



IBM BusinessConnect 2014

A New Era of Smart

5th May 2014 | Armani Hotel Dubai



IBM BusinessConnect 2014

A New Era of Smart



Information Security Is Becoming a Big Data Analytics Problem

Neil MacDonald
Gartner 2012



[In the News](#)[Proofpoint Article News Feed](#)[Proofpoint Video News Feed](#)[Media Contacts](#)[Awards](#)[Join Our Team](#)

Proofpoint Uncovers Internet of Things (IoT) Cyberattack

More than 750,000 Phishing and SPAM emails Launched from "Thingbots" Including Televisions, Fridge

SUNNYVALE, Calif. – January 16, 2014. Proofpoint, Inc., (NASDAQ: PFPT), a leading security-as-a-service provider, has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000

[Talk Now](#)

1-877-634-7660 (US)
[Other countries](#)

[Try it Now](#)

Request an evaluation,
audit or demo.

[Live Demo](#)

Sign up for our privacy
and protection live demo.





**40 Million Credit
Cards and Debit
Cards Stolen from
PoS**



Android based Cars may pose various Security and Privacy Issues

Monday, January 06, 2014 Swati Khandelwal

[g+1](#) [206](#) [Like](#) [234](#) [Share](#) [122](#) [Tweet](#) [105](#) [Reddit](#) [2](#) [Share](#) [16](#) [ShareThis](#) [450](#)





Security Intelligence and Big Data

Structured,
analytical,
repeatable

Security Intelligence Platform

Real-time Processing

- Real-time network data correlation
- Anomaly detection
- Event and flow normalization
- Security context & enrichment
- Distributed architecture



Security Operations

- Pre-defined rules and reports
- Offense scoring & prioritization
- Activity and event graphing
- Compliance reporting
- Workflow management

Creative,
exploratory,
intuitive

Big Data Platform

Big Data Processing

- Long-term, multi-PB storage
- Unstructured and structured
- Distributed Hadoop infrastructure
- Real-time stream computing
- Preservation of raw data
- Enterprise Integration



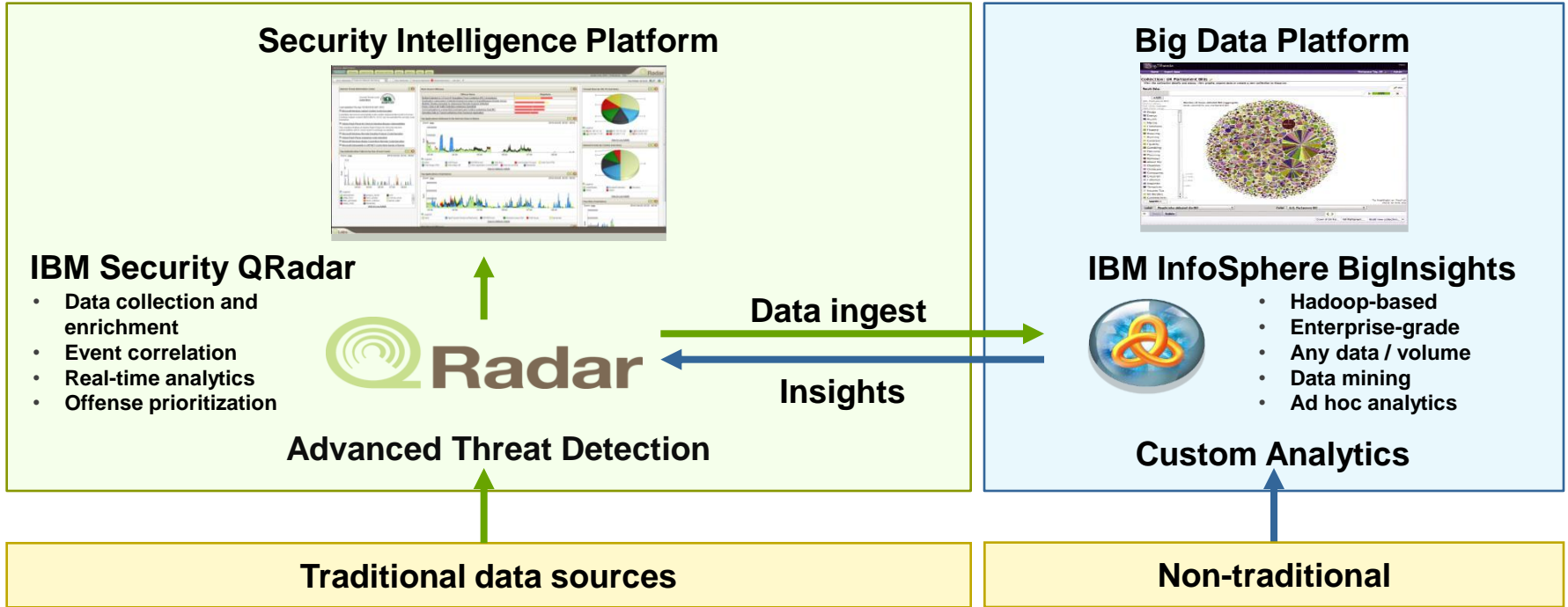
Analytics and Forensics

- Advanced visuals and interaction
- Predictive & decision modeling
- Ad hoc queries
- Interactive visualizations
- Collaborative sharing tools
- Pluggable, intuitive UI

IBM
Big Data
Security
Analytics



Extending Security Intelligence with Big Data





“Big Value from Big Data” – Common use cases



Targeted & advanced threat discovery




Full spectrum fraud detection



Insider threat analysis

<p>Customer Problem</p>	<p>Organizations need help in identifying advanced threats and zero-day attacks</p>	<p>Fraudulent claims, account takeovers, and invalid transactions cause substantial losses – and many organizations are unaware the fraud is being committed</p>	<p>As repositories of private information expand, the cost of data loss by insiders action grows, whether intentional or through human error</p>
<p>Technical Challenges</p>	<ul style="list-style-type: none"> ▪ Collection of high volume network and DNS events ▪ Rapidly changing identifiers ▪ Analytics to find subtle indicators ▪ Integration of external intelligence 	<ul style="list-style-type: none"> ▪ Collection of user, application and network activity ▪ Unstructured data analysis ▪ Long-term baselining capabilities ▪ Integration with fraud workflow 	<ul style="list-style-type: none"> ▪ Collection of inter- and intra-company communications ▪ Sentiment and linguistic analysis ▪ Ability to identify anomalies and outliers ▪ Integration with IAM solutions



Global Securities Clearing Corporation Proactively Addressing Cyber Security Threat with Big Data

Solution Capabilities

- IBM QRadar - Security Intelligence Event Management Platform
- InfoSphere BigInsights – enterprise class Hadoop analytics

Need

- Correlation & anomaly detection of security and network data – real-time and historical
- Ability to analyze larger volumes and varieties of data - security, email, social media, business process, transactional, device, and other data

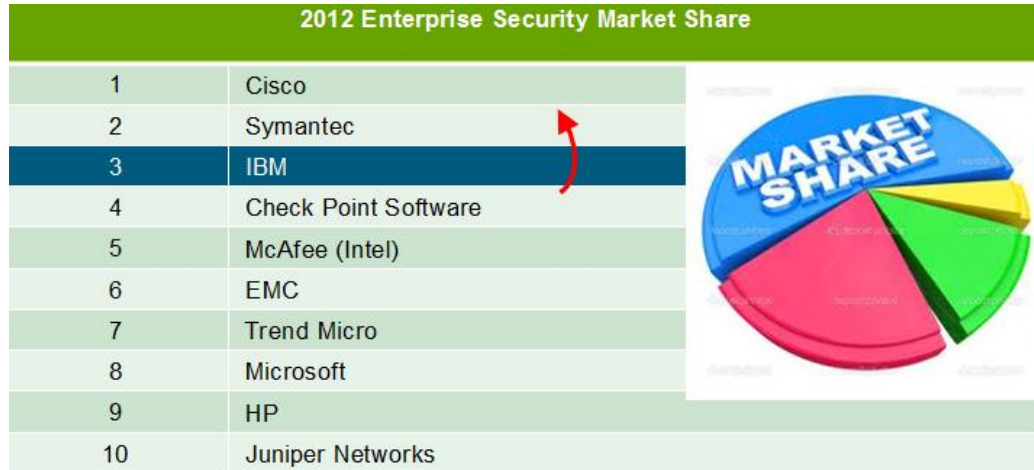
Benefits

- Can now actively ‘hunt’ for cyber-attackers targeting their networks



2014: Solidifying IBM's leadership in the security market

- **2011:** IBM announces the acquisition of Q1 Labs
- **2012:** Formation of IBM Security Systems
- **2013:** 5 consecutive quarters of double-digit growth and the acquisition of Trusteer
- **2014:** Leadership in the industry



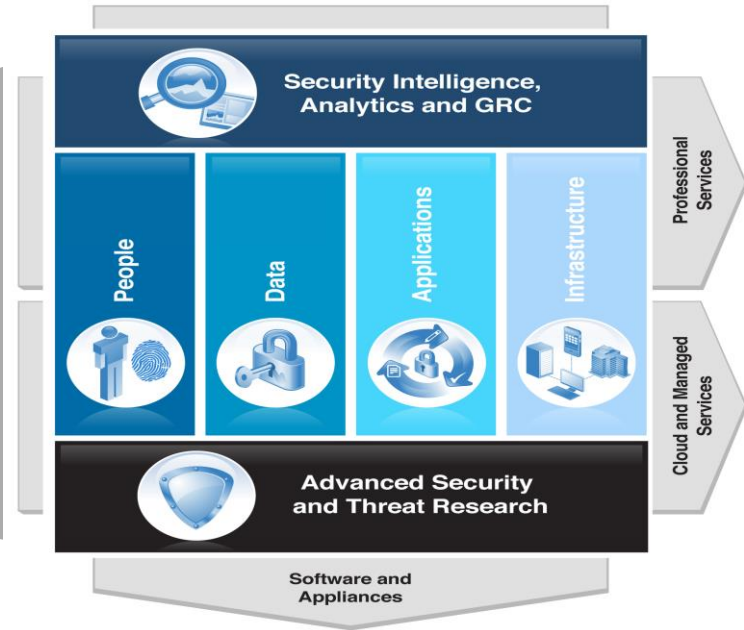
Source: IDC Worldwide IT Security Products 2013-2017 Forecast and 2012 Vendor Shares, December 2013, IDC #245102



IBM Security Systems

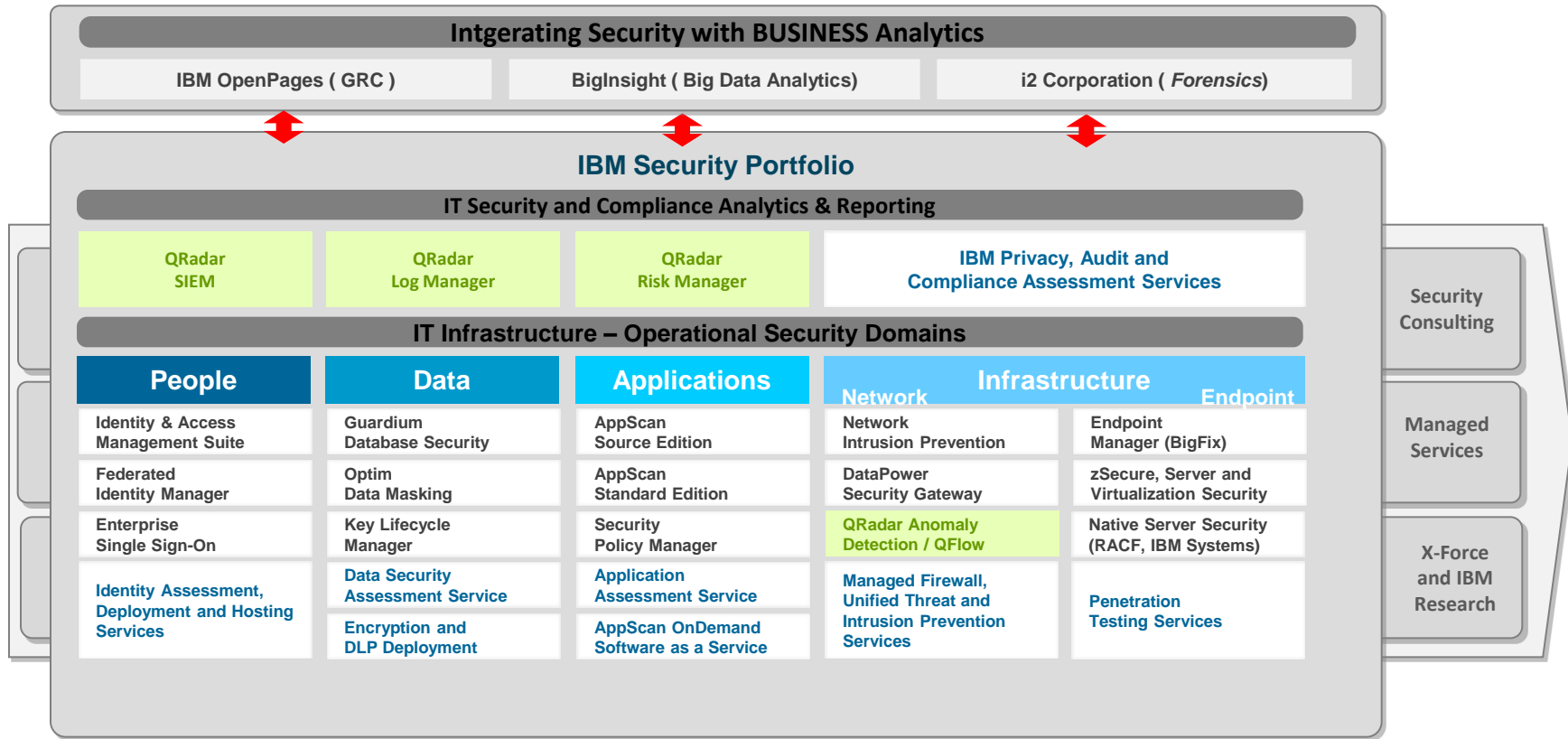
- Unique Security Framework
- \$1.8B investment in innovative technologies
- 6K+ security engineers and consultants
- Largest vulnerability database
- Award-winning X-Force® research
- Analyst recognized Leadership in every segment

IBM Security Framework



Intelligence ● Integration ● Expertise

IBM Security Systems: The industry's most comprehensive Smart Security portfolio





Thank You