

 Stay ahead.

Innovate2013

The IBM Technical Summit

開發者大會





雲端、行動、海量資料下的 終極資安管理

林育震 (Julian Lin)
台灣IBM公司 技術長
大中華區軟體事業群技術總監

Innovate2013

The IBM Technical Summit

開發者大會



資安大趨勢



Advanced Threats

Sophisticated, targeted attacks designed to gain continuous access to critical information are increasing in severity and occurrence



Advanced Persistent Threats
Stealth Bots Targeted Attacks
Designer Malware Zero-days

Mobile Computing

Securing employee-owned devices and connectivity to corporate applications are top of mind as CIOs broaden support for mobility



Cloud Computing

Cloud security is a key concern as customers rethink how IT resources are designed, deployed and consumed



Enterprise Customers




Regulation and Compliance

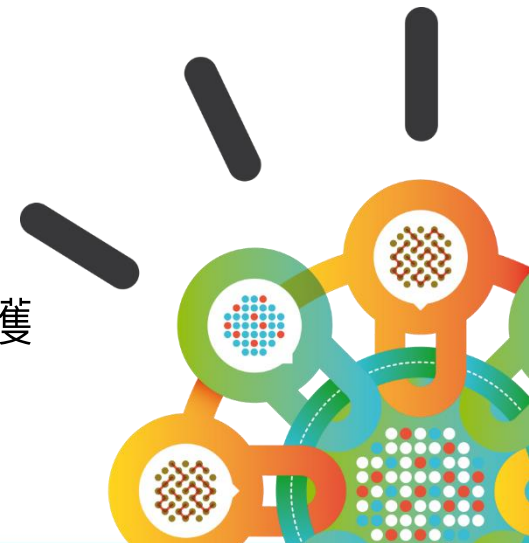
Regulatory and compliance pressures are mounting as companies store more data and can become susceptible to audit failures





內容

- 
- 從傳統到雲端運算技術的演進
 - 雲端運算正改變對內與對外的商業服務模式
 - 雲端運算的安全考量
 - 後PC時代需要行動力
 - 行動安全威脅的種類
 - 如何做到行動安全
 - 行動安全的參考方案
 - Web 2.0產生大量的資料
 - 傳統的資料倉儲已經無法支援完整決策
 - 海量資料的安全處理方案
 - 海量資料的安全結合整體安全
 - 除了資訊安全還要重視隱私保護
 - IBM的安全框架配合產品與服務提供您全方位的保護





從傳統到雲端運算技術的演進

Results from IBM cloud computing engagements



Increasing speed and flexibility	Test provisioning	Weeks	Minutes
	Change management	Months	Days/hours
	Release management	Weeks	Minutes
	Service access	Administered	Self-service
	Standardization	Complex	Reuse/share
	Metering/billing	Fixed cost	Variable cost
	Reducing costs	Server/storage utilization	10–20%
Payback period		Years	Months

SOURCE: Based on IBM and client experience



雲端運算正改變對內與對外的商業服務模式



Private cloud

- Development Cloud
- Testing Cloud
- Desktop Cloud
- Factory Cloud
-
- IT infrastructure is becoming Cloud



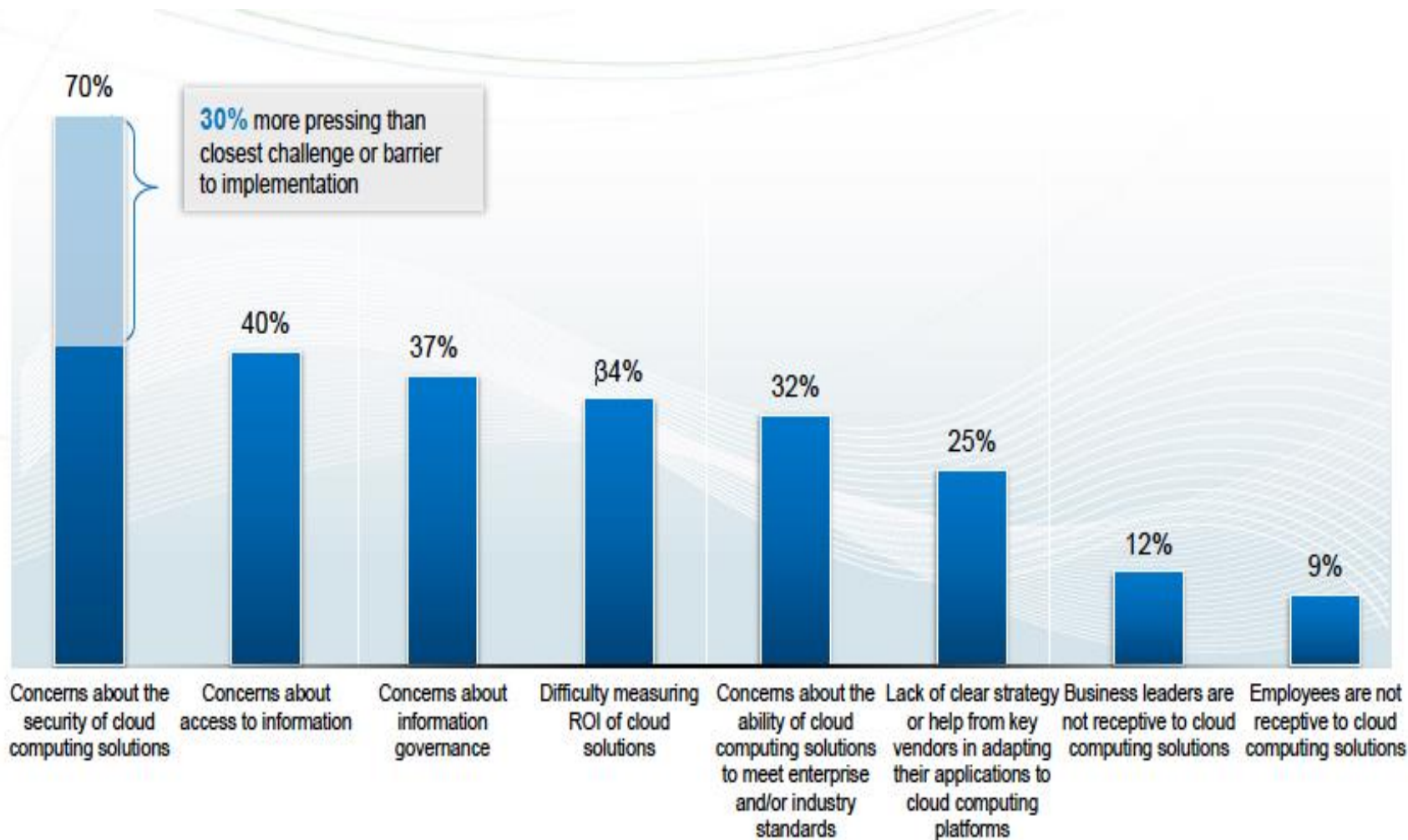
Public cloud

- Amazon EC
- MS Office 365
- IBM Lotus Live
- IBM Smart Cloud Enterprise Plus
- Tend Micro Anti-virus
- PC Home Stores
- e-Invoice Cloud
-
- Business service is already Cloud



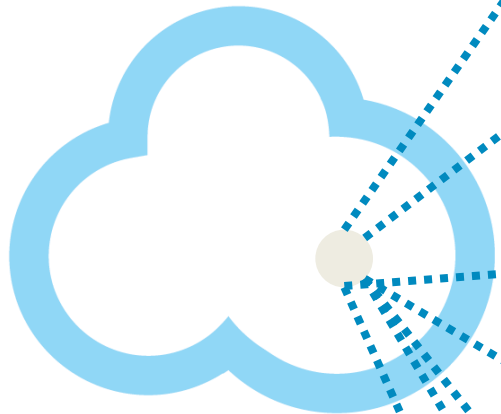


但是邁入雲端最大的阻礙是安全疑問





雲端運算的安全考量



1.

Manage the registration and control the access of thousands or even millions of Cloud users in a cost-effective way

2.

Ensure the safety and privacy of critical enterprise data in Cloud environments without disrupting operations

3.

Provide secure access to applications in the Cloud

4.

Manage patch requirements for virtualized systems

5.

Provide protection against network threat and vulnerabilities in the Cloud

6.

Protect virtual machines

7.

Achieve visibility and transparency in Cloud environments to find advanced threats and meet regulatory and compliance requirements





保護雲端資料的四個步驟

1

Understand, define policy

- Discover where sensitive data resides
- Classify and define data types
- Define policies and metrics

2

Secure and protect

- Encrypt, redact and mask virtualized databases
- De-identify confidential data in non-production environments

3

Actively monitor and audit

- Monitor virtualized databases and enforce review of policy exceptions
- Automate and centralize the controls needed for auditing and compliance (e.g., SOX, PCI)
- Assess database vulnerabilities

4

Establish compliance and security intelligence

- Automate reporting customized for different regulations to demonstrate compliance in the Cloud
- Integrate data activity monitoring with security information and event management (SIEM)



保護虛擬伺服器

New complexities

- Dynamic relocation of VMs
- Increased infrastructure layers to manage and protect
- Multiple operating systems and applications per server
- Elimination of physical boundaries between systems
- Manually tracking software and configurations of VMs
- Hypervisor is attack vector

Before Virtualization



- 1:1 ratio of OSs and applications per server

After Virtualization



- 1:Many ratio of OSs and applications per server
- Additional layer to manage and secure

• There have been 100 vulnerabilities disclosed across all of VMware's virtualization products since 1999.*

• 57% of the vulnerabilities discovered in VMware products are remotely accessible, while 46% are high risk vulnerabilities.*



IBM是雲端安全第一名

IBM Research and Papers

- Special research concentration in cloud security, including white Papers, Redbooks, [Solution Brief – Cloud Security](#)

IBM X-Force

- Proactive counter intelligence and public education <http://www.ibm.com/security/xforce/>

IBM Institute for Advanced Security

- Cloud Security Zone and Blog ([Link](#))

Customer Case Study

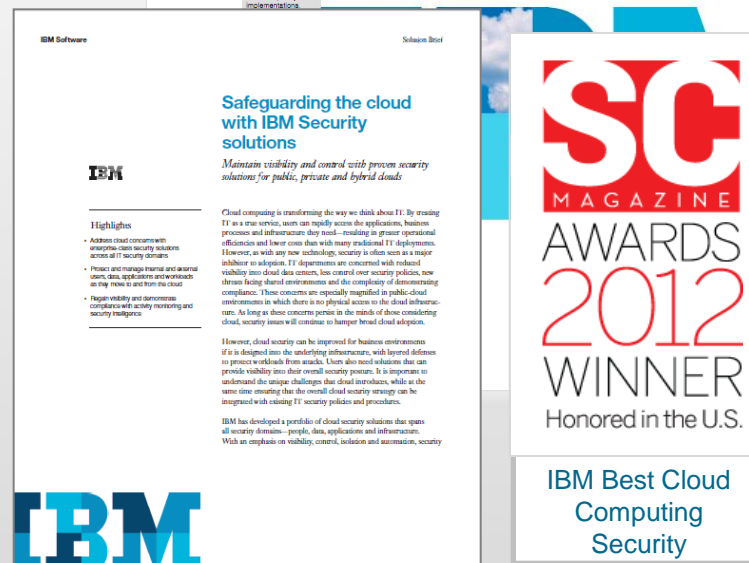
- EXA Corporation creates a secure and resilient private cloud ([Link](#))

Other Links:

- IBM Media series – SEI Cloud Security ([Link](#))
- External IBM.COM : IBM Security Solutions ([Link](#))
- External IBM.COM : IBM SmartCloud– security ([Link](#))
- IBM SmartCloud security video ([Link](#))



IBM Point of View:
Security and Cloud Computing



Innovate2013
The IBM Technical Summit



後PC時代需要行動力



Employees

34%
employees in 2012 are mobile
(Source: IDC*)

Mobile/Wireless/Cloud



Web/Desktop



Client/Server



Host/Mainframe



Mobile Applications

85 billion
mobile applications will be
downloaded in 2012
(Source: IDC)

Security

8X
increase in security risk
driven by proliferation of
mobile data and devices

“Consumerisation of IT”

62%
individual-liable (BYOD*) devices used for
business, compared to 38% corporate-liable
in 2012
(Source: IDC*)

Unified Communications (UC)

78%
of multinational corporations plan to adopt
mobile UC by 2015, including mobile video
streaming and conferencing

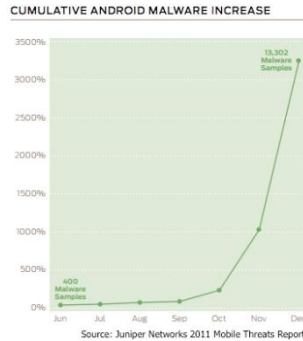


行動安全威脅的種類



Malware

- Malware existed in various forms (viruses, worms, Trojans, spyware) has been constantly increasing.
- 25,000 mobile malware apps were identified as of the second quarter of 2012--a 417 percent rise from the first quarter. (Trend)
- No platform is immune. Malicious applications on increase in all app stores
- “Zeus for Mobile”
- First large scale mobile botnet in 1Q2012 – RootStrap (Symantec)



Loss and Theft

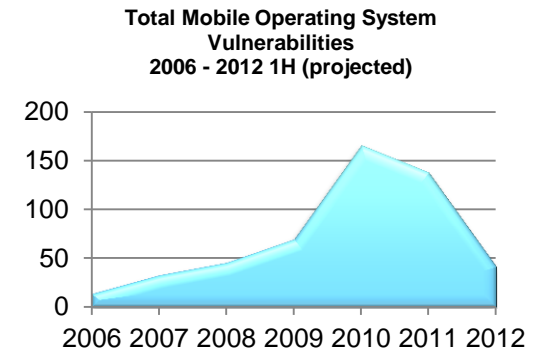
- A survey of consumer users found that one out of every three users has ever lost a mobile device.
- 2011 study - 36 percent of consumers in the United States have either lost their mobile phone or had it stolen. (Symantec)
- The major benefits of mobile devices (size and portability) unfortunately come with the big risk of losing sensitive data that has to be accepted but can be mitigated.
- Cell phone theft in New York City jumped from eight percent of robberies 10 years ago to more than 40 percent today (CBS News)

Communication

- SMS toll fraud continues as one of primary exploited areas
- Bluetooth is an exploited vector because a device in a discoverable mode can be easily discovered and lured to accept a malicious connection request.
- “Man in the middle” attacks have been demonstrated to be possible with several platforms using Wi-Fi links.
- Phishing or pharming attacks can leverage multiple channels: email, SMS, MSS, and voice

OS vulnerability based attacks

- Mobile OS vulnerabilities continue to be discovered at significant rates
- Always on and connected, mobile device is a prime target for hit-and-run network-based attacks and exploiting zero-day vulnerabilities.



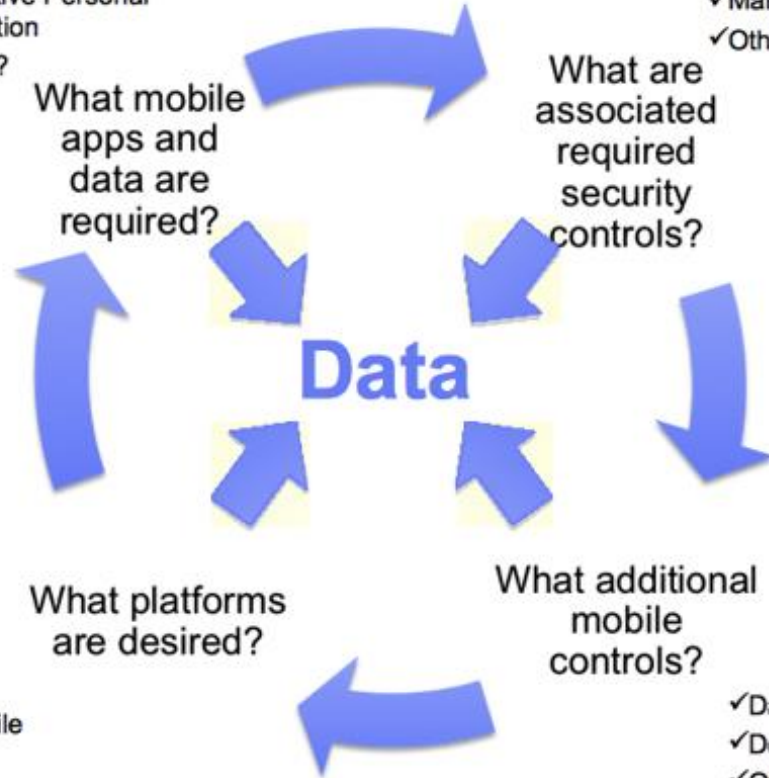


如何做到行動安全



- ✓eMail
- ✓Contacts
- ✓Calendar
- ✓Intranet Access
- ✓Sensitive Personal Information
- ✓Other?

- ✓Security Policy
- ✓Password
- ✓Device Timeout
- ✓Disk Encryption
- ✓Malware Protection
- ✓Other?



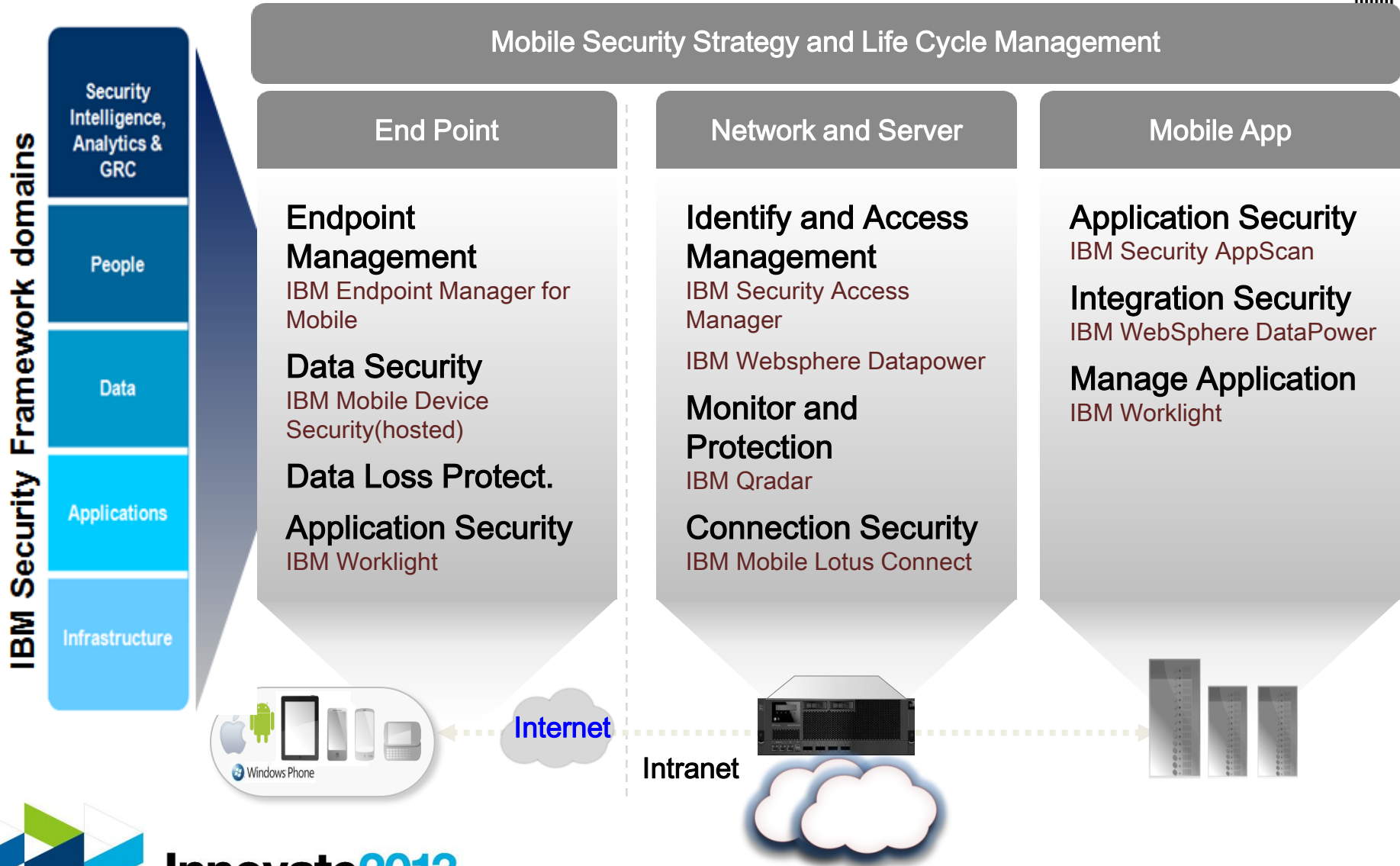
- Blackberry
- Windows Mobile
- Symbian
- iOS
- Android

What additional mobile controls?

- ✓Data Wipe
- ✓Device Kill
- ✓Other?



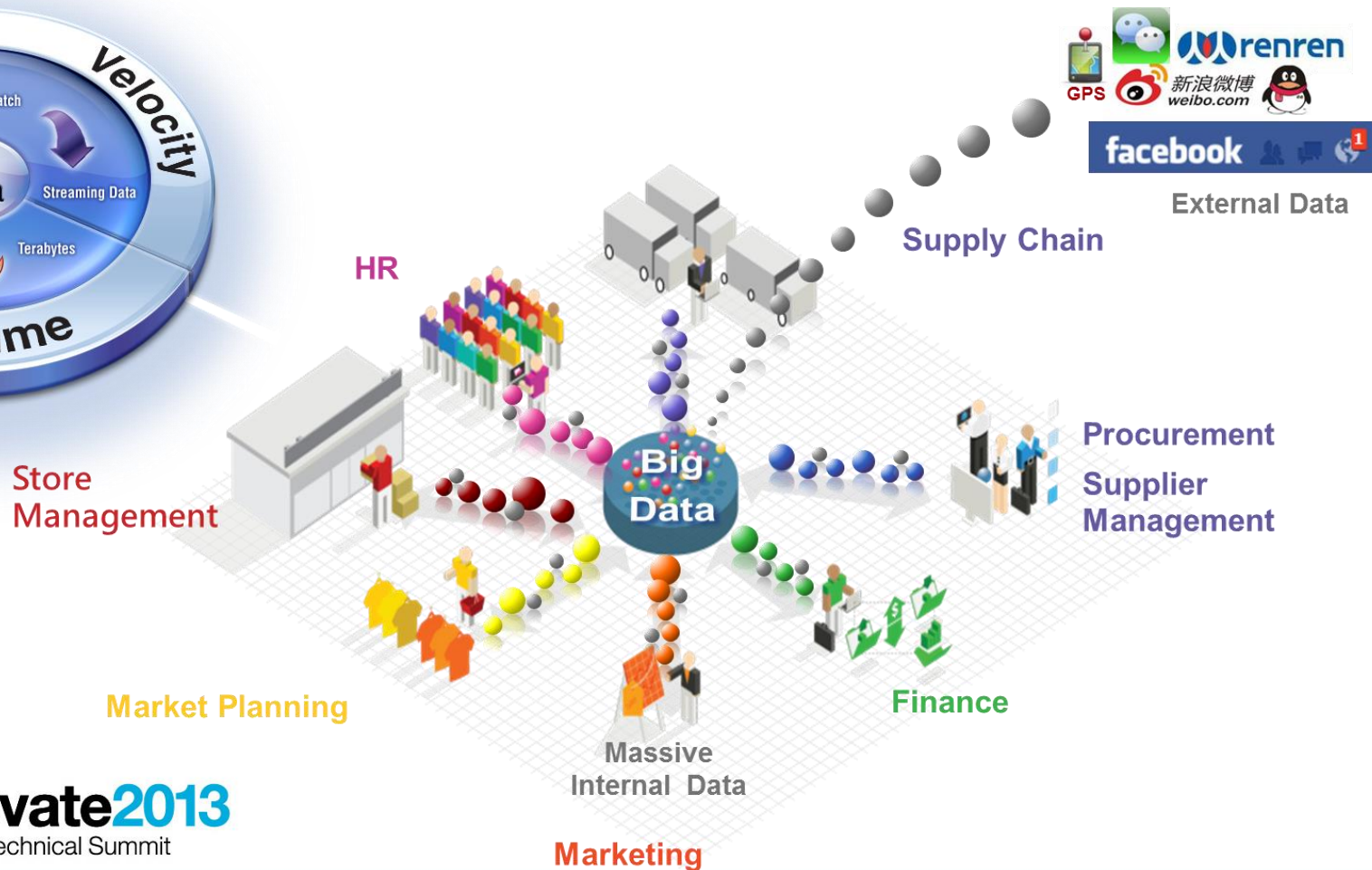
行動安全的參考方案



Web 2.0產生大量的資料

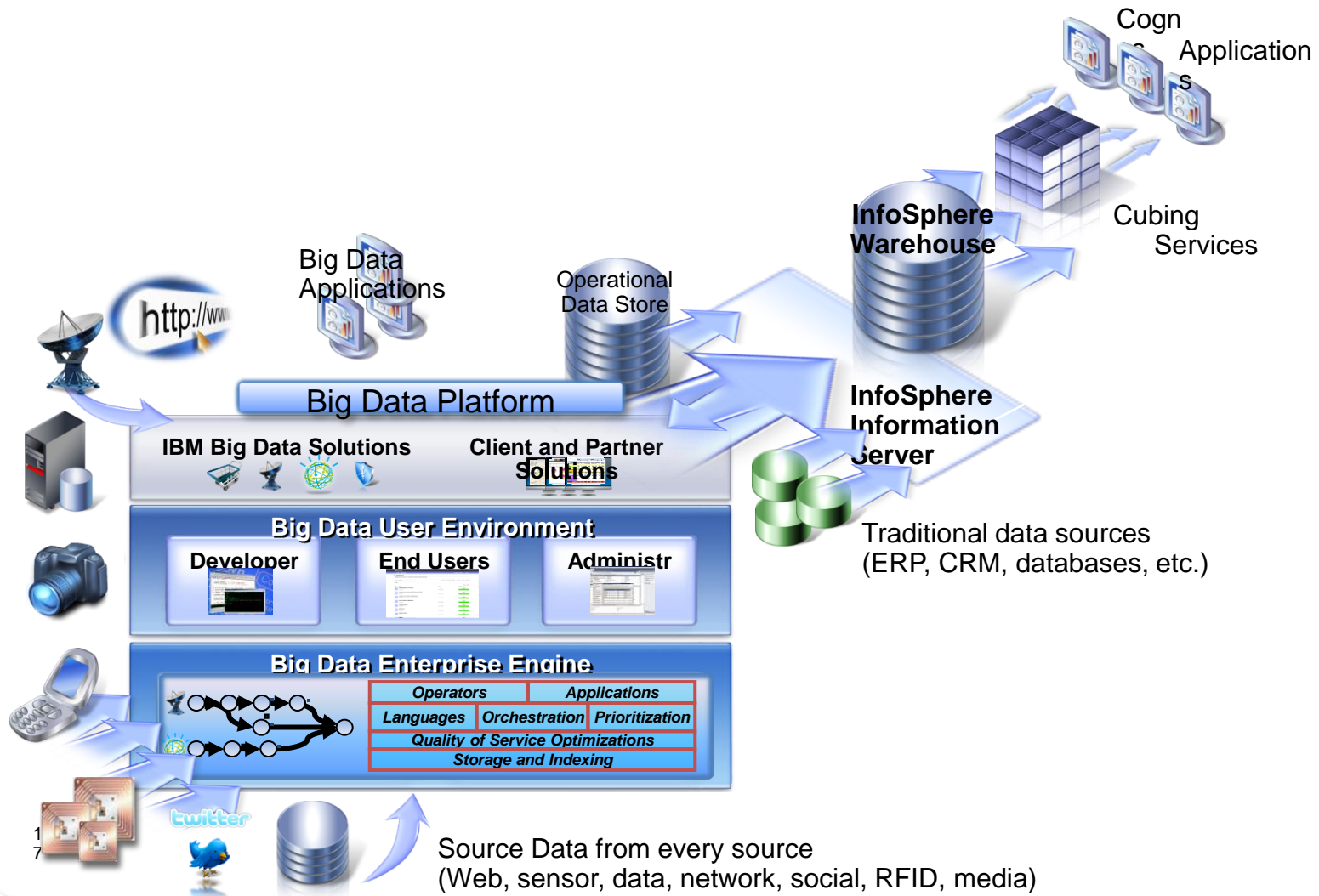


-  INSTRUMENT
-  INTERCONNECT
-  INTELLIGENT



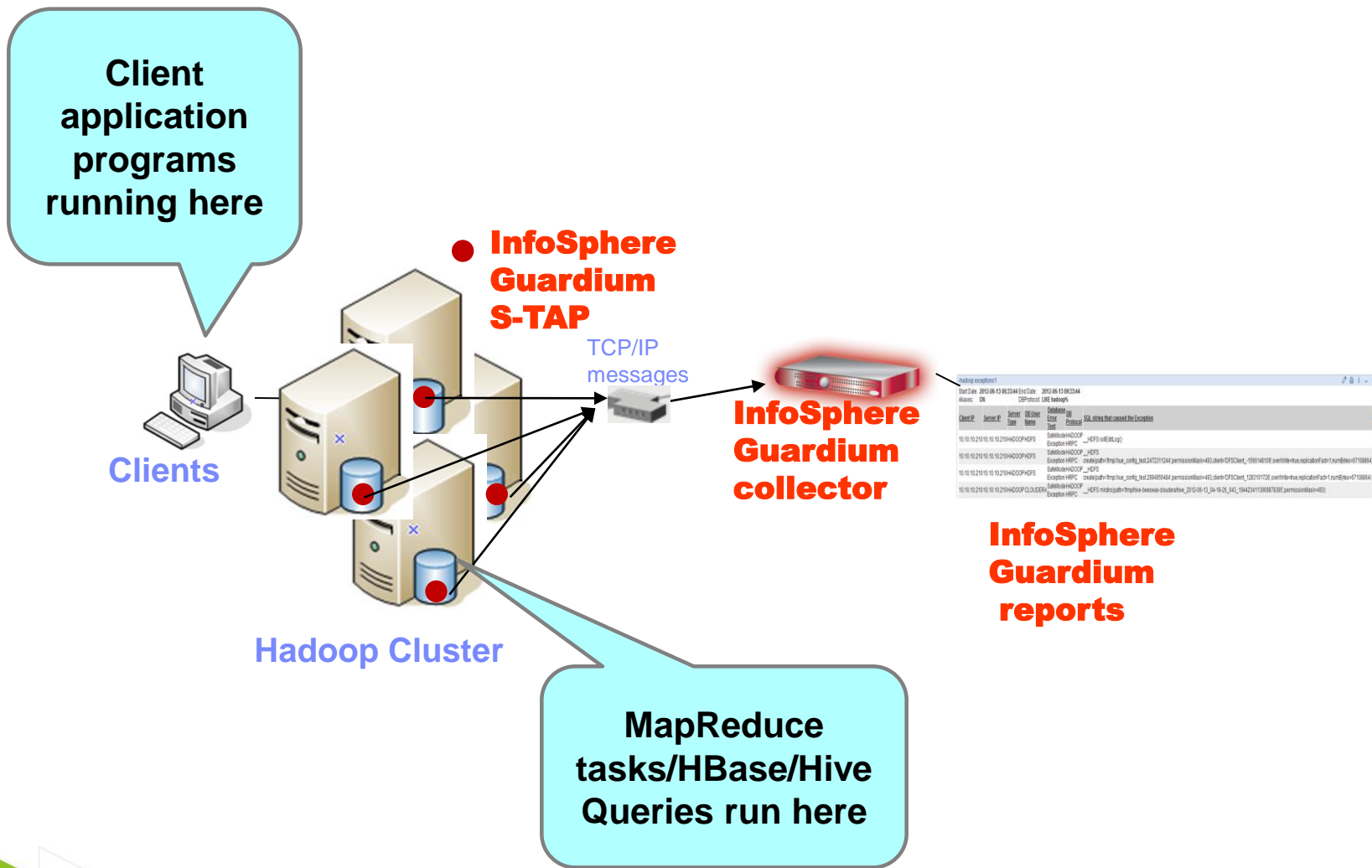


傳統的資料倉儲已經無法支援完整決策





海量資料的安全處理方案



Hadoop 的監控訊息參考報表



For example: hbase createTable you only see 2 commands in hbase report but all the other messages will be here

full_sql for ALL messages for a particular command

Hadoop - Full Message Details report

Start Date: 2012-09-06 09:11:46 End Date: 2012-09-07 12:11:46
 Aliases: OFF Message_Details: LIKE %hbase-%
 SERVER_IP: LIKE %

Timestamp	Server Type	Client IP	Server IP	DB User Name	Source Program	Message
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...complete', struct:2={struct:1='/hbase/hbase-H4/.tmp/tableinfo.0000000001', REDUCE_1513337435_9', struct:3={struct:1='BP-943274971-9.70.145.113-1344287392934', ...}
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP CLIENT PROGRAM	...eName='hbase-H4', key='IS_ROOT', value='false', key='IS_META', ...
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...struct:1='rename', struct:2={struct:1='/hbase/hbase-H4/.tmp/tableinfo.0000000001', struct:2='/hbase/hbase-0001', struct:3='org.apache.hadoop.hdfs.protocol.ClientProtocol', varint:4=1}
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...struct:1='mkdirs', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321', struct:2=...
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...struct:1='getFileinfo', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321/logs', ...}
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...message {struct:1='mkdirs', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321/logs', struct:2=...
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...message {struct:1='getFileinfo', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321.oldlogs', ...}
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...message {struct:1='mkdirs', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321.oldlogs', struct:2=...
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...message {struct:1='create', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321/logs/hlog.1346945011093', ...}
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.113	HBASE	HADOOP PROTOBUF CLIENT PROGRAM	...struct:1='getFileInfo', struct:2={struct:1='/hbase/hbase-H4/3b32d9d23a1d6ca686c3b49de9c50321', struct:2=...
2012-09-06 11:23:31.0	HADOOP	9.70.145.113	9.70.145.117	HBASE	HADOOP CLIENT PROGRAM	...HBASE multi(regionName='.META.', 1', regionName=#02 9hbase-H4., 1346945011024.3b32d9d23a1d6ca686c3b49de9c50321.7FFFFFFF ')

Hadoop - Exception Report

Start Date: 2012-09-07 11:59:57 End Date: 2012-09-11 11:59:57
 Aliases: OFF ExceptionNo: LIKE %

Exception Timestamp	Server Type	Server IP	Client IP	User Name	Exception Description	SQL string that caused the Exception	Database Error Text	Count of Exceptions
2012-09-10 12:01:55.0	HADOOP	9.70.148.183	9.70.144.203	SVORUGA101	AccessControl Exception	__HDFS mkdirs(path='/user/svoruga', permissionMask=493)	AccessControl Exception1	1

No permission to create directory



海量資料的安全結合整體安全



Advanced Security Analytics & Correlation Engine

Data Sources

- Security Devices
- Server and Host Logs
- Network and Virtual Activity
- Database Activity
- Application Activity
- Vulnerability and Config Data
- Threat Intelligence Feeds
- User Activity and Behavior
- Web, Blogs, & Social Activity
- Business Transactions
- Unstructured data (e.g. Email)



Real-time Processing

- Focus on HOT, real-time data
- Event normalization
- Real-time correlation
- Data enrichment



Security Operations

- Detailed security metrics
- Activity & event graphs
- Incident management
- Compliance reporting



Big Data Security Workbench

Big Data Warehouse

- Storage for HOT, Warm & cold data
- Unstructured and structured
- Distributed infrastructure
- Preserves raw data
- Scalable platform
- Large-scale machine learning
- Hadoop-based backend



Big Data Analytics and Forensics

- Advanced visuals and interaction
- Predictive and decision modeling
- Ad hoc and historical queries
- Transaction and geo analysis
- Custom reports and dashboards
- Pluggable UI
- Collaborative sharing tools

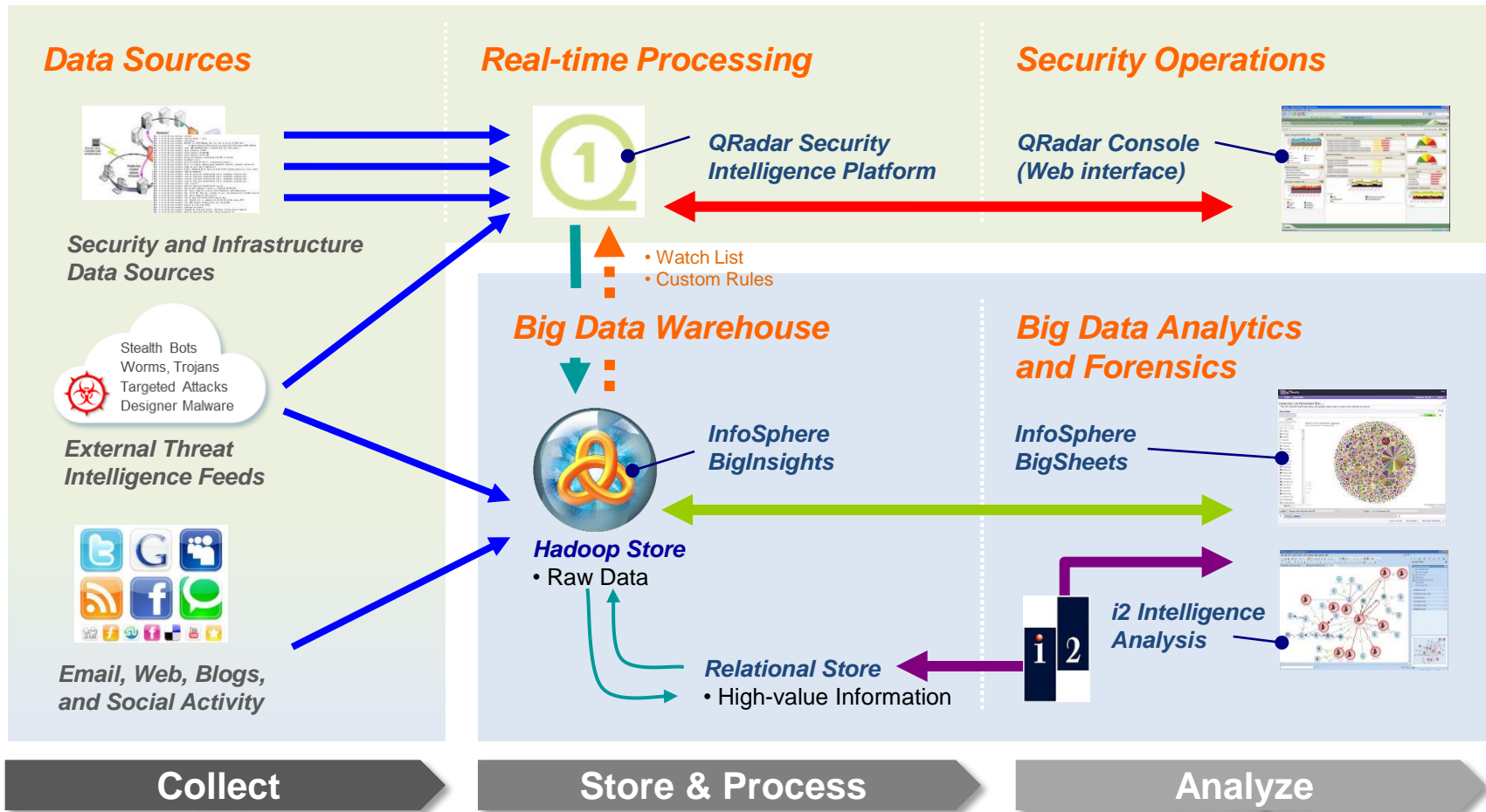


Collect

Store & Process

Analyze

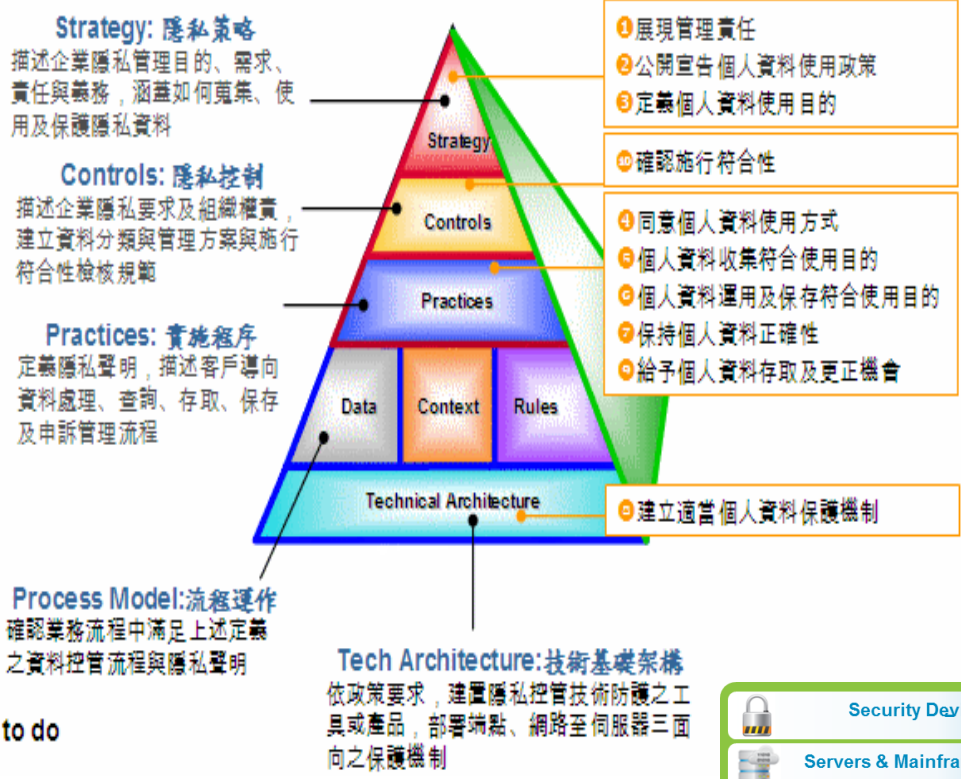
海量資料的的安全結合整體安全





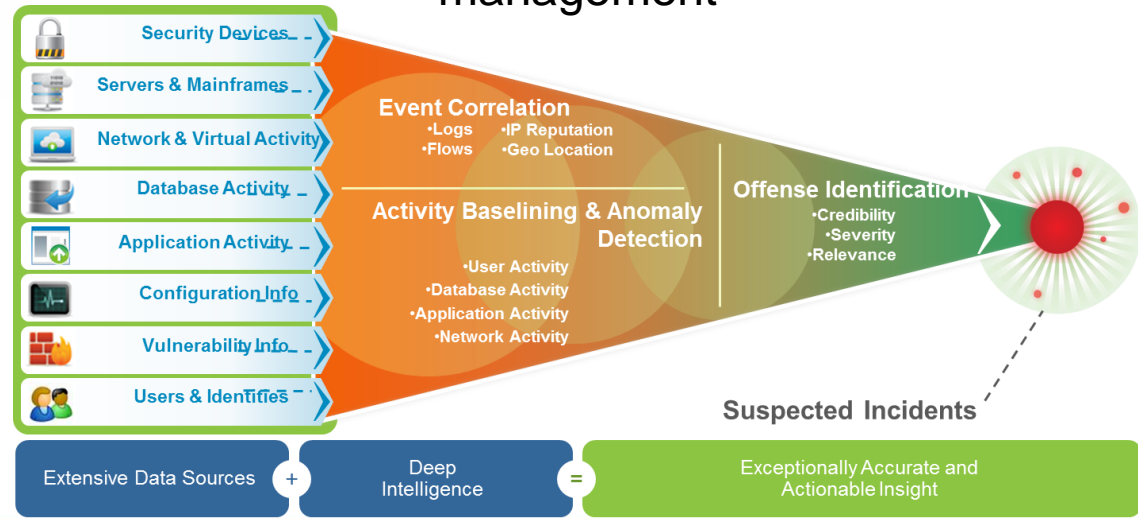
除了資訊安全還要重視隱私保護

What to do



IBM Privacy Protection Framework

End-to-End Security
Information Event correlation,
real-time alert, compliance
management



IBM的安全框架配合產品與服務 提供您全方位的保護



IBM Security Framework

