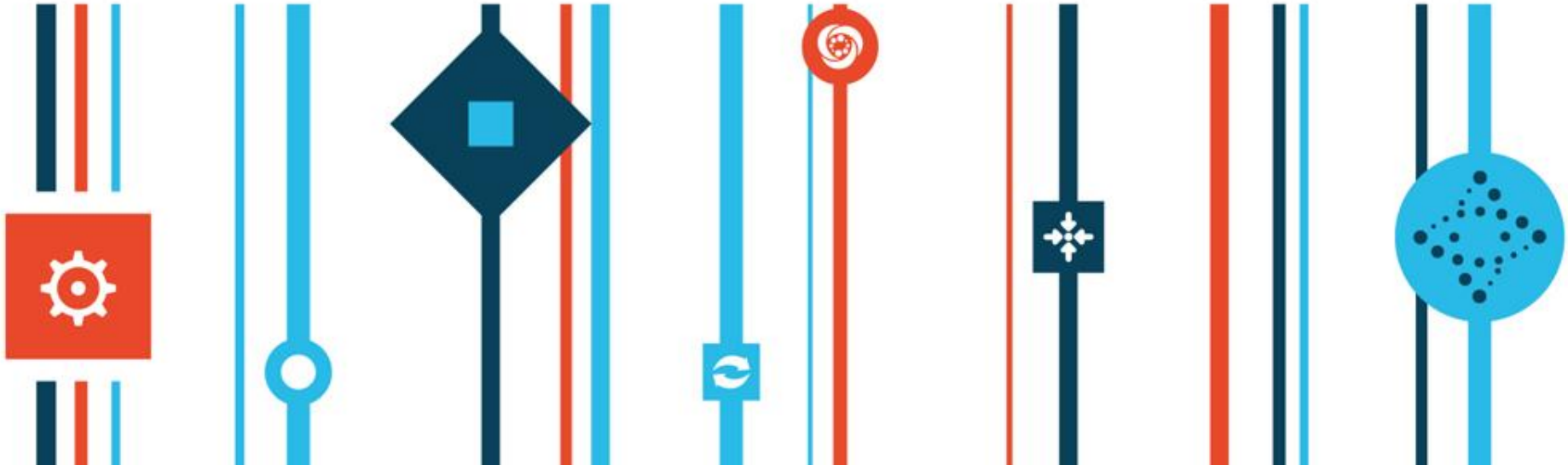
云时代的安全管理

袁文宗
IBM大中华区云计算中心业务经理
perryy@cn.ibm.com



IBM云计算中心成立已有一段时间

- 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，也参与中国电子学会云计算专委会委员,代表 IBM针对云计算的技术研究与标準制定
- 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

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

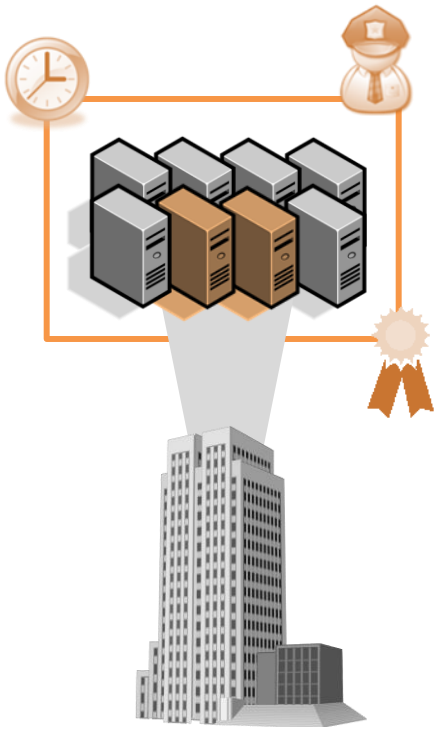
Ambrose Bierce, The Devil's Dictionary

那么，对于过去和现在的资产，我们拥有控制权

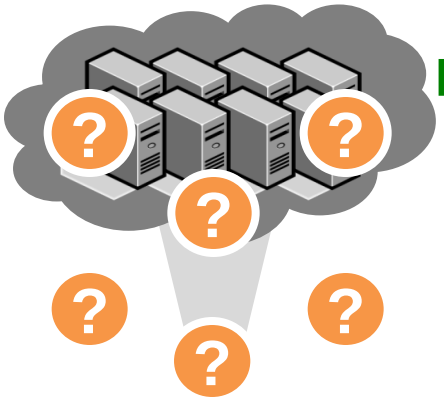
data, application, processes

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

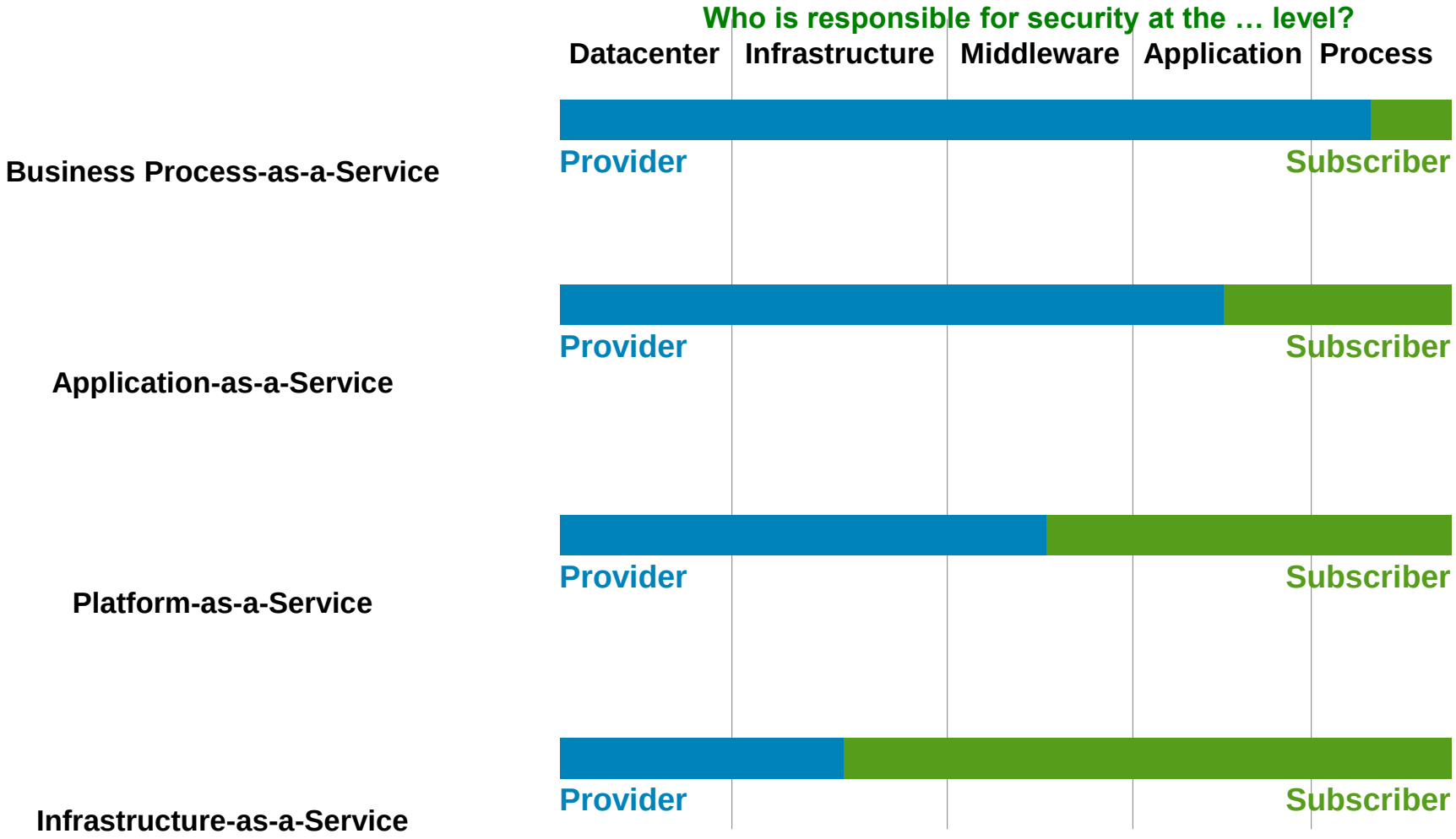


Doubt for your assets ”somewhere” in the Cloud?

Ask questions for each Assets in the Cloud

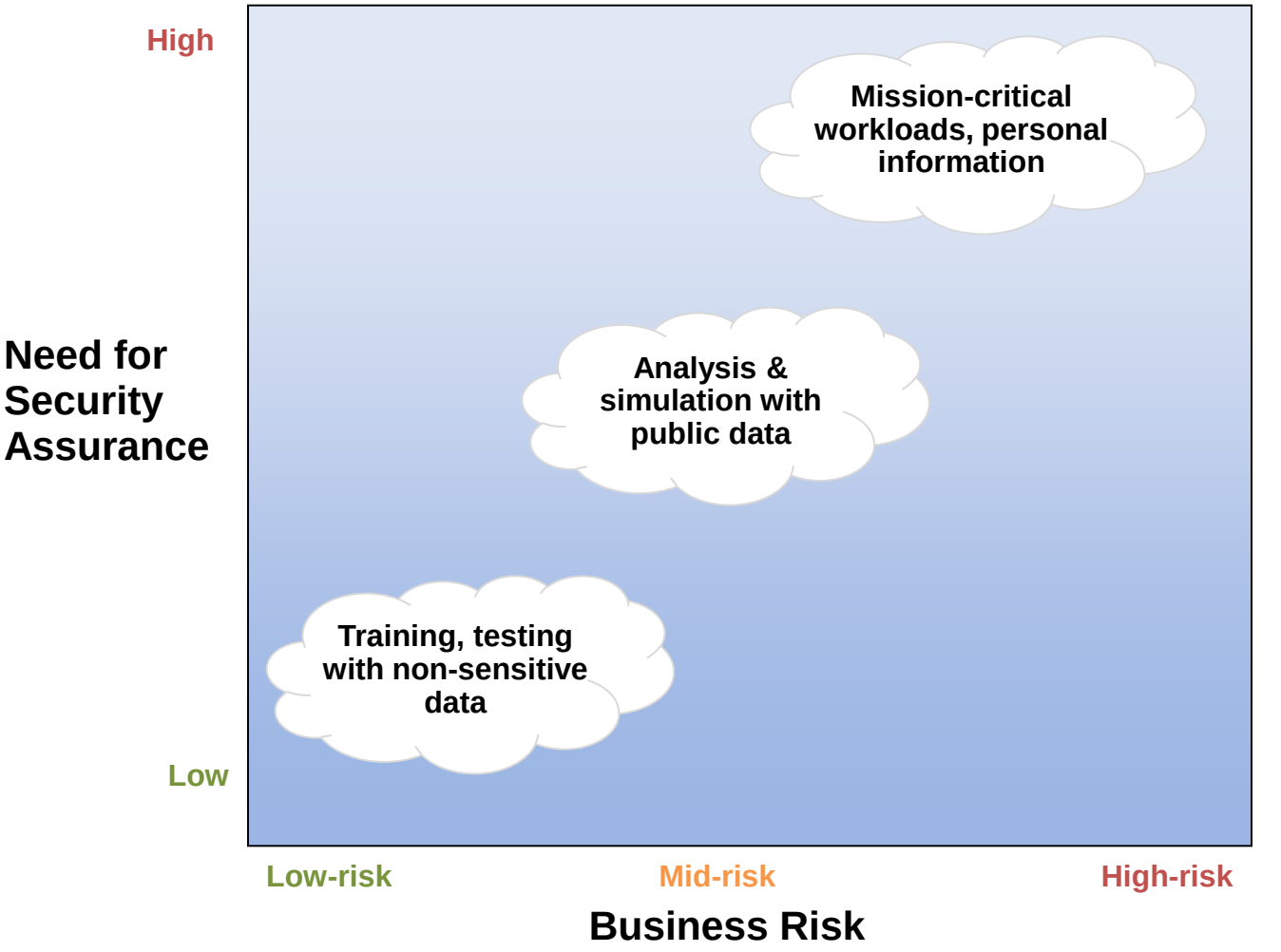
Who Has Control?	**How would we be harmed if…**
Where is it located?	an employee of our cloud provider accessed the asset?
Where is it stored?	the asset became widely public and widely distributed?
Who backs it up?	the process or function were manipulated by an outsider?
Who has access?	the process or 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



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



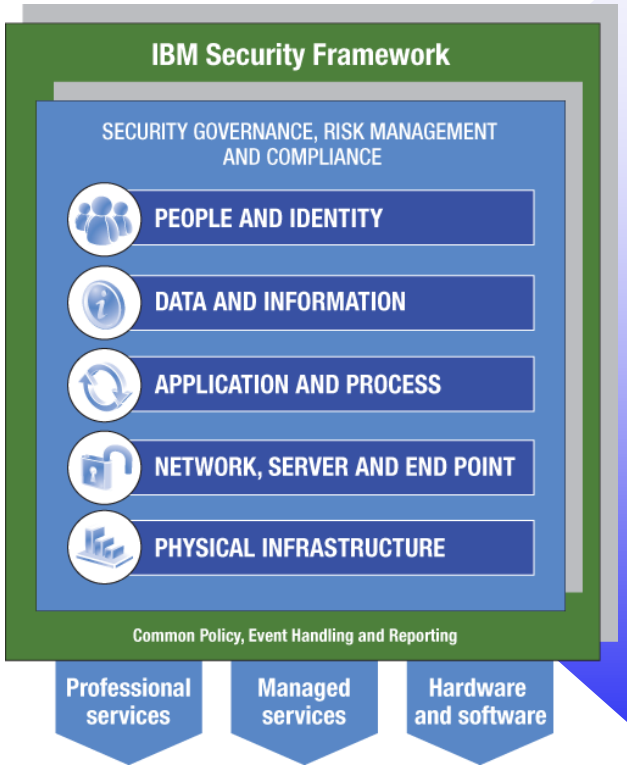
Tomorrow's high value / high risk workloads need:

- 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



- ***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***

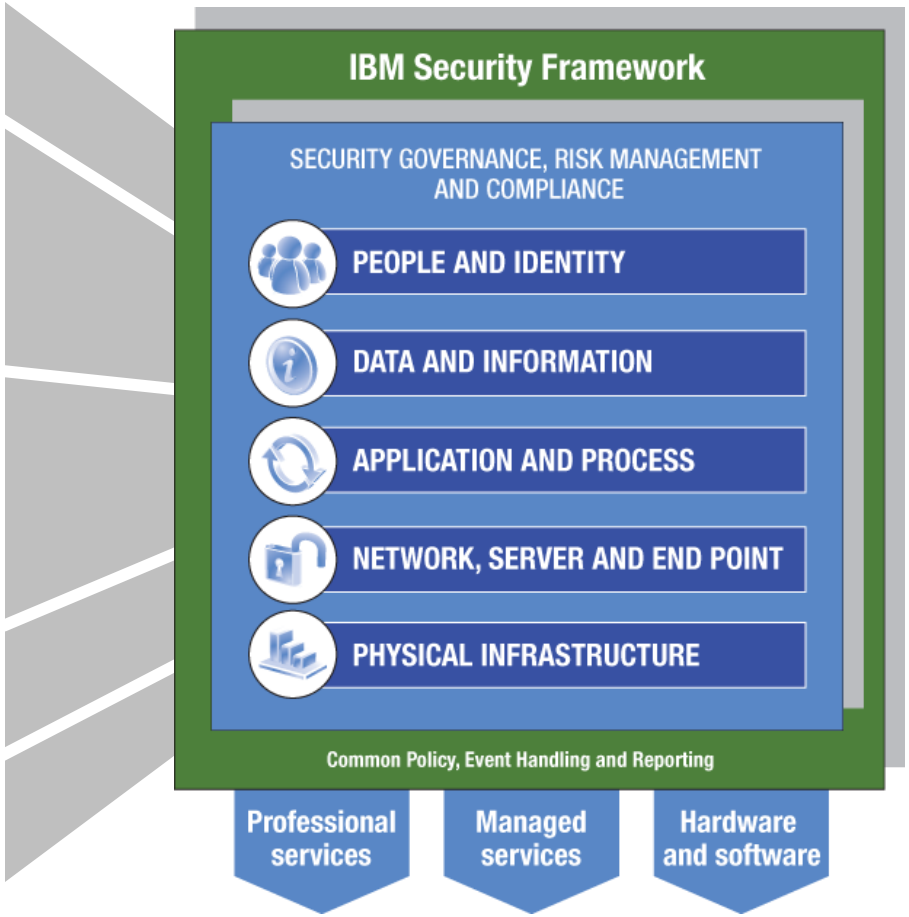
Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security;

IBM RedGuide REDP-4528-00, July 2009

Gartner的报告正好反应了安全的五大类考量

…that map directly to the IBM Security Framework.

- **Privileged User Access**
- **Data Segregation**
- **Data Recovery**
- **Investigative Support**
- **Regulatory Compliance**
- **Data Location**
- **Disaster Recovery**



Gartner: Assessing the Security Risks of Cloud Computing, June 2008

再细分看有多样解决之道

= 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

Data Masking

Database Monitoring and Protection

SIEM and Log Mgmt

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

Physical Security Services

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.

Edit Vi

Back

ess htt

Go Link

ogle Search Bookmarks Find Check AutoFill Sign In

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

Enter your username
and password to Sign In

Username:

Password:

Sign In

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

NOTICE: 2008 MSS Billing Changes

Virtual Security Operations Center

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

ERNST & YOUNG LLP

2005 FROST & SULLIVAN Customer Service Innovation Award

one

Local intranet

VSOC portal demo

Vulnerability Manager

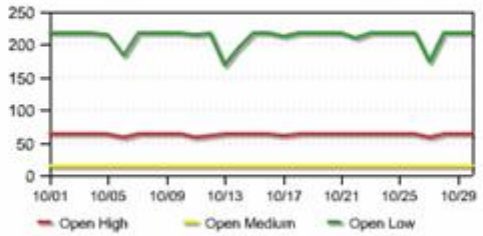
Portal User [LOGOUT]
Last Login: Oct 30, 2007 22:04 GMT

Vulnerabilities Breakdown

View all vulns »

Vulnerability Trend by Severity

View all vulns »



Active Vulnerabilities

View all vulns »

Severity	Count
High	56
Medium	14
Low	219
Total	289

Remediation Status

View tickets »

» Create a new subordinate user

Subordinate	Assets	Tickets
Al Hutcherson	10	28
Alden Hutchison	6	25
Alestra	3	22
Tom Wallace	8	20
Sneha Gokal	2	18

Results for Recently Completed Scans

View schedules »

Of your 25 active scan schedules, 0 are currently running and 2 have errors.

» Create a new scan schedule *(76,868 external IPs left)*

Start Time	Schedule Name	Scan Type	Interval	Assets	Vulnerabilities
10/31/07 01:01	Tuesday Scan	External	Weekly	239	27
10/30/07 15:01	Chris Schedule Weekly	External	Weekly	1	0
10/30/07 12:01	Chris Scan	External	Weekly	0	0
10/30/07 01:01	Monday Scan	External	Weekly	239	27
10/29/07 03:01	Discovery2	External	Weekly	1	0
10/29/07 03:01	Sunday Scan	External	Weekly	1	0
10/29/07 01:01	Sunday Scan	External	Weekly	239	27
10/28/07 21:01	D3 Max	External	Weekly	31	0
10/28/07 20:01	D3-abort-2-weekly	External	Weekly	28	0
10/28/07 19:01	Sunday-L5	Internal	Weekly	4	30

10 Most Severe Vulns

View all vulns »

Name	Status	Severity	Risk	Ticket
Snmp Set Guessabl...			10.0	707086
SNMPv1Discovery			10.0	709779
SNMPv1Discovery			10.0	707663
SNMPv2Discovery			10.0	709784
SNMPv2Discovery			10.0	707922

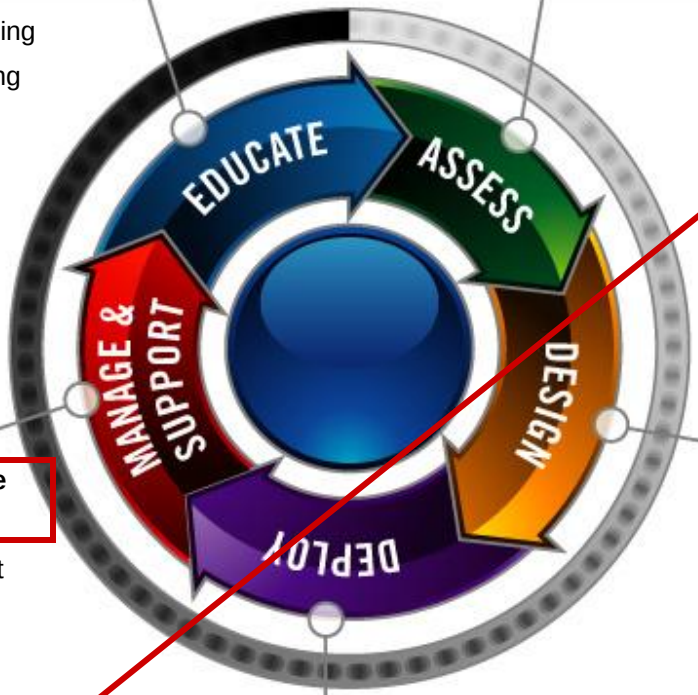
安全顾问服务

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

Phase 3. Deployment

- Deployment Services
- Migration Services

Solution Focus Areas

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

People and Identity

•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

Privileged User Access

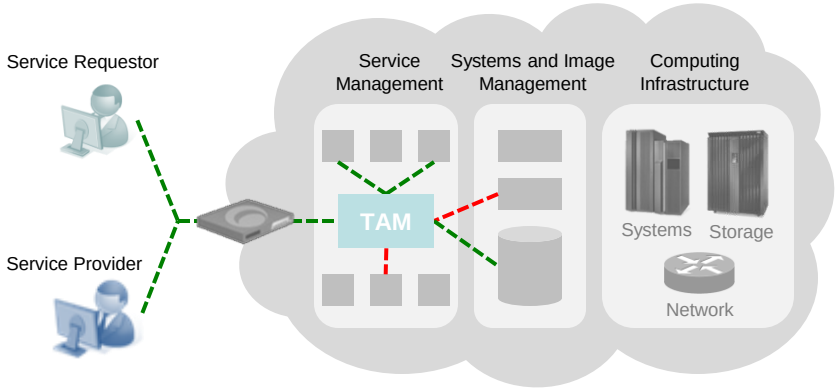
Separation of administrative and user roles in a cloud environment

Tivoli Access Manager (TAM)

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.



Cloud Identity Federation

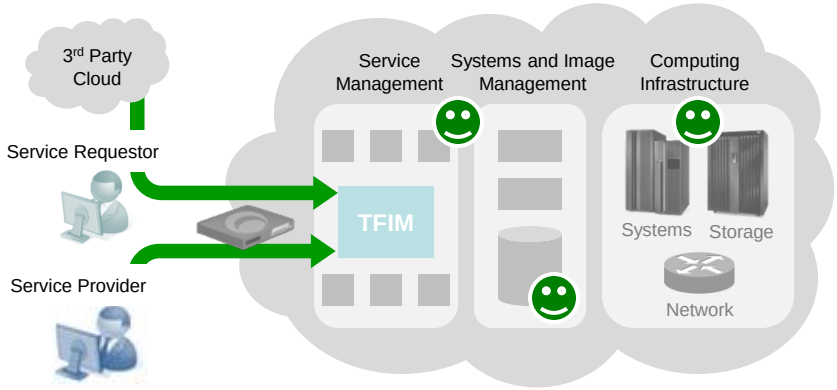
Single access method for users into cloud and traditional applications

Tivoli Federated Identity Manager (TFIM)

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.



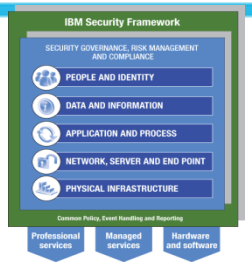
Data & Information

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

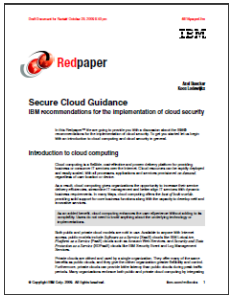
•The Key elements of IBM's strategy are:

- 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.



IBM Security Framework



IBM Cloud Security Guidance Document

IBM Security Products and Services

Data and Information

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

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 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

Application & Process

- **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

Compliance and Auditing

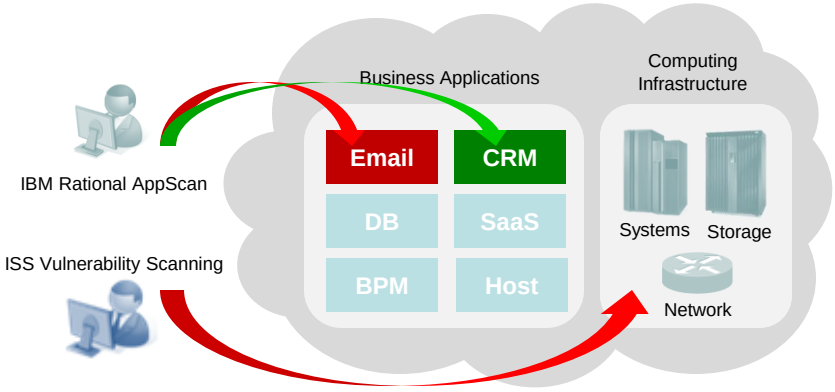
Vulnerability and compliance checking of cloud applications

IBM Rational AppScan & IBM ISS Vulnerability Assessment Services

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.



Investigative Support

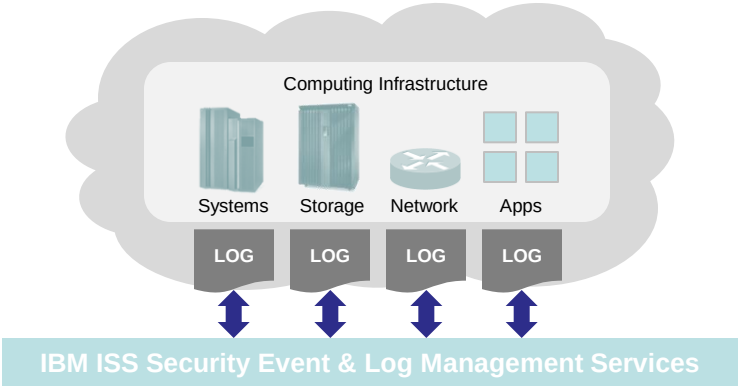
Ability to inspect and audit a cloud provider's logs and records

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

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

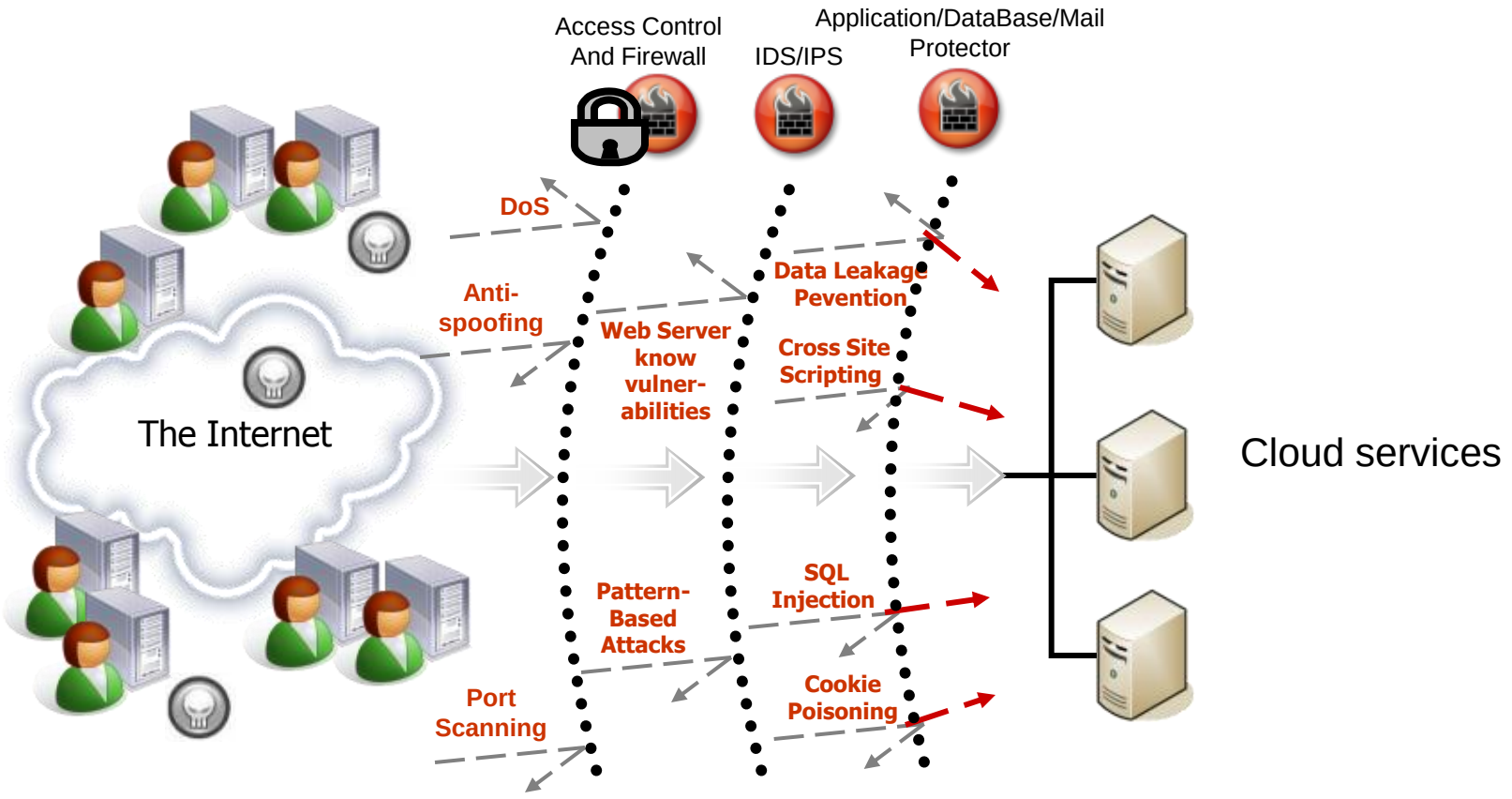


Network, Server & Endpoint

•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



Layers of a typical Cloud Service

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

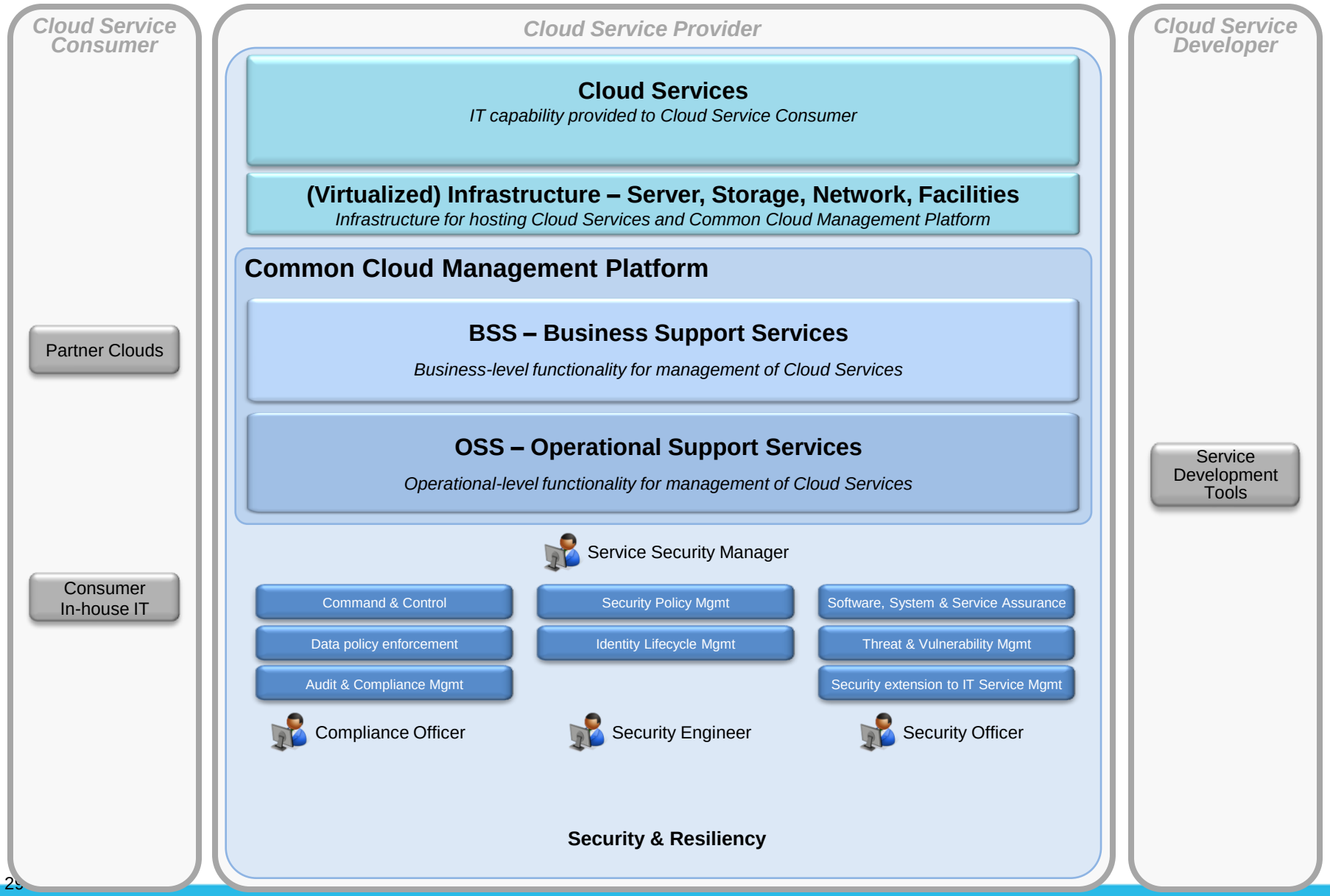
Operational Support Services
Infrastructure Provisioning
Instance, Image, Resource / Asset Mgmt

Virtualized Resources
Virtual Network, Server, Storage

System Resources
Network, Server, Storage

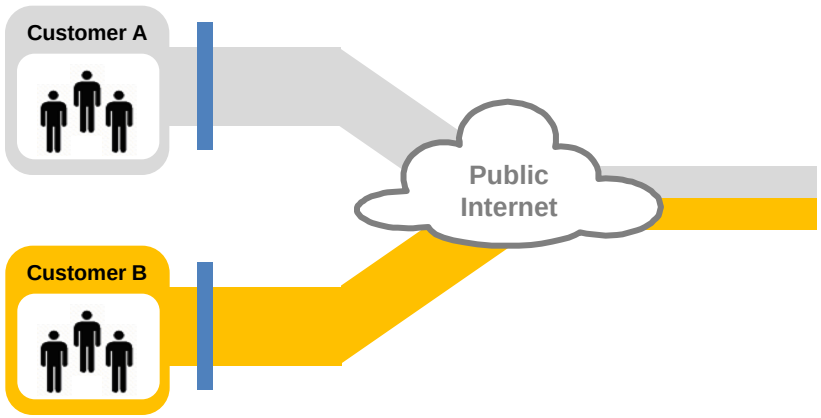
Physical System and Environment

云计算的管理平台就在论述安全的工作

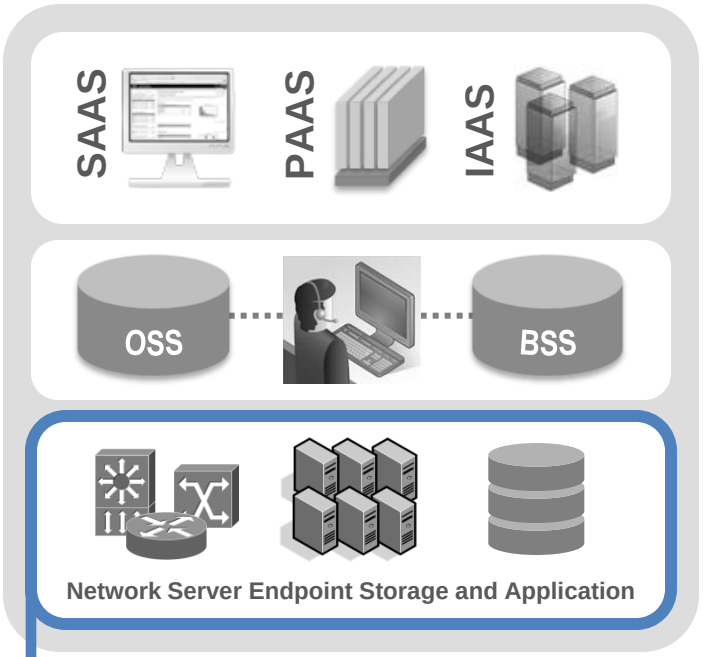


IBM Security Initiatives

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.

Virtualization Security

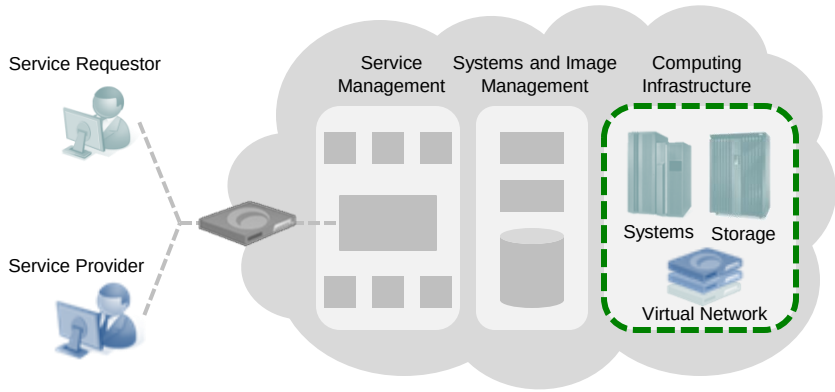
Security for pools of high performance virtualized resources

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.

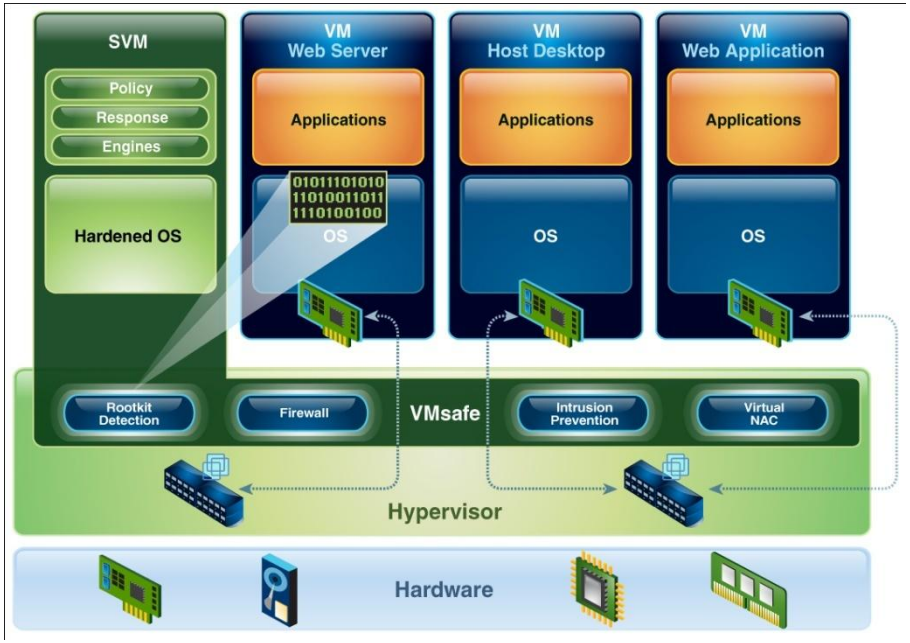
Cloud Use Case: Security of the virtualization stack that enables flexible, rapid provisioning across heterogeneous servers and hypervisors.

Deployment Scenario: In the virtual data center.



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

धन्यवाद
Hindi

多謝
Traditional Chinese

ขอบคุณ
Thai

Спасибо
Russian

Gracias
Spanish

Thank You
English

شكرا
Arabic

Obrigado
Brazilian Portuguese

감사합니다
Korean

多谢
Simplified Chinese

Danke
German

Grazie
Italian

Merci
French

நன்றி
Tamil
Tamil

ありがとうございました
Japanese