Securing the Cloud 2013

Kurtis E. Minder, CISSP

Goal

A general discussion on cloud trends, the security implications, problems, and the ecosystem of solutions on the market.

Disclaimer

I am not going to tell you how to secure the cloud.

I am going to talk about many vendor solutions, I am not an expert on any of them.

I will express my own opinions and they do not reflect those of Northwestern or of my current or past (or future) employers.

Please ask me questions.

I am going to ask you some questions too.

Agenda

me
CISSP
Cloud Definition
Cloud Uses
Cloud Security for Enterprise
Security for Cloud Infrastructure
Additional Concerns
Industry Response
Q&A

me.

18 Years in the Information Systems Industry
(12 Years in Infosec)

Many hats
(all white)

Security Engineering Background

Sales and Business Development

Product & Marketing

Services, Telecom, Appliance Vendors, Cloud

CISSP

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Management
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations, and Compliance
- Physical (Environmental) Security

The CISSP was the first credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

Cloud, Defined

NIST Definition*

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

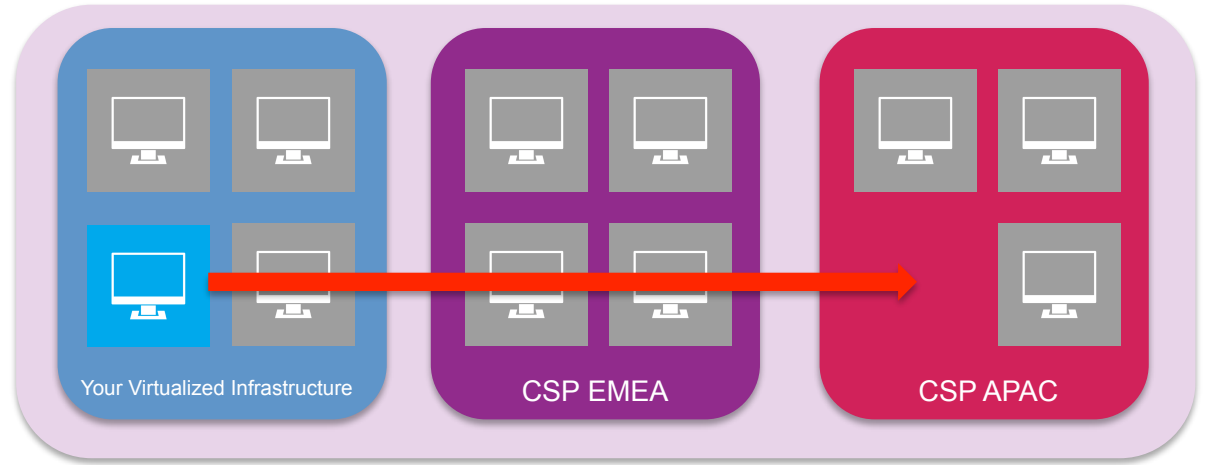
*SP800-145

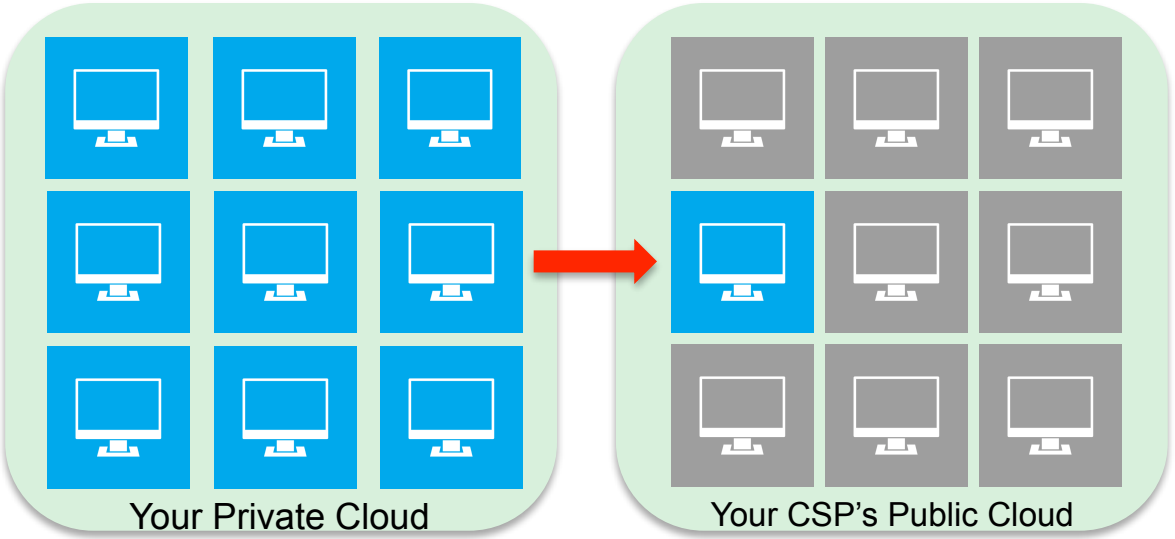
Cloud Computing Offerings

- **Infrastructure as a Service (IaaS)** (Sometimes Hardware as a Service HAAS)
  - Outsourcing of equipment to SP - Examples are Storage, Processing, “Elastic Computing”
- **Platform as a Service (PaaS)**
  - Outsourcing of the computing platform to SP - Allows for custom development and flexibility (OS or web platform delivered as a service)
- **Software as a Service (SaaS)**
  - Complete application outsourced (WP, SF.com, etc.)

Cloud Use Cases

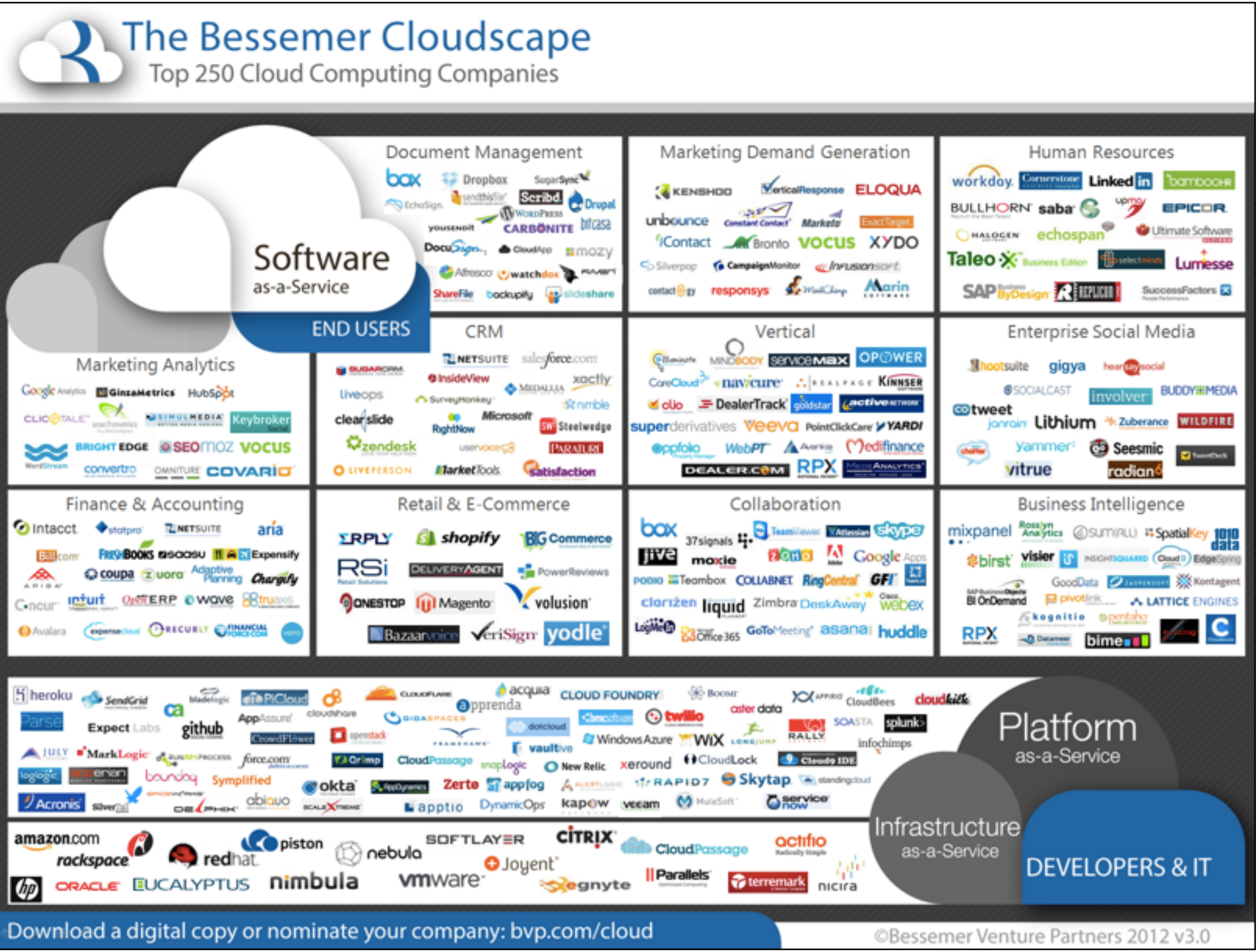
- Elastic Services
- Pay as you go
- Utility Computing
- No capital expenditure
- Offsite Storage
- Disaster Recovery
- App Replication
- Mobility Applications
- BYOD Support





The Bessemer Cloudscape

Top 250 Cloud Computing Companies



Download a digital copy or nominate your company: bvp.com/cloud

Cloud Security for Enterprise

How do I control these SaaS apps?

Too many security appliances!

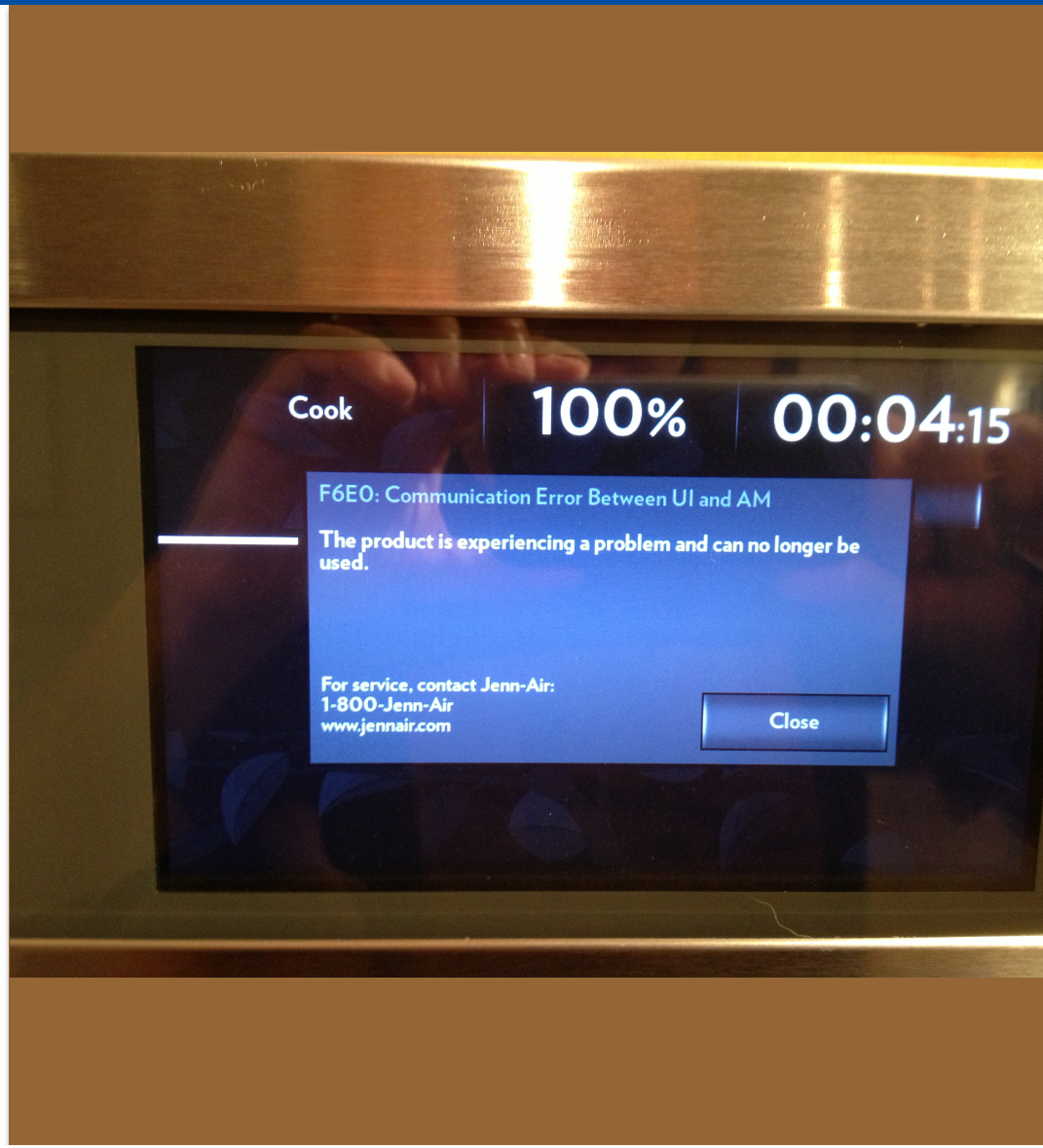
Is my data secure?

Who has access to what?

My users are using the cloud without me!
(Shadow IT)

How do I get rid of the appliances? The Cloud.

- Carrier / Service Provider Solutions
  - “Clean Pipe” or Security Services as a Utility
  - Shared Services Model (Multi-tenancy)
  - Integrating with the carrier backbone
- Vendor / Provider Solutions
  - Secure Web Gateway
  - DNSSec



Security as a Service

- Alternative to purchasing premise equipment
- Often provided by an Managed Security Services Provider / Carrier
- No capital expenditure
- Outsource log / compliance responsibilities

zscaler®

iMPERVA®

verizon

ArcticWolf™

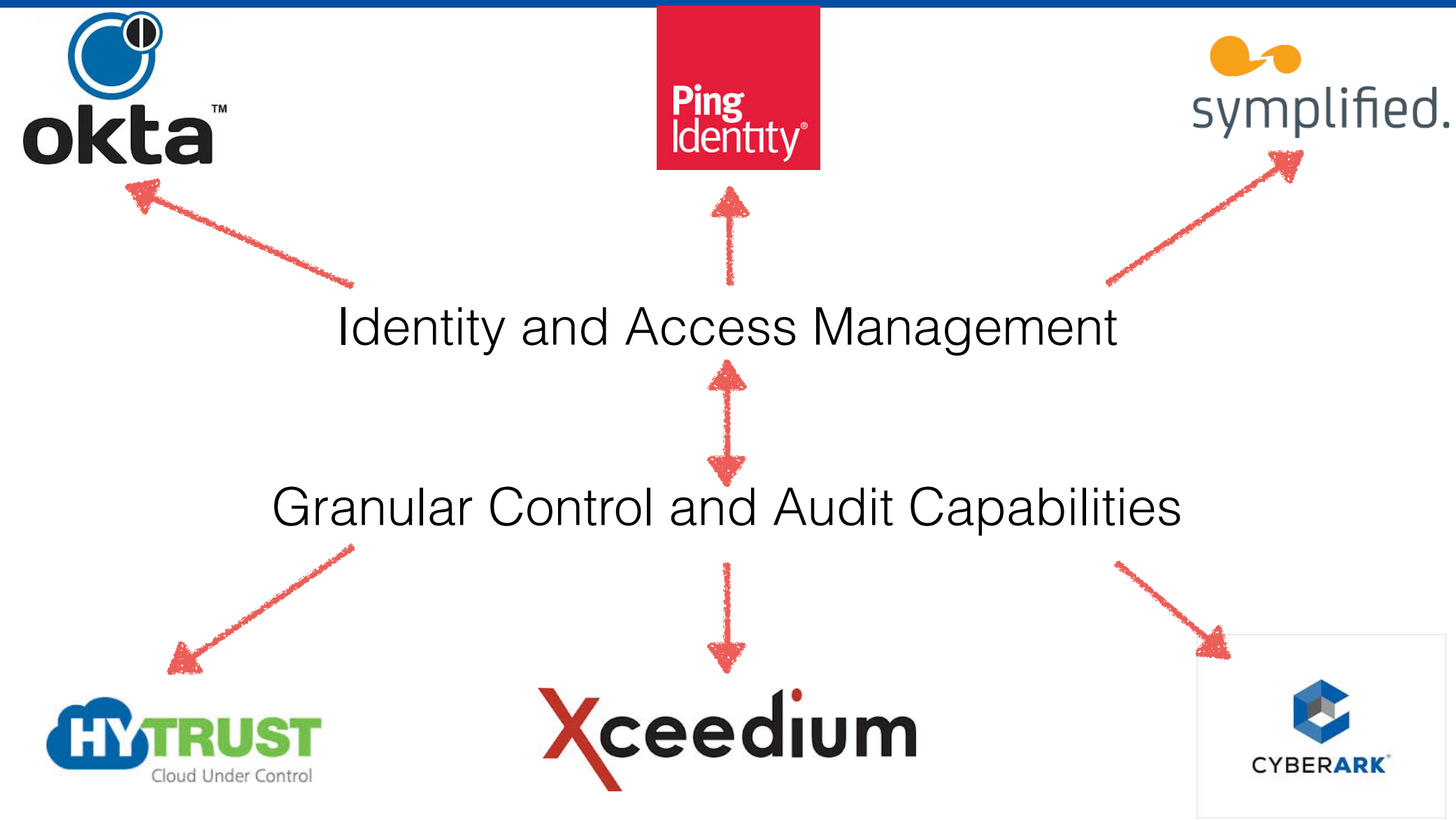
Securing the Data in the

Encryption.
Encapsulation.

Securing the data at rest (on disk)

Securing the data in use (in memory)

Access, Authorization



Control

"Shadow IT is a term often used to describe IT systems and IT solutions built and used inside organizations without organizational approval. It is also used, along with the term "Stealth IT," to describe solutions specified and deployed by departments other than the IT department."

This is easier to do now. Thanks Cloud.

Discover, audit, control….

skyhigh adallom netskope

Cloud Infrastructure

SAAS, IAAS, PAAS need Security!

Are there Security focused providers?

What are the traditional security players doing?

Securing THE Cloud

There are some service providers wholly focused on “Secure Cloud Services”.

Vendors have started to shift towards virtualized instances of their traditional security products.

There are virtualization specific solutions on the market providing security tailored to the unique problems in the space.

Additional Points

Is there anyone there to help?

Do I trust my CSP?

The law is catching up but……

Do you trust your CSP?

- Multi-tenant Data Stores...what does that mean?
- Cross contamination (CANVAS, CloudBurst)
  - If another cloud customer is compromised, can it spread?
  - Is the Hypervisor hardened?
  - How is log data handled/stored?
    - Forensics / Incident Response
- Many CSPs are now claiming “compliant clouds” where they have sponsored a data center level audit for FISMA, PCI, etc.
  - If this is the case, know that your assets were in scope!

The Legal Lag

- If an incident occurs, what is the provider's responsibility?
- How can log data be extracted? How quickly?
- Can data evidence be extracted in a legally admissible format?
- Does the contract allow you to run Incident Response test plans? Will the provider participate?

NIST References

NIST Definition of Cloud Computing: SP 800-145

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

U.S. Government Cloud Computing Technology Roadmap, Release 1.0: SP 500-293

FedRAMP = Federal Risk and Authorization Management Program

Cloud Security Alliance

- Vendor and customer supported organization driving standards in cloud computing and cloud security.
  - Sees itself as a “standards incubator”
  - Works closely with the Federal Government and NIST
  - Created the CSA S.T.A.R. Registry:
    - The CSA Security, Trust & Assurance Registry (STAR) is a publicly accessible registry that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering contracting with. It is a simple but powerful idea, cloud providers post self assessments of their cloud services, CSA makes these assessments publicly available and cloud consumers can use this data to make informed purchasing decisions.
  - Formulating a Cloud Trust Protocol to provide more transparency
    - “The CloudTrust Protocol (CTP) is the mechanism by which cloud service consumers (also known as “cloud users” or “cloud service owners”) ask for and receive information about the elements of transparency as applied to cloud service providers.”

Security Guidance

Security Guidance for Critical Areas of Focus in Cloud Computing.14 Domains - Version 3.0
http://www.cloudsecurityalliance.org

Cloud Architecture

Governance and Enterprise Risk Management

Legal: Contracts and Electronic Discovery

Compliance and Audit

Information Management and Data Security

Portability and Interoperability

Traditional Security

Business Continuity and Disaster Recovery

Data Center Operations

Incident Response

Notification and Remediation

Application Security

Encryption and Key Management

Identity and Access Management

Virtualization and Security as a Service

Concluding

The Cloud is providing tremendous opportunity for efficiency in the enterprise

It is also breaking things.

Solutions abound, be ready for an onslaught of vendor fixes.

Have a plan.

Collaborate with the standards bodies like CSA.

Follow NIST publications on Cloud and InfoSec.

Danke!

Questions?

Need to reach me?

Kurtis Minder - kurtis@kurtisminder.com - 847-902-3325 (m)

kurtisminder (Skype)

www.linkedin.com/in/kurtisminder

@kurtisminder (Twitter)