Neil Readshaw – Chief Security Architect, GTS Cloud Services

February 2013

Smarter systems for a smarter planet:

System z® Forum

Secure and resilient cloud computing
for the modern enterprise

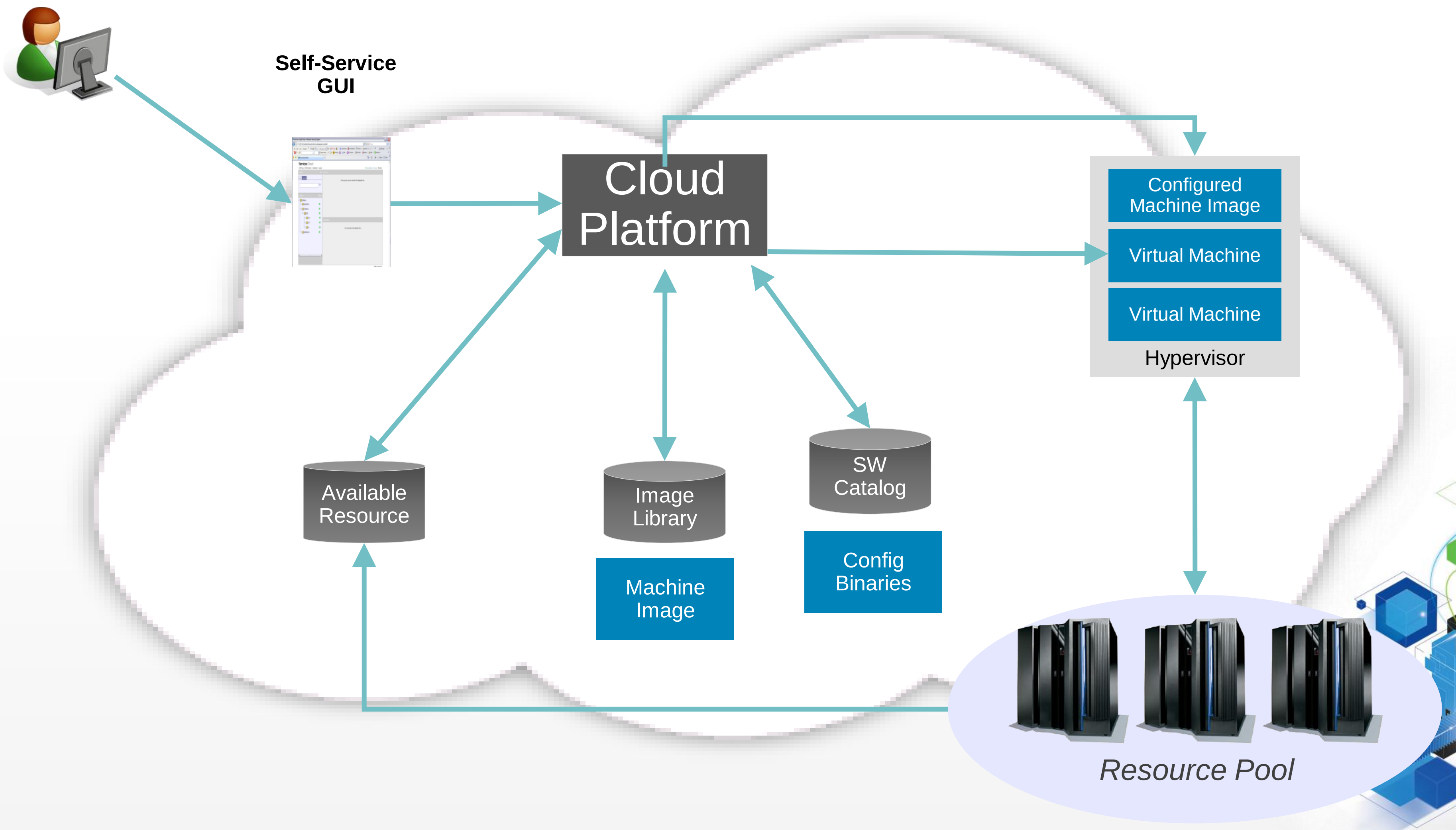
Securing Workloads in a System z Cloud

What to expect and how to be prepared

By the end of this presentation, you will...

- Understand the new security risks with providing cloud services within an enterprise
- Recognize the need for governance and compliance management for workloads running on the cloud
- Receive an introduction to approaches for securing cloud workloads
- Know how IBM can help

Scenario: zLinux cloud for enterprise workloads



Self-Service GUI

Cloud Platform

Configured Machine Image

Virtual Machine

Virtual Machine

Hypervisor

Available Resource

Image Library

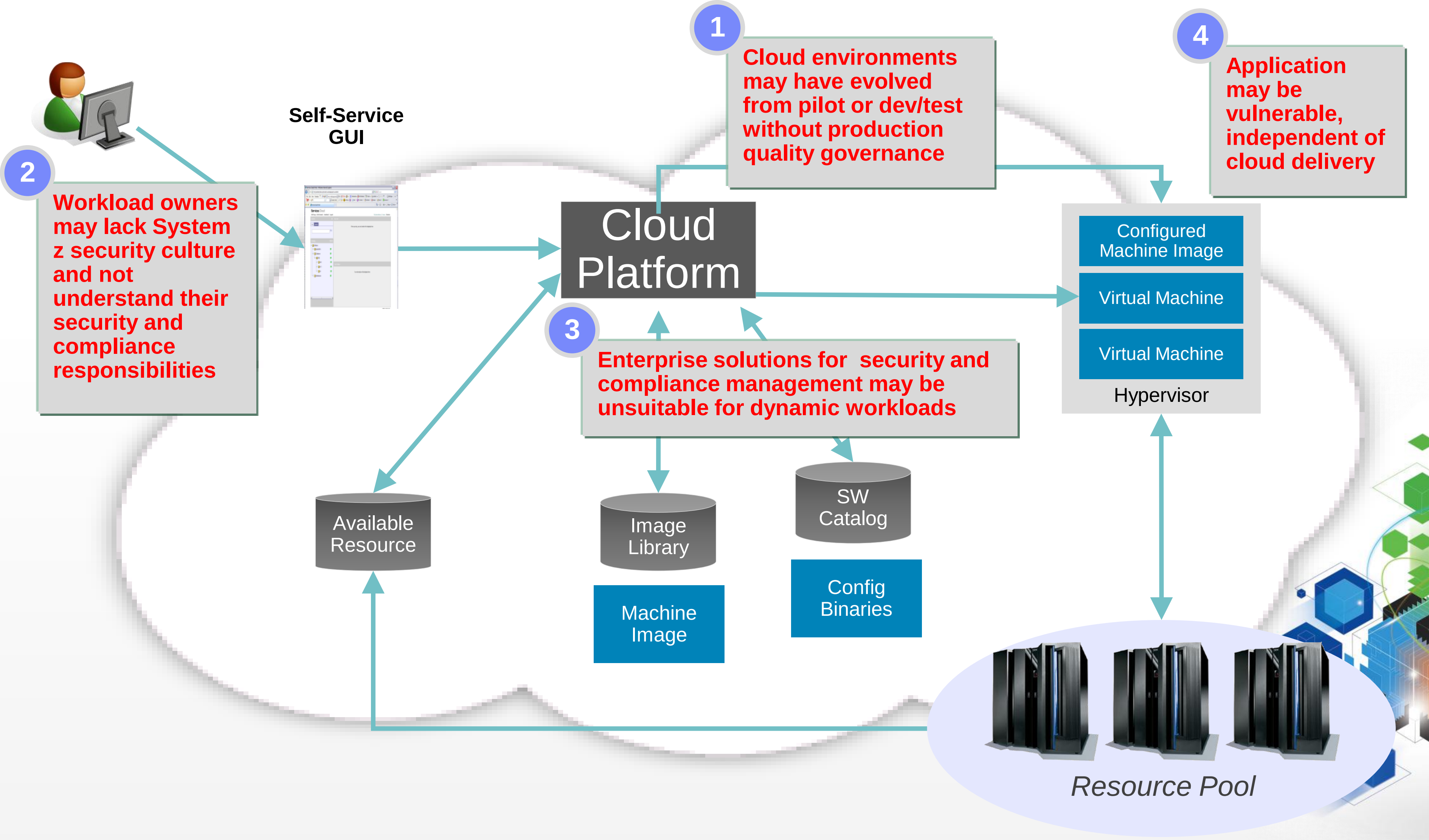
Machine Image

SW Catalog

Config Binaries

Resource Pool

Security risks and compliance considerations for workloads running on a System z cloud



1 Cloud environments may have evolved from pilot or dev/test without production quality governance

2 Workload owners may lack System z security culture and not understand their security and compliance responsibilities

3 Enterprise solutions for security and compliance management may be unsuitable for dynamic workloads

4 Application may be vulnerable, independent of cloud delivery

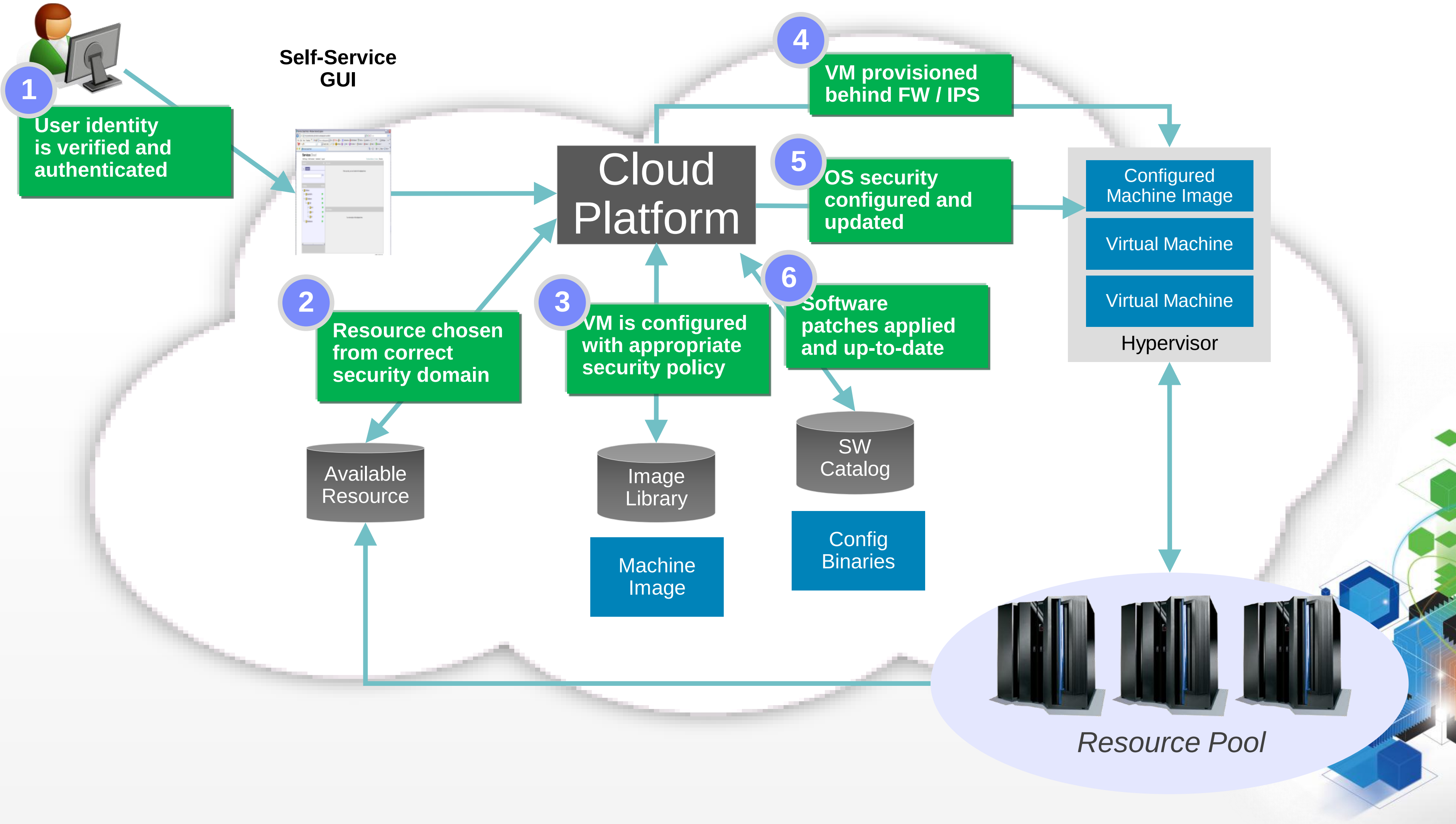
Solution approaches need to be a combination of people, process and technology

Risk	Potential Solution Approach	How IBM can help
1. Cloud environments may have evolved from pilot or dev/test without production quality governance	Enterprise security policy evolves to be cloud aware, supported by processes and tools	IBM Security Consulting Services for Cloud Security (strategy and roadmap)
2. Workload owners may lack System z security culture and not understand their security and compliance responsibilities	Educate the users of their responsibilities, ongoing not one-time Simplify those responsibilities through tooling and automation	IBM Security Identity Manager IBM Tivoli Endpoint Manager family (Patch Management and Security and Compliance)

Solution approaches need to be a combination of people, process and technology

Risk	Potential Solution Approach	How IBM can help
3. Enterprise solutions for security and compliance management may be unsuitable for dynamic workloads	Cloud workloads are secure when created and automatically kept up to date throughout their lifecycle	IBM Tivoli Endpoint Manager family (Patch Management and Security and Compliance)
4. Application may be vulnerable, independent of cloud delivery	Make the people and processes in the application supply chain security aware by employing a secure software development lifecycle for developed *and acquired* applications	IBM Security AppScan family (including as a cloud delivered service) IBM Rational Policy Tester – Privacy Edition InfoSphere Guardium family

Applying security best practices to our scenario



1 User identity is verified and authenticated

Self-Service GUI

Cloud Platform

2 Resource chosen from correct security domain

3 VM is configured with appropriate security policy

4 VM provisioned behind FW / IPS

5 OS security configured and updated

6 Software patches applied and up-to-date

Available Resource

Image Library

Machine Image

SW Catalog

Config Binaries

Configured Machine Image

Virtual Machine

Virtual Machine

Hypervisor

Resource Pool

References

- Redbook: Security for Linux on System z
  - http://www.redbooks.ibm.com/Redbooks.nsf/RedbookAbstracts/sg247728.html?Open

- Solution Brief: Getting started with a cloud on System z can be quick, easy and effective
  - http://public.dhe.ibm.com/common/ssi/ecm/en/tis14142usen/TIS14142USEN.PDF?CT=ISM0090

- IBM Cloud Security
  - http://www.ibm.com/cloud-computing/us/en/security.html

- IBM Security Systems
  - http://www-142.ibm.com/software/products/au/en/category/SWI00

- IBM Security Services
  - http://www-935.ibm.com/services/au/en/it-services/security-services.html