Cesare Radaelli

Cloud e Sicurezza: binomio necessario per le aziende che innovano

PCTY2011

Pulse Comes to You

Agenda:

- Cloud security Perception

- Example of a cloud application in action

- IBM Security offering for cloud

Cloud computing represents the "Industrialization of IT," similar to when:

- Telcos automated traffic through switches to assure service and lower cost.
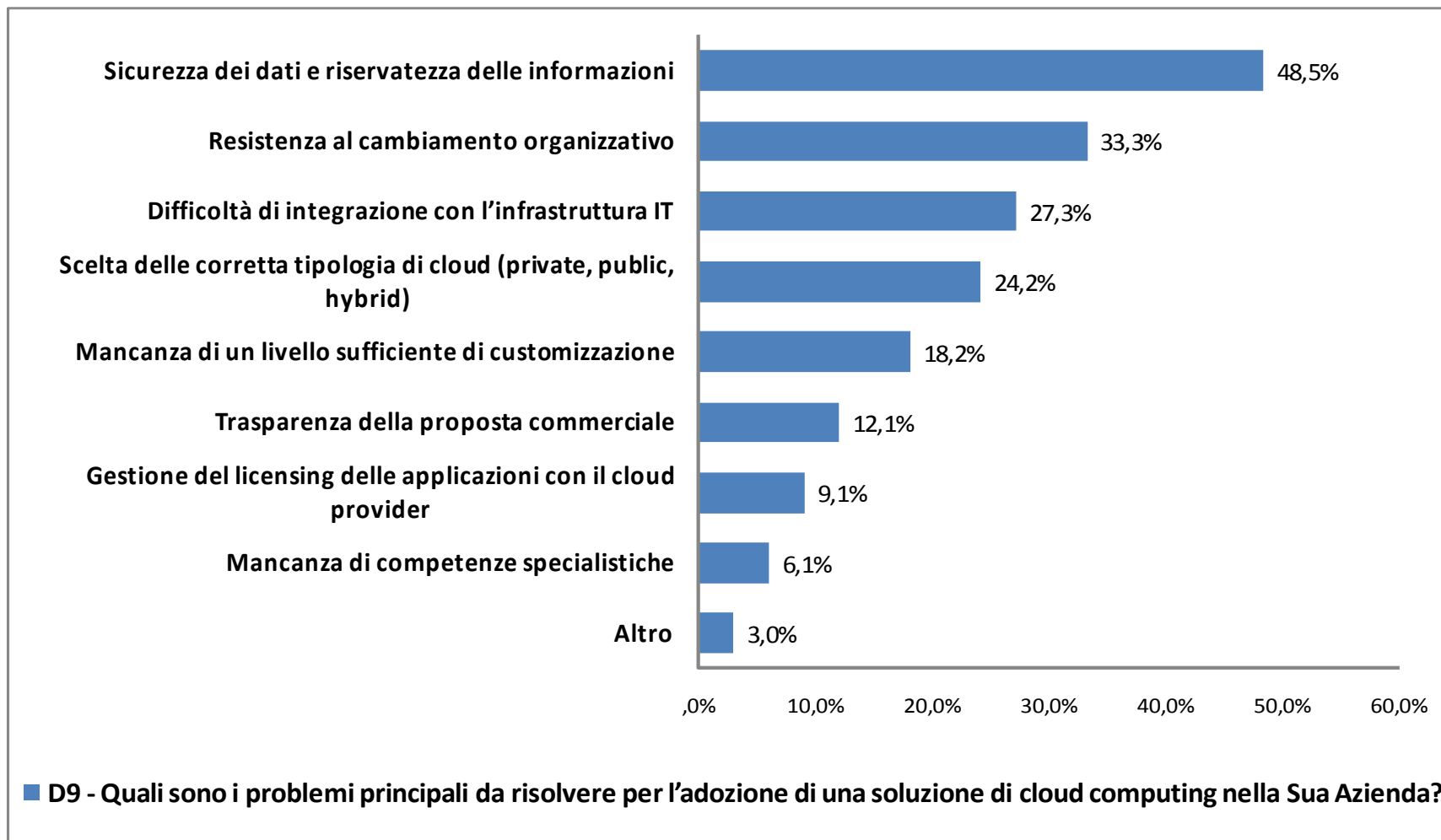
- Manufacturers started using robotics to improve quality and lower cost.

- Banks built the automated teller machine network to improve service and lower cost.
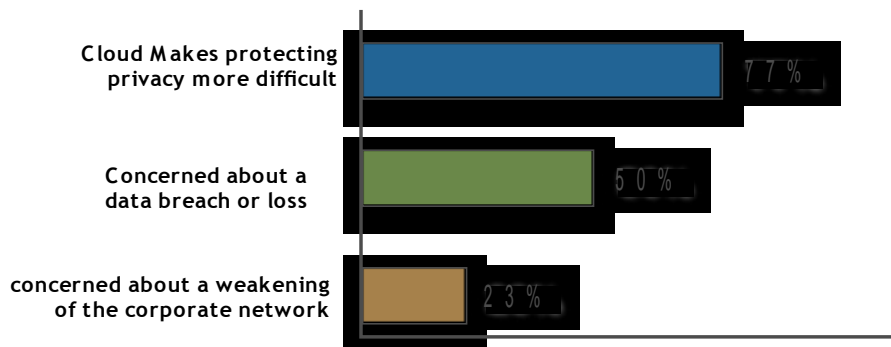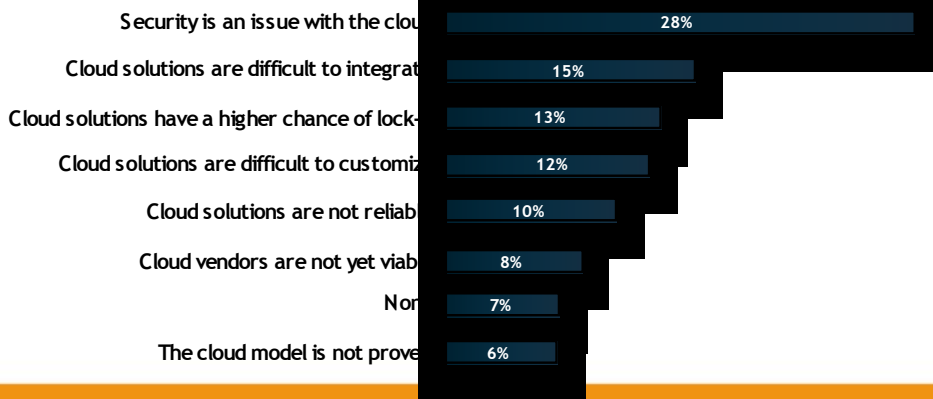
Main inhibitors for Cloud adoption

Sicurezza dei dati e riservatezza delle informazioni — 48,5%
Resistenza al cambiamento organizzativo — 33,3%
Difficoltà di integrazione con l'infrastruttura IT — 27,3%
Scelta delle corretta tipologia di cloud (private, public, hybrid) — 24,2%
Mancanza di un livello sufficiente di customizzazione — 18,2%
Trasparenza della proposta commerciale — 12,1%
Gestione del licensing delle applicazioni con il cloud provider — 9,1%
Mancanza di competenze specialistiche — 6,1%
Altro — 3,0%

Axis: ,0% 10,0% 20,0% 30,0% 40,0% 50,0% 60,0%

■ D9 - Quali sono i problemi principali da risolvere per l'adozione di una soluzione di cloud computing nella Sua Azienda?

Fonte: IDC Italy Cloud Computing Quick Poll, marzo 2011 (N=35)

Security in the Cloud

A recent Appirio survey of 150+ mid to large-sized firms that have already adopted cloud applications:
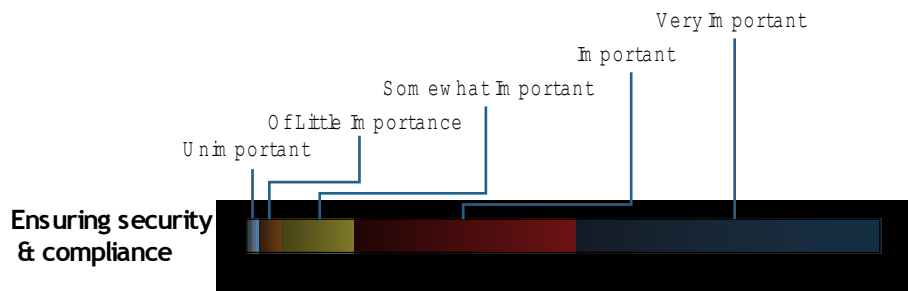
According to IBM's Institute for Business Value 2010 Global IT Risk Study, cloud computing raised serious concerns among respondents about the use, access and control of data

Very Important

Important

Somewhat Important

Of Little Importance

Unimportant

Ensuring security & compliance

Security is an issue with the clou	28%
Cloud solutions are difficult to integrat	15%
Cloud solutions have a higher chance of lock-	13%
Cloud solutions are difficult to customiz	12%
Cloud solutions are not reliab	10%
Cloud vendors are not yet viab	8%
Non	7%
The cloud model is not prove	6%

Cloud Makes protecting privacy more difficult	77%
Concerned about a data breach or loss	50%
concerned about a weakening of the corporate network	23%

PCTY2011
Pulse Comes to You

Agenda:

- Cloud security Perception

- Example of a cloud application in action

- IBM Security offering for cloud

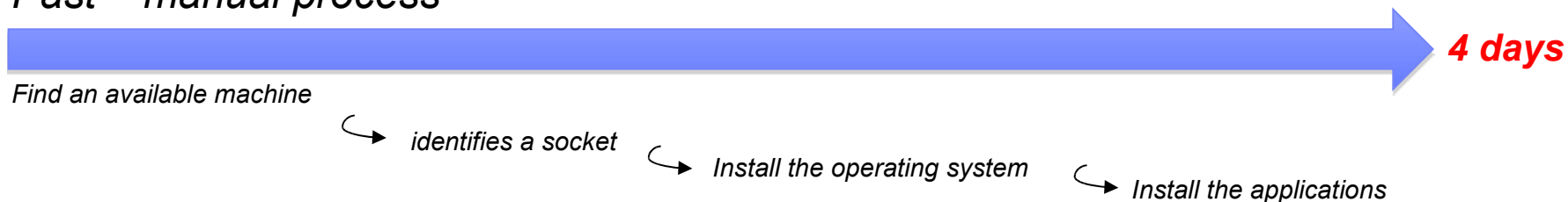# Tivoli IT must become more intelligent in providing services

- **As a result of growth and acquisitions, we had 38 laboratories, each with its own infrastructure. This creates inefficiency and increased costs of CAPEX and OPEX**

- **The increasing complexity 'in our system required that the IT services become standardized, efficient, safe and easy access**

- **It was necessary to have a Service Management system that give us visibility, control and automation services for both IT services business**

- **We had to create a new model of delivery and use of IT services**

- **In 2009 we saved $ 3.1M due to the Cloud**
  - The cloud infrastructure allows the average utilization of 60% of resources compared to the initial 5-9%
  - 1055 servers have been relocated, 280 sent to stock, and 174 virtualized
  - Each VM saves in costs ~ $ 2.700 per year (start of production, security, green)
  - Re-use of images instead of buying new hardware
  - Site consolidation has led to big savings on infrastructure (energy, air conditioning, space etc.)
  - We expect a further increase in the efficiency of expenditure

- **Increase service levels through the provision of services rapidly, consistently and with fewer errors**
  - Allocation automated self-service **(from 4 days to 15 minutes)**
  - Mitigate the risk associated with plans to purchase significant hardware development and testing
  - The IT department can focus on value-added services
  - Opportunity to share the environment during development and testing

- **Learn from experience**
  - The IT staff can now focus in providing new services
  - More 'than 1,800 users, up
  - 2200 VM growing as more servers are virtualized
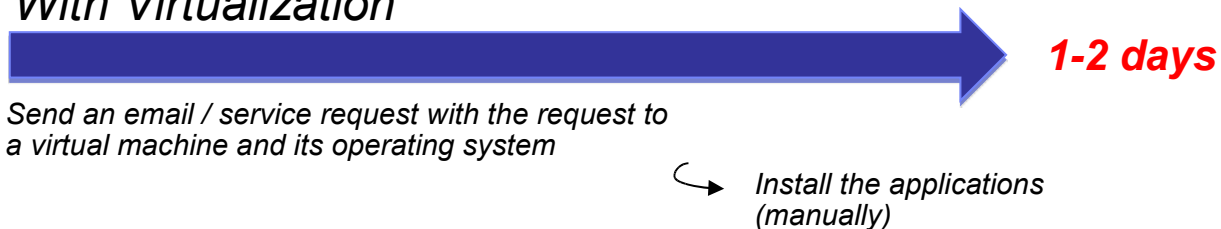 - Management of the global cloud, providing localized service

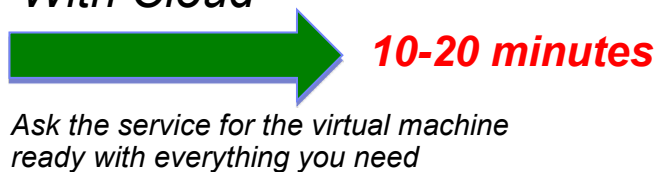# Example: a person of the test requires a Windows machine with Websphere and DB2

Past – manual process

4 days

Find an available machine

↳ *identifies a socket*

↳ *Install the operating system*

↳ *Install the applications*

With Virtualization

1-2 days

Send an email / service request with the request to a virtual machine and its operating system

↳ *Install the applications (manually)*

With Cloud

10-20 minutes

Ask the service for the virtual machine ready with everything you need

Risks are real...

Amazon's Web Services outage: End of cloud innocence?

By Larry Dignan | April 22, 2011, 7:27am PDT

Summary

Cloud computing is learning the harsh reality of resiliency as Amazon Web Services' outage has crossed its second day. Meanwhile, startups and a host of other AWS customers are in uncharted waters. What have we learned?

Topics

SLA, Data Center, Apartment, Amazon Web Services, Web Service, Amazon.com Inc., Outage, AWS, AWS Fallout, Service Level Management, more +

Cloud computing is learning the har[...]
Web Services' outage has crossed [...]
and a host of other AWS customers [...]

On Wednesday, the common belief [...]
infrastructure on AWS completely. S[...]
Things like availability zones—for a[...]
single point of failure. Some startup[...]
didn't.

Given that AWS' North Virginia data[...]
more than 24 hours, it's clear you n[...]
You need a backup for your cloud p[...]

Also: Amazon's N. Virginia EC2 clust[...]
triggered problems

• Whether it's Amazon or Microsof[...]

The good news for AWS customers [...]
coming online again. Amazon said i[...]

2:41 AM PDT We continue to mak[...]

Tech Center: **Database Security**

📧 E-mail this page | 🖨 Print this page | ➕ BOOKMARK ▪️🔲🔳 ...

Hack Of PlayStation Network Threatens Personal Data Of 77 Million Users

After a week of downtime, Sony comes clean about hack, promises to restore service

Apr 27, 2011 | 01:05 PM | 0 Comments

By Tim Wilson
Dark Reading

Sony is struggling to restore service -- and customer confidence -- following the hack of its PlayStation network, which serves an estimated 77 million people.

The gaming giant has provided little information on the nature of the hack, but it is telling users that their personal data could very well be at risk.

"We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network," says Sony in a blog.

**Databas[...]

lessons lear[...]
breaches, as [...]

vulnerability a[...]
tools in the IE[...]

**Other rep[...]

Agenda:

- Cloud security Perception

- Example of a cloud application in action

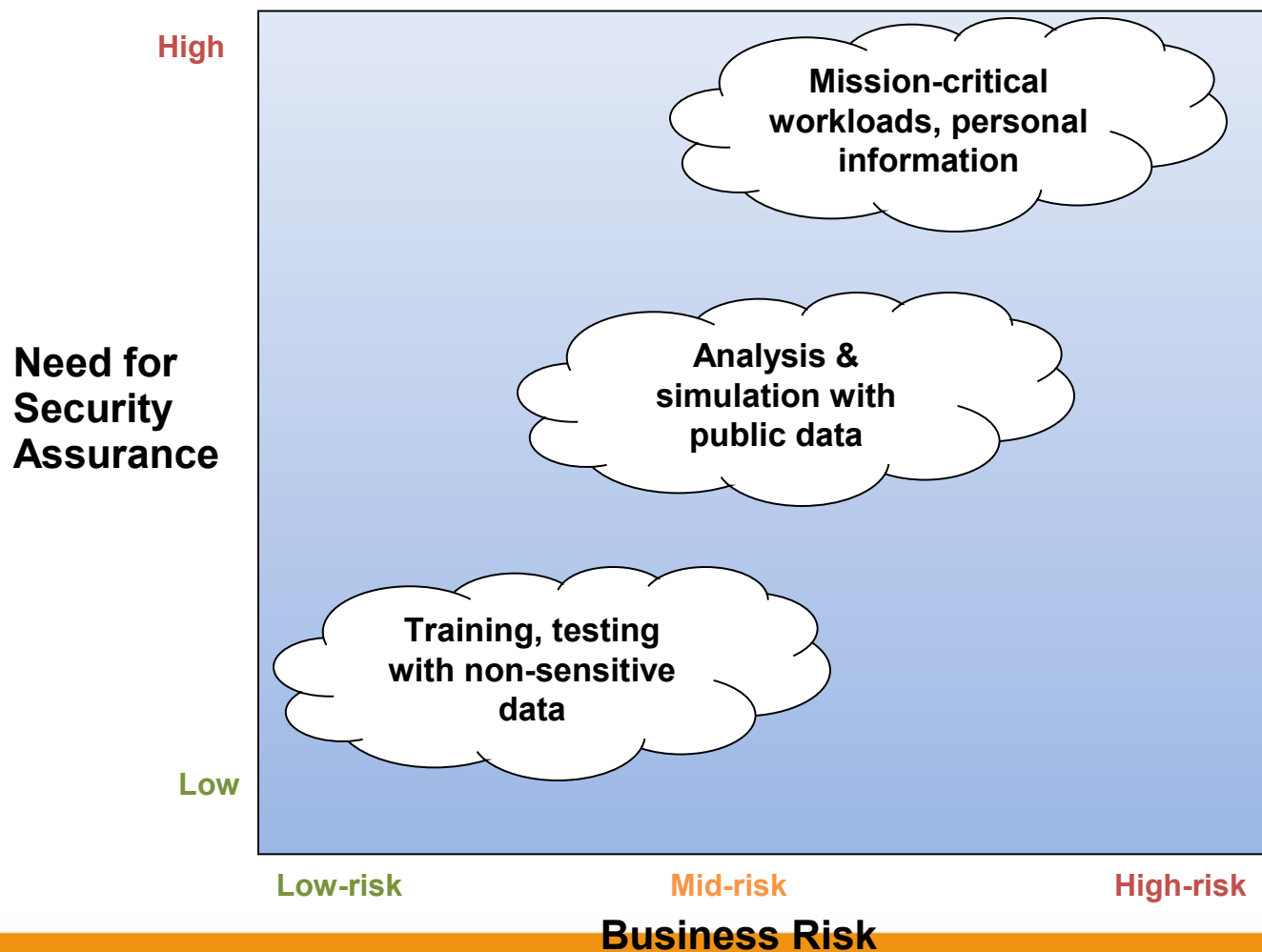- IBM Security offering for cloud

IBM's approach to Cloud Security

At IBM we understand the cloud and we also understand that
"One Size Does not Fit All"

One-size <u>does not</u> fit-all:
Different cloud workloads have different risk profiles

High

Mission-critical workloads, personal information

Tomorrow's high value / high risk workloads need:
- Quality of protection adapted to risk
- Direct visibility and control
- Significant level of assurance

Analysis & simulation with public data

Need for Security Assurance

Today's clouds are primarily here:
- Lower risk workloads
- One-size-fits-all approach to data protection
- No significant assurance
- Price is key

Training, testing with non-sensitive data

Low

Low-risk   **Mid-risk**   **High-risk**

Business Risk

IBM's Strategy for Cloud Security

IBM Security Framework:
*Risk management-based
approach to security*

IBM Security Framework

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

Common Policy, Event Handling and Reporting

Professional Services | Managed Services | Hardware and Software
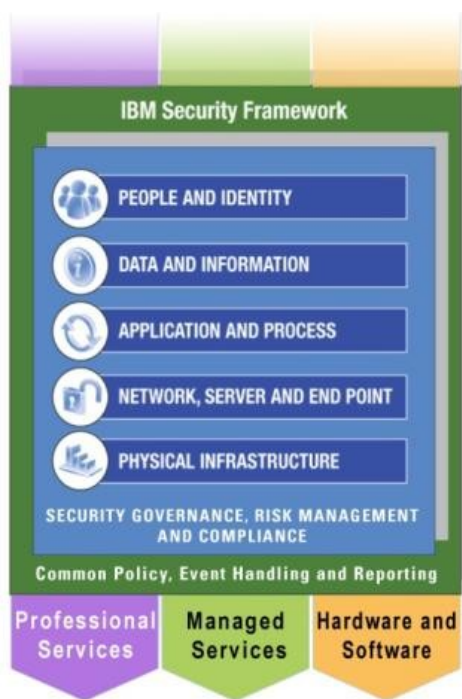
**Provider of
Security Products for Clouds**

**Provider of
Cloud-based Security Services**

**Provider of
Secure
Clouds**

PCTY2011
Pulse Comes to You

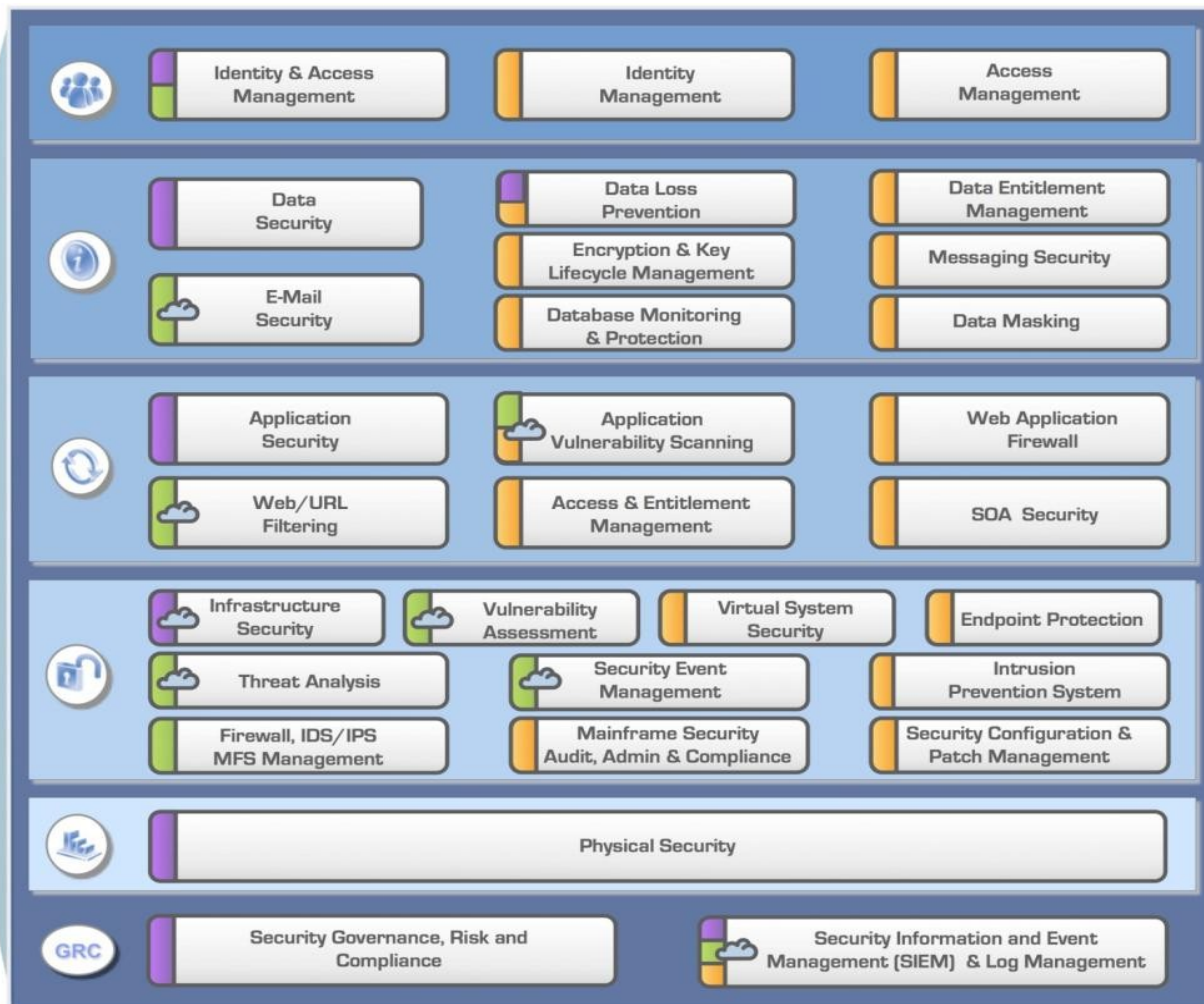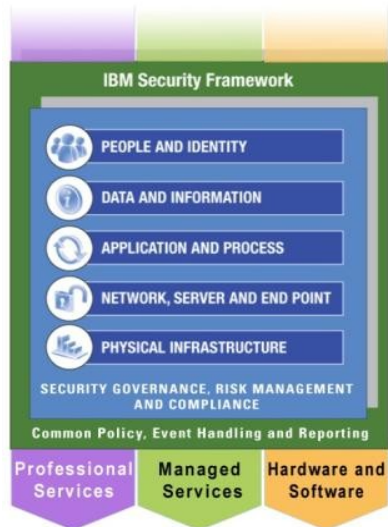# Extension for Advanced Security Management

- Support authentication and trust in federated environment
- Prevent sprawl of privileged users

- Support data location, segregation, availability and lifecycle
- Intelligent backup and recovery of data

- Protection of code
- Application maintenance (updates & rollback)

- Protection of potentially very distributed architectures
- Segregation of multi-tenant environments
- Secure virtualization servers and virtual systems

- Compliance of the infrastructure
- Audit & reporting
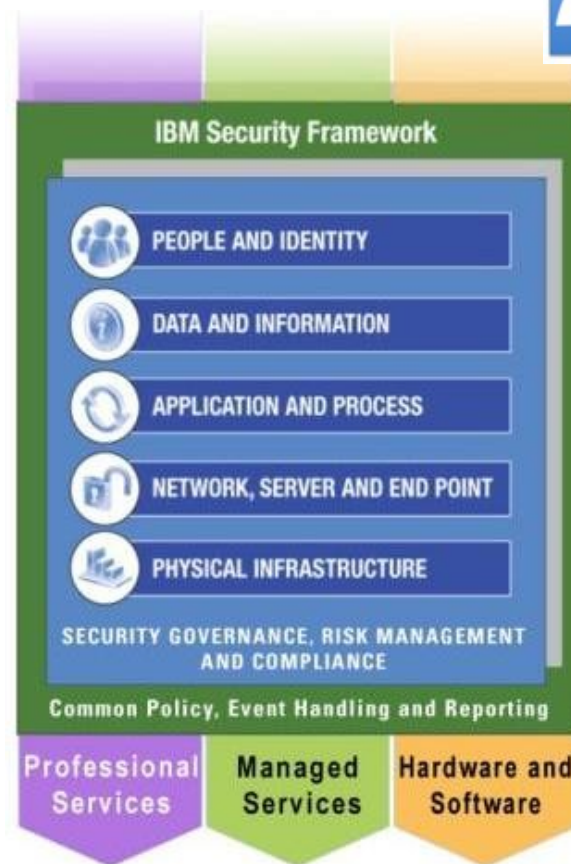
Industry leading security protects your cloud from becoming a malware superhighway

IBM Security Framework

Security governance, risk management and compliance

IBM Security Framework

Customers require **visibility** into the security posture of their cloud.

Implement a governance and audit management program

IBM Cloud Security Guidance Document

- Establish 3rd-party audits (SAS 70, ISO27001, PCI)
- Provide access to tenant-specific log and audit data
- Create effective incident reporting for tenants
- Visibility into change, incident, image management, etc.
- Support for forensics and e-Discovery

Supporting IBM Products, Services and Solutions

IBM Security Products and Services

IBM Security Risk Assessment

Assessing security to create a roadmap to reduced risk

A comprehensive evaluation of an organization's existing security policies, procedures, controls and mechanisms.

IBM Resiliency Consulting Services

Assessment and planning – resilient cloud validation

A comprehensive evaluation of an organization's existing disaster recovery plans and alignment to the environment.

People and Identity

IBM Security Framework

Customers require **proper authentication** of cloud users.

IBM Cloud Security Guidance Document

Implement strong identity and access management

Privileged user monitoring, including logging activities, physical monitoring and background checking

Utilize federated identity to coordinate authentication and authorization with enterprise or third party systems

A standards-based, single sign-on capability can help simplify user logons for both internally hosted applications and the cloud.

Supporting IBM Products, Services and Solutions

IBM Security Products and Services

IBM Tivoli Federated Identity Manager

Securely manage cloud identities

Employ user-centric federated identity management to increase customer satisfaction and collaboration

IBM Tivoli Security Information and Event Manager

Optimize security & compliance efforts

Monitor user activity for accidental or malicious activity that could put information at risk

Data and Information

IBM Security Framework

Customers cite **data protection** as their **most important** concern.

Ensure confidential data protection

IBM Cloud Security Guidance Document

- Use a secure network protocol when connecting to a secure information store.

- Implement a firewall to isolate confidential information, and ensure that all confidential information is stored behind the firewall.

- Sensitive information not essential to the business should be securely destroyed.

Supporting IBM Products, Services and Solutions

IBM Security Products and Services

IBM Data Security Services

Protect data and enable business innovation

Solutions for network data loss prevention, endpoint encryption, endpoint data loss prevention, and log analysis

IBM Information Protection Services

Continuous data protection

- Remote Data Protection Services
- Email Management Express
- Fastprotect Online

Application and Process

IBM Security Framework

Customers require **secure cloud applications** and **provider processes**.

Establish application and environment provisioning

- Implement a program for application and image provisioning.
- A secure application testing program should be implemented.
- Ensure all changes to virtual images and applications are logged.
- Develop all Web based applications using secure coding guidelines.

IBM Cloud Security Guidance Document

Supporting IBM Products, Services and Solutions

IBM Security Products and Services

IBM Rational AppScan

Secure testing for web application vulnerability

Solution features a scalable enterprise architecture that enables centralized scanning of multiple applications simultaneously

IBM WebSphere DataPower XML Security Gateway XS40

Secure web facing applications vulnerability at the code level

Solution features an integrated appliance that provides ongoing security protection, policy management, and governance for securing web facing applications

Network, Server and End Point

IBM Security Framework

Customers expect a **secure** cloud **operating environment**.

IBM Cloud Security Guidance Document

Maintain environment testing and vulnerability/intrusion management

- Isolation between tenant domains

- Trusted virtual domains: policy-based security zones

- Built-in intrusion detection and prevention

- Vulnerability Management

- Protect machine images from corruption and abuse

IBM Security Products and Services

Supporting IBM Products, Services and Solutions

IBM Virtual Server Security for VMware

Protection of cloud-based infrastructure

Provides market-leading intrusion prevention, firewall and visible security for virtual environments

IBM Endpoint Data Protection

Remote protection of sensitive data

- Prevent data access when a device is lost or stolen
- Protect sensitive data when stored, accessed, transmitted or shared
- Monitor usage of sensitive data
- Enforce policies at the end-user level

Physical Security

IBM Security Framework

Customers expect **cloud data centers** to be **physically secure**.

Implement a physical environment security plan

IBM Cloud Security Guidance Document

- Ensure the facility has appropriate controls to monitor access.

- Prevent unauthorized entrance to critical areas within facilities.

- Ensure that all employees with direct access to systems have full background checks.

- Provide adequate protection against natural disasters.

Supporting IBM Products, Services and Solutions

IBM Security Products and Services

IBM Physical Security Services
Defend and help secure physical environments
A full suite of digital security solutions and site assessments that can be integrated with your network and IT systems

IBM Managed Security Services has Global Reach and Leverages Our Tivoli and IBM Research Capabilities

9 Security Operations Centers	+	9 Security Research Centers	+	11 Security Solution Development Centers	+	133 Monitored Countries	+	900+ Professional Services Security Consultants	+	600+ field security specialists	+	4,500 Security Delivery Experts	+	400+ security operations analysts

- **20,000+ Devices under Contract**
- **3,700+ MSS Clients Worldwide**
- **9 Billion+ Events Managed Per Day**

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

Why IBM for Cloud Security

- IBM has the expertise to assist clients in all aspects of cloud security

- IBM has a proven methodology, based on type of cloud (public, private, hybrid) and intended workloads

- Client's should keep in mind that clouds are a specific example of IT infrastructure. IBM's approach to securing IT infrastructure is end-to-end, starting with a solid approach to governance, risk and compliance.

- Security is often viewed as a major inhibitor to cloud adoption. IBM's view is that a properly designed and operated cloud can indeed meet client security requirements.

Thank you!

Cesare Radaelli

IBM Security Solutions

Security TT Leader
Italy

Circonvallazione Idroscalo
 20090 Segrate, Italy

Tel +39 348 5219272
cesare.radaelli@it.ibm.com