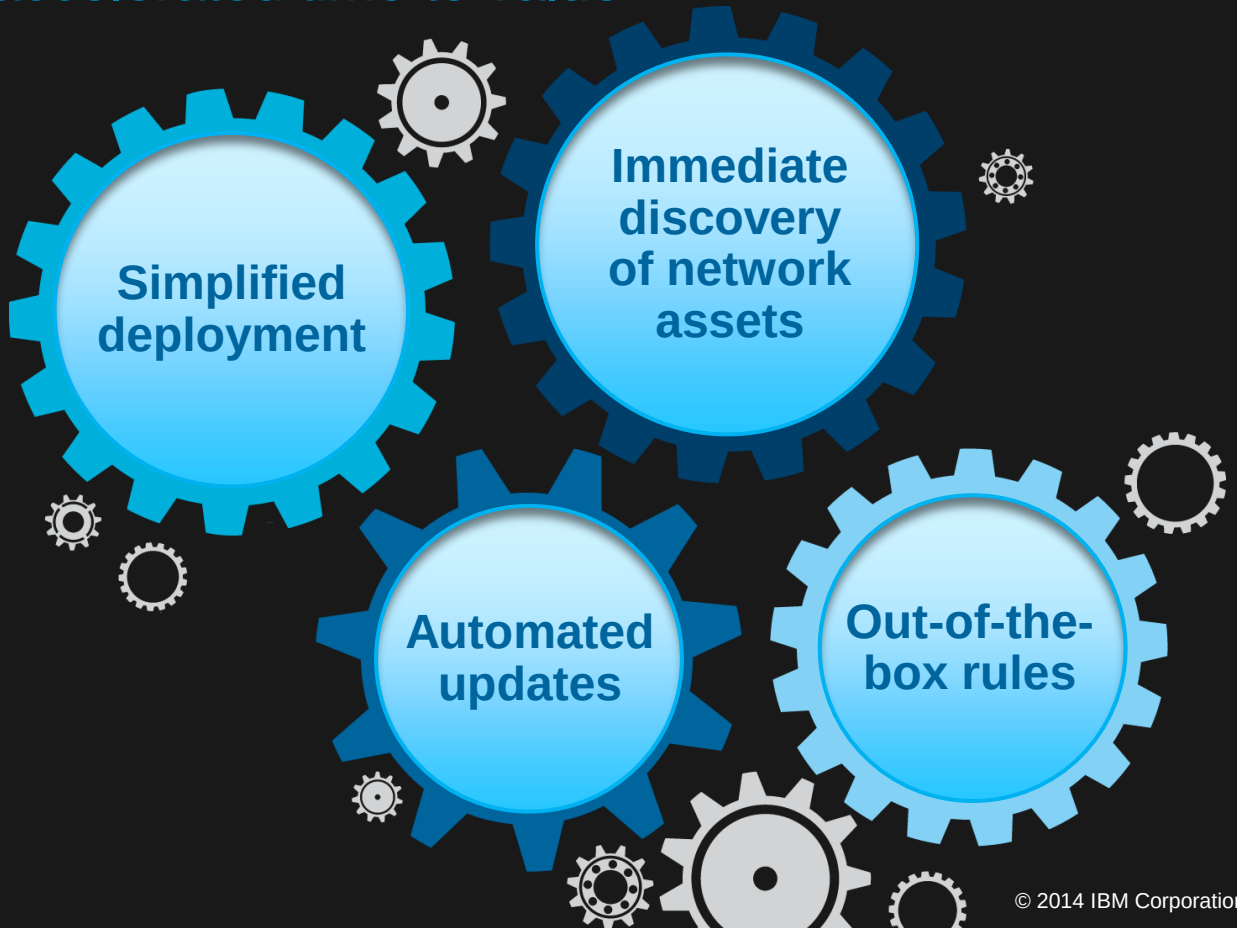
Answering questions to help prevent and remediate attacks



Driving simplicity and accelerated time to value

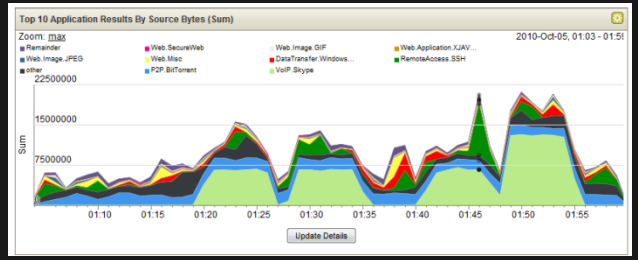
IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute
Independent Research



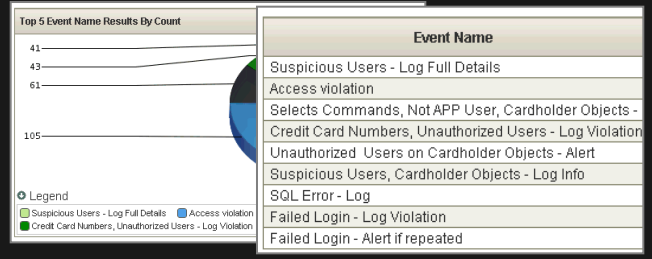
Differentiated by deep network and user activity analytics

Behavior monitoring and flow analytics



Network Traffic Doesn't Lie

Activity and data access monitoring



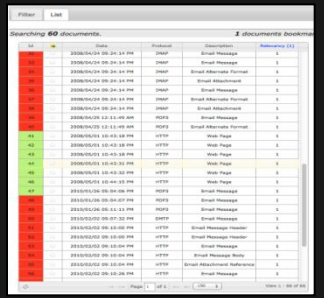
Improved Breach Detection

Stealthy malware detection

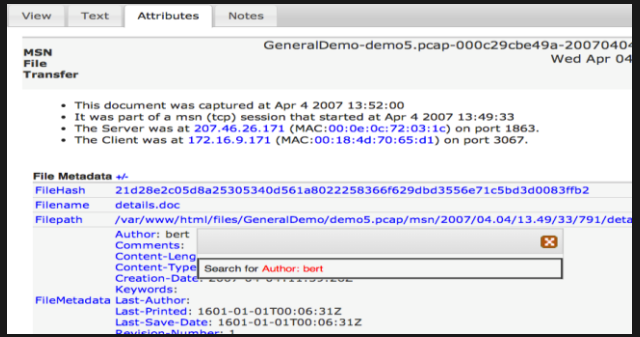
Irrefutable Botnet Communication

Intuitive data exploration and navigation reduces impact

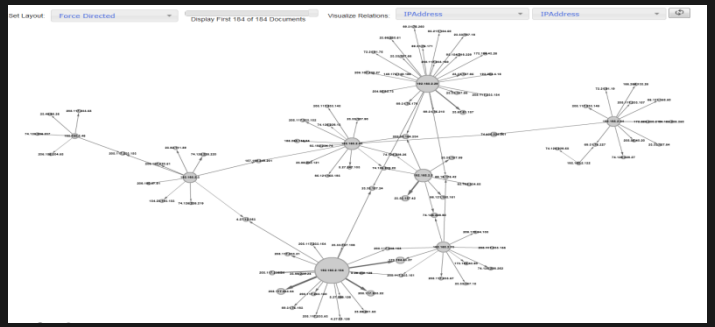
Survey: Retrace the activities in a chronological order



Searchable Results: Quickly pivot on data items to go where the data takes you



Visual Analytics: Navigate the data using visual indications of correlations between data items



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

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

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

financial information provider tracks

250 activity baselines

and saved

50-80%

on staffing versus alternative solutions

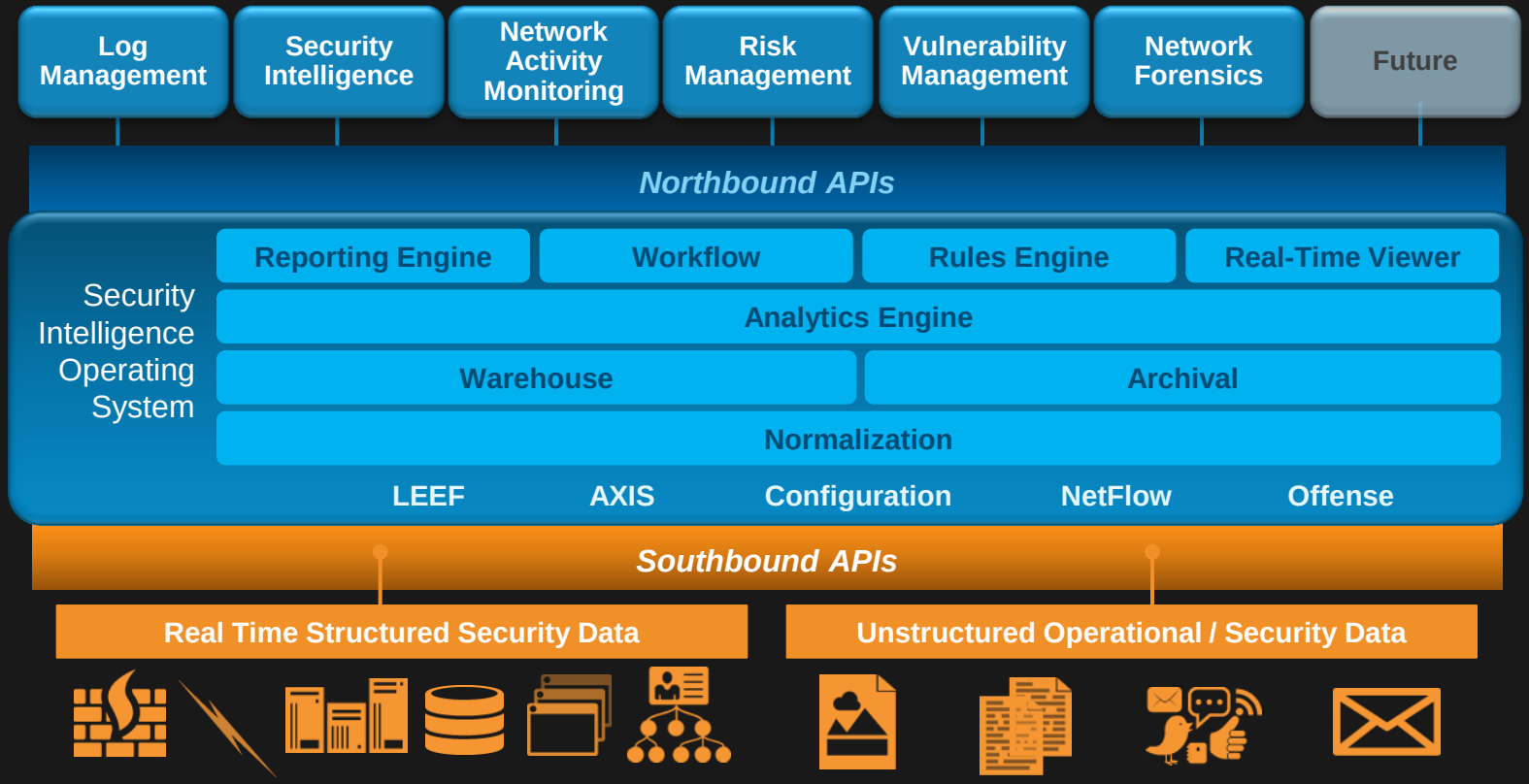
Business challenge

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

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

Delivering intelligence through a purpose-built, extensible platform



Consolidation and integration help reduce costs and increase visibility

	Traditional SIEM *6 products from 6 vendors are needed*				IBM Security Intelligence and Analytics
Flows	Arbor Networks		Lancope		Riverbed Technology
Packets	RSA			Solera Networks	
Vulnerabilities	Qualys		Rapid 7		Tenable Network Security
Configurations	AlgoSec	FireMon	Skybox Security	Tufin	RedSeal Networks
Logs	LogLogic			Splunk	
Events	HP ArcSight		McAfee		RSA

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

Intelligence, integration, automation to stay ahead of the threat

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 risk

Engage entire lifecycle of risk management for network and security infrastructures

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