

IBM Smarter Planet Cloud Security

Martin Borrett

Lead Security Architect, NE Europe - IBM Security Solutions



PCTY2010 
Pulse Comes to You

Optimising the World's Infrastructure

South Bank – 3rd November 2010



Categories of Cloud Computing Risks



Less Control

Many companies and governments are uncomfortable with the idea of their information located on systems they do not control. Providers must offer a high degree of security transparency to help put customers at ease.



Compliance

Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications. Comprehensive auditing capabilities are essential.



Data Security

Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure. Authentication and access technologies become increasingly important.



Reliability

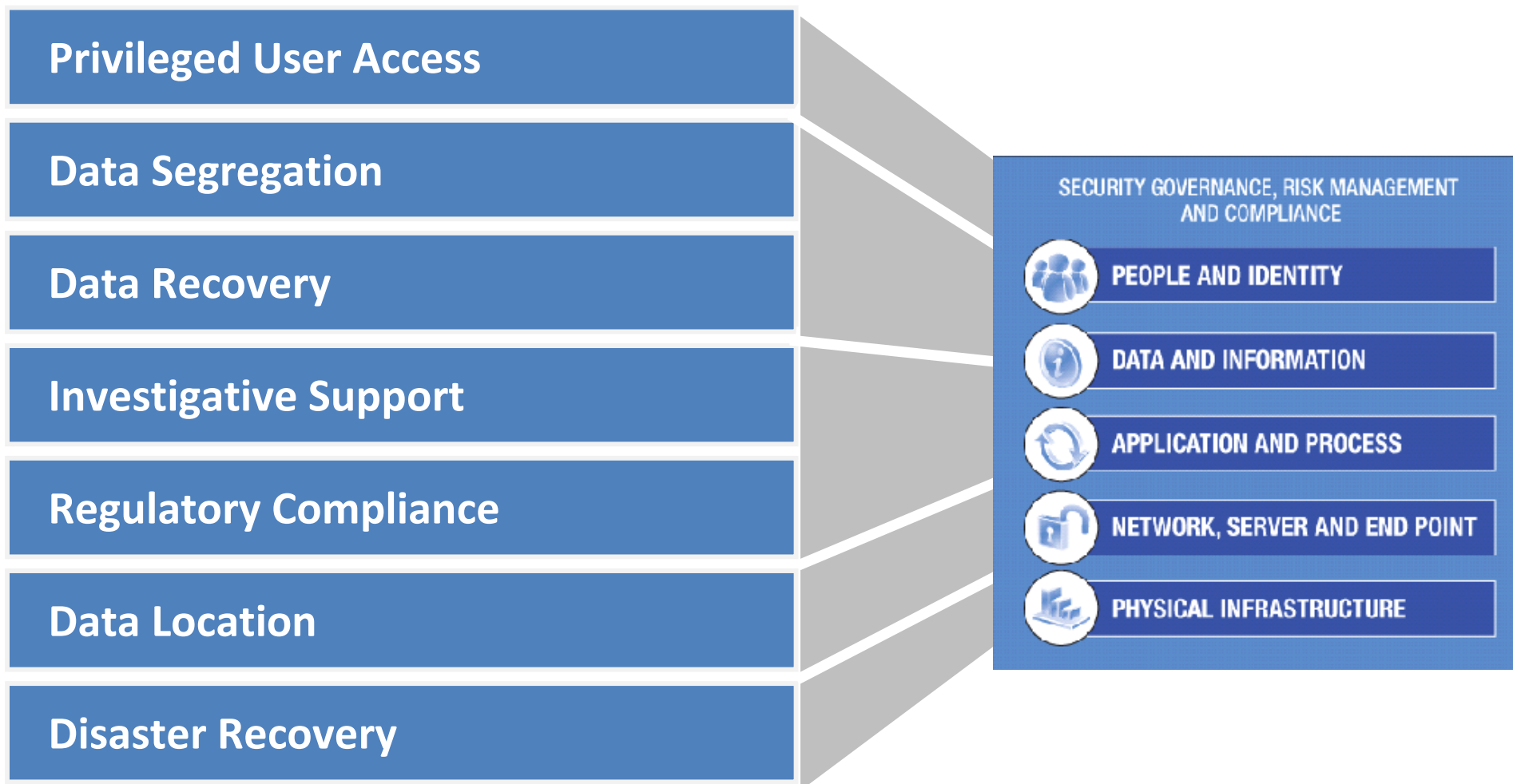
High availability will be a key concern. IT departments will worry about a loss of service should outages occur. Mission critical applications may not run in the cloud without strong availability guarantees.



Security Management

Providers must supply easy controls to manage firewall and security settings for applications and runtime environments in the cloud.

Gartner reports on security risks of cloud computing



[Gartner: Assessing the Security Risks of Cloud Computing, June 2008](#)

Security Framework



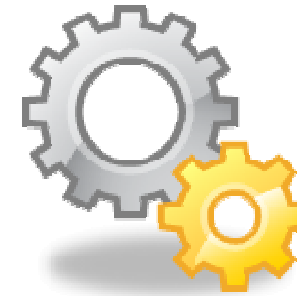
Describes the business landscape of security

IBM Cloud Security Guidance



Describes the technology landscape

IBM Capabilities & Offerings to Help



Catalogues of products, services and solutions

Coarse grained

Fine grained

IBM

People and Identity



Identity Life Cycle Management

User Management

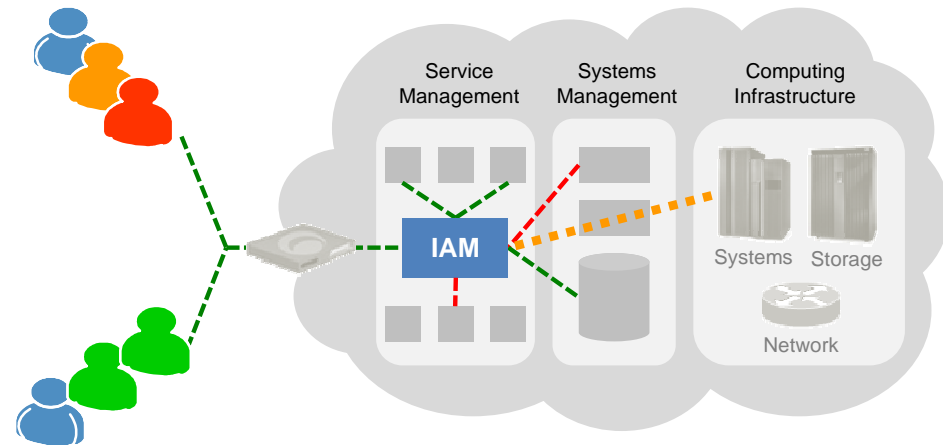


User access, business logic to applications. Separation of administrative and user roles in a cloud environment

Summary: User life cycle management, access management and single sign-on solution that manages the difficulty of executing security policies across a wide range of Web and application resources.

Cloud Use Case: Validation and processing of user identity information. Addresses the need of authentication of users to the cloud ecosphere.

Deployment Scenario: Positioned at Application Server to authenticate access to back end and management functions.



Federated Identity

Cloud Identity Federation

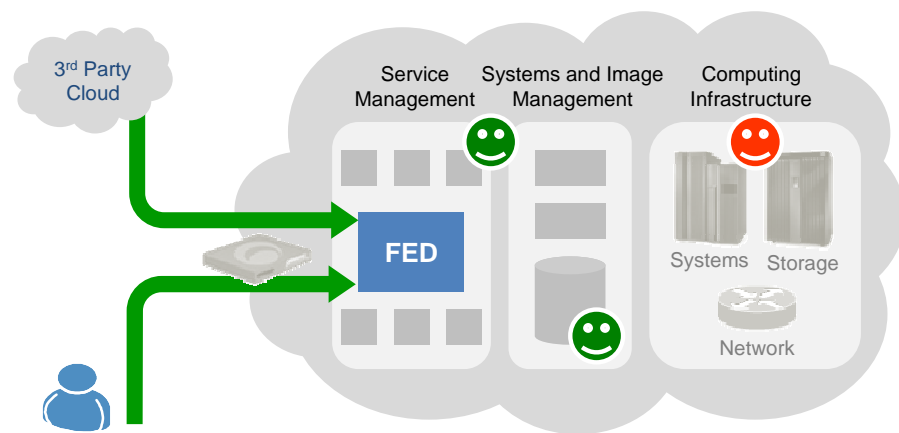


Single access method for users into cloud and traditional applications

Summary: Federation enables trust between SOA-based initiatives by connecting users to services across business domains and helps enterprises strengthen and automate user access rights.

Cloud Use Case: Validation and processing of user identity information. Addresses the need of authentication of users to the cloud ecosphere.

Deployment Scenario: Positioned at Application Server to authenticate access to back end and management functions.



Data and Information



Audit

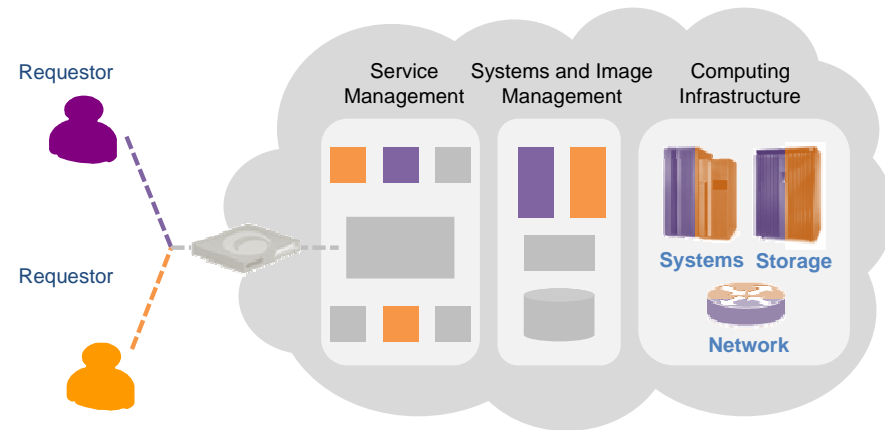
Managing shared data resources within a multi-tenant environment

Audit

Summary: How can I reduce the cost and pain associated with tracking and controlling who touched what data when

Cloud Use Case: Application isolation, OS containers, encrypted storage, VLANs and other isolation technologies provide a secure multi-tenant infrastructure.

Deployment Scenario: At the systems, storage, and networking layers of the cloud.



Data Encryption

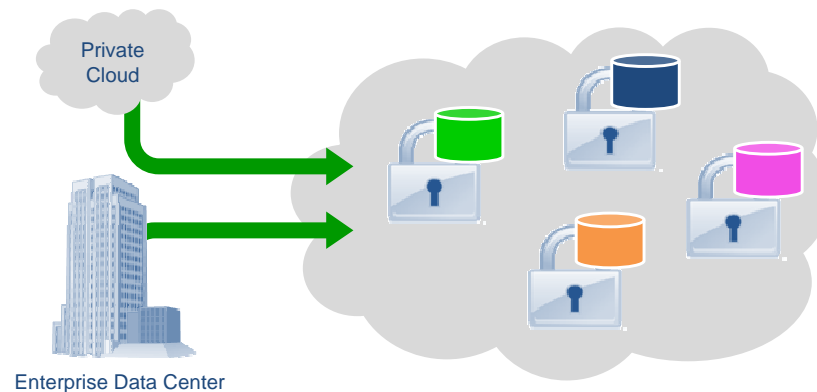
Secure storage and recovery of data stored remotely in the cloud

Data security at rest

Summary: Provides a cost-effective way to meet legal discovery, hold and retention requirements. Assures data is available to the right people, at the right time & Data Protection and prevention of Data Loss or Data Leakage

Cloud Use Case: Remote data protection to provide business continuity and resiliency to customer datacenters and private clouds.

Deployment Scenario: Automatically backs up data to secure cloud data centers via your existing network.



Network, Server, and Endpoint



Enterprise Security Solutions

Enterprise Security



Security for existing IT infrastructure as it extends to the cloud

Summary: Reduce cost and a secure computing environment that minimizes the potential risk posed by security threats. OS level policy compliance

Cloud Use Case: Flexible policy management, web threat protection, application control, OS security.

Deployment Scenario: In the traditional enterprise IT environment.



Virtualised Security

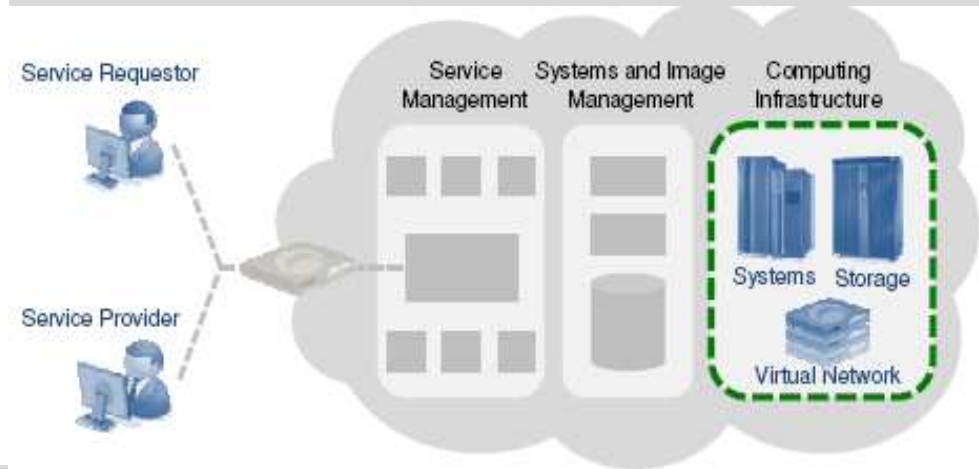
Virtualization Security



Security for pools of high performance virtualized resources

Summary: broadest set of virtualization capabilities platforms are built with security as a requirement, not an afterthought. Virtual appliances, strengthen defenses by eliminating additional threats.

Cloud Use Case: Security of the virtualization stack - enabling flexible, rapid provisioning across heterogeneous servers and hypervisors.



Application and Process



Vulnerability Assessment Services

Vulnerability

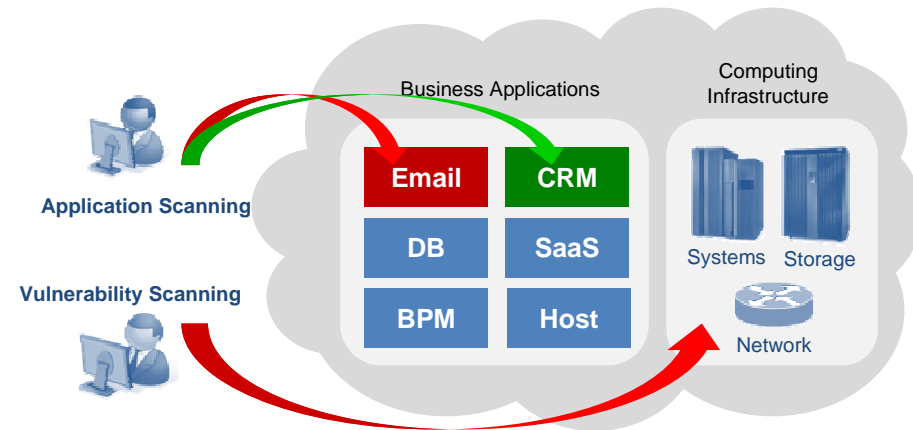


Vulnerability and compliance checking of cloud applications

Summary: Tests for common Web application vulnerabilities including SQL-Injection, Cross-Site Scripting and Buffer Overflow. Performs automated scans to identify OSes, apps, and their respective vulnerabilities.

Cloud Use Case: External or internal testing of cloud applications and their hosted infrastructure.

Deployment Scenario: Internal testing and remote security services.



Security Information & Event Management Service (SIEM) & Detection/Prevention Services

Investigative Support

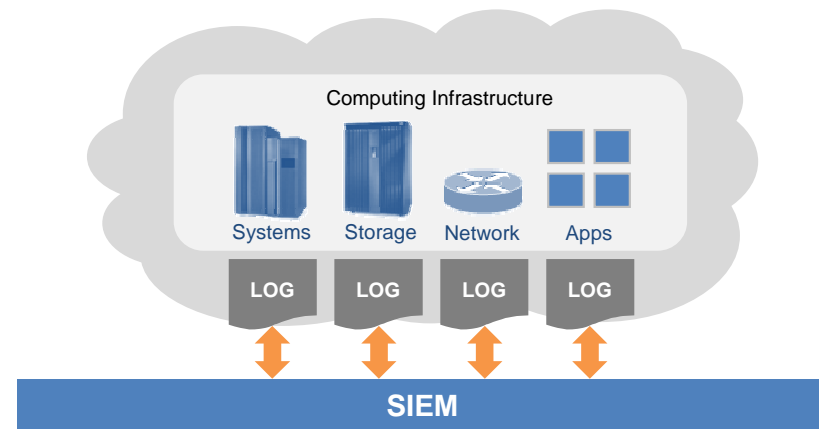


Ability to inspect and audit a cloud provider's logs and records

Summary: Security Information & Event Management Service enables corporations to compile event and log files from network applications and operating systems, as well as security technologies, into one seamless platform.

Cloud Use Case: Improves the speed of conducting security investigation and archives forensically-sound data, admissible as evidence in a court of law, for a period of up to seven years.

Deployment Scenario: Remote





- Enterprise Single Sign-On Marketscope – Strong Positive (September 2009)
- User Provisioning Magic Quadrant (September 2009)
- Security Information & Event Management Magic Quadrant (May 2009)
- Web Access Management Magic Quadrant (November 2008)
- Managed Security Services Providers, North America Magic Quadrant (April 2009)
- Managed Security Service Providers, Europe Marketscope – Strong Positive (May 2008)
- Managed Security Service Providers, APAC Marketscope - Strong Positive (May 2008)



- Risk Consulting Services Wave (March 2009)
- Managed Security Services Wave (October 2007)



#1

- #1 Identity & Access Management (2008)
- #1 Identity Management Provider (2007)
- #1 Security & Vulnerability Management Software Worldwide (2007)
- #1 Vulnerability Assessment Software Worldwide (2007)
- #1 Application Vulnerability Assessment Software Worldwide (2007)

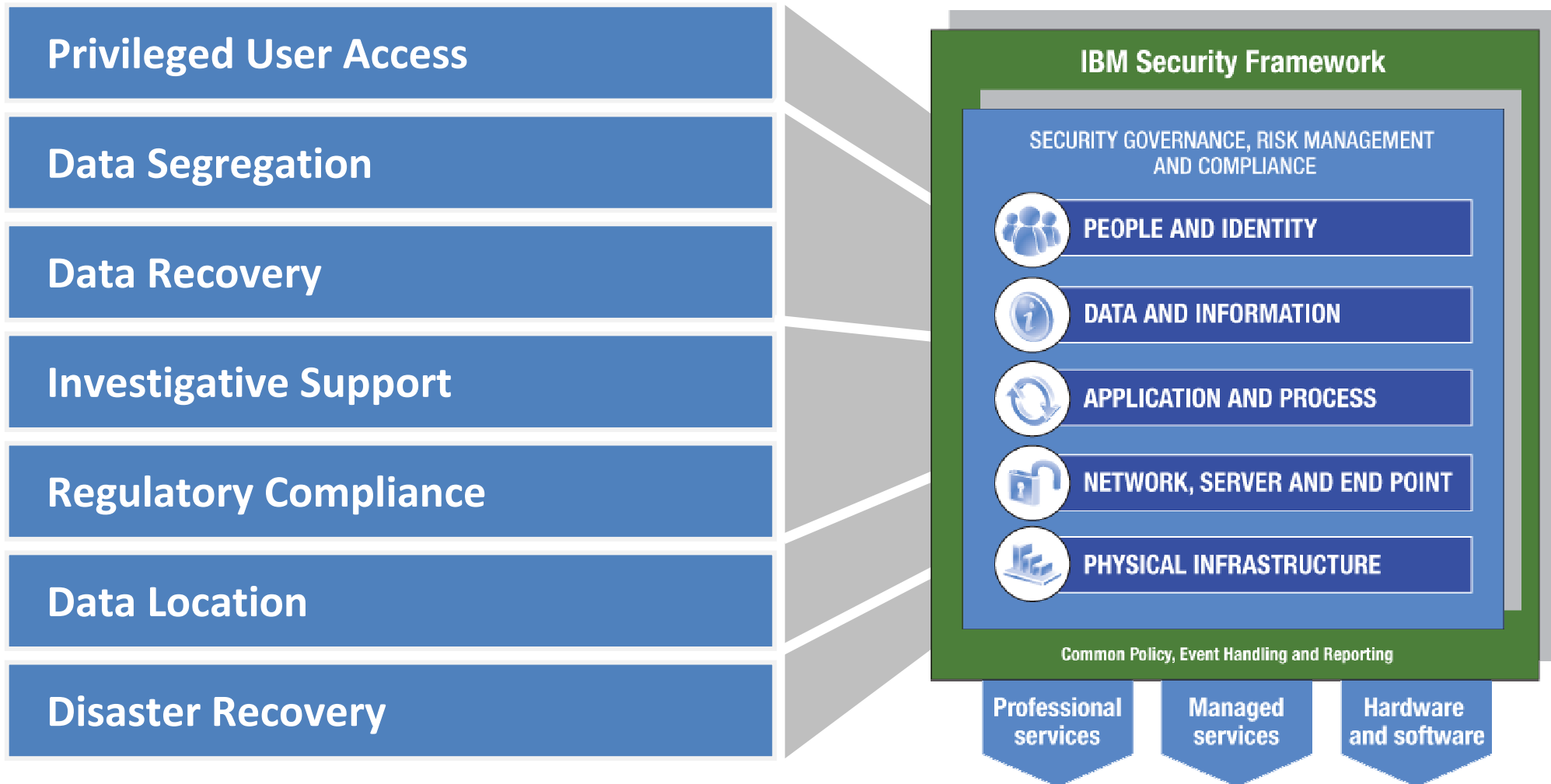


#1

- Managed Security Services (2008, 2009)
- North American Network Security Infrastructure Protection Company of the Year (2008, 2009)
- North American Video Surveillance Software Developer Company of the Year (2008, 2009)
- #1 Vulnerability Assessment Provider (2006, 2007, 2008)
- IDS/IPS Market Leader (2007)
- Global Application Security Product Line Strategy Award (2008).

Gartner reports on security risks of cloud computing

...that map directly to the IBM Security Framework.



IBM Security Framework



- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 40+ years of proven success securing the zSeries environment
- Already managing more than 1.7B security events per day for clients
- IBM Security Framework, Security Blueprint

BEST SECURITY COMPANY



WINNER
IBM Corporation
www.ibm.com/security

Founded in 1911, IBM has been a security industry leader for nearly 90 years, helping CxOs and IT professionals secure their corporate infrastructures with solutions that go beyond just collections of niche products. Customers rely on IBM for the planet's most secure databases, applications, operating systems, storage and servers.

IBM offers comprehensive security solutions and services addressing compliance, applications, data, identity and access management, networks, threat prevention, systems security, email, encryption, virtualization and cloud security.

Through an end-to-end approach to security across people and identity, data, applications, compliance, networks, servers and the physical infrastructure, IBM offers security capabilities that are among the top in the industry. With multiple leadership awards in market presence and technology innovation, IBM is able to offer more than 120 security products and the experience of over 15,000 researchers, developers and SMEs focused on security initiatives.

IBM clients around the world gain the benefit of integrated security solutions that reduce

the cost and complexity of managing security solutions from multiple vendors.

World-class security support services from IBM provide the technical and operational expertise needed to maximize security investment. By providing a global network of support centers to assist customers worldwide, often in their native language, IBM partners with its customers around the clock to solve any implementation and technical issues.

This support is available regardless of client location or implementation method of hardware, software and/or managed security services. IBM provides a variety of support levels - from self-help to tiered levels - enabling customers to choose the one that best meets their needs. IBM is recognized for its outstanding customer support and consistently high customer satisfaction.

The company has staked a firm claim in the security marketplace and emerged as a market leader capable of meeting any global organization's security needs through an integrated, diverse and flexible portfolio of products and services across key industries.

With a strong, deep and broad security portfolio, IBM is in a strong position, able to leverage its considerable assets and reputation and provide innovative technologies and intellectual property that address both today's vulnerabilities and newly emerging threats.



To learn more about IBM Security Solutions, please contact your IBM Representative or IBM Business Partner.



Visit our website at www.ibm.com/security

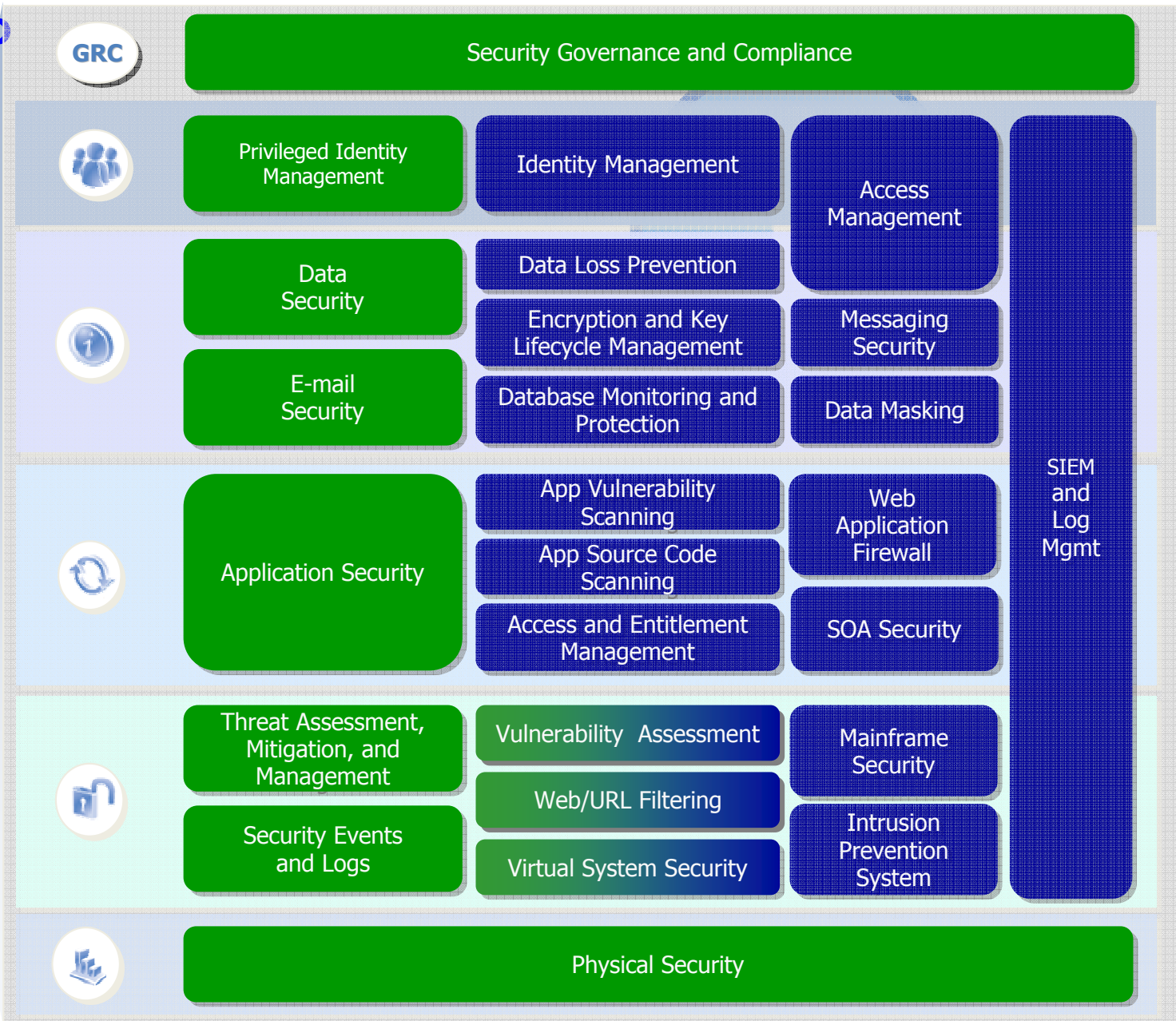


Security acquisitions:



IBM Security portfolio

 = **Services**
 = **Products**





U.S. Air Force Selects IBM to Design and Demonstrate Mission-Oriented Cloud Architecture for Cyber Security (Feb 04, 2010)



Advanced cyber security and analytics technologies capable of protecting sensitive national data

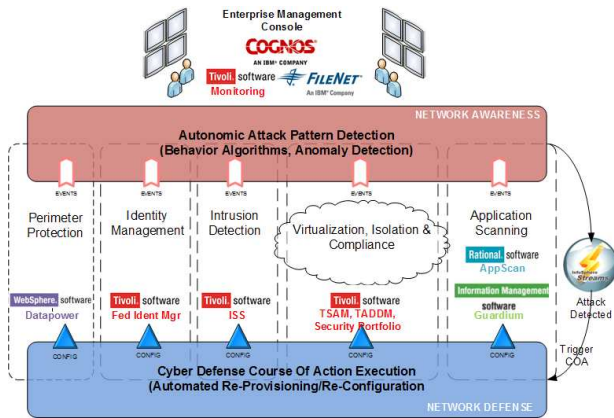
MOCA is Mission Oriented CLOUD Architecture

Achieving new levels of situation awareness

Real time processing of sensors, monitors, and devices

Enhanced security, policy management, and compliance management

IBM Secure Cloud Core



Pre-integrated Cloud, Analytics and Cyber Security Technologies

IBM Cloud Security Guidance



Cloud Security Best Practices

Secure Cloud Customization



Services engagement to implement Cyber Security Approach

Country-specific Cyber Policies and Patterns

Technology Base

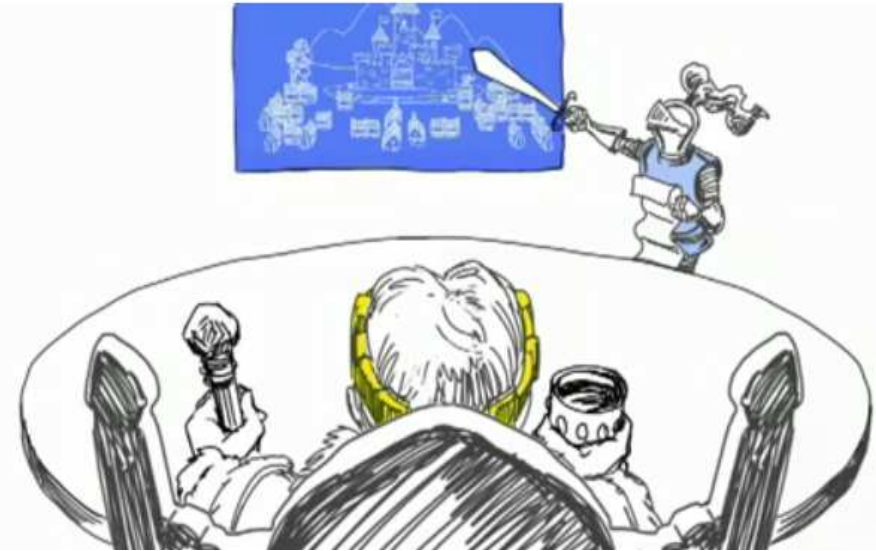
IBM
SECURE CLOUD

Security in the Cloud

Who can do this better than IBM?



The King, the Dragon and the Secure Cloud



ibm.com/software/Tivoli
ibm.com/ibm/cloud/

 Click in play mode

A
Smarter
Planet



Cloud computing