

Every System z Cloud Has An Iron Lining: *What Cloud Security Means In Mainframe Environments*

Brian W. Hugenbruch, CISSP - bwhugen@us.ibm.com -  @Bwhugen



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, IBM Systems, IBM System z10®, IBM System Storage®, IBM System Storage DS®, IBM BladeCenter®, IBM System z®, IBM System p®, IBM System i®, IBM System x®, IBM IntelliStation®, IBM Power Architecture®, IBM SureOne®, IBM Power Systems™, POWER®, POWER6®, POWER7®, POWER8®, Power®, IBM z/OS®, IBM AIX®, IBM i, IBM z/VSE®, IBM z/VM®, IBM i5/OS®, IBM zEnterprise®, Smarter Planet™, Storwize®, XIV®, PureSystems™, PureFlex™, PureApplication™, IBM Flex System™, Smarter Storage

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

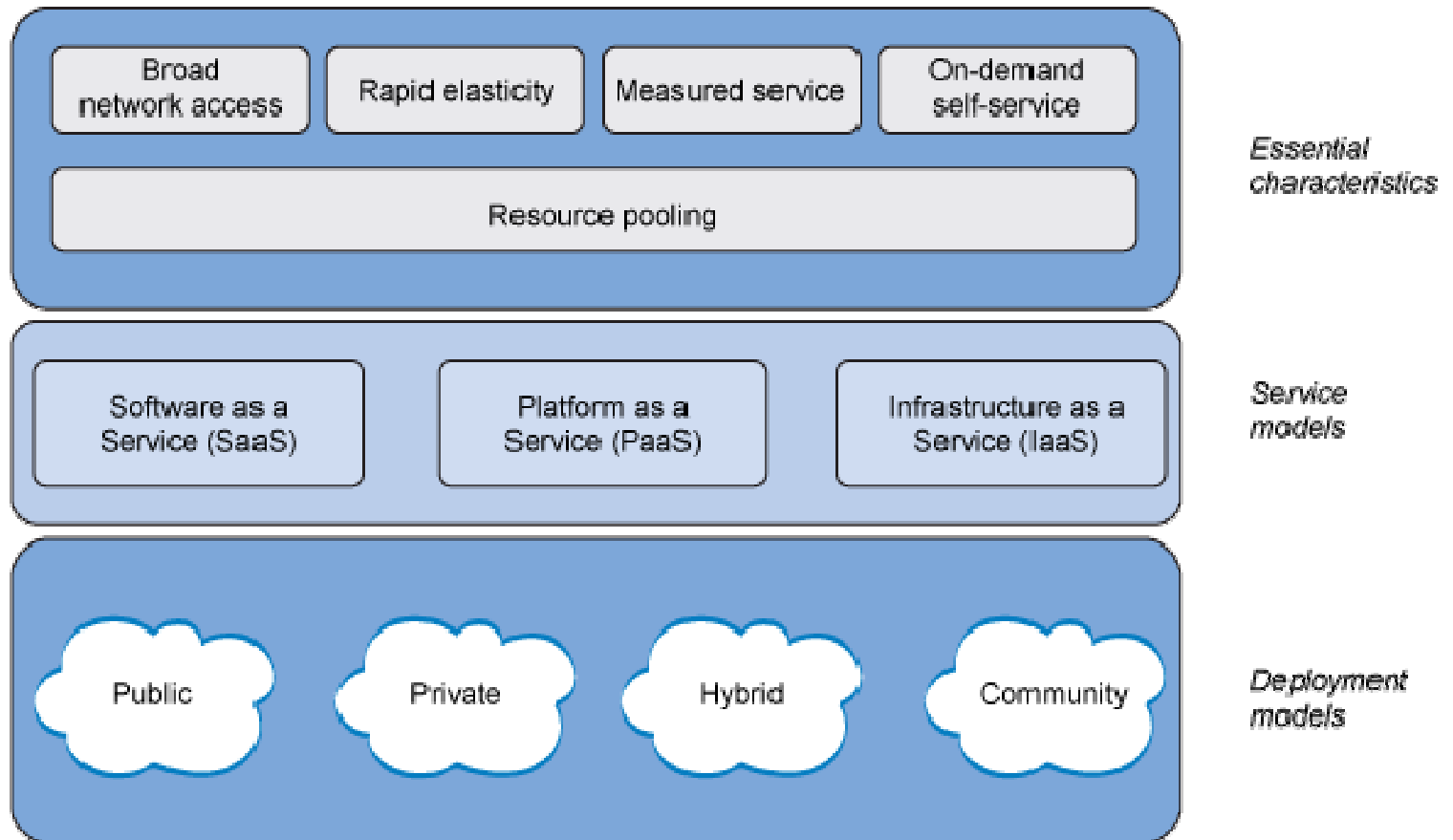
Agenda

- **What is a Cloud Environment?**
- **What is Cloud Security?**
 - The cloud and its predators in their natural habitat
 - Incident Response
 - Identity Management
 - Security-as-a-Service
 - Cloud security considerations
- **How does Security function in (and "under") a System z Private Cloud?**
- **Summary, Questions, and References**

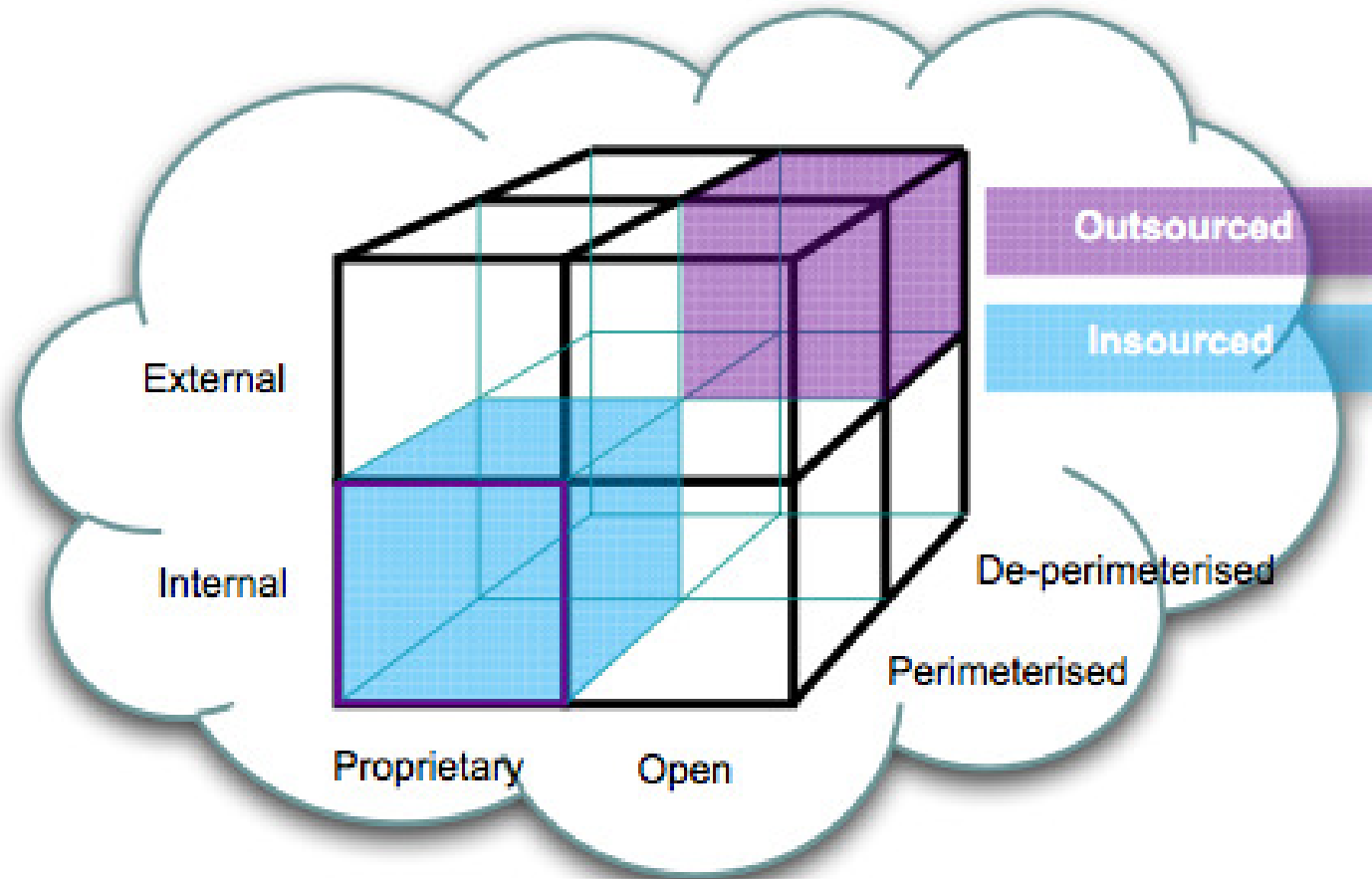
What is a Cloud Environment?

"Clouds come floating into my life,
no longer to carry rain or usher storm,
but to add color to my sunset sky."

- Rabindranath Tagore, *Stray Birds*, Verse 292 (1916)

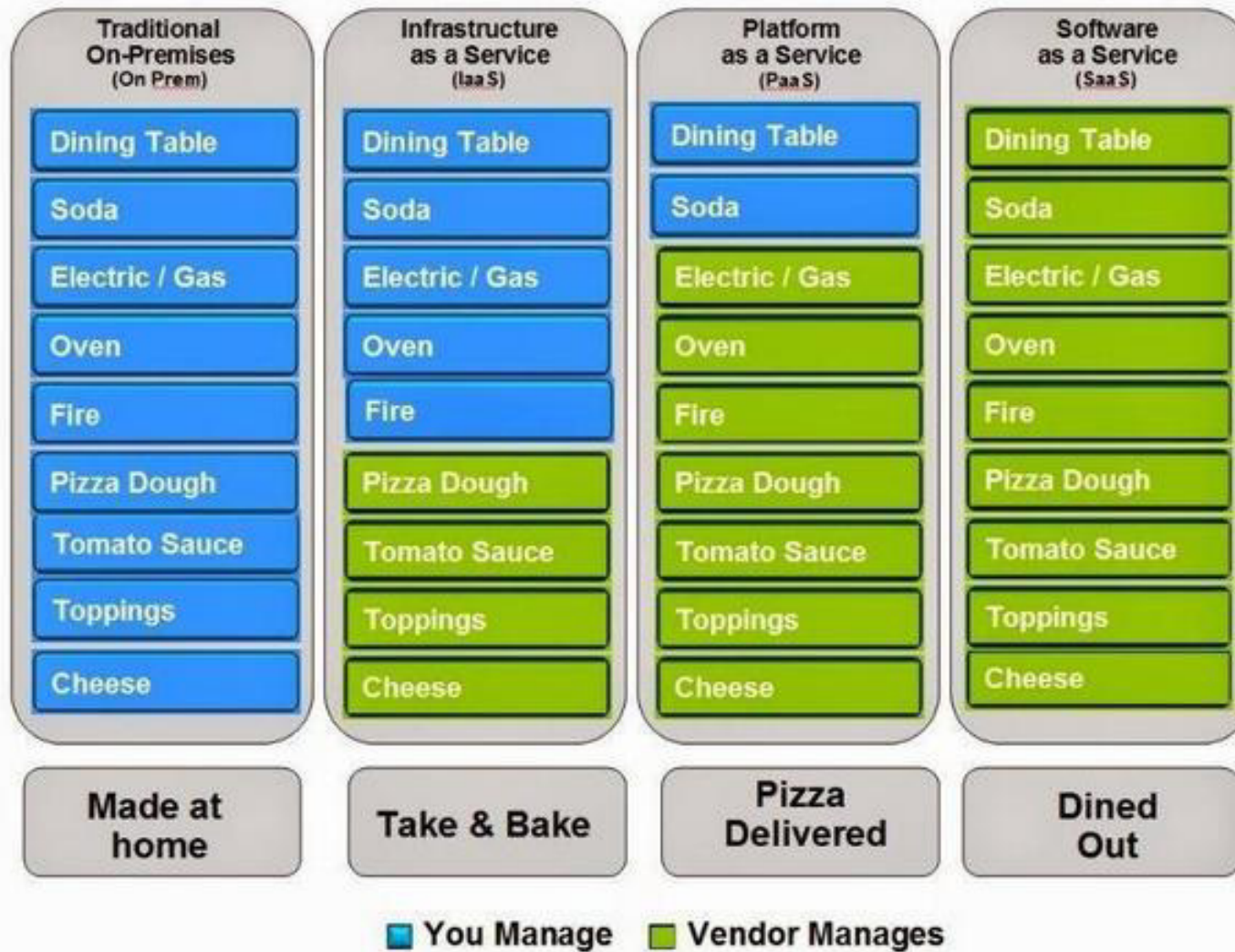


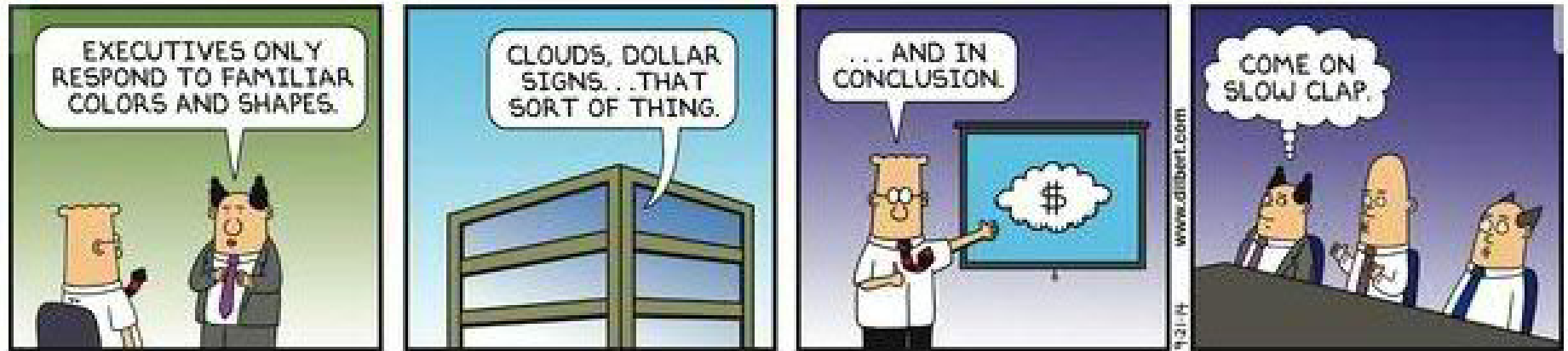
"The NIST Definition of Cloud Computing" (NIST SP 800-145)



The Cloud Cube Model

Pizza as a Service

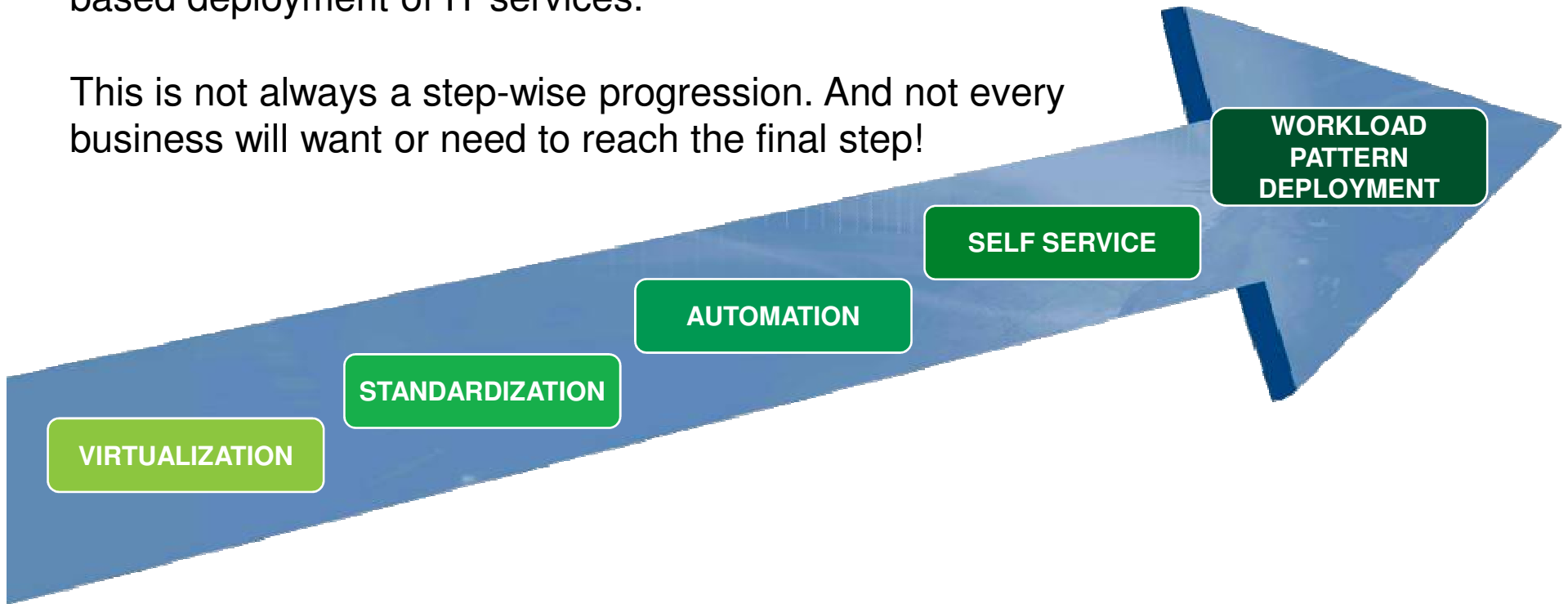





Cloud is not a technology. Instead, it is a way of positioning resources to exploit services at scale.

We first need to first understand that **Cloud is a journey** - beginning with virtualization and consolidation of environments and ending with workload pattern-based deployment of IT services.

This is not always a step-wise progression. And not every business will want or need to reach the final step!



... so what sort of cloud should we build today?

Build it. 
Build and run your private or hybrid cloud.

What's the best infrastructure for my cloud?

How do I maintain choice and flexibility?

How do I rapidly deploy & operate my cloud?

How do I manage my hybrid environment?

There are **opportunities** which come with a **private** cloud.

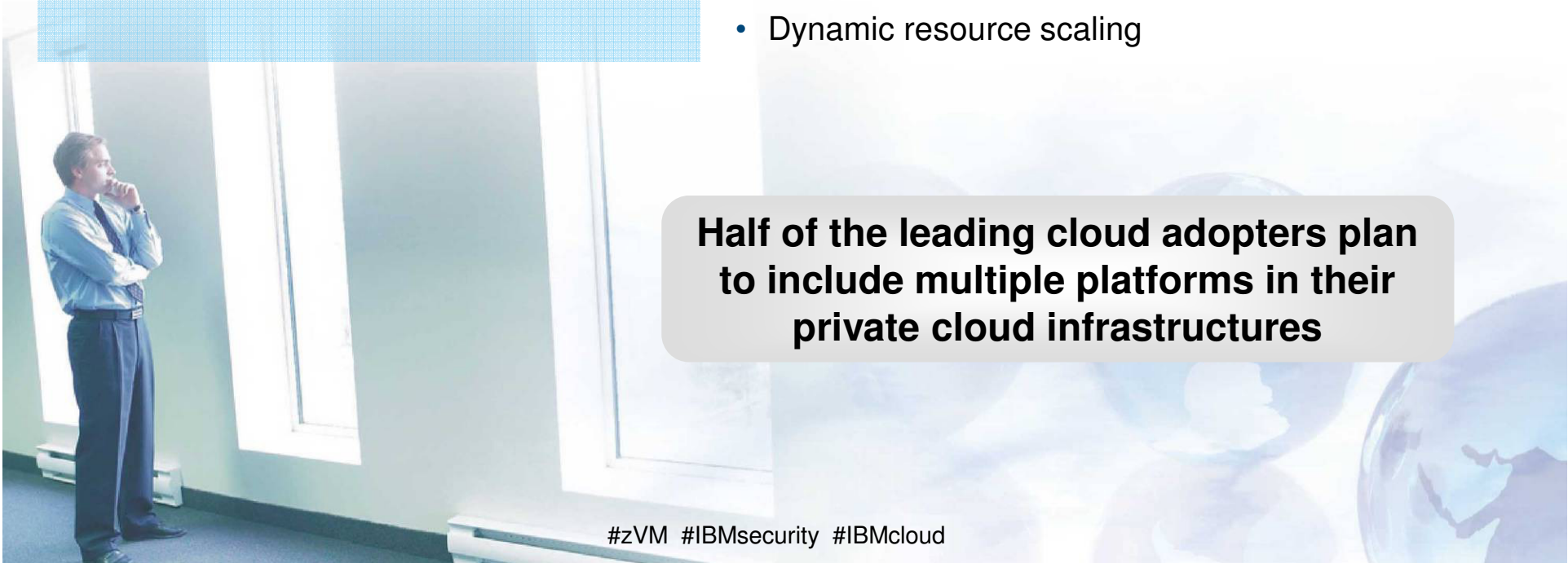
Clients are looking for benefits from private clouds

- Higher availability of systems and applications
- Lower total costs and better utilization of hardware
- Labor savings and improved quality of IT services
- Secure start behind enterprise firewall

And are preparing infrastructure to build the foundation

- Highly virtualized infrastructure
- Standardized virtual workloads
- Web-based provisioning
- Dynamic resource scaling

Half of the leading cloud adopters plan to include multiple platforms in their private cloud infrastructures



IBM Cloud: Think it. Build it. Tap into it.



IBM Enterprise Cloud System

Trusted Cloud. Simply Delivered.



Open Linux Environment

- Red Hat/SUSE
- 3000+ Applications



Fully Automated Cloud Orchestration & Monitoring



openstack

Hypervisor and Virtualization Management



Utility Pricing and MSP Flexible Financing

Trusted, 24/7 IBM Support



Award Winning Hardware Design



- Integrated
- Delivered in 30-45 Days
- Production Ready in Hours

- 99.99%+ Availability
- EAL4 Server Security
- Available June 20, 2014

... but how do you secure one of these things, anyway?



What is Cloud Security?

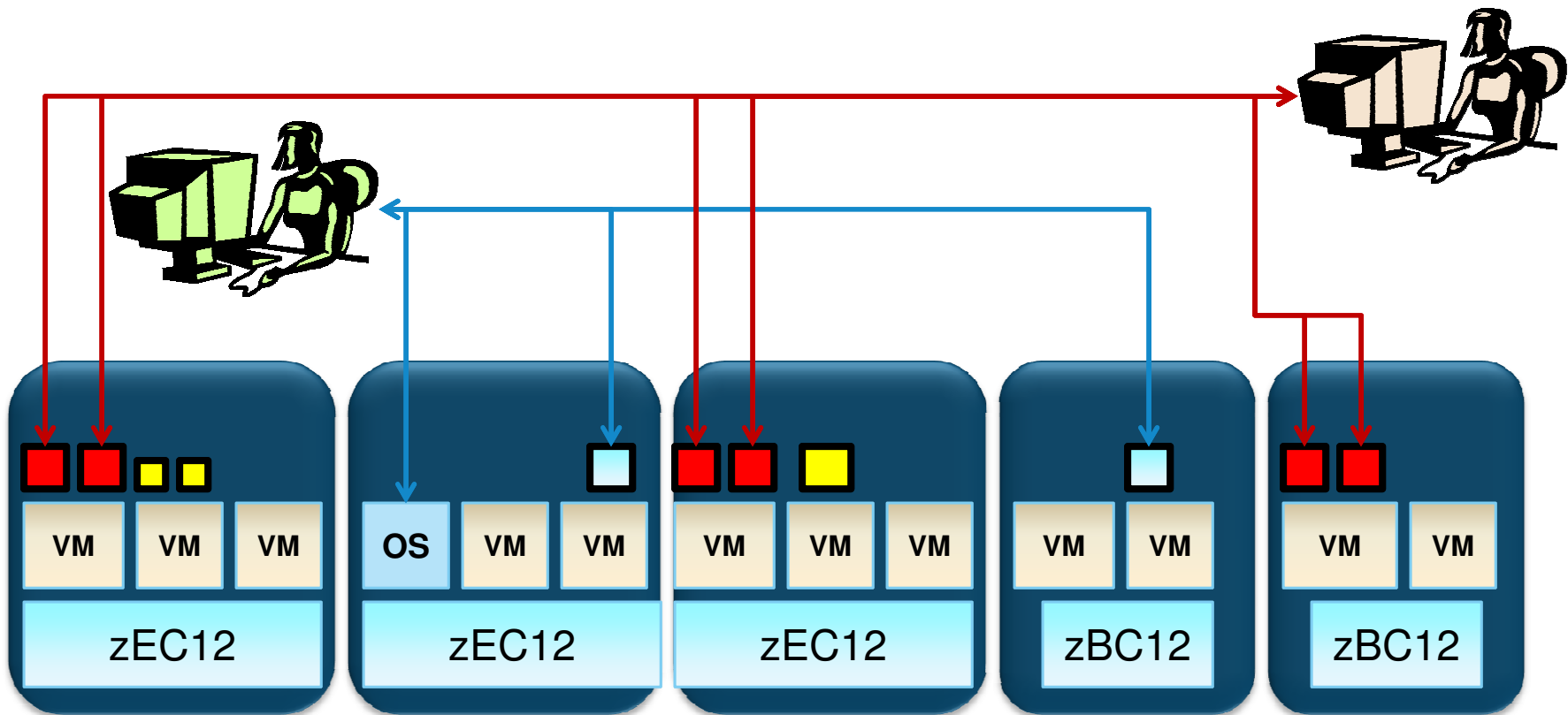
“And you all know, Security
Is Mortals' chiefest Enemy.”

-- Shakespeare, *Macbeth*, Act III, Scene 5 (1623)



What is cloud security?

- If a *cloud* is an information system infrastructure with the capacity to provide rapid scaling, self-service provisioning, and pooled resources ... then **Security** in the cloud means securing that **infrastructure** ... and their **services**



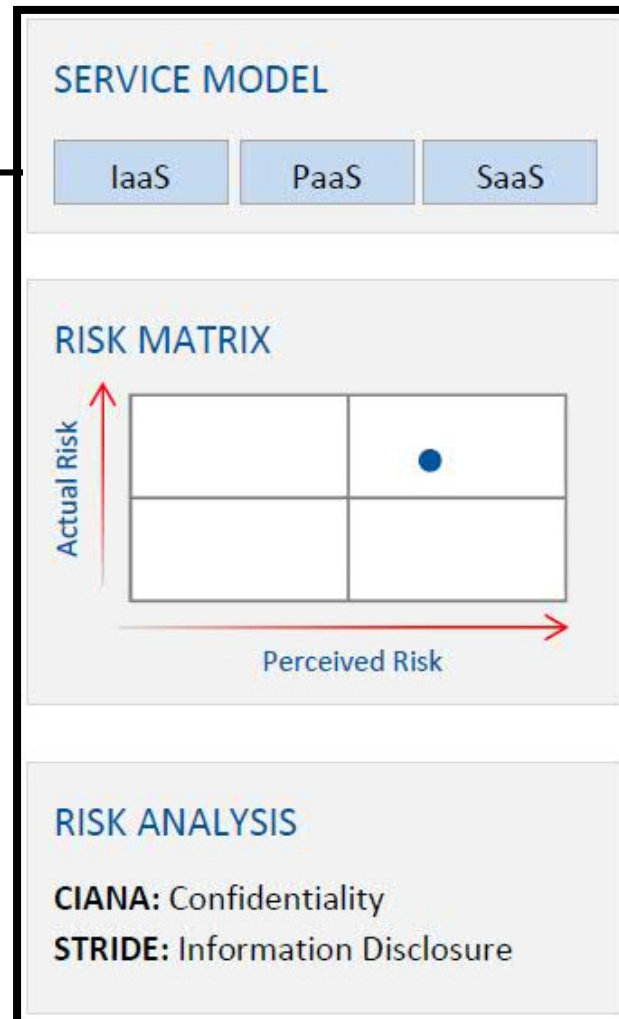
A best practices approach to security intelligence, auditing and compliance management



The "Notorious Nine" Threats to Cloud Environments

(Cloud Security Alliance, as of 2013)

1. **Data Breaches**
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse and Nefarious Use
8. Insufficient Due Diligence
9. Shared Technology Issues



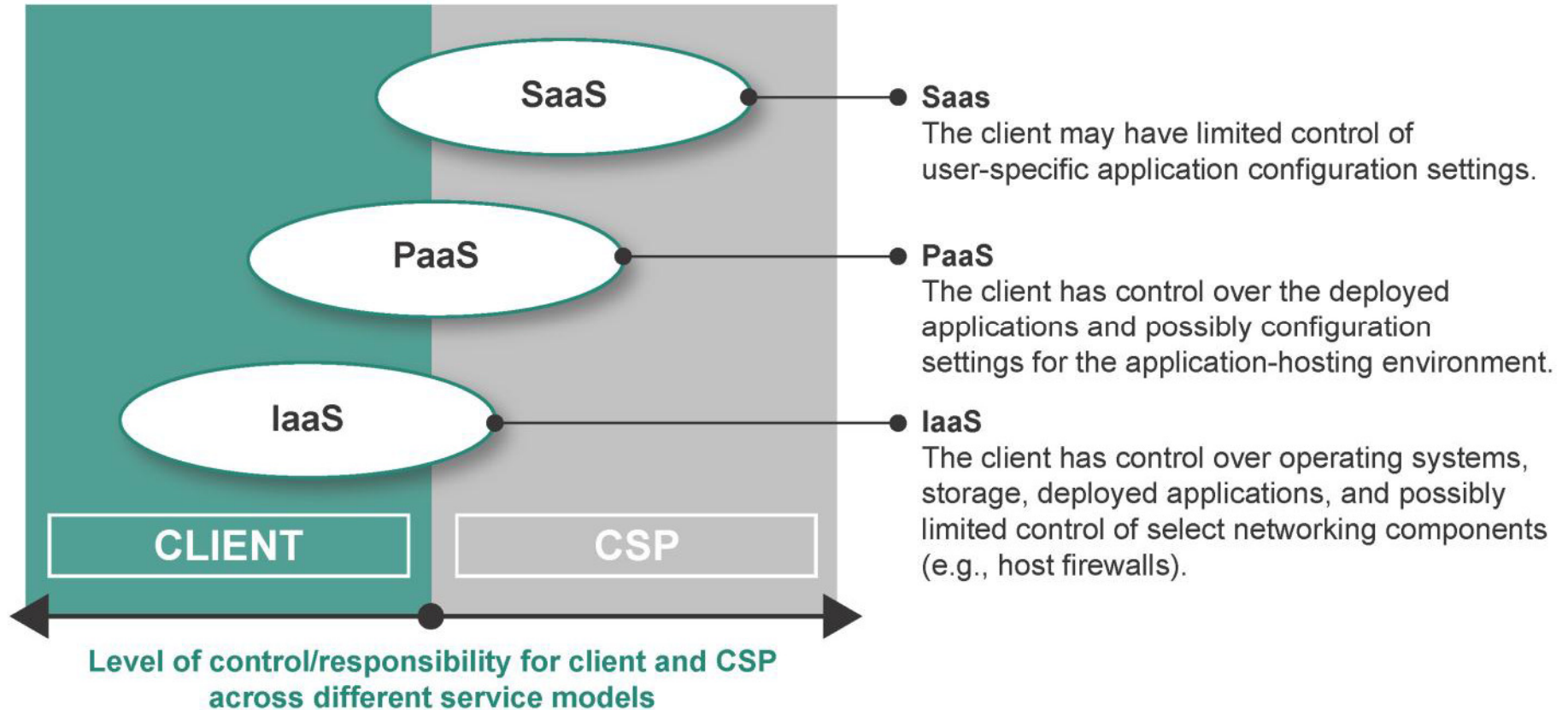
Risks in a Cloud Environment

(List condensed from Payment Card Industry Data Security Standard (PCI DSS v2))

1. How do we restore or recover it in an emergency?
2. Where does the data actually reside?
 - Are there backups elsewhere in the cloud?
 - Is there a lifecycle plan?
 - How is data classified when in the cloud?
 - How is data encryption and key management handled?
 - How do we "decommission" a cloud at the end of its lifecycle?
3. How is Identity management handled in the cloud context?
 - Administrator authorization is not Cloud end-user authorization
 - End-user authorization is not virtual machine / workload authorization
 - Workload authorization better not be administrator authorization
4. Are the cloud interfaces secure, controlled, and audited?
5. Has multi-tenancy been established in this cloud deployment?
6. **Who owns the data, really?**



"But whose fault is it?"

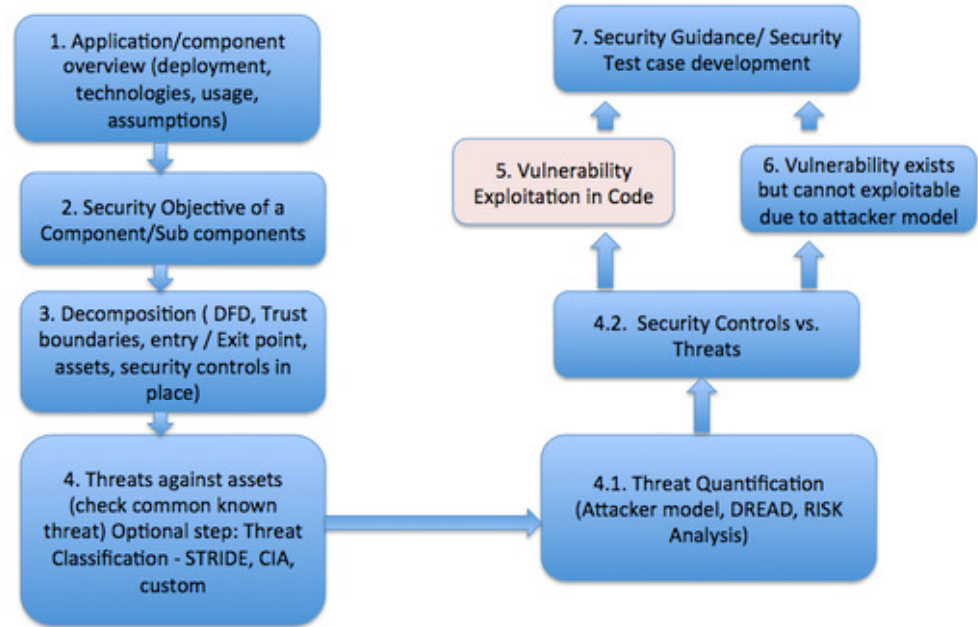


"But whose fault is it?"

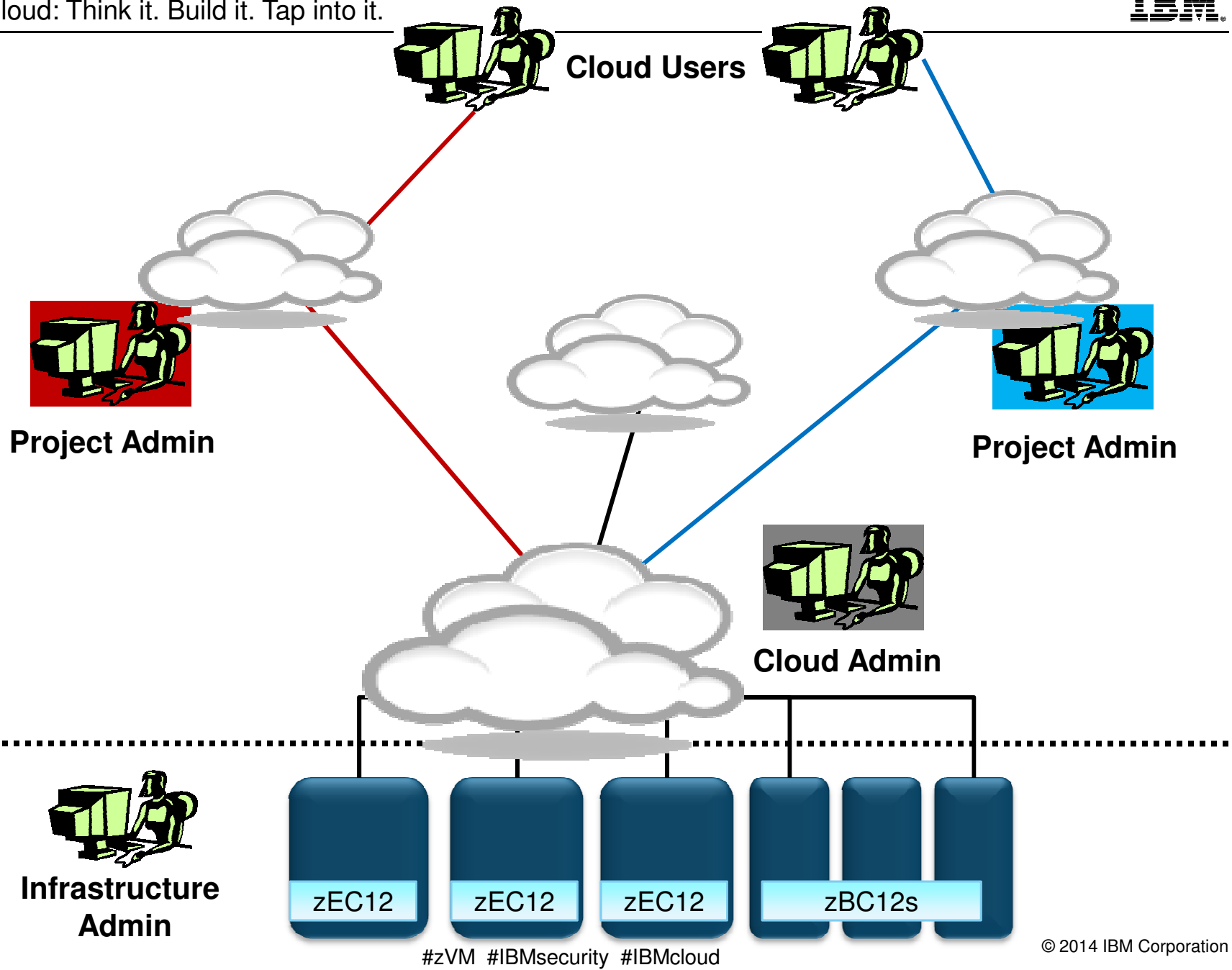
PCI DSS Requirement	Example responsibility assignment for management of controls		
	IaaS	PaaS	SaaS
1: <i>Install and maintain a firewall configuration to protect cardholder data</i>	Both	Both	CSP
2: <i>Do not use vendor-supplied defaults for system passwords and other security parameters</i>	Both	Both	CSP
3: <i>Protect stored cardholder data</i>	Both	Both	CSP
4: <i>Encrypt transmission of cardholder data across open, public networks</i>	Client	Both	CSP
5: <i>Use and regularly update anti-virus software or programs</i>	Client	Both	CSP
6: <i>Develop and maintain secure systems and applications</i>	Both	Both	Both
7: <i>Restrict access to cardholder data by business need to know</i>	Both	Both	Both
8: <i>Assign a unique ID to each person with computer access</i>	Both	Both	Both
9: <i>Restrict physical access to cardholder data</i>	CSP	CSP	CSP
10: <i>Track and monitor all access to network resources and cardholder data</i>	Both	Both	CSP
11: <i>Regularly test security systems and processes</i>	Both	Both	CSP
12: <i>Maintain a policy that addresses information security for all personnel</i>	Both	Both	Both
<i>PCI DSS Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers</i>	CSP	CSP	CSP

Incidence Response and Threat Analysis

- Where did you store your **Incidence Response Plan**?
- Are you (provider or consumer) logging your operations?
- Are you meeting legal requirements?
- Are the logs tamper resistant?
- Can you detect cloud-layer threats?
- Is cloud infrastructure isolated from cloud users?
- Can you find / isolate the infected component?



- All of these apply to modern Enterprise environments, *regardless* of Cloud usage.
- **Remember**: the consumer / provider model complicates the notion of "collecting audit logs"



Security-as-a-Service

- **Security-as-a-Service** is another way of looking at security
 - Rather than focusing on maintaining traditional security when moving to a cloud environment ...
 - SecaaS focus on securing both cloud and traditional workloads via cloud-based services
- But there are **a lot of things** which can be classified as SecaaS:
 - Identity Services
 - Data Loss Prevention
 - Web Security
 - Email Security
 - Intrusion Management, Detection, Prevention ...
 - Security Information and Event Management (SIEMaaS)
 - Encryption (Crypto-as-a-Service)
 - Business Continuity and DR (DRaaS?)
 - Network Security
 -

What are the security *considerations* inherent in a cloud environment?

From NIST SP 800-144: "Guidelines on Security and Privacy in Public Cloud Computing"

Governance and Compliance	Laws and Regulations, Data Location, Electronic Delivery
Trust	Insider Access, Data Ownership, Composite Services, Visibility, Ancillary Data, Risk Management
Architecture	Attack Surface, Virtual Network Protection, Virtual Machine Images, Client-Side Protection
Identity and Access Management	Authentication, Access Control
Software Isolation	Hypervisor Complexity, Attack Vectors
Data Protection	Value Concentration, Data Isolation, Data Sanitization
Availability	Temporary Outages, Prolonged/Permanent Outages, Denial of Service
Incident Response	Data Availability, Incident Analysis and Resolution

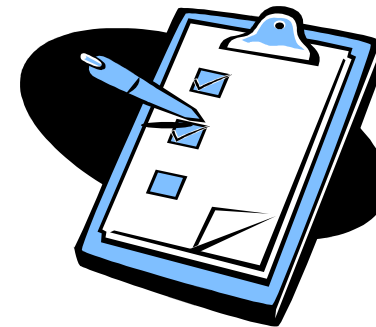
What are the security *recommendations* for a cloud environment?

From NIST SP 800-144: "Guidelines on Security and Privacy in Public Cloud Computing"

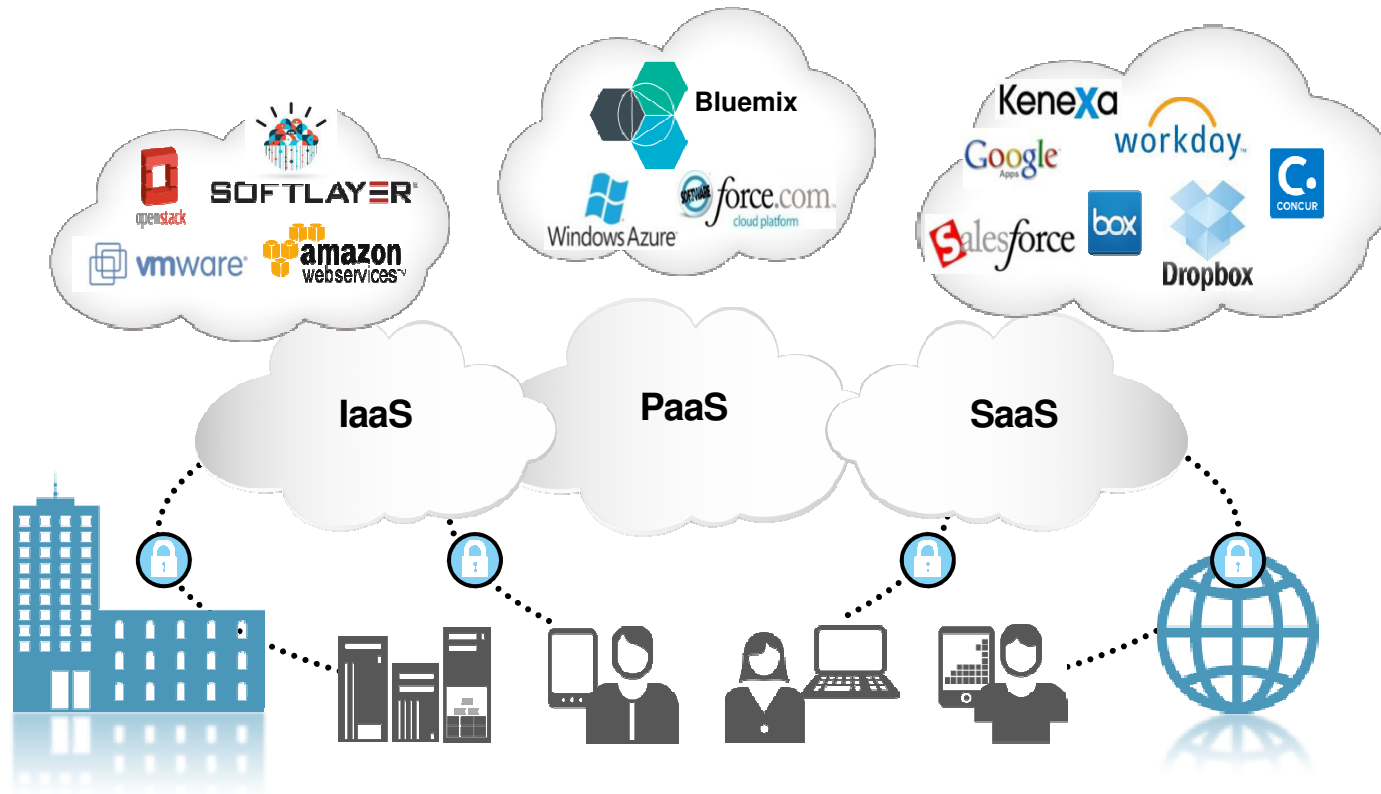
Governance	Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
IdEA Mgmt	Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstated in a timely and organized manner.
Incident Response	Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Cloud Security Alliance (CSA) STAR Self-Assessment (Security, Trust & Assurance Registry)

- 140 question checklist for cloud providers (be they public, hybrid, or **private**)
 - Some are technical; some correspond to business continuity, DR, software lifecycle ...
 - Questions are all mapped to NIST SP 800-53, PCI DSS v2, PCI DSS v3 ...
- Questions correspond to CSA's Cloud 13 Security Domains of Cloud Knowledge
 - Available as a spreadsheet for analysis over time, tracking exceptions
 - A lot of public and hybrid cloud providers (e.g., Softlayer) have completed these assessments for cloud security assurance purposes
- <https://cloudsecurityalliance.org/star/self-assessment/>



Yours or theirs ... know your Cloud and know your Data.



How does Security Function in (and under) a System z Private Cloud?

"If you have built castles in the air,
your work need not be lost;
that is where they should be.
Now put the foundations under them."

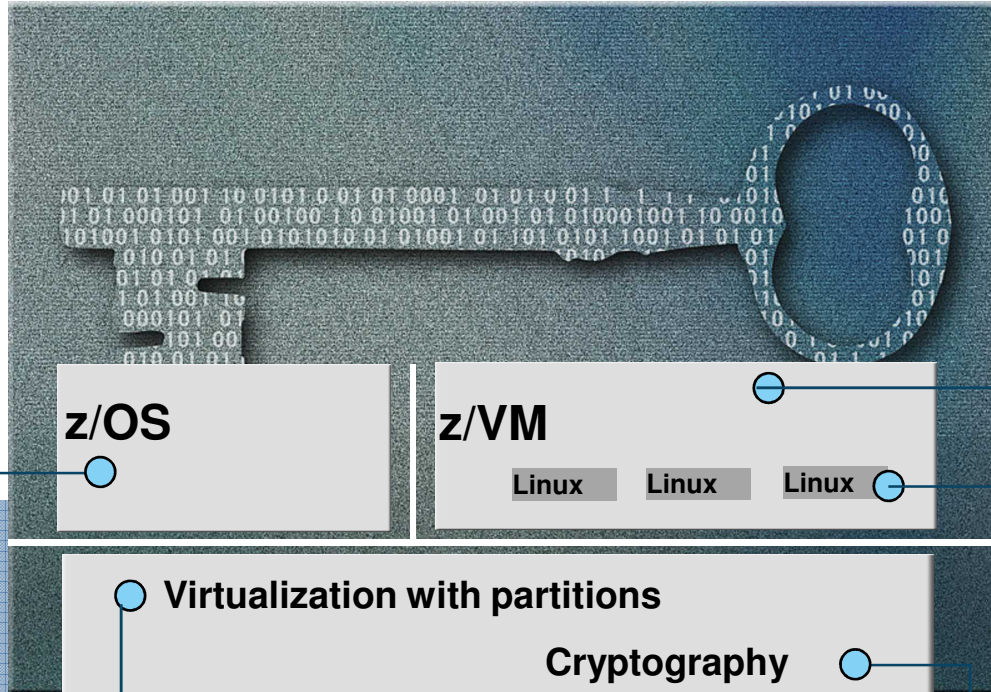
-- Henry David Thoreau, *Walden* (1854)

This button looks like it'll do the trick.



System z Security Certifications

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/OS

- Common Criteria EAL4+
 - z/OS 1.12 , z/OS 1.13 (OSPP)
- Common Criteria EAL5+
 - RACF V1R12 (OSPP)
 - RACF V1R13 (OSPP)
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
- FIPS 140-2
 - System SSL z/OS 1.13
 - z/OS ICSF PKCS#11 Services – z/OS 1.13
- Statement of Integrity

z/VM

- Common Criteria EAL 4+
 - z/VM 6.1 + RACFVM: OSPP with –LS and –VIRT
 - z/VM 6.3 + RACFVM in process
- FIPS 140-2 Level 1
 - z/VM 6.1 System SSL
 - z/VM 6.3 System SSL
- System Integrity Statement

Linux on System z

- Common Criteria
 - SUSE SLES11 SP2 certified at EAL4+ with OSPP
 - Red Hat EL6.2 EAL4+ with CAPP and LSPP
- OpenSSL - FIPS 140-2 Level 1 Validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

Virtualization with partitions

Cryptography

- zEnterprise 196 & zEnterprise 114
 - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
- System zEC12 & BC12
 - Common Criteria EAL5+ with specific target of evaluation -- LPAR: Logical partitions
- Crypto Express2 Coprocessor, Crypto Express3 & Crypto Express4s
 - FIPS 140-2 level 4 Hardware Evaluation
 - Approved by German ZKA
- CP Assist
 - FIPS 197 (AES)
 - FIPS 46-3 (TDES)
 - FIPS 180-3 (Secure Hash)

Enterprise Cloud System - Offering Components

(Now with Security automatically included)

▪ Server:

- IBM zEnterprise® EC12 or IBM zEnterprise BC12 (zEC12, zBC12)

▪ Storage:

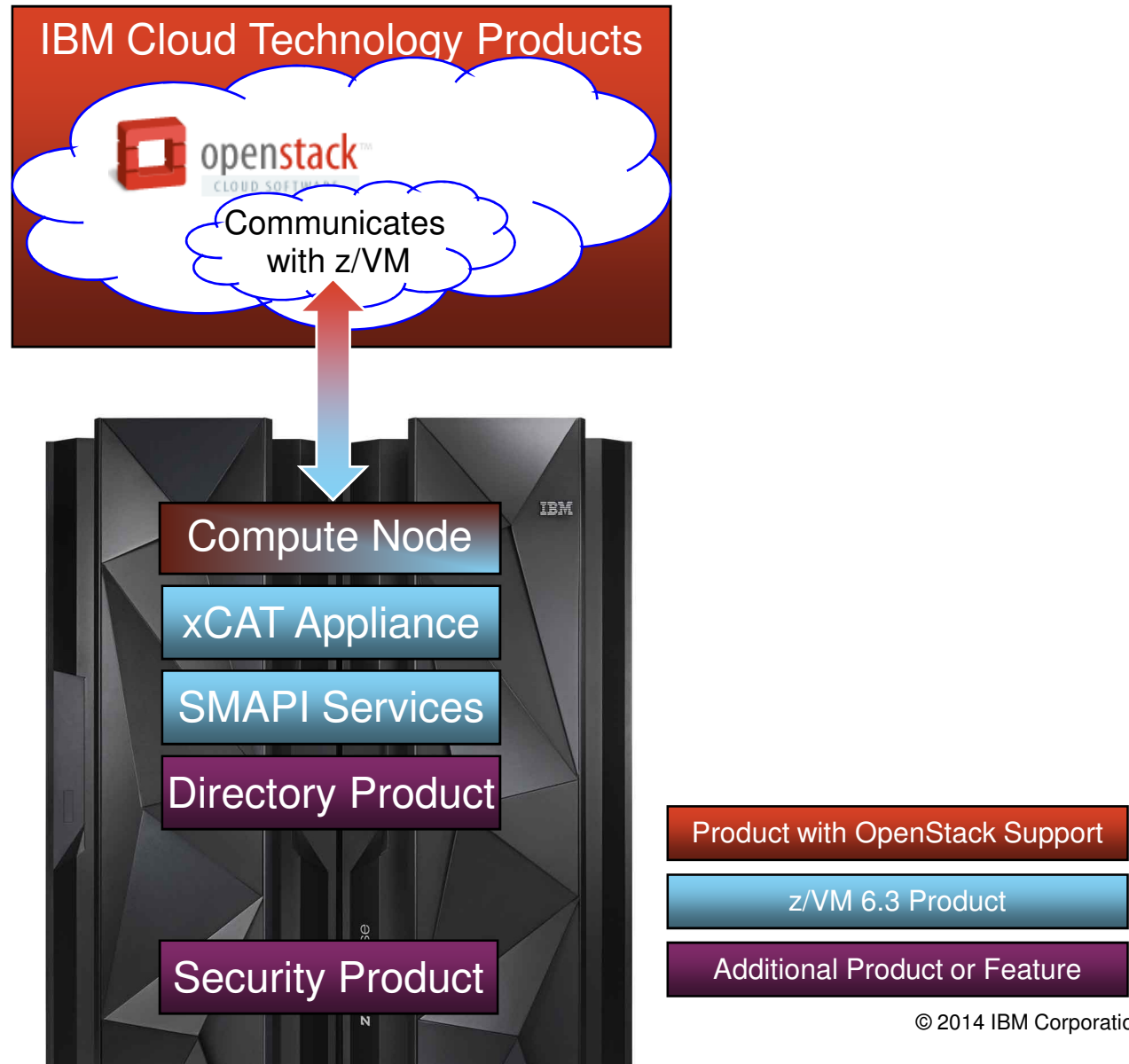
- IBM DS8870 or Storwize® V7000

▪ Software:

- z/VM® 6.3 with following features:
 - **Directory Maintenance (DirMaint™) Feature**
 - **Resource Access Control Facility (RACF®)**
 - Performance Toolkit for VM™ Feature
 - **Single System Image (SSI) Feature**
- IBM Wave for z/VM
- Cloud Management Suite:
 - OMEGAMON® XE on z/VM and Linux
 - Tivoli Storage Manager
 - SmartCloud Orchestrator
- Operations Manager for z/VM
- Backup and Restore Manager for z/VM



The view from 10,000 Meters ...



Cloud Management Solutions from IBM

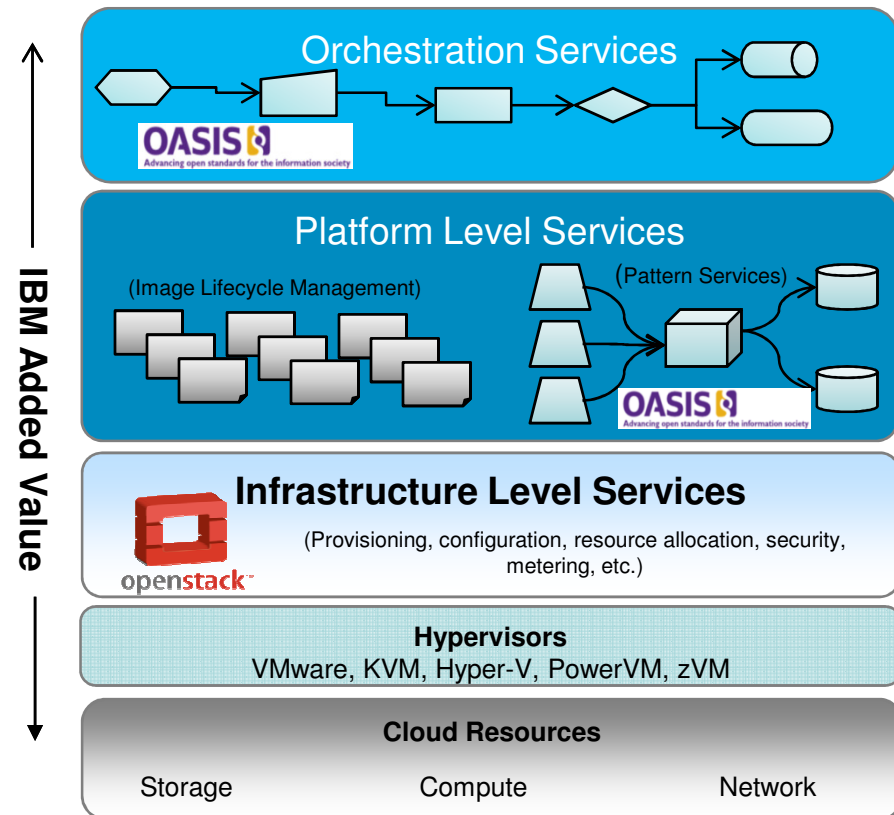
Modular Capabilities – Common Cloud Management Services

IBM Cloud Orchestrator for Infrastructure, Platform & advanced Orchestration Services

- Eases coordination of complex tasks and work-flows necessary to deploy applications
- Deploy application topologies or patterns

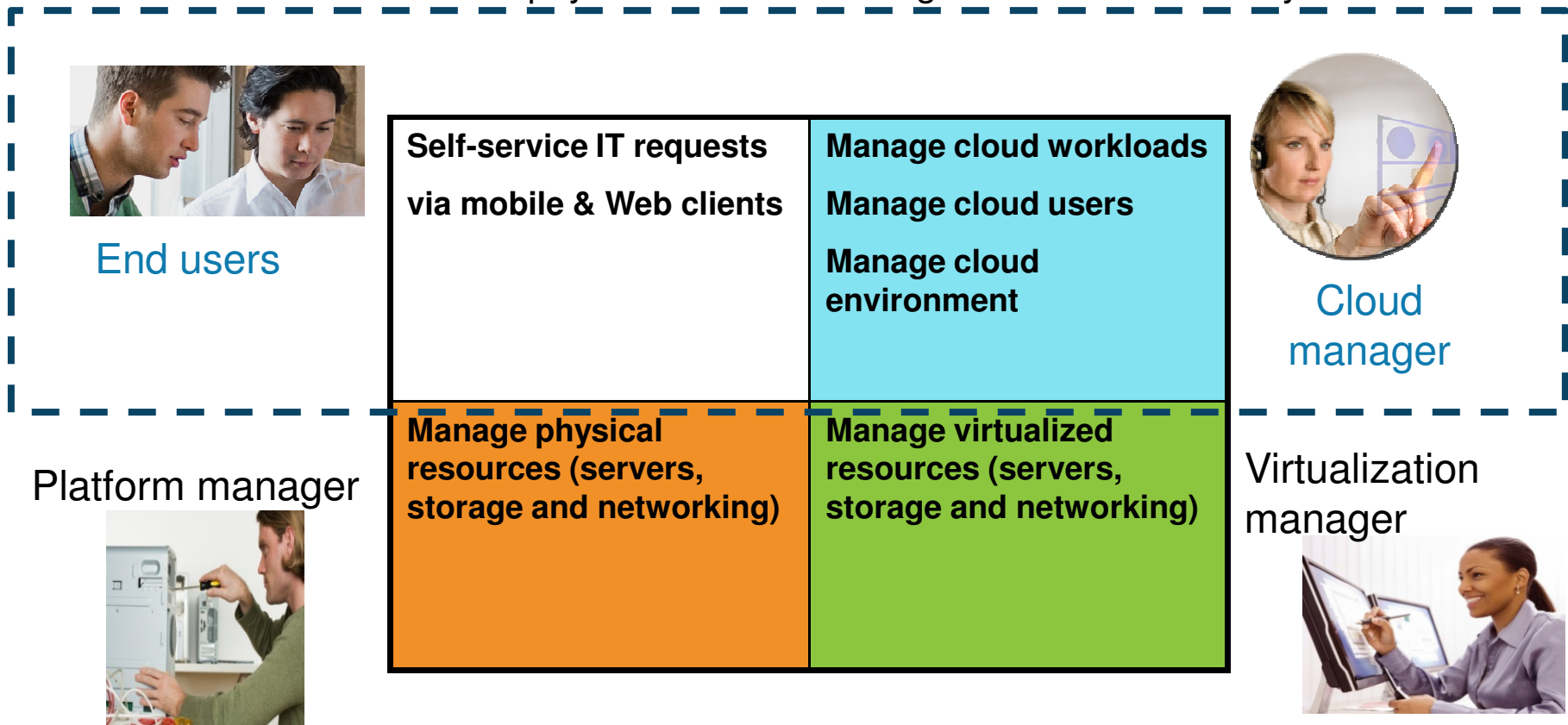
IBM Cloud Manager with OpenStack for basic Infrastructure Cloud Services

- Cloud provisioning and automation based on OpenStack
- End-user support isolated to particular resource groups or tenants
- Administrative support constrained to particular cloud implementations, with no "skydiving" into the infrastructure layer

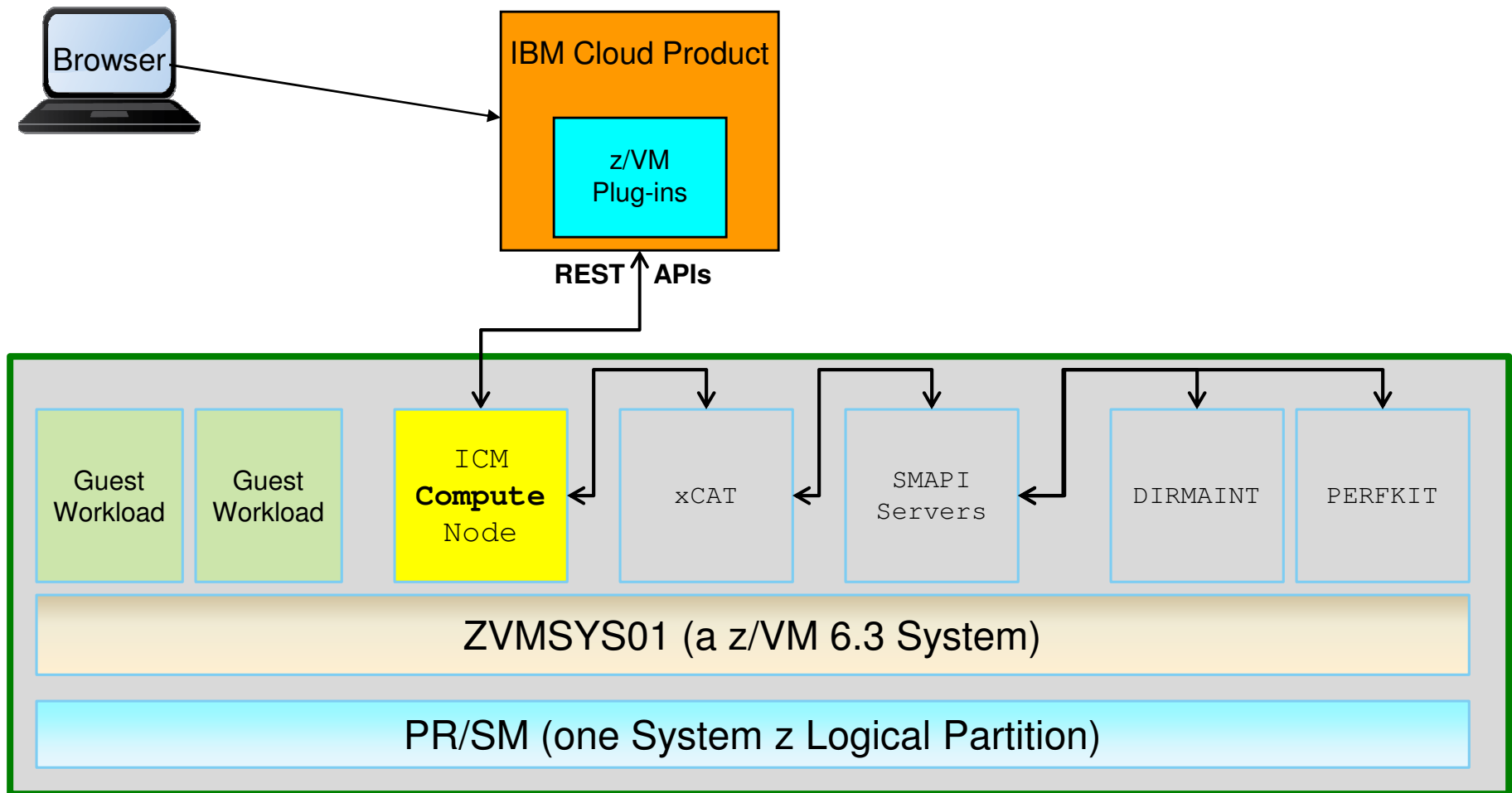


Roles and Controls in IBM Cloud Manager with OpenStack

- End users have more leeway to provision, request, and return infrastructure
- Admins can configure and manage workload without the need for infrastructure know-how, but:
- Neither infrastructure nor physical resource management are obviated by the cloud.



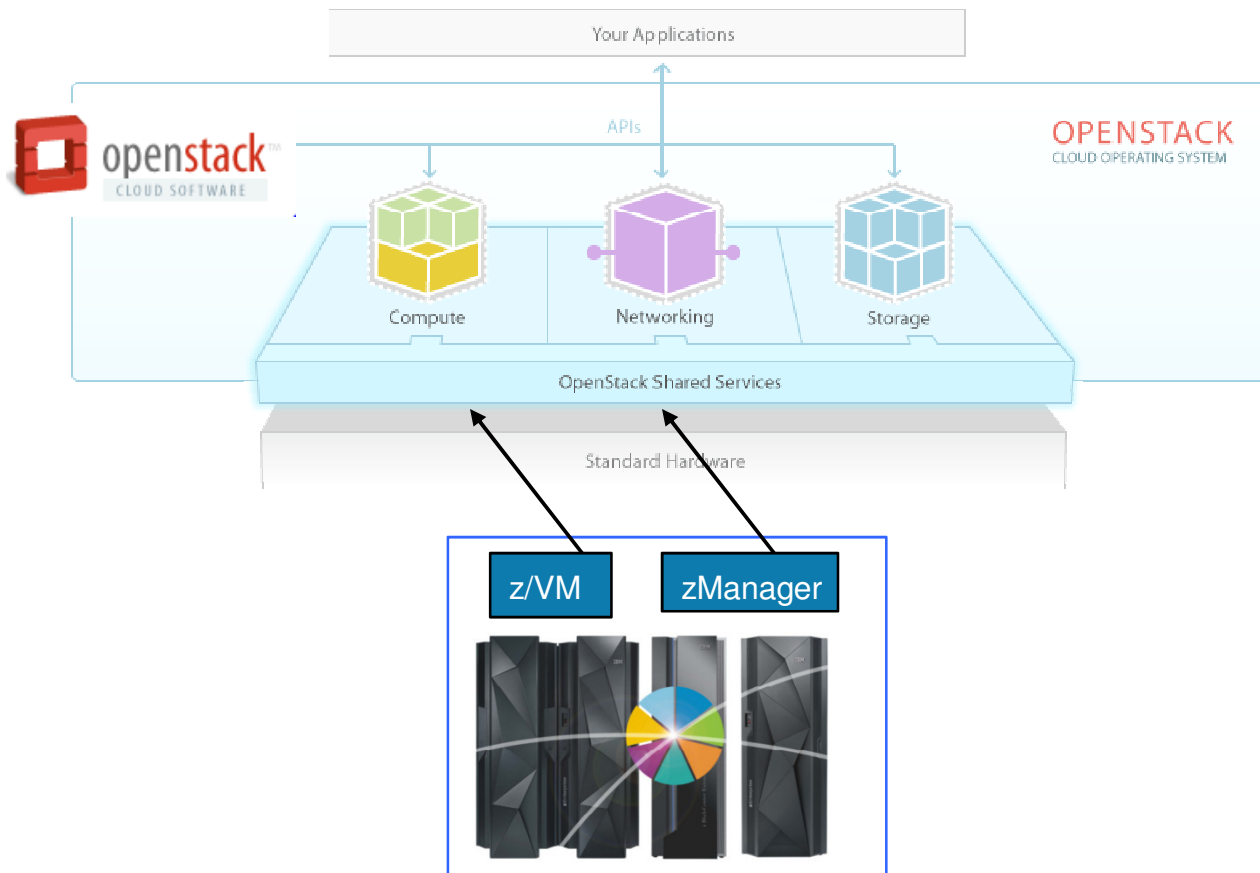
z/VM 6.3 Systems Management



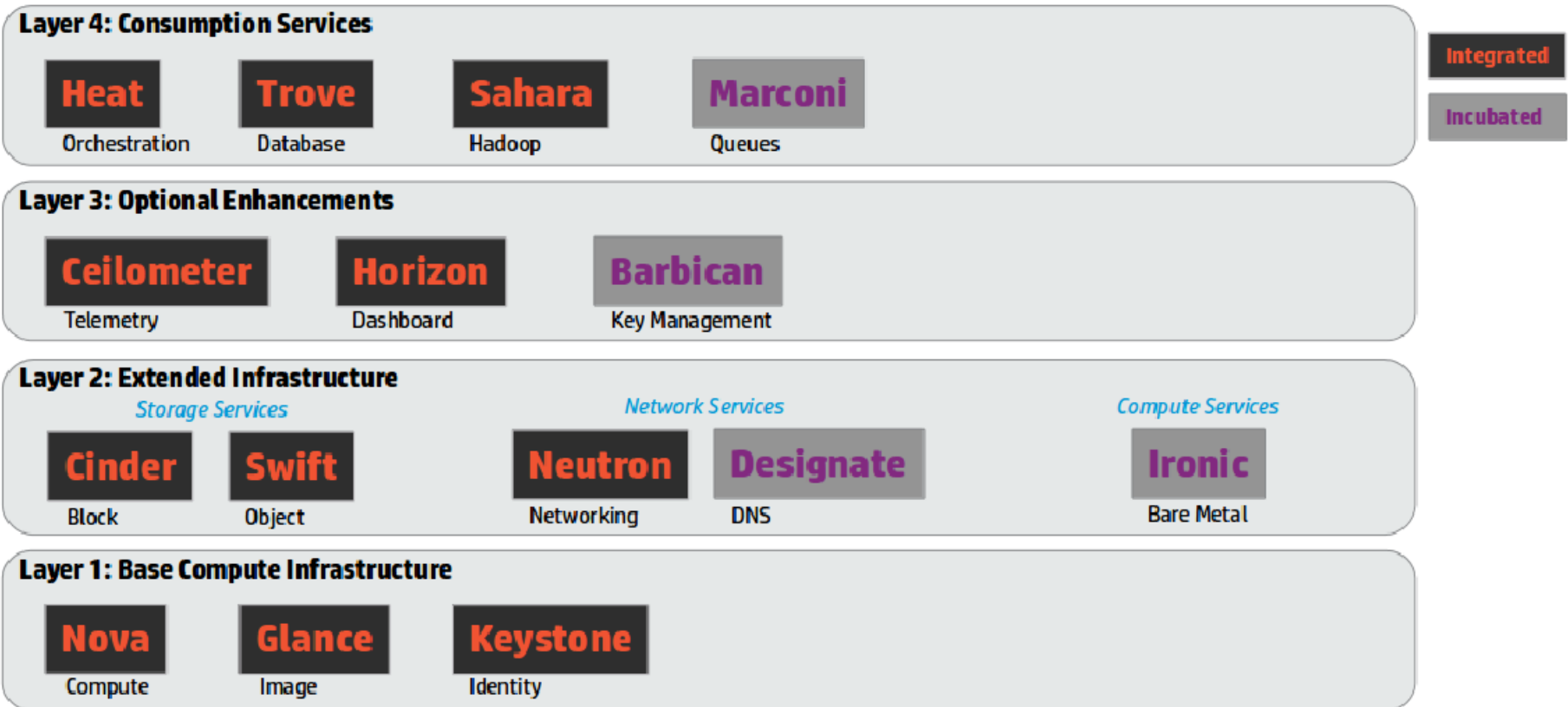
System z and the OpenStack API Model

Self-Service **Cloud Management Application** Multi-Tenant
(including SmartCloud technologies)

Services Catalog Billing and Charge-back

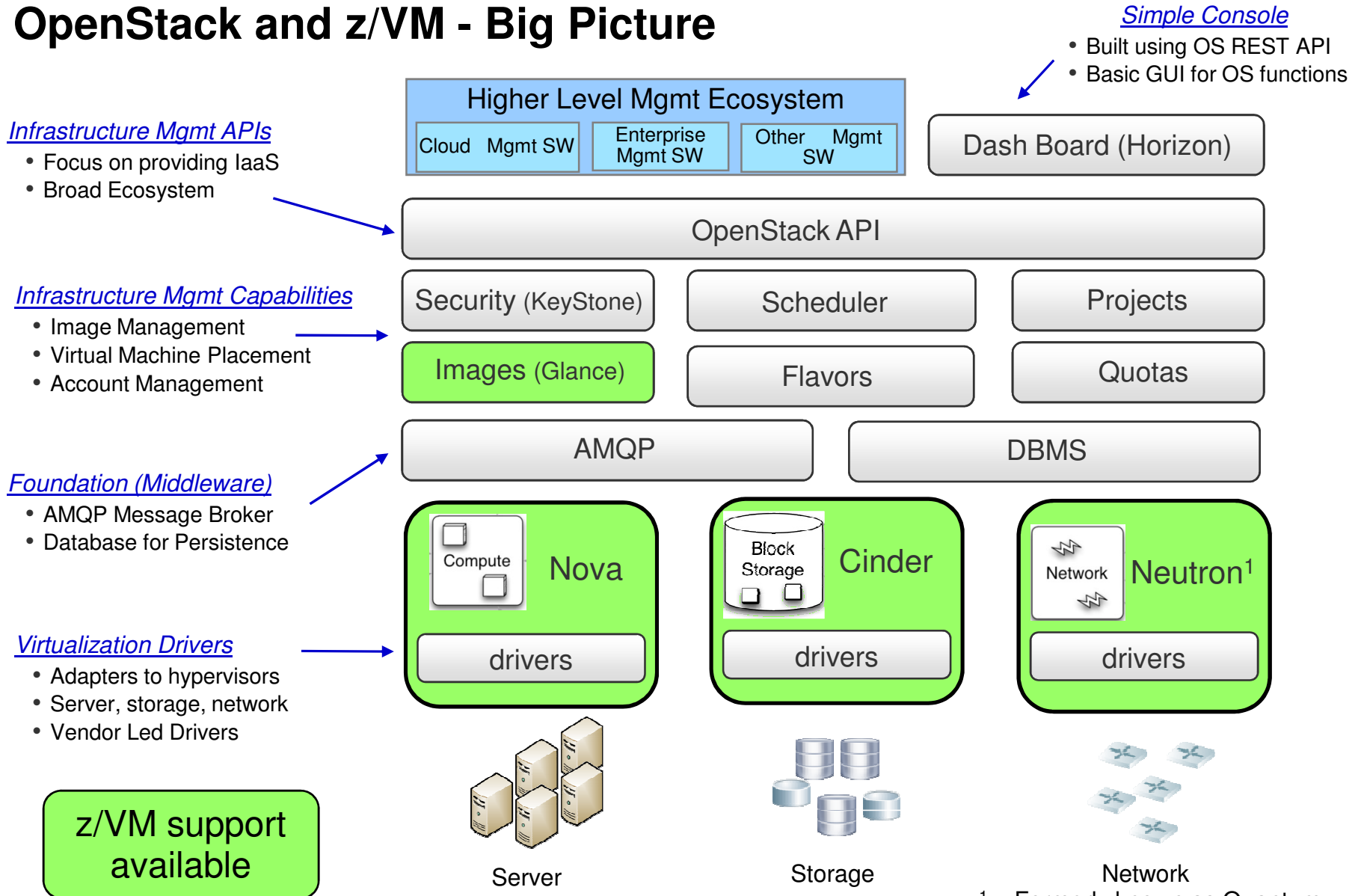


OpenStack as Layers (Compute Centric View)



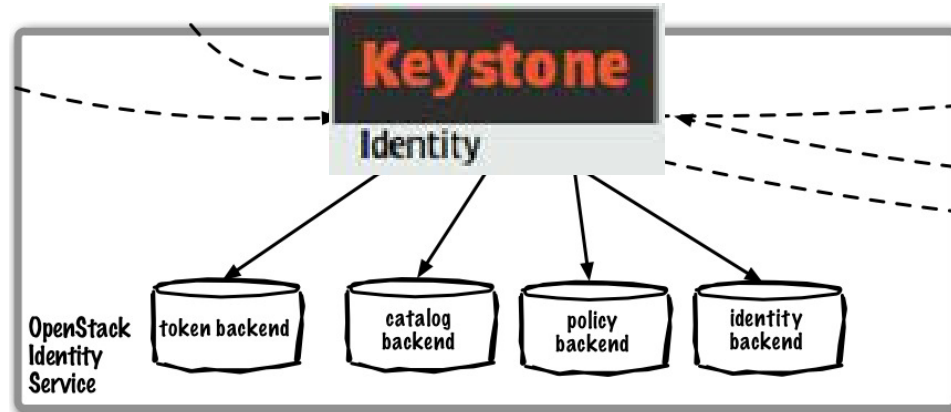
<http://hackstack.org/x/blog/2013/09/05/openstack-seven-layer-dip-as-a-service/>

OpenStack and z/VM - Big Picture



¹ – Formerly known as Quantum.

Identity Services in OpenStack Keystone



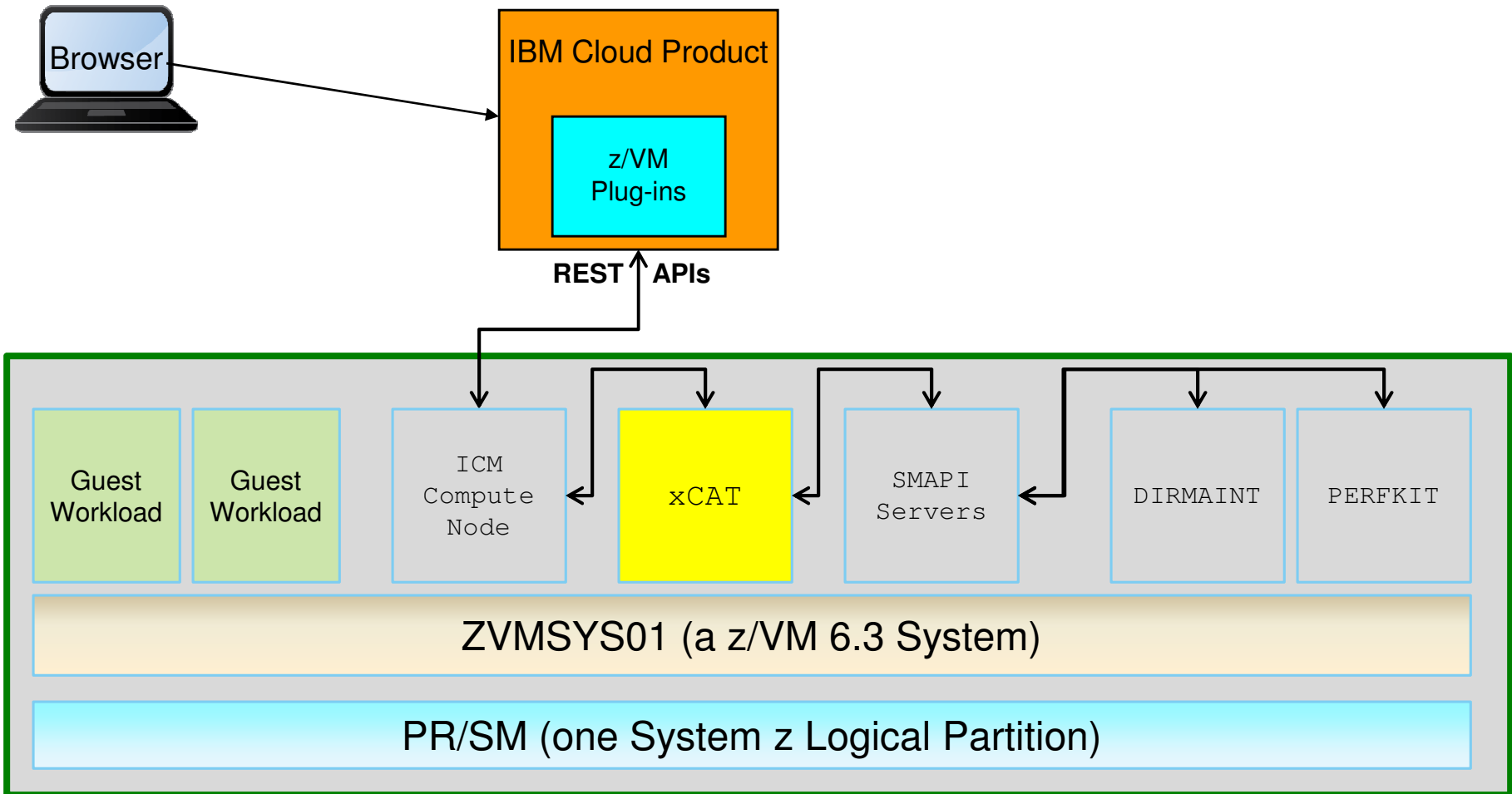
Core Use Cases:

- Installation-wide authentication and authorization to [OpenStack](#) services

Key Capabilities:

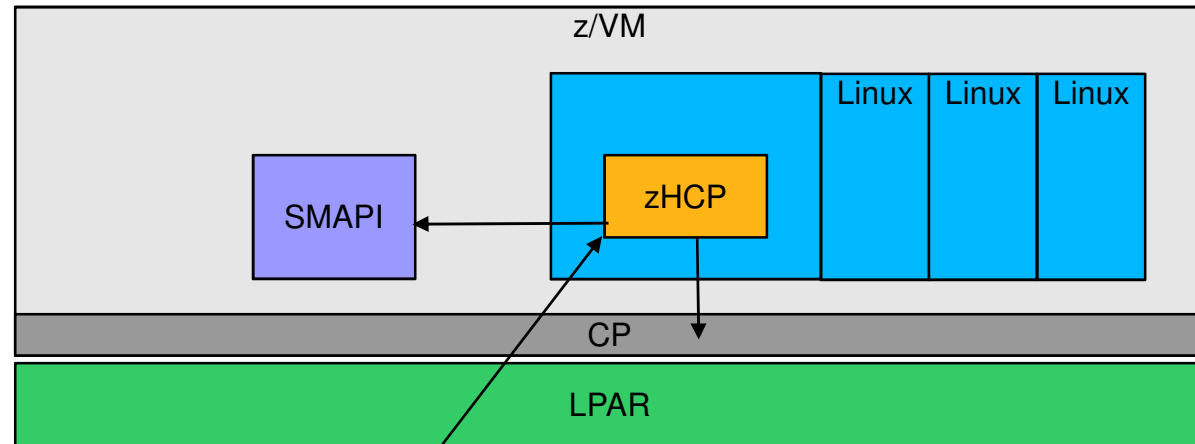
- Authenticate user / password requests against multiple backends (SQL, LDAP, etc) (Identity Service)
- Validate / manage tokens used authentication (Token Service)
- Endpoint registry of available services (Service Catalog)
- Authorize API requests (Policy Service)
- Domain / Project / User model with RBAC for access to compute, storage, networking

z/VM 6.3 Systems Management

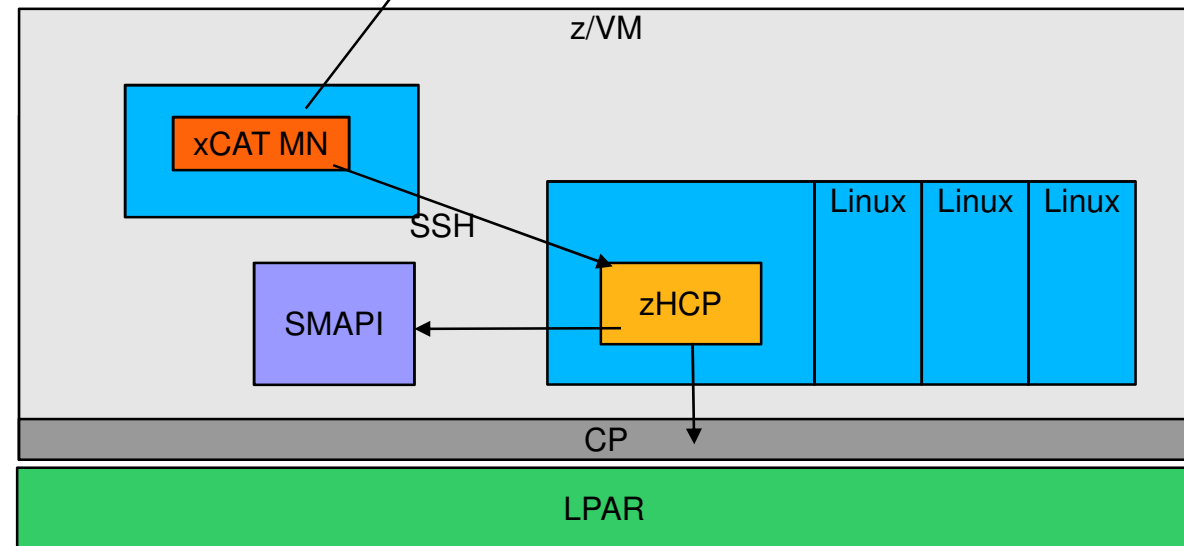


How xCAT Manages z/VM

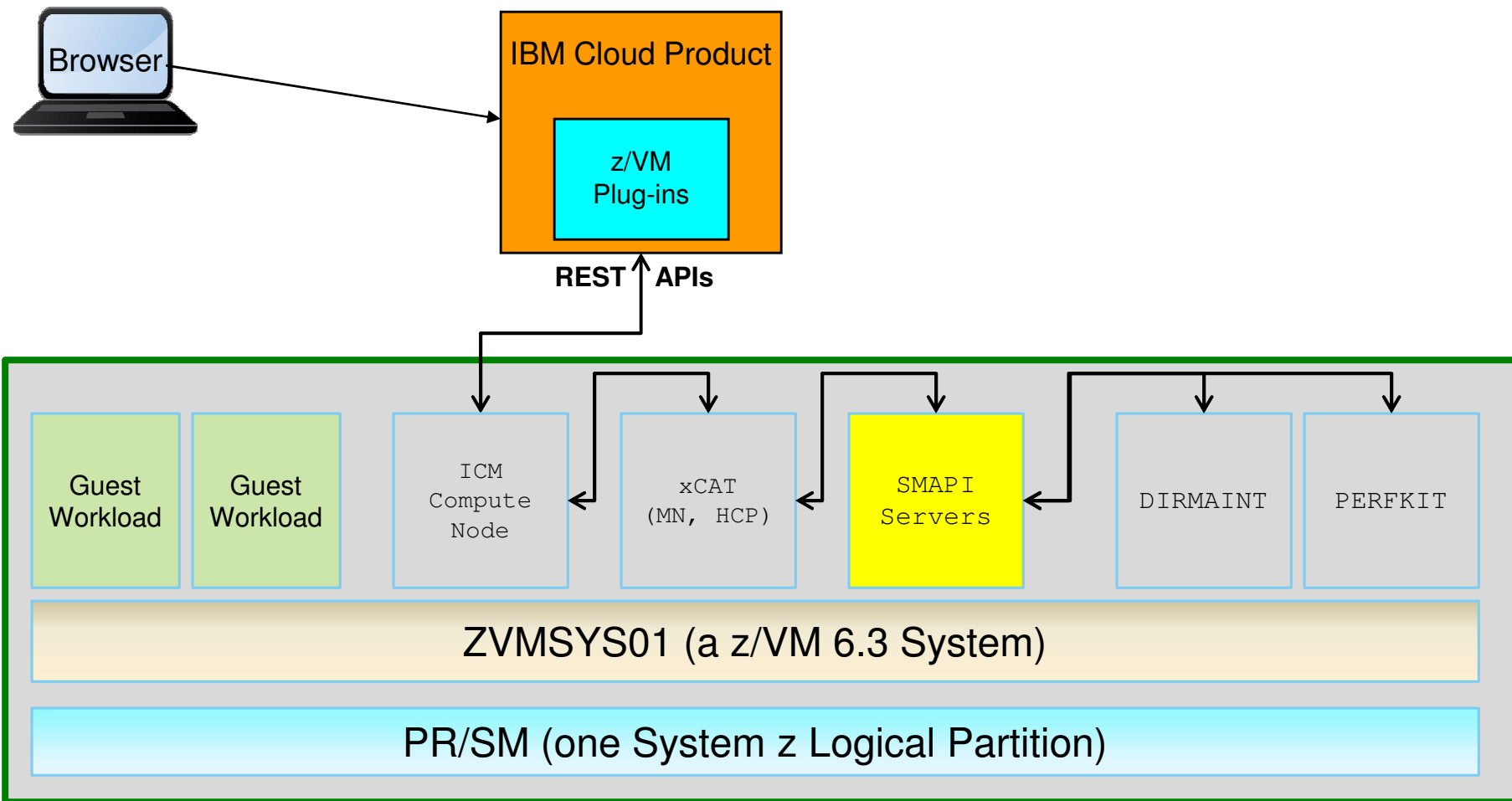
zHardware Control Point:
Manages other VMs via Systems Management APIs and CP Commands. Each z/VM system needs to have a zHCP



xCAT Maintenance Node: Central management server. Only one MN is needed for multiple systems.



z/VM 6.3 Systems Management



Securing z/VM Systems Management API (SMAPI) Machines

The SMAPI virtual machines receive instructions from other programs

These tools are authorized in a SMAPI control file

- Authorize **per requesting VM, per target, per function**

Connections to SMAPI can either be via TCP/IP or via IUCV

- If using IUCV, use discretion in assigning IUCV statements to the directory
- If using TCP/IP, consider encrypting with TLS. Configure a secure port, e.g.:

```
PORT  
44444 TCP VSMREQIN      SECURE VSMCERT1
```

SMAPI will need RACFVM authorities to do its job.

- See “Appendix F” of the *z/VM Systems Management Application Programming Guide*
- *Audit SMAPI requests as appropriate!*

Securing z/VM Systems Management API (SMAPI) Machines

New virtual machines come preinstalled with z/VM 6.3:

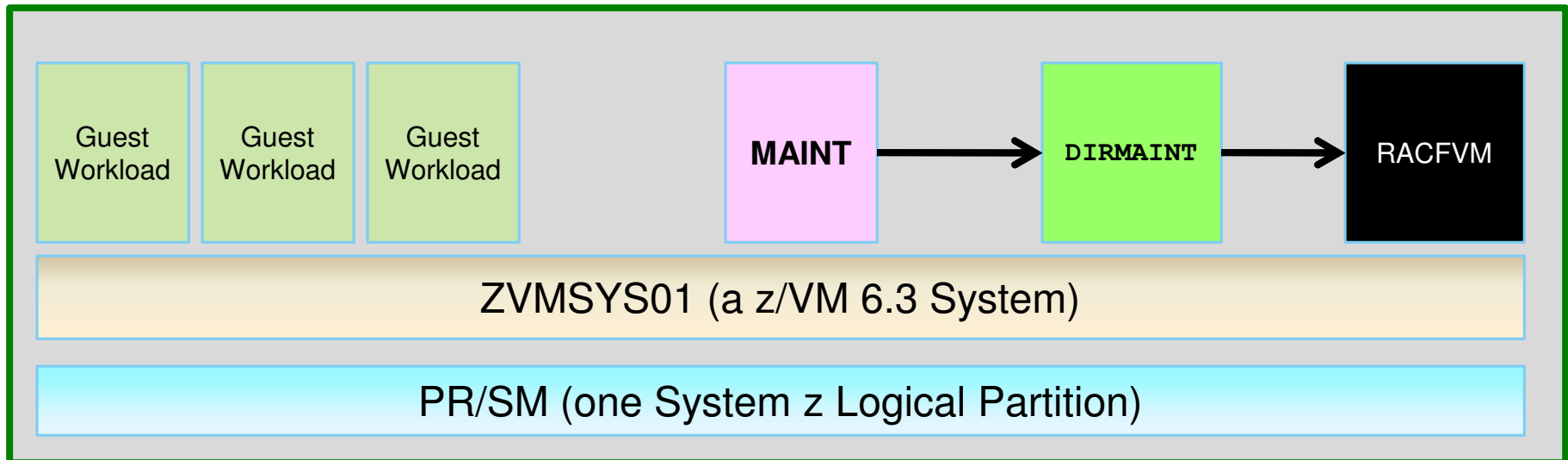
- Defined as Multiconfiguration Virtual Machines (one per SSI member)
- Class G by default, but will need access to certain commands from Classes A, B, and C.
- OPTION LNKNOPAS by default
- Will use their own separate VSWITCH – isolated network traffic
- If you're **not** using this support, convert them to NOLOG.
 - As you would with any other preinstalled virtual machine, right?

None of these tools remove the need for an ESM:

- **Do** give these new virtual machines appropriate RACF accesses to do their jobs
- **Do not** let them exceed the scope of their responsibility

The DirMaint-RACF Connector

- An exit between the Directory Maintenance Facility and RACF for VM
 - Enable in **CONFIGRC.DATADVH** (the initial EXEC is DVHRUN.EXEC)
 - Translates system admin tasks (e.g., the creation of a minidisk) to security policy
 - Lessens need for two administrators (one system, one security) to be work in tandem
 - Local plug-ins can be written, added, and enabled for extra functionality



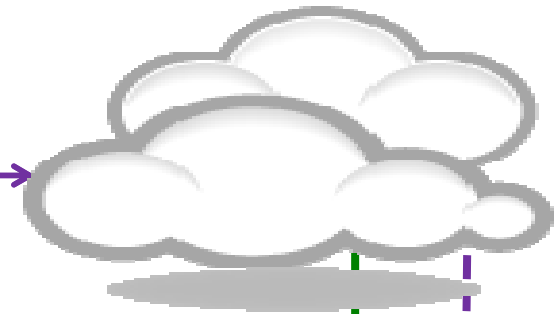


A cloud end-user sees ...

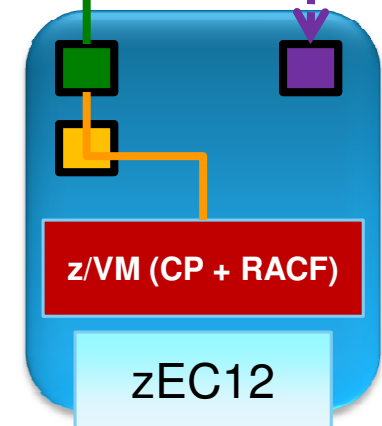
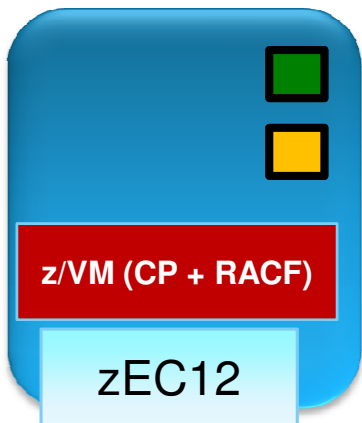


- A cloud end-user enters a command: "Start this Linux Guest."
- A return code comes back upon success (or failure) of the command
- The guest has booted. (We hope.)
- End-user comes back later and relocates the guest. That was easy!

A cloud end-user doesn't see ...



- A cloud consumer starts a virtual machine
- Consumer authenticates to cloud interfaces (ICM, OpenStack, LDAP)
- Authorization is based on cloud definitions (ICM, OpenStack)
- Command is sent from controller to ...
 - ... Compute node to xCAT via REST APIs (HTTPS)
 - xCAT Mgmt node translates and transmits to zHCP (SSH)
 - zHCP in turn sends to SMAPI (TLS-encrypted)
 - SMAPI worker machines have been authorized to start machines when requested by xCAT (IdEA Management)
 - SMAPI transmits the request to CP
 - CP IPLs the virtual machine, defining guest boundaries and privilege classes (PEP)
 - RACFVM definitions define infrastructure tenancy and authorities (PDP)
 - A decision is made! Return to start!

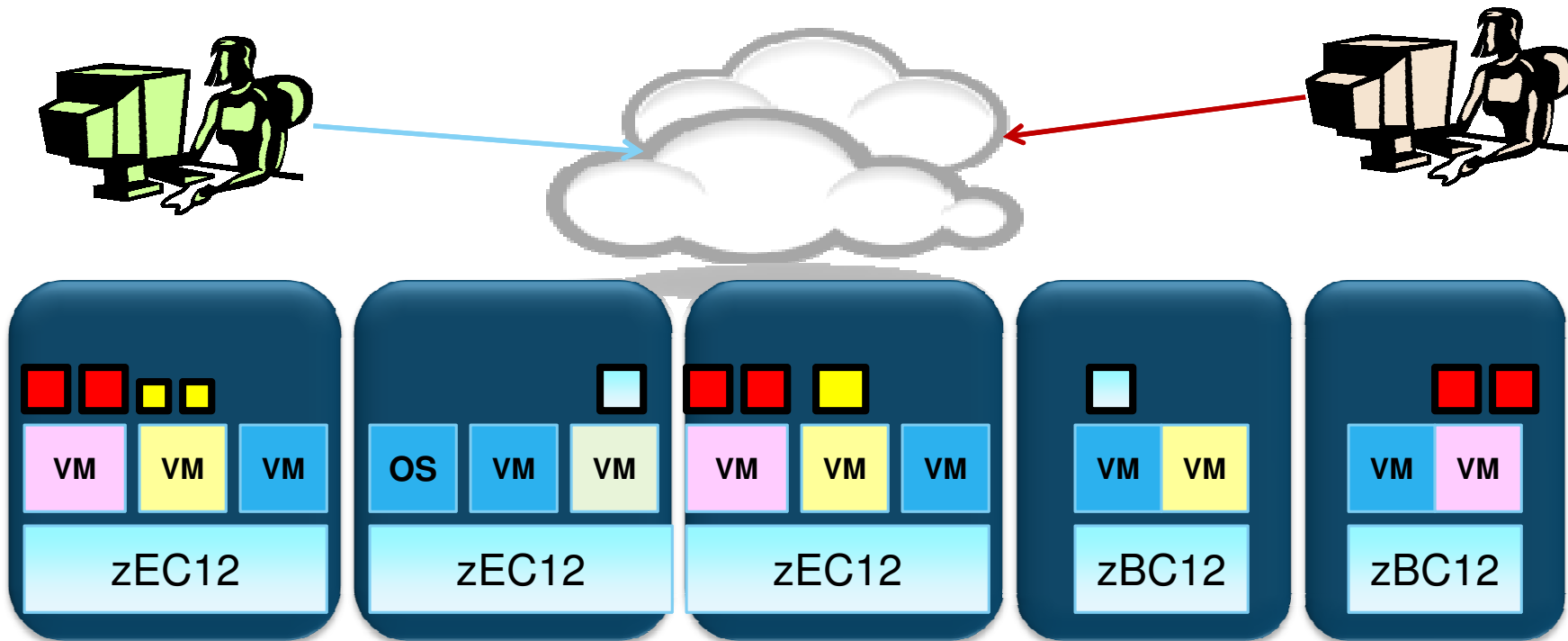


Summarizing Security Mechanisms in a z Private Cloud

System z Cloud Layer	Security Mechanism	Risks Addressed
IBM Cloud Manager with OpenStack	<i>Projects Roles and RBAC Identity Management</i>	Account Hijacking Malicious Insiders
OpenStack (Compute Node)	<i>Tenancy HTTPS (encryption)</i>	Insecure APIs Denial of Service
xCAT	<i>Identity Management SSH (encryption)</i>	Insecure APIs Abuse and Nefarious Use
SMAPI	<i>RBAC by API TLS (encryption)</i>	Insecure APIs Malicious Insiders
DirMaint for z/VM	<i>Resource Access Controls Auditing</i>	Data Loss Insufficient Due Diligence
z/VM (CP with RACFVM)	<i>Guest Isolation Privilege Classes RBAC Security Zones Auditing (SMF)</i>	Data Breaches Account Hijacking Abuse and Nefarious Use Insufficient Due Diligence Shared Technology Issues

Security in a System z Private Cloud

- There is a difference between **cloud-level security** (for the consumers **and/or** the **cloud administrators**) and **infrastructure-level security** (for your system administrators, security administrators, and the virtual machines themselves)
- Administrator privilege does not necessarily reflect workload privilege



Summary

"Sooner or later you're going to realize,
just as I did, that there's a difference between
knowing the path ... and walking the path.

-- *The Matrix* (1999)

Security Tips for the Cloud

Don't forget the basics

- Access controls and incidence response don't go away in the cloud
- Be mindful of asset-tracking, data flow, and change management
- Your data will be of varying classifications – exploit multi-tenant features as pertinent!

*Leverage cloud to **enhance** security*

- Cloud offers rapid scale of environments and networking
- Security as a Service (for varying definitions of security)
- Standardizing means less variability, which may mean fewer surprises

Understand your provider's capabilities – and get it all in writing

- Whether your provider is part of your company or a third party
- Establish clear roles and communication paths for escalations and incident management
- Understand where the data resides (for regulatory and geopolitical reasons)
... and who owns it.

Security in a System z Private Cloud

The components which underpin a System z Cloud work together to secure:

- The underlying **Infrastructure** (z/VM, RACF/VM, DirMaint, SMAPI)
- The **Services** provided by the cloud
- The layering of mechanisms provide a **defense in depth** against vectors of attack
- **Auditing clouds** will help to measure risk and validate compliance

Cloud is more secure than you think, but don't make assumptions:

- There is a long chain of **authorization**, **authentication**, and **auditing** which underpins security in this environment
- A lot of these are functions that already exist in today's System z installations
- But don't let the promise of cloud obscure the need for infrastructure security

For More Information (z/VM)

- **z/VM Security:** <http://www.vm.ibm.com/security/>
- **z/VM Systems Management :** <http://www.vm.ibm.com/sysman/>
- **OpenStack Enablement for z/VM:** <http://www.vm.ibm.com/sysman/openstk.html>
- **IBM Enterprise Cloud Computing:** <http://www-03.ibm.com/systems/z/solutions/cloud/>

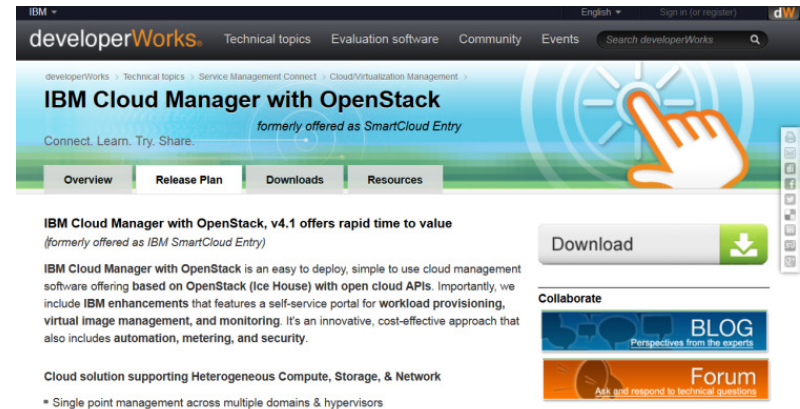
- **IBM Cloud Manager with OpenStack on SMC:**
<http://www.ibm.com/developerworks/servicemanagement/cvm/sce/index.html>

- **IBM Systems for Cloud Computing Infrastructure:**
<http://www-03.ibm.com/systems/infrastructure/us/en/cloud-servers/>

Contact Information:

[Brian W. Hugenbruch](mailto:bwhugen@us.ibm.com), CISSP
z/VM Security Design and Development
[bwhugen at us dot ibm dot com](mailto:bwhugen@us.ibm.com)

 @Bwhugen



IBM Cloud Manager with OpenStack, v4.1 offers rapid time to value
(formerly offered as IBM SmartCloud Entry)

IBM Cloud Manager with OpenStack is an easy to deploy, simple to use cloud management software offering based on OpenStack (Ice House) with open cloud APIs. Importantly, we include IBM enhancements that features a self-service portal for workload provisioning, virtual image management, and monitoring. It's an innovative, cost-effective approach that also includes automation, metering, and security.

Cloud solution supporting Heterogeneous Compute, Storage, & Network
* Single point management across multiple domains & hypervisors

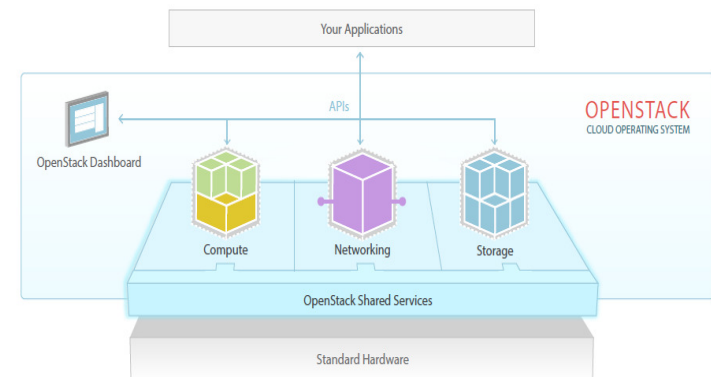
For More Information (Cloud Compliance and Standards)

- **NIST SP 800-144: "Guidelines on Security and Privacy in Public Cloud Computing"**
<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>
- **NIST SP 800-145: "The NIST Definition of Cloud Computing"**
<http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- **NIST SP 800-146: "Cloud Computing Synopsis and Recommendations"**
<http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf>
- **PCI DSS v2: "PCI DSS Cloud Computing Guidelines"**
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Contact Information:

[Brian W. Hugenbruch](#), CISSP
z/VM Security Design and Development
[bwhugen at us dot ibm dot com](mailto:bwhugen@us.ibm.com)

[@Bwhugen](#)



Dank u

Dutch

Merci

French

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

감사합니다

Korean

Tack så mycket

Swedish

धन्यवाद

Hindi

תודה רבה

Hebrew

Obrigado

Brazilian
Portuguese

谢谢

Chinese

Dankon

Esperanto

Thank You

ありがとうございます

Japanese

Trugarez

Breton

Danke

German

Tak

Danish

Grazie

Italian

நன்றி

Tamil

děkuji

Czech

ขอบคุณ

Thai

go raibh maith agat

Gaelic

In case of emergency, break glass for
Backup Slides

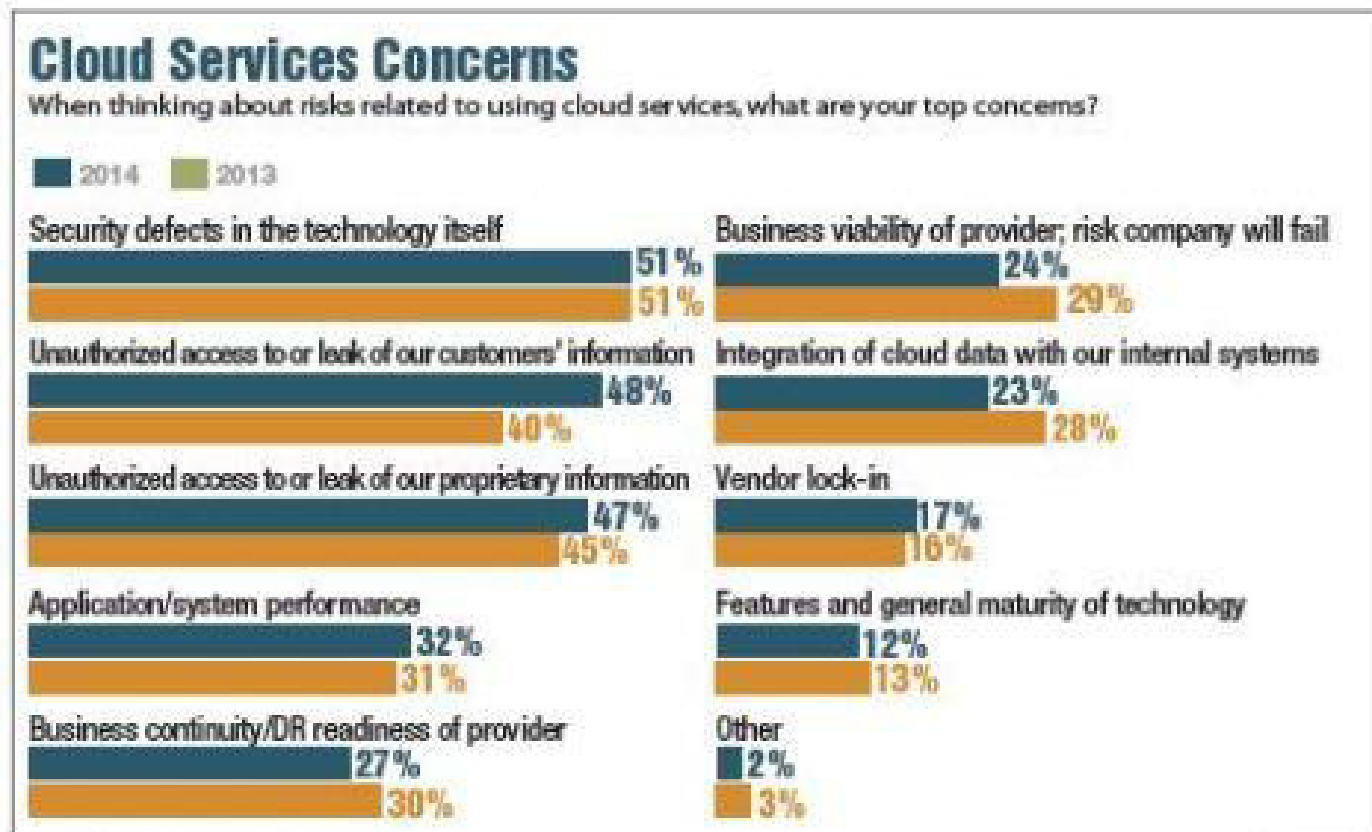


What is a Cloud Environment?

"I said, 'A line will take us hours maybe;
Yet if it does not seem a moment's thought,
Our stitching and unstitching has been naught."

-- William Butler Yeats, 'Adam's Curse' (1903)

Security remains a major concern for cloud adopters ...



Note: Three responses allowed

R9990914/9

Base: 360 respondents in August 2014 and 419 in February 2013

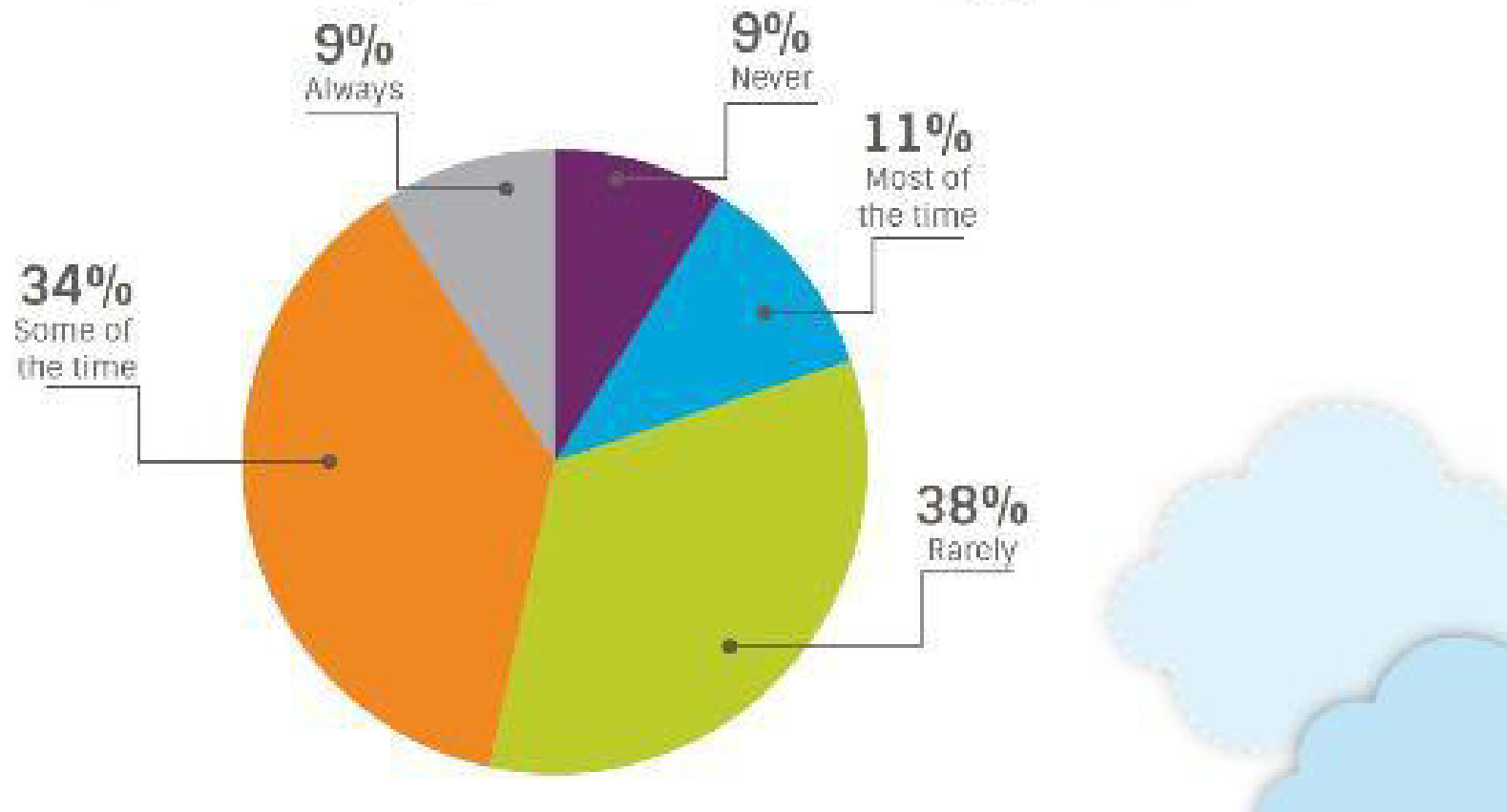
Data: InformationWeek State of Cloud Computing Survey of business technology professionals at organizations with 50 or more employees

Source: Information Week, "State of Cloud Survey"

<http://reports.informationweek.com/abstract/5/12536/Cloud-Computing/State-of-Cloud-Survey.html>

... yet, IT security isn't always in the loop about these decisions ...

How often is the IT security team involved in the decision making process about cloud resources?



Source: SafeNet, "The State of Cloud Information Governance", October 2014 (PDF)



Where IBM Wave Fits in the Cloud Blueprint

Integrate

Virtualization
*Infrastructure &
Virtualization Management*

Differentiation

- Rapid deployment of Linux virtual servers for less than \$1 a day
- Industry leading "gold standard" security for tenant isolation
- Elastic scaling achieved by dynamically adjustable capacity at sustained performance
- Simplified and empowered virtualization management with IBM Wave
 - z/VM
 - IBM Wave
 - Linux on IBM System z®

Automate

Entry Level Cloud
Standardization & Automation

Standardization

- Automated provisioning and de-provisioning
- Pool standardized virtualized building blocks
- Plug-and-play capacity across hardware generations
- Capture and catalog virtual images in the data center
- Automated methods for faster delivery of services with higher levels of control
 - xCAT
 - SmartCloud Entry*

Orchestrate

Advanced Cloud
Service Lifecycle Management

Service Management

- Integrated virtualization management with IT service delivery processes
- Self-service provisioning
- Automated service lifecycle management including dynamic instantiation of cloud services
- Pay for use
- Optimize IT resources to reinvent business processes
 - Cloud Ready for Linux on System z
 - SmartCloud Provisioning*
 - SmartCloud Orchestrator*

* System z support currently in development

OpenStack Release Names

- These codenames are chosen by popular vote. Codenames are cities or counties near where the corresponding OpenStack design summit took place, with some exceptions to the rule.
- "Bonus points for sounding cool."
- **Austin:** The first design summit took place in Austin, TX
- **Bexar:** The second design summit took place in San Antonio, TX
- **Cactus:** Cactus is a city in Texas
- **Diablo:** Diablo is a city in the bay area near Santa Clara, CA
- **Essex:** Essex is a city near Boston, MA
- **Folsom:** Folsom is a city near San Francisco, CA
- **Grizzly:** Grizzly is an element of the state flag of California (summit in San Diego, CA)
- **Havana:** Havana is an unincorporated community in Oregon (summit in Oregon)
- **Icehouse:** Ice House is a street in Hong Kong
- **Juno:** Juno is a locality in Georgia
- **Kilo:** Paris (or, at least, Sèvres) is the home of the Kilogram artifact