云时代的安全管理
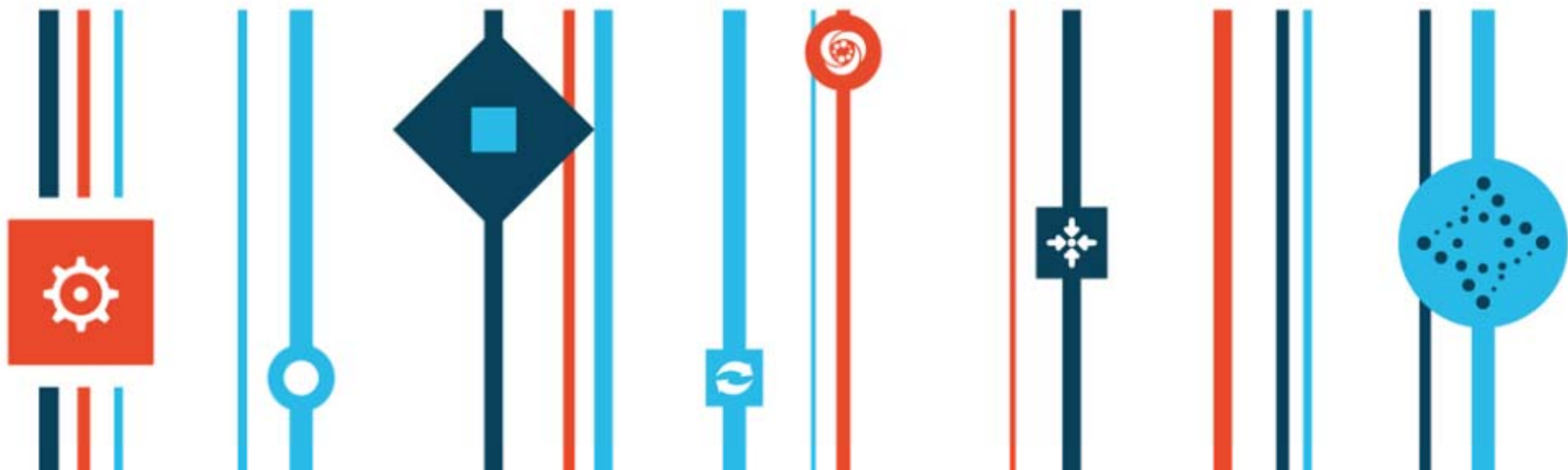
袁文宗

IBM大中华区云计算中心业务经理

perryy@cn.ibm.com

- 云计算实验室成立已超过**7年**历史

- 我们致力於云计算相关软硬件产品及服务在各行业的整体应用解决方法

- 我们也发表白皮書及出版書籍

- 另外，也叄与中国电子学会云计算专委会委员,代表 IBM针对云计算的技朮研究与标準制定

- 我们也將持续在云计算投入大量资金及人员

提纲

- 云计算安全的挑战

- 云计算安全的考虑因素与架构

- 云计算安全的机会

云计算是过去积累技术的有效集成，以一种崭新应用模式的表现结果

- 由于涉及的技术层面较为复杂，因此普遍被误为是一种全新的技术
- 过去的资讯安全孤岛并不能因为采用云计算架构就完全解决安全问题
- 云计算是在解决工作流程问题

调查发现，采用云计算最重要的考虑因素就是安全

80%
Of enterprises consider security the #1 inhibitor to cloud adoptions

48%
Of enterprises are concerned about the reliability of clouds

33%
Of respondents are concerned with cloud interfering with their ability to comply with regulations

*"**How can we be assured that our data will not be leaked** and that the vendors have the technology and the governance to **control its employees from stealing** data?"*

*"**Security is the biggest concern.** I don't worry much about the other "-ities" – reliability, availability, etc."*

*"**I prefer internal cloud to IaaS. When the service is kept internally**, I am more comfortable with the security that it offers."*

Source: Driving Profitable Growth Through Cloud Computing, IBM Study (conducted by Oliver Wyman)

然而安全的问题，每个调查报告的侧重点各有不同

Gartner: Top Risks (2008)
- Privileged user access
- Regulatory compliance
- Data location
- Data segregation
- Recovery
- Investigative support
- Long-term viability

Source: Gartner Research, 2008

ENISA: Top Risks (2009)
- Loss of governance
- Lock-in
- Isolation failure
- Compliance risks
- Management interface compromise
- Data protection
- Insecure or incomplete data deletion
- Malicious insider

Source: European Network and Information Security Agency, 2009

CSA: Top Threats (2010)
- Abuse and misuse of cloud
- Insecure interfaces and APIs
- Malicious insiders
- Shared technology issues
- Data loss or leakage
- Account or service hijacking
- Unknown risk profile

Source: Cloud Security Alliance, 2010

IBM X-Force (2010)
- Obtain information
- Gain privilege
- Gain access
- File manipulation
- Denial of service
- Data manipulation
- Bypass security

Source: IBM X-Force, 2010

首先，先针对云计算安全做一个定义

Confidentiality, integrity, availability
of business-critical IT assets

stored or processed on a cloud
computing platform

Cloud Computing

Software as a Service

Utility Computing

Grid Computing

**There is nothing new under the sun
but there are lots of old things we don't know.**

Ambrose Bierce, The Devil's Dictionary

那么，对于过去和现在的资产，我们拥有控制权

**data, application,
processes**

We Have Control
It's located at our premises
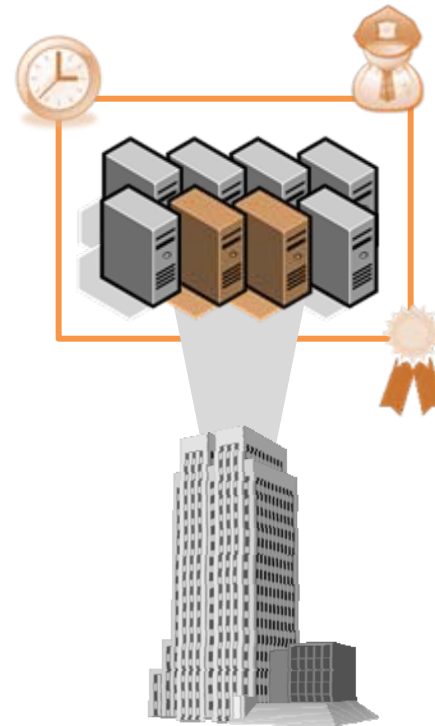It's stored in our server X,Y, Z
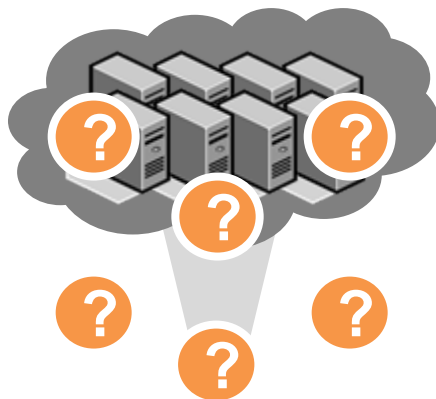We have backups in place
We have access control
Our uptime is sufficient
The auditors' are happy
Our security team is engaged

对于未来进入云计算的资产安全考虑必须更周全

Doubt for your assets "somewhere" in the Cloud?

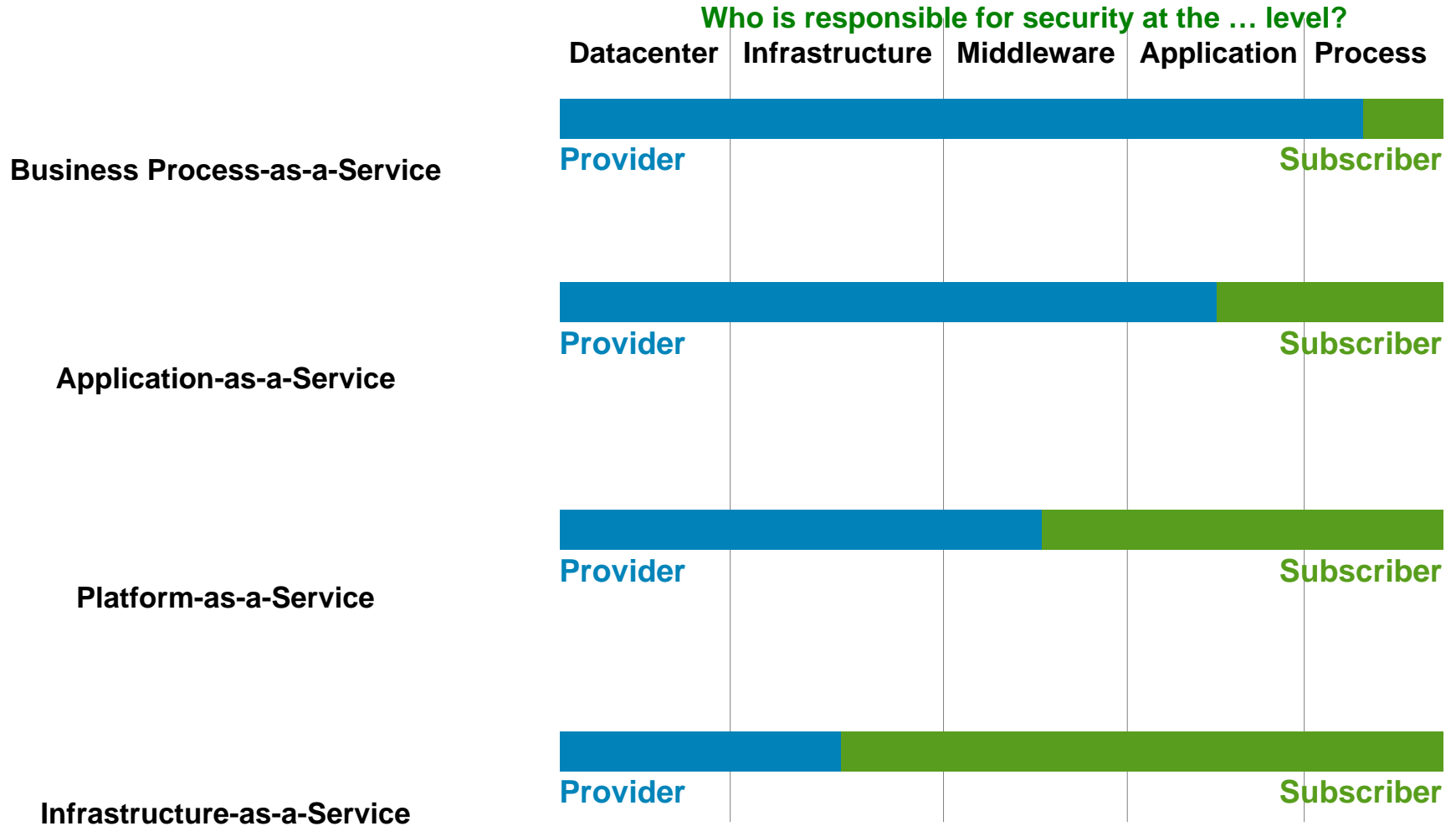**Ask questions for each Assets in the Cloud**

Who Has Control?	How would we be harmed if…
Where is it located?	an employee of our cloud provider accessed the asset?
Where is it stored?	the asset became widely public and widely distributed?
Who backs it up?	the process or function were manipulated by an outsider?
Who has access?	the process or function failed to provide expected results?
How resilient is it?	the information/data were unexpectedly changed?
How do auditors observe?	the asset were unavailable for a period of time?
How does our security team engage?	the asset were unable to fulfill the compliances?
	the information/data were stolen?

至于安全责任的归属也必须明确

Who is responsible for security at the … level?

	Datacenter	Infrastructure	Middleware	Application	Process

Business Process-as-a-Service

Provider   Subscriber

Application-as-a-Service

Provider   Subscriber

Platform-as-a-Service

Provider   Subscriber

Infrastructure-as-a-Service

Provider   Subscriber

Provider/Subscriber service agreement determines actual responsibilities.

考虑云计算运用的风险，从适当规划应用范围开始

High

Need for Security Assurance

Low

Mission-critical workloads, personal information

Analysis & simulation with public data

Training, testing with non-sensitive data

Low-risk   Mid-risk   High-risk

Business Risk

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

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

从IBM的角度来看有五大安全范畴

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

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

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009

Give the right users access to the right resources at the right time

Protect sensitive business data

Keep applications available and protected from malicious use.

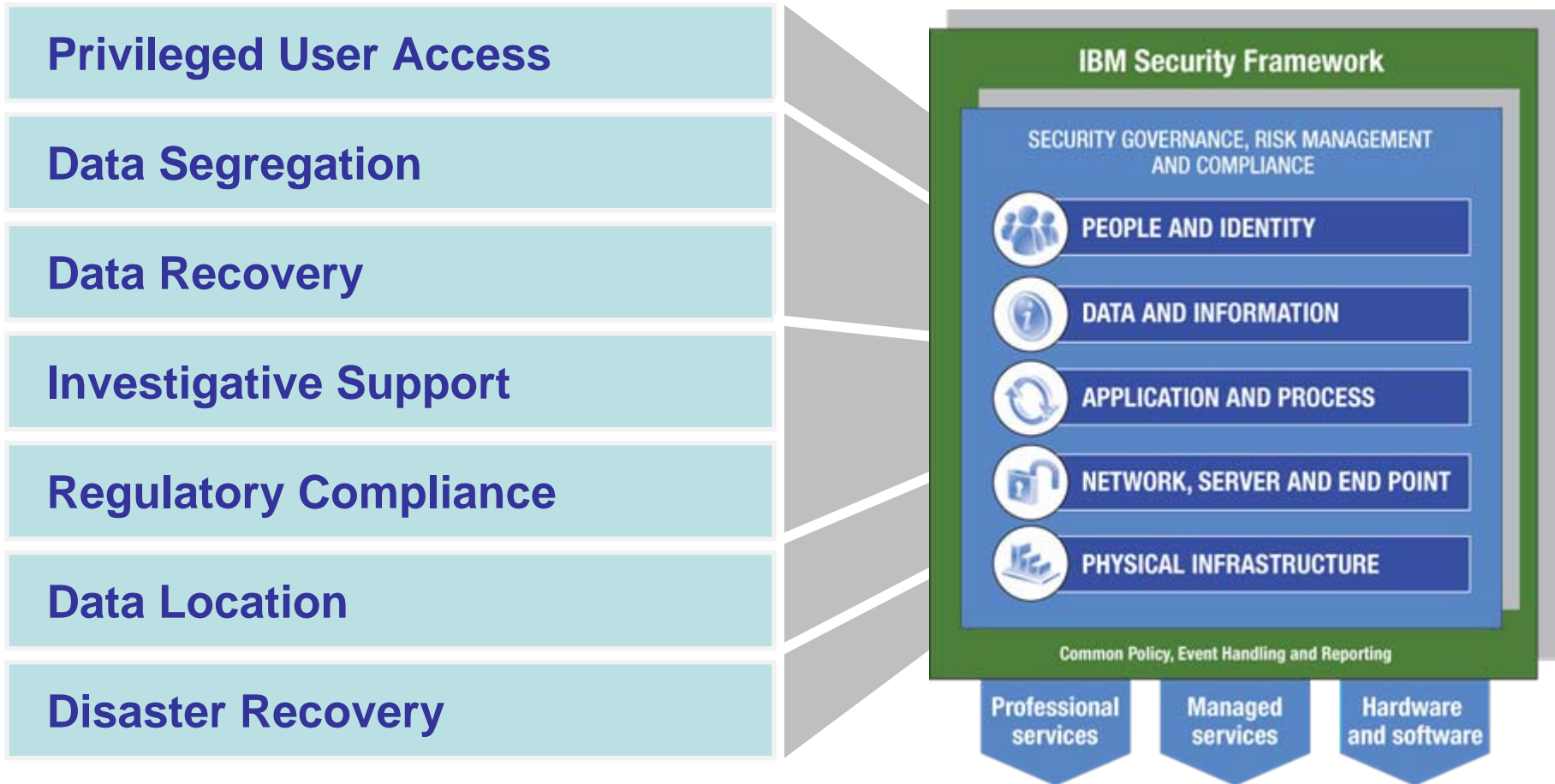**Optimize service availability by mitigating risks**

Provide actionable intelligence and improve effectiveness of physical infrastructure security

再细分看有多样解决之道

智揽云海 云领未来
2010 IBM 云计算高峰论坛

= Services
= Products

Security Governance and Compliance Services

Identity and Access Mgmt. Services
Identity Management
Access Management

Data Security Services
Data Loss Prevention
Messaging Security

E-mail Security
Encryption and Key Lifecycle Management

Database Monitoring and Protection
Data Masking

Application Security Services
App Vulnerability Scanning
Web App Firewall

App Source Code Scanning

Access and Entitlement Management
SOA Security

Threat Assessment, Mitigation, and Mgmt. Services
Vulnerability Assessment
Mainframe Security

Web/URL Filtering
Virtual System Security

Security Events and Logs
IPS

SIEM and Log Mgmt

Physical Security Services

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

Common Policy, Event Handling and Reporting

Professional services

Managed services

Hardware and software

Each customer will have access to the portal to view their results. Each scan will run for 4 consecutive weeks and the customer will have access to the portal to view their results for 45 days.

ess 🔘 htt   ▼ ➡ Go   Link

oogle g ▼   ▼   Search ▼ 🗔 ▼ 🌐 ✚ ▼   📧 ▼ ⭐ Bookmarks ▼   🔍 Find ▼ ✓ Check ▼   📋 AutoFill ▼   🔧 ▼ ⚪ Sign I

IBM ®   **Internet Security Systems**
Managed Security Servi

Each customer will be given a temporary username and password in which they will later be prompted to change.

ALERTCON 1

Virtual Security Operations Center

nter your username
nd password to Sign In

Jsername: [   ]

Password: [   ]

[Sign In]

Access from your mobile device at
https://portal.mss.iss.net/mss/waplogin.mss

NOTICE: 2008 MSS Billing Changes

Security Operations Center Announcement

At the present time, all services are actively being delivered from our Global Security Operations Centers in North America, South America, Europe, and Asia. All systems within the Security Operations Centers are operating under normal conditions.

Currently, there are no Internet Emergencies active or pending. In the event of an Internet Emergency, a status update will be provided at this URL, and Managed Security Services customers will be notified accordingly.

How Does the Managed Services Portal Benefit You?

The Managed Services Customer Portal offers secure real-time access to reports, charts and utilities, enabling staff to quickly review logs, submit policy changes and enter service requests. Managed Services customers maintain high levels of security awareness and control, while protection experts perform day-to-day security management tasks.

SC MAGAZINE
AWARDS
2006
WINNER

SC MAGAZINE GLOBAL AWARDS 2005 WINNER   **SC** MAGAZINE GLOBAL AWARDS 2004 WINNER

SysTrust
刯 ERNST & YOUNG LLP

2005 FROST & SULLIVAN
Customer Service Innovation Award

安全顾问服务

智揽云海 云领未来
2010 IBM 云计算高峰论坛

Phase 5.
Education

- IBM Security Product Training
- Security Awareness Training

Phase 1.
Assessment

- **Application Security Assessment**
- **Information Security Assessment**
- **Penetration Testing**
- **PCI Assessment (US and International)**
- **SCADA Assessment**
- **Policy and ISO 17799 Gap Analysis**

Phase 4.
Management
and Support

- **Emergency Response Service**
- **Forensic Analysis Service**
- Staff Augmentation and Support

Phase 2.
Design

- Implementation Planning
- Network Security Architecture Design
- Policy Design and Development
- Standards and Procedures Development

Solution Focus Areas

Phase 3.
Deployment

- Deployment Services
- Migration Services

IBM PSS Solution Focus Areas

- Application Security Assessments
  - Remote attack simulation in which security experts attempt to penetrate an application, using techniques similar to those used by malicious attackers
  - Identification and exploitation of application vulnerabilities to determine application security and accessibility of data
- Information Security Assessments
  - A comprehensive evaluation of overall security posture, internally and externally – security policies, procedures, controls and mechanisms as well as physical security, networks, servers, desktops and databases
- Penetration Testing
  - Real-life network attack simulation in which security experts attempt to penetrate a network mimicking the techniques used by malicious attackers
  - Determination of network vulnerabilities while demonstrating how attackers can significantly impact your business
- PCI Assessments
  - Assessment of companies that accept, store or process credit card information for compliance with the Payment Card Industry (PCI) Data Security Standard
  - IBM ISS is recognized as a Qualified Security Assessor, certified to complete PCI Assessments
- Emergency Response Services
  - Incident response, preparedness planning and forensic analysis experts
  - Responds quickly to attacks in progress
  - Works with customers to develop customized emergency response plans to minimize the effect of future attacks
  - Available as a subscription service or on an as-needed basis
- SCADA Assessments
  - Assessment of Supervisory Control and Data Acquisition (SCADA) systems used in the energy and utilities, manufacturing and pharmaceutical industries
  - Provides recommendations for improving the security of critical systems vital to national infrastructure

Application Security Assessment – Methodology

- **Information Gathering**
  - Investigation of application design and programming from the developer's perspective to determine format for testing

- **Technical Testing**
  - Assessment of the application to uncover security vulnerabilities and weaknesses

- **Targeted Source Code Review** – Optional add-on
  - Consultants review portions of the application code to gain further insight into identified problems
  - Targeted, cost-effective review of the application code to provide solid recommendations for improving the code for greater security

- **Deliverables**
  - Detailed report on the application's current security posture and detailed recommendations for remediating any vulnerabilities discovered

•IBM Clouds are designed to ensure that the common issues related to people and Identity are adequately addressed

•**In the Cloud User Identity and Access Management both play as much of a role in protecting one's assets as Data protections. As a result of this IBM clouds are design to provide organizations with the tools necessary for security related to persons and their identity**

- Privileged User Access
  • Access Management
  • Identity Management
- Federated Identity Management
- Privileged Account Management

People and Identity
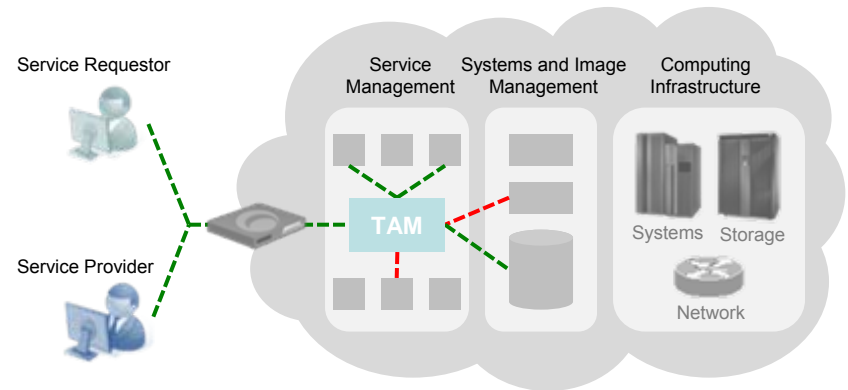
Tivoli Access Manager (TAM)

Privileged User Access

Separation of administrative and user roles in a cloud environment

Summary: 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.

Service Requestor

Service Provider

Service Management   Systems and Image Management   Computing Infrastructure

TAM

Systems   Storage

Network

Tivoli Federated Identity Manager (TFIM)

Cloud Identity Federation

Single access method for users into cloud and traditional applications

Summary: TFIM 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.

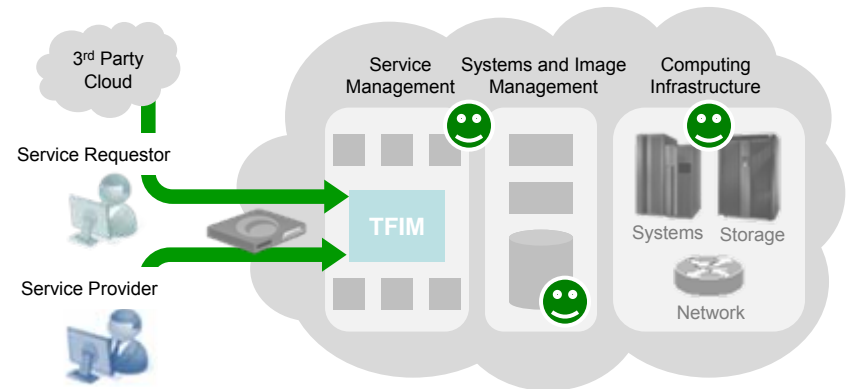**Deployment Scenario**: Positioned at Application Server to authenticate access to back end and management functions.

3rd Party Cloud

Service Requestor

Service Provider

Service Management   Systems and Image Management   Computing Infrastructure

TFIM

Systems   Storage

Network

•**Data protection is the primary concern of most organizations, it intertwined with all the other elements of cloud security**

•The Key elements of IBM's strategy are:

- – Data Segregation
- – Encryption
- – Segmentation
- – Accessibility
- – Data Recovery
- – Data Redaction & Termination
- – Virtual Image Destruction
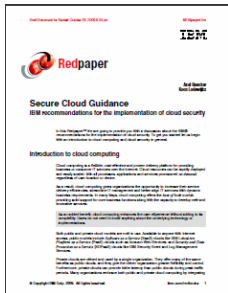- – Data Leakage Prevention

But Cloud Security is not just About Data Protection.

Data and Information

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

IBM Security Framework

IBM Cloud Security Guidance Document

Ensure confidential data protection

- 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 Tivoli Security Information and Event Manager
Protect data and enable business innovation
Solutions for network data loss prevention, endpoint encryption, endpoint data loss prevention, and log analysis

- **When engaging in the cloud organizations need to consider how they will build security into their models up front, and how they plan to manage those aspects**
- The Key elements of IBM's strategy are:
  - Compliance and Auditing
  - Investigative Support
  - Policy Management
    - Policy Provisioning
  - Secure Provisioning
    - Image Management
  - Application & Testing
    - Application Scanning
    - Secure Coding Practices

Application and Process

IBM Rational AppScan & IBM ISS Vulnerability Assessment Services
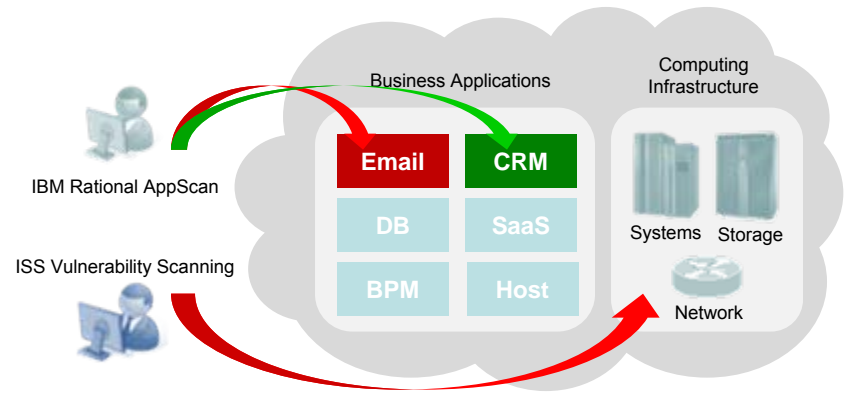
Compliance and Auditing

Vulnerability and compliance checking of cloud applications

Summary: IBM Rational AppScan scans and tests for common Web application vulnerabilities including SQL-Injection, Cross-Site Scripting and Buffer Overflow. IBM ISS Professional Security Services 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.

IBM Rational AppScan

ISS Vulnerability Scanning

Business Applications

Email   CRM

DB   SaaS

BPM   Host

Computing Infrastructure

Systems   Storage

Network

IBM Audit Technologies & IBM ISS Security Event and Log Management Service (SELM)

Investigative Support

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

Summary: The IBM ISS Security Event and Log 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

Computing Infrastructure

Systems   Storage   Network   Apps

LOG   LOG   LOG   LOG

IBM ISS Security Event & Log Management Services
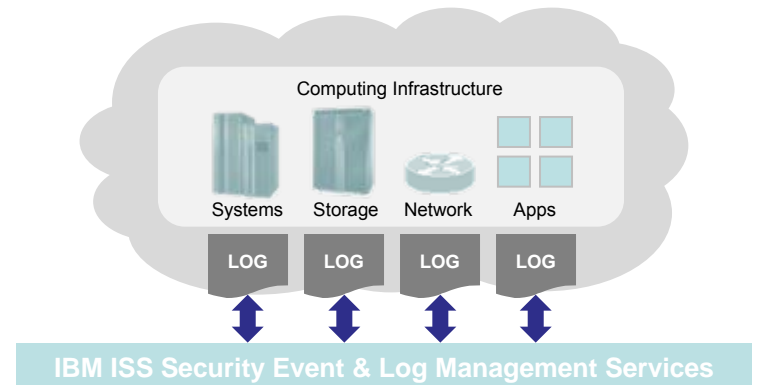
•**Network Protections play a critical role in cloud Security, IBM Clouds use a variety of technologies to ensure their customers are adequately protected**

– Server Security
– Network Security
  • Network Segmentation
– Virtualization Security
  • Intrusion Prevention, Detection
  • Extrusion Prevention
– Browser Security
  • Secure Communications
– Patch Management

Network protection
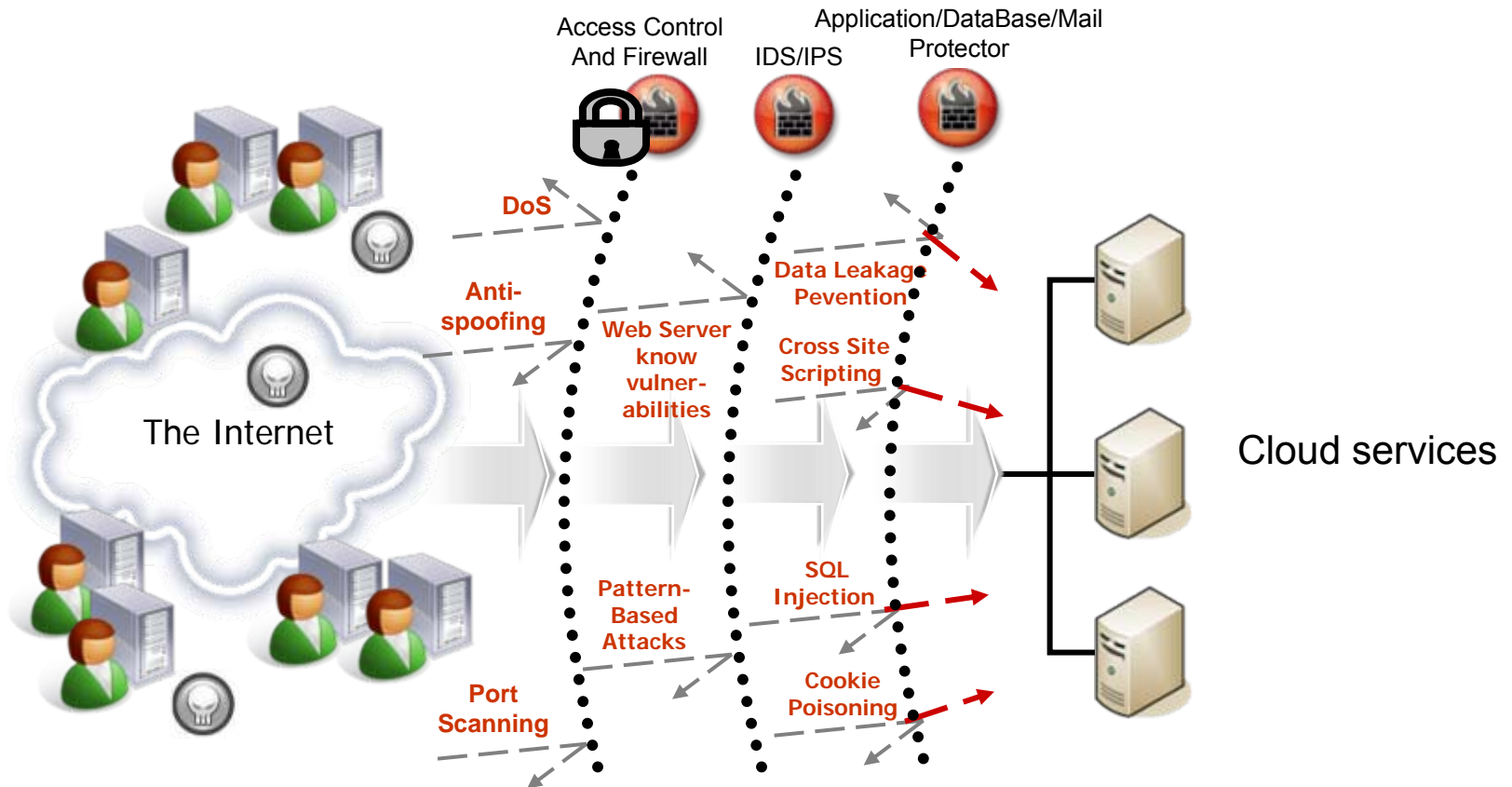
智揽云海 云领未来
2010 IBM 云计算高峰论坛

Cloud Delivered Services

Application as a service
Application software licensed for use as a service provided to customers on demand

Platform as a service
Optimized middleware – application servers, database servers, portal servers

Infrastructure as a service
Virtualized servers, storage, networking

Cloud Platform

Business Support Services
Offering Mgmt, Customer Mgmt, Ordering Mgmt, Billing

Operational Support Services
Infrastructure Provisioning Instance, Image, Resource / Asset Mgmt
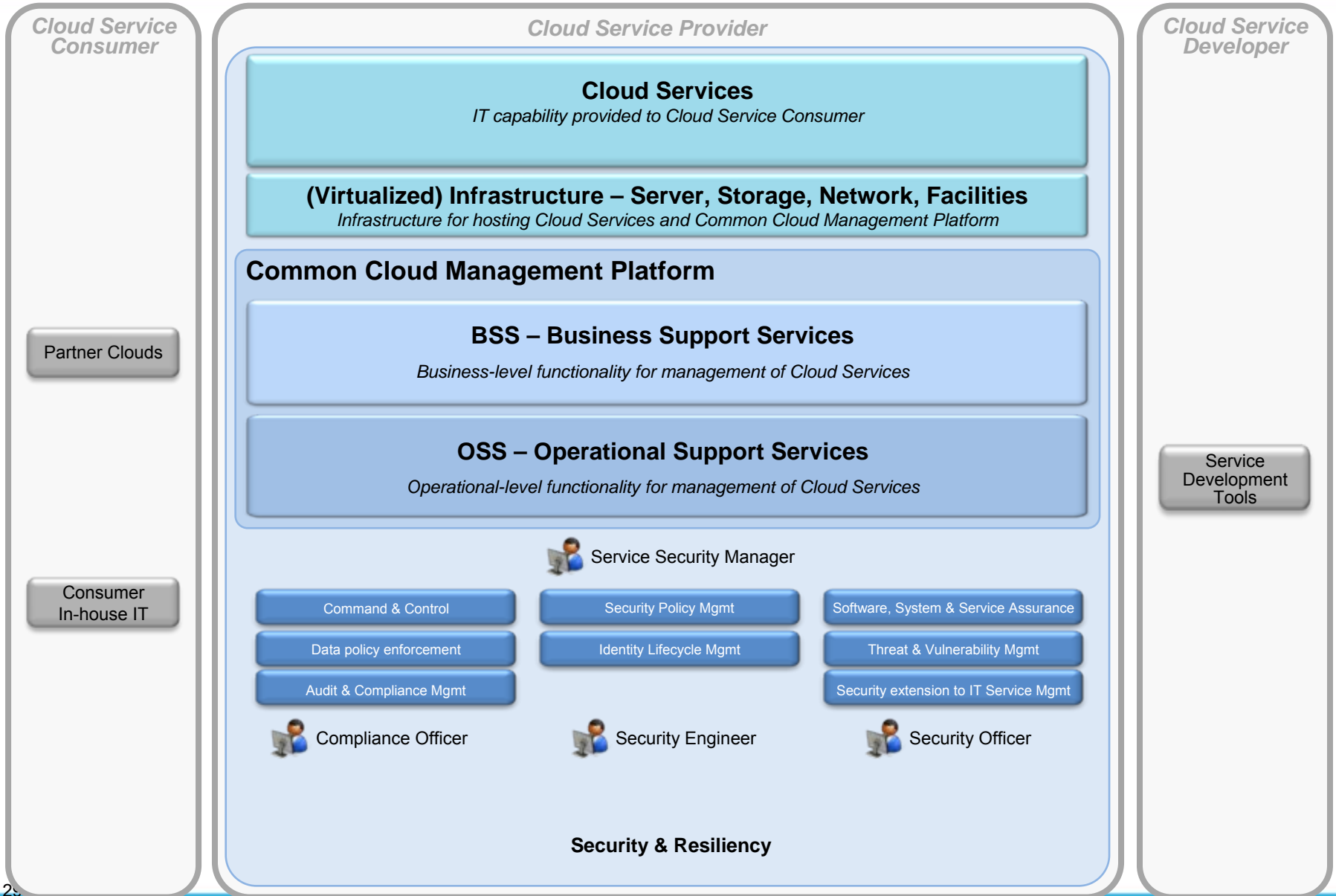
Virtualized Resources
Virtual Network, Server, Storage

System Resources
Network, Server, Storage

Physical System and Environment

SAAS

PAAS

IAAS

WORKFLOW

REPORTING

Perimeter

Local Area Network (LAN)

Hosts and the Data Center

智揽云海 云领未来
2010 IBM 云计算高峰论坛

Cloud Service Consumer

Cloud Service Provider

Cloud Service Developer

Cloud Services
IT capability provided to Cloud Service Consumer

(Virtualized) Infrastructure – Server, Storage, Network, Facilities
Infrastructure for hosting Cloud Services and Common Cloud Management Platform

Common Cloud Management Platform

BSS – Business Support Services

Business-level functionality for management of Cloud Services

OSS – Operational Support Services

Operational-level functionality for management of Cloud Services

Partner Clouds

Consumer In-house IT

Service Development Tools

Service Security Manager

Command & Control	Security Policy Mgmt	Software, System & Service Assurance
Data policy enforcement	Identity Lifecycle Mgmt	Threat & Vulnerability Mgmt
Audit & Compliance Mgmt		Security extension to IT Service Mgmt

Compliance Officer   Security Engineer   Security Officer

Security & Resiliency

智揽云海 云领未来
2010 IBM 云计算高峰论坛
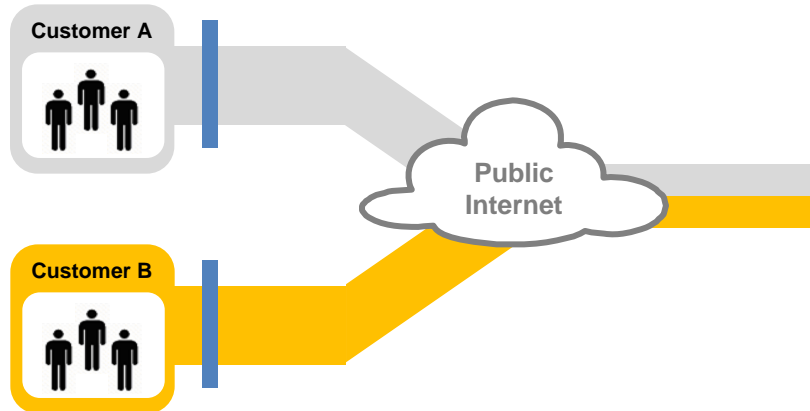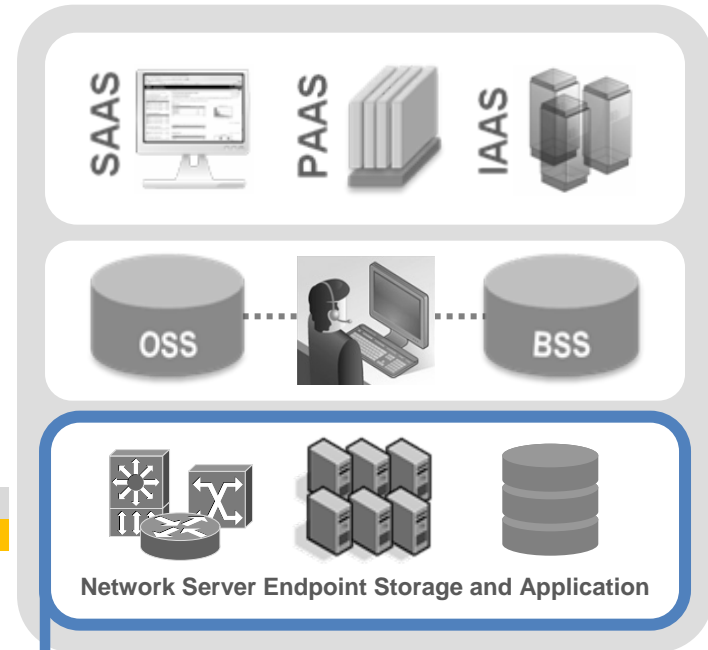
IBM Security Initiatives

Offers a broad portfolio of security products and services to help build a **secure cloud infrastructure**

IBM Cloud Offerings

- Intrusion prevention
- Firewall
- Anti-Malware
- Anti-Spam
- URL Filtering
- Web application protection
- VPN

- Virtualization protection
- Host protection (server and desktop)
- Messaging security
- Vulnerability management
- Vulnerability remediation
- Data leakage prevention
- Endpoint Secure Control

Key cloud solutions supported by IBM

Threat & Vulnerability Management

Data & Information Protection Mgmt

Risk & Compliance Assessment

Network, Server & Endpoint

Enterprise Security

Security for existing IT infrastructure as it extends to the cloud

IBM Enterprise Security Solutions

Summary: IBM ISS security products and services driven by X-Force research, Tivoli Security Software to reduce cost and risk, and IBM Systems create a highly secure computing environment that minimizes the potential risk posed by security threats.

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

Deployment Scenario: In the traditional enterprise IT environment.

Systems Security

Software Security

Network Security

Security Services

Virtualization Security

Security for pools of high performance virtualized resources

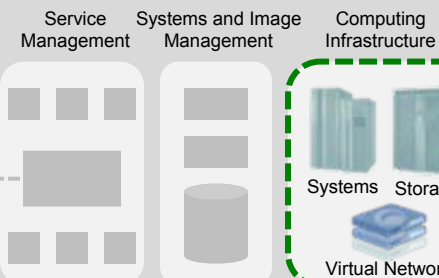### IBM Systems and IBM Virtualization Security

Summary: IBM offers the industry's broadest set of virtualization capabilities. Relying on over 40 years of heritage and attention to security, IBM virtualization platforms are built with security, not as an afterthought, but as a requirement. ISS Proventia Server stops threats inside VMs.

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

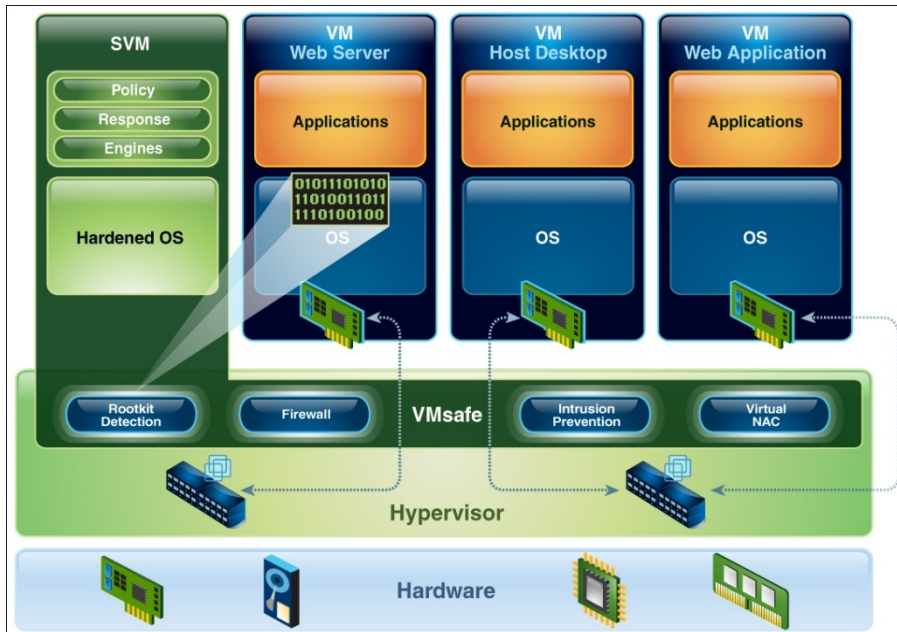**Deployment Scenario**: In the virtual data center.

Service Requestor

Service Provider

Service Management   Systems and Image Management   Computing Infrastructure

Systems   Storage

Virtual Network

Integrated threat protection for Virtualization Security

Offers broadest, most integrated, defense-in-depth virtualization security with *one product*

- Provides dynamic protection for every layer of the virtual infrastructure

- Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure

- Increases ROI of the virtual infrastructure with easy to maintain, easy to deploy security

- Firewall
- VMsafe Integration
- Rootkit Detection
- Intrusion Detection & Prevention
- Inter-VM Traffic Analysis
- VM Sprawl Management
- Network Policy Enforcement
- Automated Protection for Mobile VMs (VMotion)

- Auto Discovery
- Virtual Infrastructure Auditing (Privileged User Access)
- Virtual Network Segment Protection
- Virtual Network-Level Protection
- Virtual Network Access Control
- Central Management
- Web Application Protection
- Virtual Patch

云计算的机会在协助简化安全的控制与防护

People and Identity	▪ **Centralized** Identity and Access Control policies ▪ **Well-defined** set of input/output **interfaces** ▪ **Consistent** enrollment, proofing, validation and management of a trusted user
Information and Data	▪ Computing services running in **isolated domains** as defined in **service catalogs** ▪ **Default encryption** of data in motion & at rest ▪ **Virtualized storage** providing better **inventory, control, and tracking of master data**
Process & Application	▪ **Autonomous** security policies and procedures ▪ Personnel and tools with **specialized knowledge** of the cloud ecosystem ▪ **SLA-backed** availability and confidentiality
Network Server and Endpoint	▪ **Automated** provisioning and reclamation of **hardened** runtime images ▪ **Dynamic allocation** of pooled resources to mission-oriented resources ▪ **Simplified**, **built-in** security controls
Physical infrastructure	▪ **Closer coupling of systems** for management of physical and logical identity/access ▪ Strong platform of compute resources with **integrated workload-balancing and resiliency** ▪ **Highly-fortified** physical data centers

IBM is positioned to help secure Cloud Computing in 3 areas

1 **Cloud Security Consulting**

Recommendation #1:

Define, invest in, and develop Cloud Consulting Services

Offer IBM professional security services to clients engaging in cloud initiatives.

Examples:
- Cloud assessment services*
- Penetration testing for the Cloud*
- Information security assessment
- Protection policy and standards development

2 **Cloud Security Products**

Recommendation #2:

Develop a Standardized Cloud Implementation Service

Develop products and technologies to protect cloud infrastructures and their tenants.

Examples:
- Scalable chassis-based solutions
- Virtual appliances
- Integrated virtualization security
- Integrated server protection
- Proventia enhancements to better comprehend clouds (mobility, multi-tenancy)*

3 **Cloud Security Services**

Recommendation #3:

Develop and extend selected ITS Managed Services offerings

Leverage the cloud as a delivery mechanism for IBM security services.

Examples:
- Cloud-based SOC services
- Vuln management service
- Email scrubbing service
- Web content filtering service
- Security event log management
- Alliances with 3rd party services

IBM Cloud Security

总结

- 安全问题没有万灵丹，必须对症下药

- SC Magazine在2010年把 ”the best security company” 给了IBM

- 我们在致力打造有效，可靠的端到端云计算安全环境