Cloud Security Priorities

FOSDEM ‘13

Robert Clark

Introduction

Robert.Clark@hp.com

Twitter: @hyakuhei

IRC: /server freenode /query hyakuhei

The Cloud – balancing act

Balancing simplicity, cost, speed & choice with risk

The reality of cloud services

- Simplicity and agility overriding risk
- Keep pace with regulatory compliance
- Consumerization of IT

Dilemma of deploying across traditional IT or clouds

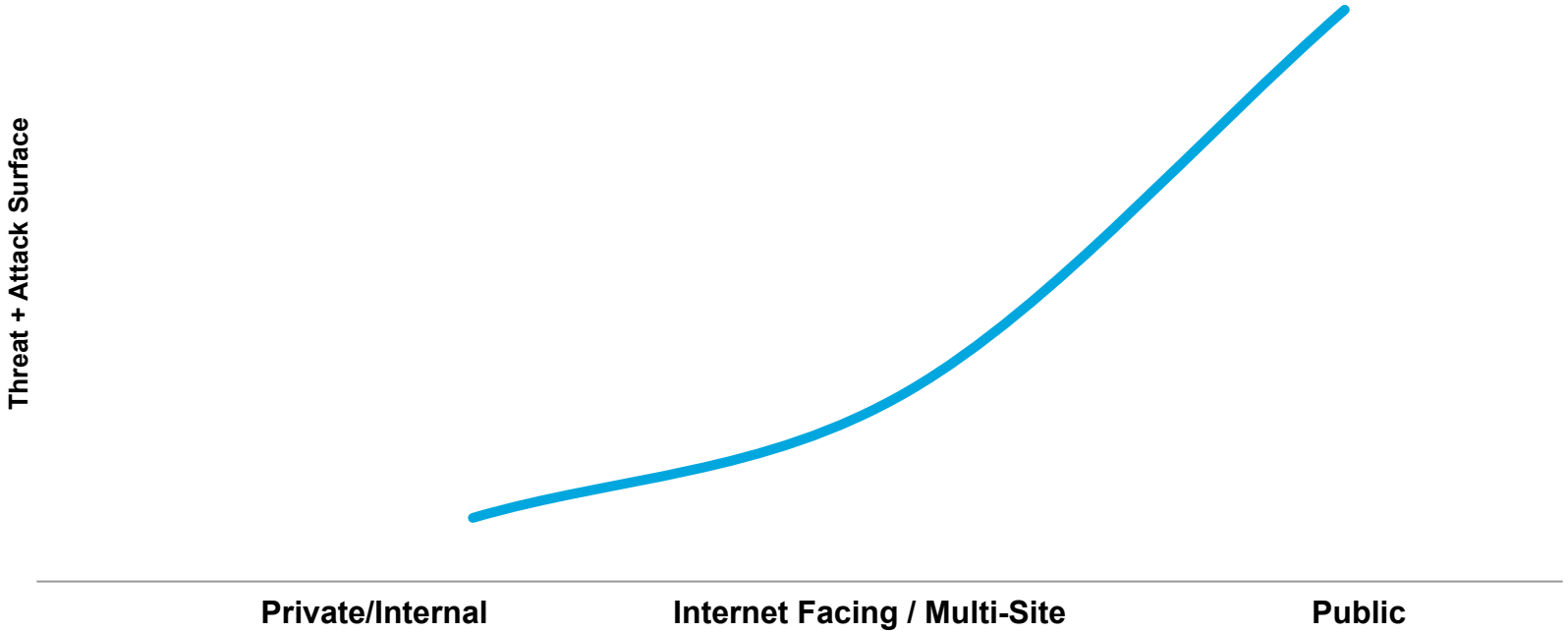
The responsibility and relationship of IT organizations fundamentally changing

HP's Commitment to OpenStack

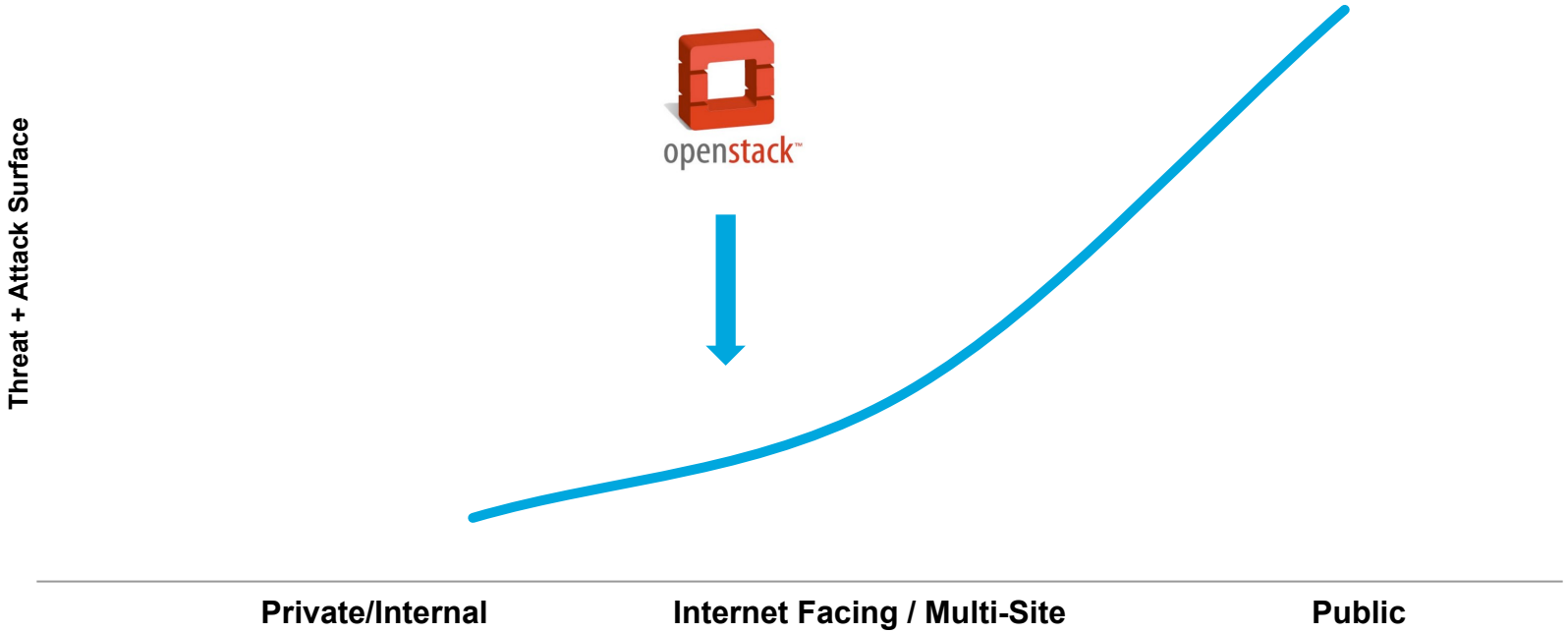
- **4th largest contributor to Folsom**
  By # of lines of code contributed
- **2nd largest employee contributor**
- **Top 3 contributor**
  - Nova, Glance, Quantum, and Keystone

Top OpenStack Contributors

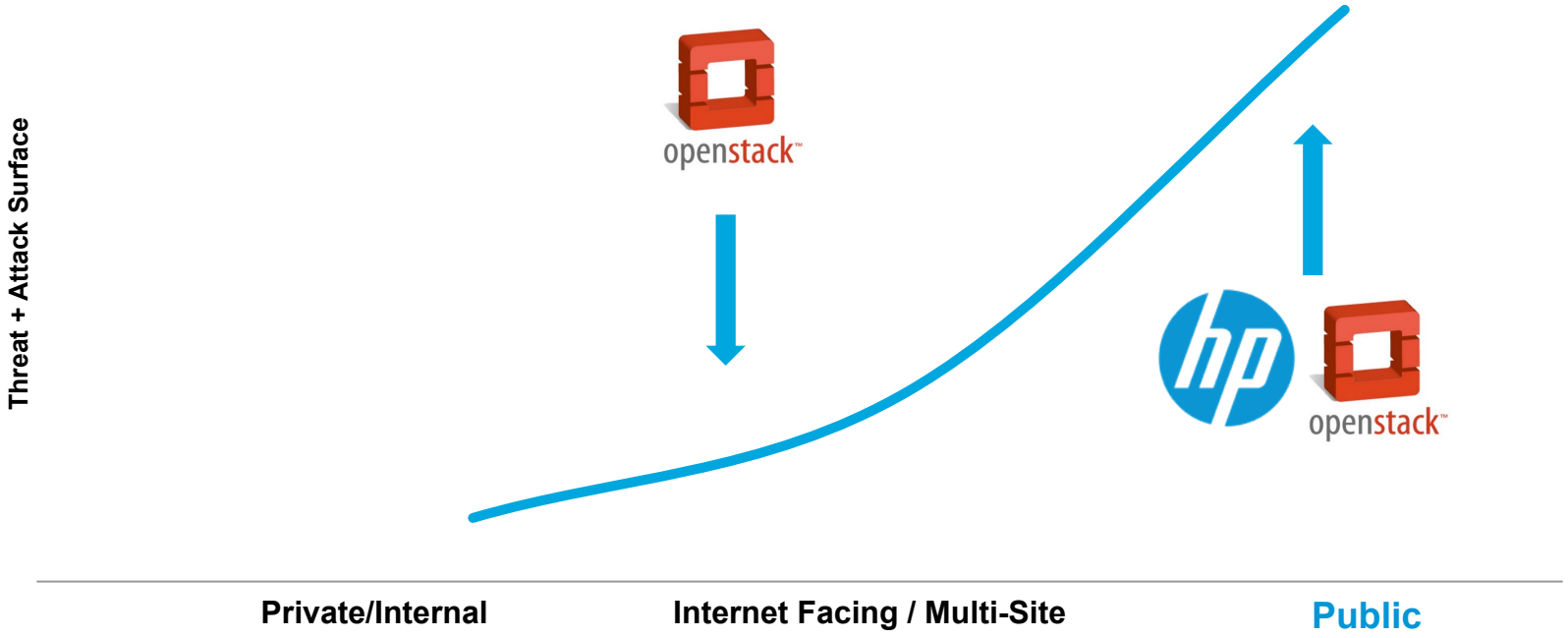
Cloud Threats



Cloud Threats



Cloud Threats



Gap Analysis

- Service Authentication
- Service Authorization
- Object Encryption
- VM DAR Encryption
- Auditability
- Availability
- Message Integrity
- Cloud-Scale IDS

Strategic Security Controls and Enhanced Security Options Required for Adoption

Private Cloud

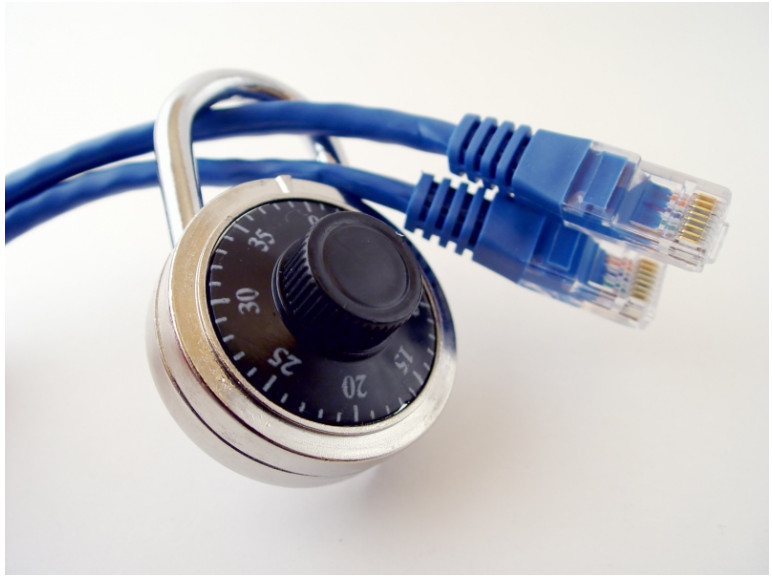
Known Quantities

You know who your users are

…and they're accountable for their actions

Private Cloud

Known Quantities



Networks are tightly controlled

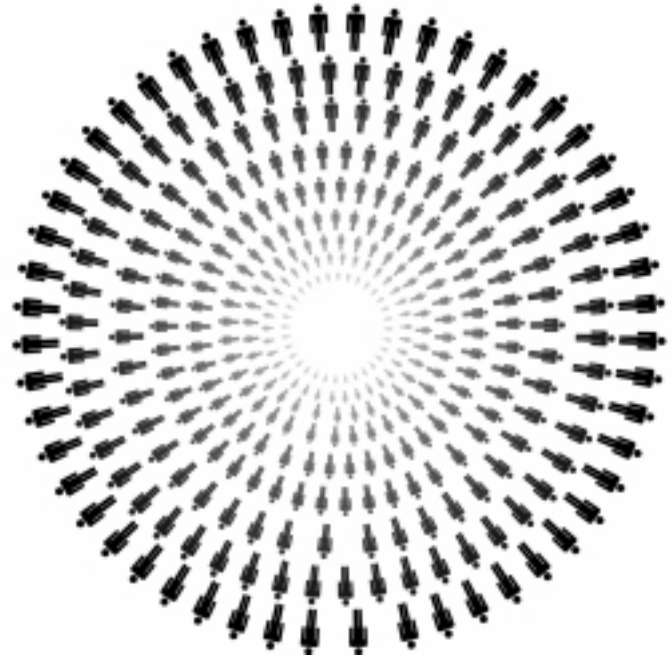
Private Cloud Trust Assertions

Trust assured through user accountability

- **Users are accountable**
- **Established routes for responsibility and attribution**
- **Defined network access controls**
- **Corporate policies constrain usage**
- **Users can be held to specific use cases**
- **Access easily tracked / revoked**
- **Many options for user control / discipline**
- **IP Reputation protected by clearly defined border policies**
- **Established abuse handling mechanisms**

Public Cloud

Unknown Quantities



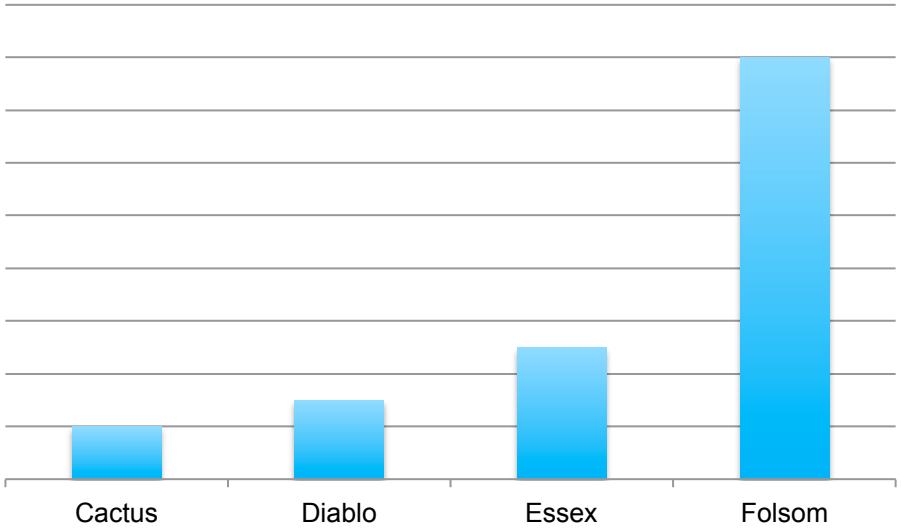
Service open to people from around the world

Public Cloud Trust Assertions

Offering services to everyone, everywhere

- **Unaccountable Users**
- **Open Network Requirements**
- **Users have almost complete control over their use of instances**
- **Almost all behavior types and profiles presented**
- **Identities are cheap, replaceable**
- **Constant battle to identify and control abusive users**

Security Interest



Approaching Critical Mass

Why Is Security Hard?

Complex and Decoupled

Nova

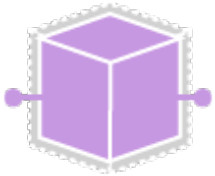
Glance

Swift

Complex and Decoupled

Nova

Quantum



Glance

Horizon

Keystone

Swift

Complex and Decoupled

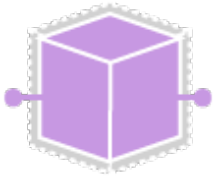
Nova

Keystone

Glance

Horizon

Quantum



Swift

DNS

Automation

Block Storage

Metering

Load Balancing

Billing

Databases

Orchestration

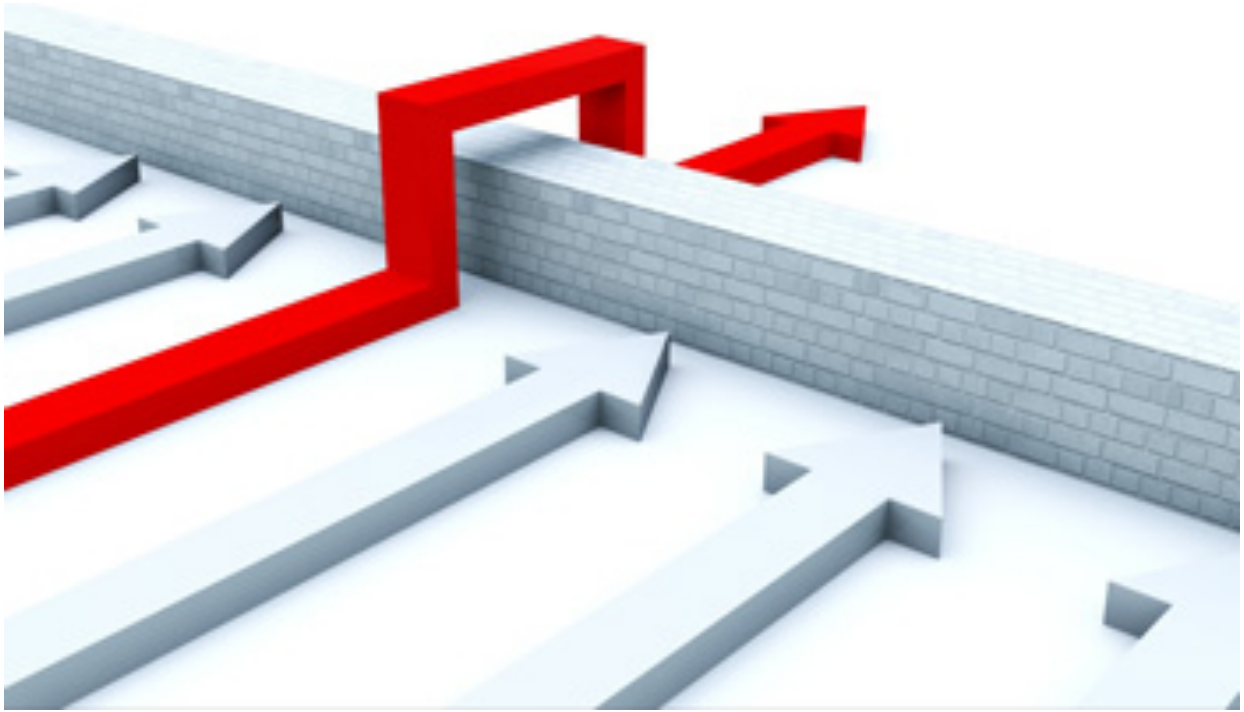
Monitoring

Alarming

Messaging

Account Maintenance

Assume a hostile network



Hypervisor Security

“VMware delivers better-than-physical security” – VMware 2008

Hypervisor Security

Blackhat 2009 – Cloudburst: A VMWare Breakout

Kostya Kirtchinsky

Hypervisor Security

Defcon 2011 – VirtuNoid: A KVM Breakout

Nelson Elhage

Hypervisor Security

US-CERT 2012 - SYSRET64: A Xen Breakout

US-CERT #649219

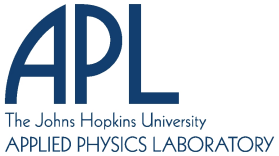
Common Mistakes

Enthusiastic Developer + Hash Algorithm + Async Crypt != Secure Design

Getting Help is Easy

OpenStack Security Group

- Initial kickoff in Fall 2012 (OpenStack Summit)
- Working to get key players involved



OpenStack Security Group

Objectives:

- **Consult**
- **Design**
- **Engage**
- **Drive**

Current Projects

OSSG Projects

- Security Notes
- Hardening Guide
- TLS/SSL Review
- Client TLS/SSL CA Auth

OpenStack Projects

- Nova Trusted Messaging / RPC
- Swift Message HMAC

Q & A

Security Notes :
http://launchpad.net/osn

OpenStack Security Group :
https://launchpad.net/~openstack-ossg

Careers

http://www.hpcloud.com

Ninjas Welcome!