数据驱动安全

2015 中国互联网安全大会
China Internet Security Conference

Cloud Security Scenario

Jay Heiser
@JayHeiser1

STRATEGIC PLANNING ASSUMPTION

Through 2020, 95% of cloud security failures will be the customer's fault.

Why it won't happen:

- If a provider failure does occur, it could have huge levels of impact.
- The cloud market continues to be financially weak.

Why it will happen:

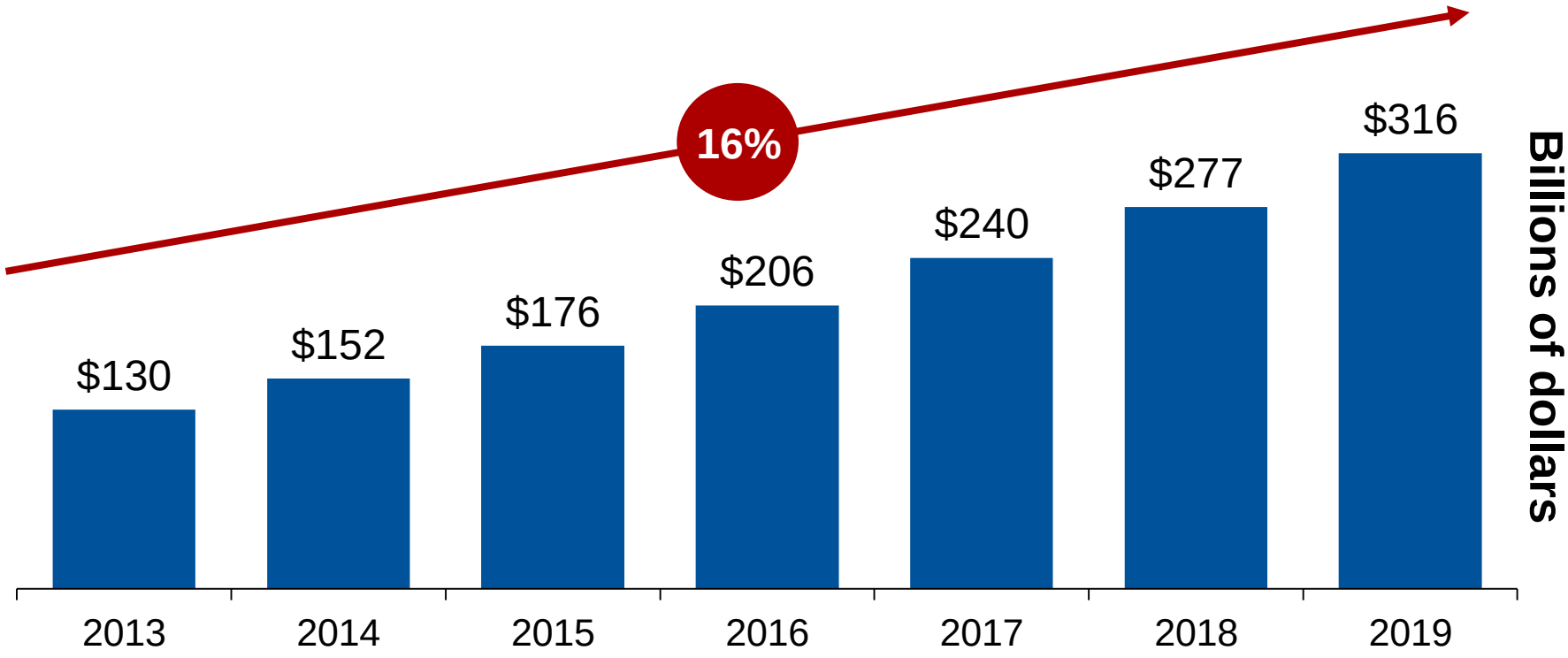
- The history of public cloud computing has been remarkably free of provider failures.
- Cloud service providers are under huge market and Internet pressure:
  - They must make security a priority. They have no choice.

KEY ISSUES

1.How worried should you be about which public cloud risks?
2.What do you need to do to manage those risks?

15.7% CAGR
Gartner Public Cloud Services Forecast, 1Q15

In the next five years, enterprises will spend $1.2 trillion on public cloud services (2015-2019)



Source: "Forecast: Public Cloud Services, Worldwide, 2013-2019, 1Q15 Update" (G00275962)

Where Is Everybody in Cloud Computing Adoption?

Don't understand the model

Struggling with the cloud strategy

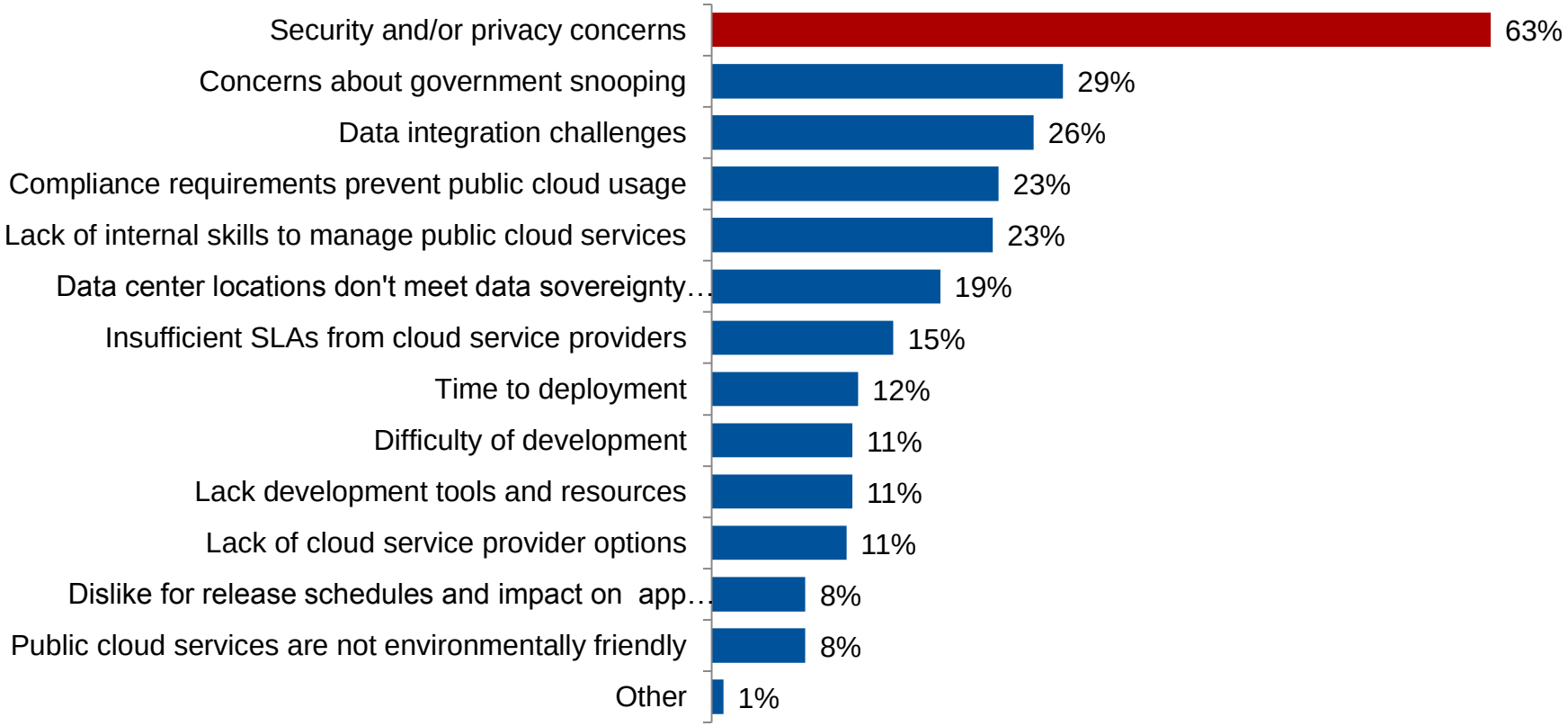
Developing best practices

Lots of clouds

What About Security? Cloud Adoption Survey (2014)

What are the top three reasons for NOT considering a public cloud-based model?

n = 210, Base: Does not primarily employ Public Cloud for IaaS, Paas and/or SaaS



Up to 3 responses allowed

Cybercriminals Are Not Stealing Cloud Storage. They Are Stealing Your User's Accounts

Phishing is the biggest source of cloud security failure.

Enterprises Are Focusing on the Wrong Party to Improve Security

Cloud services are not getting breached.

Most security incidents are the customer's fault.

The big story in cloud security is that big hacks and failures have not occurred.

Organizations Rushing to the Cloud Underestimate the Effort to Control How It Will Be Used

- Account and virtual machine management.
- Access control:
  - Inappropriate internal shares.
  - Public shares.
- Visibility and control of activity:
  - Sanctioned and unsanctioned usage.
  - Incident response.
  - E-discovery.
- Integration with other services.
- Recovery after provider bankruptcy or accident.

How will you support someone else's applications when they break?

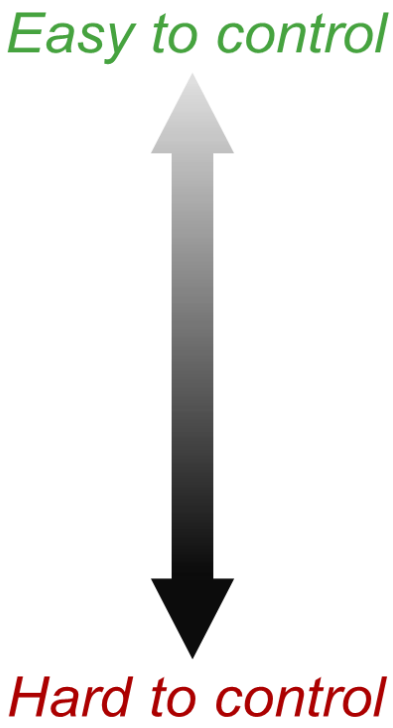
Different Cloud Models Require Different Emphasis

- Infrastructure as a service:
  - Secure remote access for people and processes
  - Prevent OS and application vulnerabilities
  - Manage and track virtual machines
- Software as a service:
  - Assess provider security posture and control features
  - Govern multiple applications from different providers
  - Ensure data is used appropriately
  - Reliably and safely connect mobile, partner and BYOD

You must explicitly and consistently address identity and access management (IAM), especially privileged access management (PAM)

50 Shades of Cloud Gray Imply Different Levels of Effort

- IT sponsored for entire enterprise:
  - IaaS, SaaS and PaaS
  - Email and personal productivity
  - File sync and share
- Department sponsored:
  - IT supports strategic services:
    - CRM, ERP, HR
  - Line of business sources other applications
- Individually used
- Partner-imposed

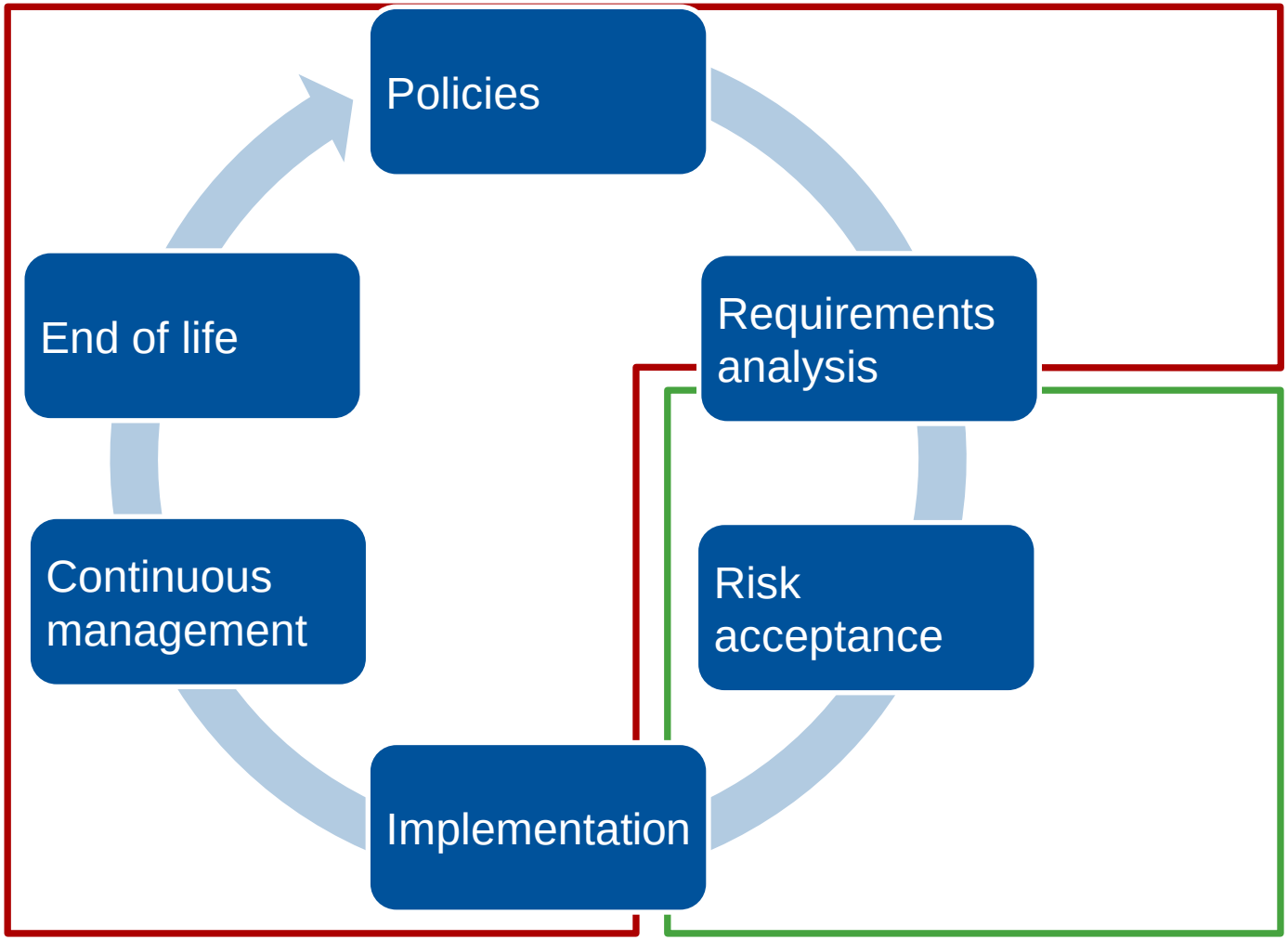


You Need a Cloud Governance Strategy

- Start with an enterprise cloud strategy:
  - What cloud services will be used in which situations
  - Who is responsible for what
- Implement policy and process:
  - Risk acceptance and service ownership
  - Cloud usage management:
    - Central management of users, data and activities
    - Continuous monitoring of vendor status
    - Incident response and recovery

Without a corporate cloud strategy, the best you can hope for is tactical security expediency

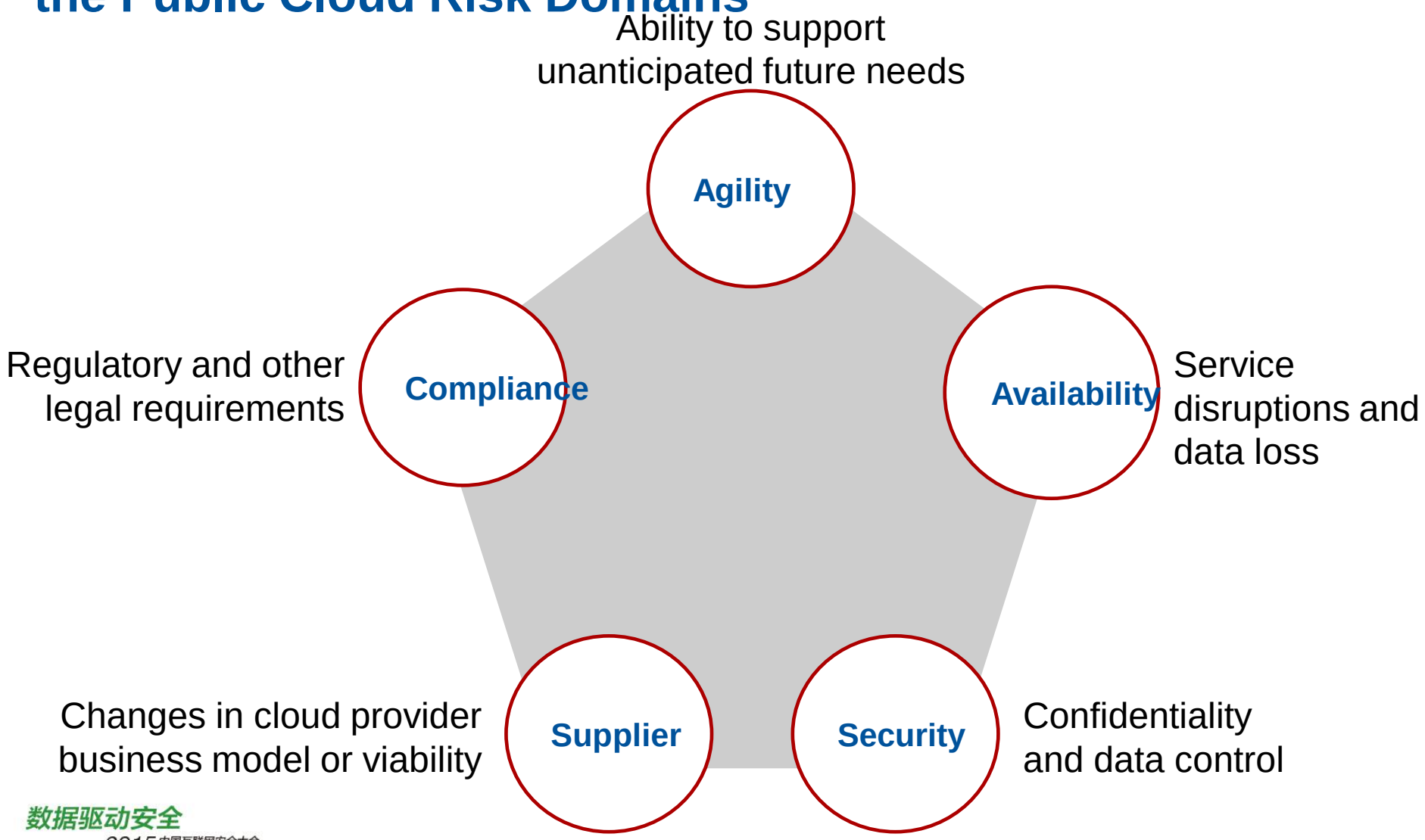
Use a Life Cycle Approach for Cloud Governance



Usually needs more attention

Most enterprises are only addressing part of the life cycle

Base Your Cloud Usage Decisions Around the Public Cloud Risk Domains



Continuous Management and Control Processes You Must Implement for All Forms of Public Cloud

- Configuration
- Identity and access management:
  - Privileged-user management
  - Identities, authentication, entitlements
- Vendor:
  - SLA, performance, delivery and financial health
- Utilization:
  - Billing accuracy, usage, cost optimization, contract rightsizing
- User activity monitoring:
  - Regulatory compliance
  - E-discovery and incident investigation
- Data Backup and recovery:
  - Contingency plan maintenance and invocation

You cannot outsource responsibility for these controls

Controls You Must Implement for IaaS

- Most important:
  - Use a workload-centric security approach
  - Use DevSecOps to ensure robust workloads
- Also important:
  - Firewall it
  - Encrypt all network traffic
  - Never patch live machines
  - Encrypt all local VM storage
  - Security and hardening for CSP, VM and OS

Requires security technical competency, but can be outsourced

Control Activities That Require a SaaS-Specific Approach

Ongoing

- Identity and access management
- User activity monitoring:
  - User and entity behavior analytics
- Compliance reporting:
  - Status of sensitive information
- Data management and archiving
- Annual application portfolio review

As needed

- Problem resolution
- File and object restoration
- Customization and integration
- Service or data recovery
- Incident response/investigation
- E-discovery
- Migration to another service
- Data destruction and archiving

Cloud Storage Encryption Can't Prevent the Most Likely Forms of Security Failure

- Cloud storage crypto cannot prevent:
  - Account hijacking.
  - Desktop compromise.
  - Weak permissions.
  - Mobile data synchronization.

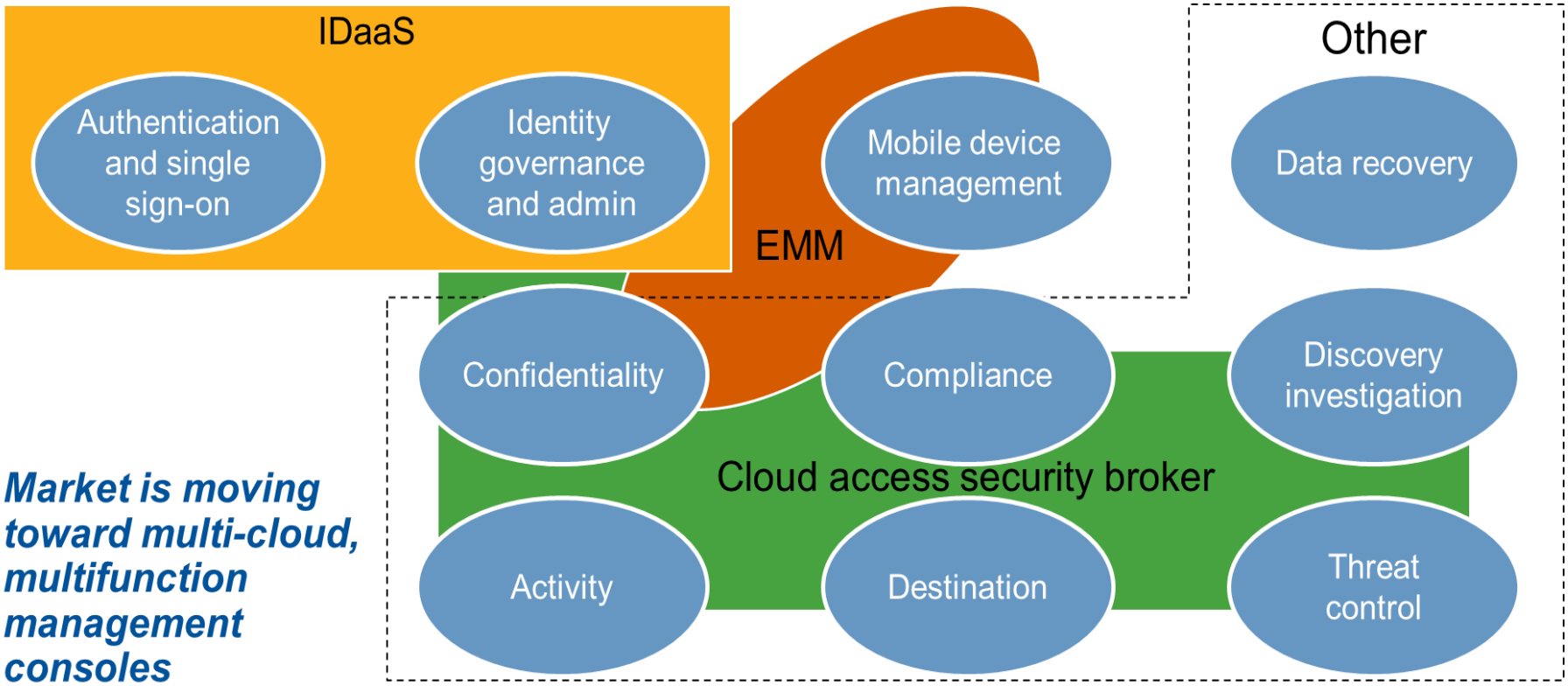
Are you treating encryption as a compliance fig leaf?

Evolving Cloud Encryption Approaches

- Relatively easy:
  - Extend data encryption to endpoints
- Becoming easier:
  - Customer-managed key (CMK)
- Difficult or impossible:
  - Format preserving
  - Searchable
  - Homomorphic

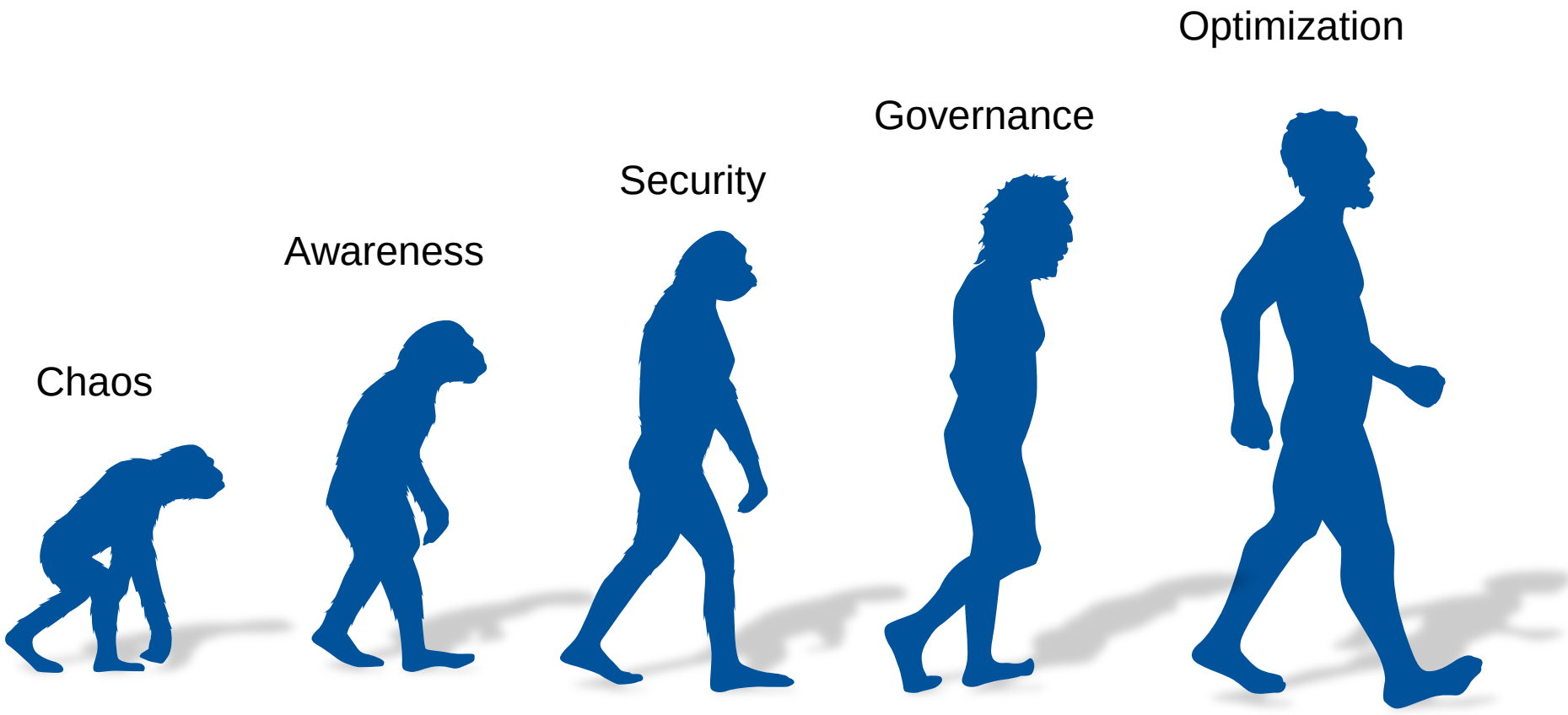
Externally applied encryption can break cloud application functionality

Growing Variety of SaaS Control Add-Ons



Market is moving toward multi-cloud, multifunction management consoles

How Evolved Is Your Cloud Control?



Don't stop at security

Recommendations

- ✓ Build cloud security and control competencies.
- ✓ Develop and enforce cloud governance policies:
  - Data classification and risk acceptance.
  - "Ownership" of data and departmental applications.
- ✓ Manage your accounts (especially privileged ones).
- ✓ Ensure that you have contingency plans.
- ✓ Demand that CSPs follow standards and provide third-party security assessments.

Be responsible for your own security.

Recommended Gartner Research

- Developing Your SaaS Governance Framework
  Jay Heiser (G00274895)
- Best Practices for Securing Workloads in Amazon Web Services
  Neil MacDonald and Greg Young (G00275221)
- A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic
  Paul E. Proctor, Daryl C. Plummer and Jay Heiser (G00261246)
- Cloud IaaS: Security Considerations
  Lydia Leong and Neil MacDonald (G00210095)
- Hype Cycle for Cloud Security, 2015
  Jay Heiser (G00272321)
- Everything You Know About SaaS Security Is Wrong
  Jay Heiser (G00260951)

For more information, stop by Gartner Research Zone.

Thanks