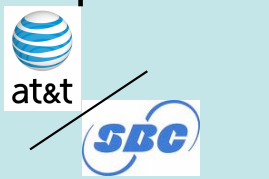
# SECURITY MODELS FOR CLOUD 2012

Kurtis E. Minder, CISSP

# INTRODUCTION

***Kurtis E. Minder, Technical Sales Professional***

## Companies:






## Roles:

- Security Design Engineer
- Systems Engineer
- Sales Engineer
- Salesperson
- Business Development
- Global Account Manager

## Actual work:

- Installation / Configuration
- Design
- Support
- Product development / POC
- Audit
- Penetration testing
- Sales / BD


# CISSP CERTIFICATION

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

# AGENDA


- Cloud, Defined
- The Business Need
- Cloud Security Models
  - Cloud Security
  - Security for Cloud Apps
  - Additional Security Concerns

# 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

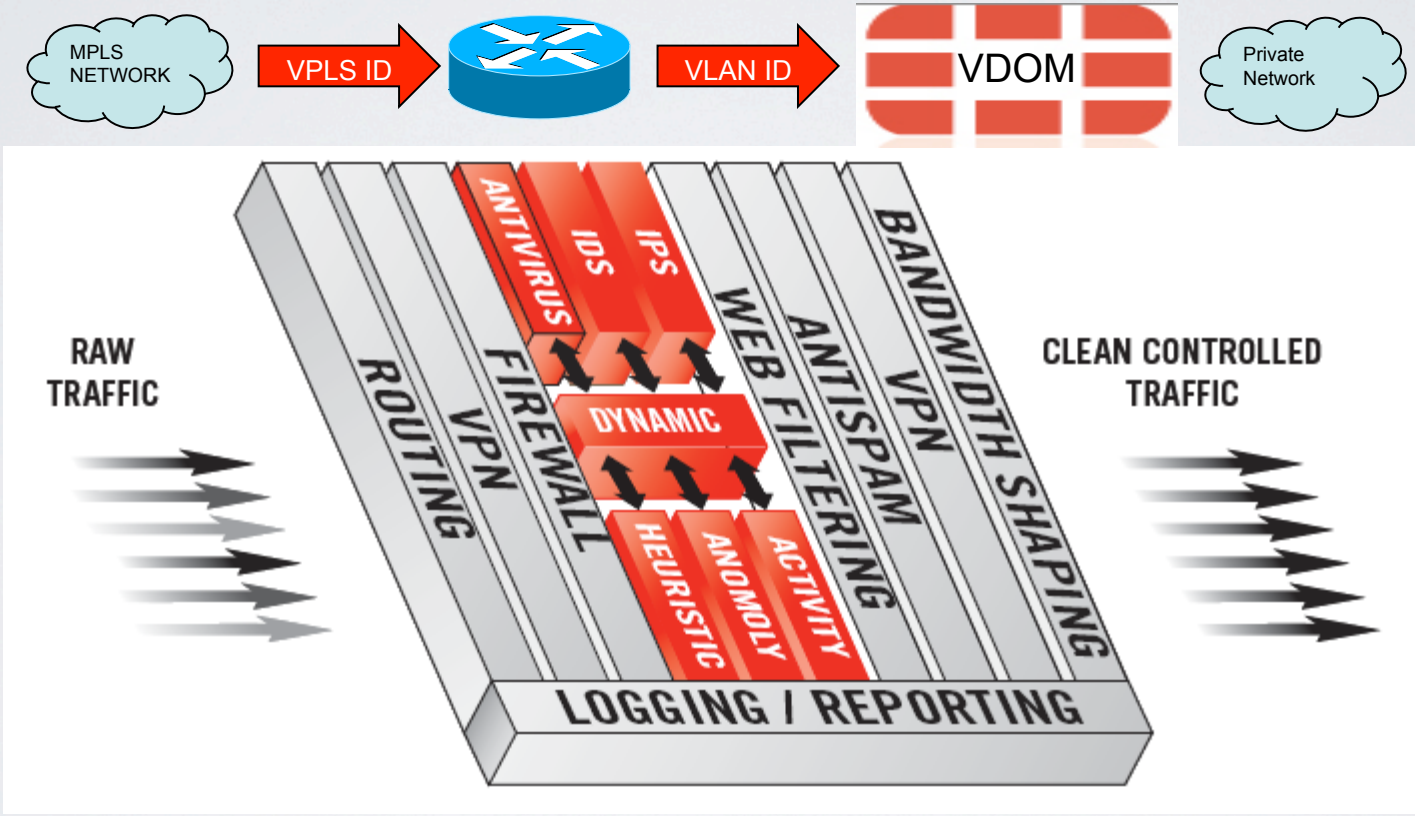
- Cloud Security, what does that mean?
  - "Clean Pipe" or Security Services as a Utility
  - Shared Services Model (Multi-tenancy)
  - Integrating with the carrier backbone
- Cloud Computing
  - SAAS, IAAS, PAAS need Security!
  - How to provision? Is it VM? Is it appliance?
  - Securing YOUR access to Cloud resources


# SECURITY AS A SERVICE

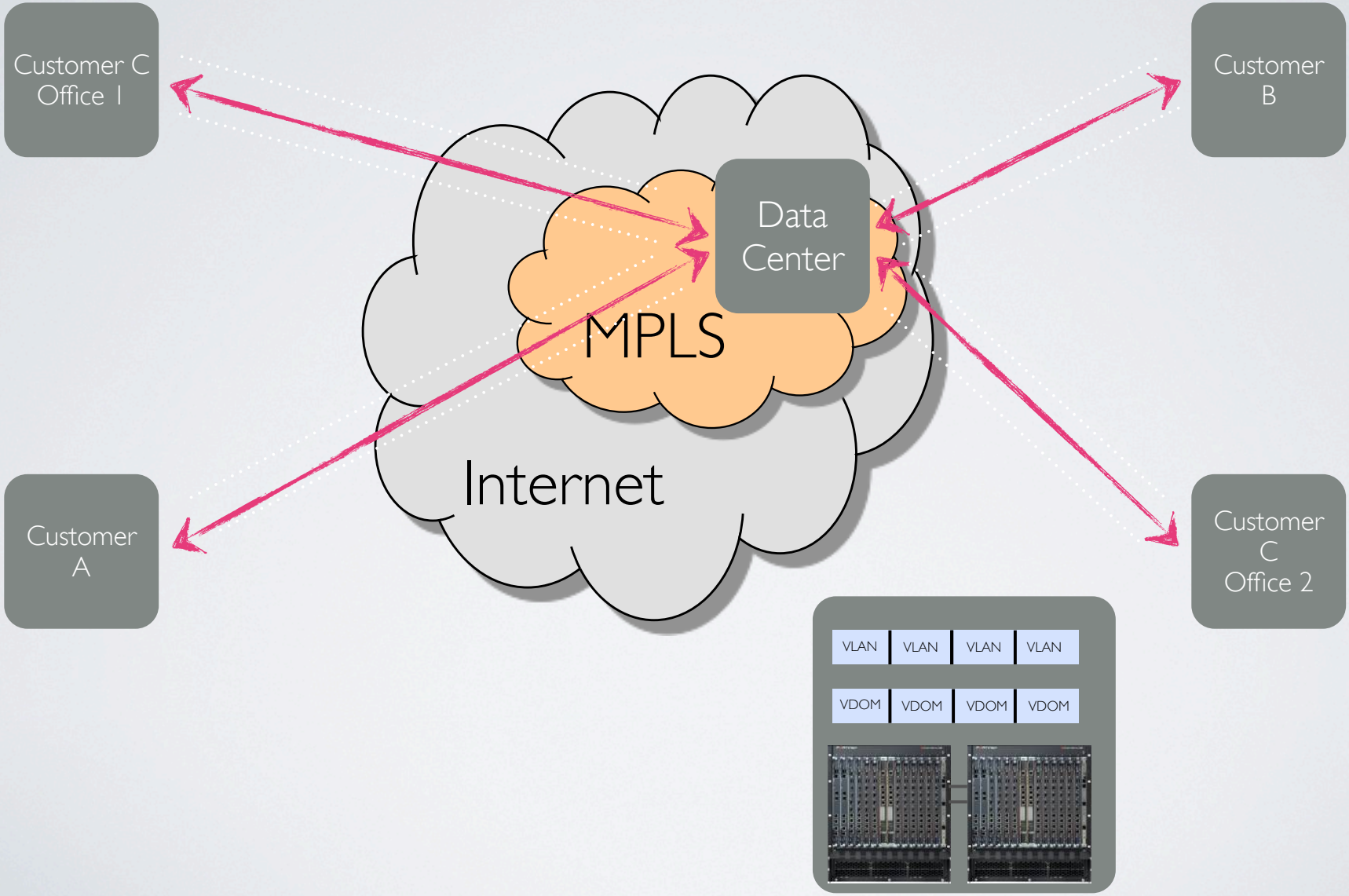
# SECURITY AS A SERVICE (CLOUD SECURITY)

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

# CLOUD SECURITY / CLEAN PIPE



# CLOUD SECURITY EXAMPLE




# CLOUD COMPUTING / SECURITY

# WHY MOVE TO CLOUD COMPUTING?

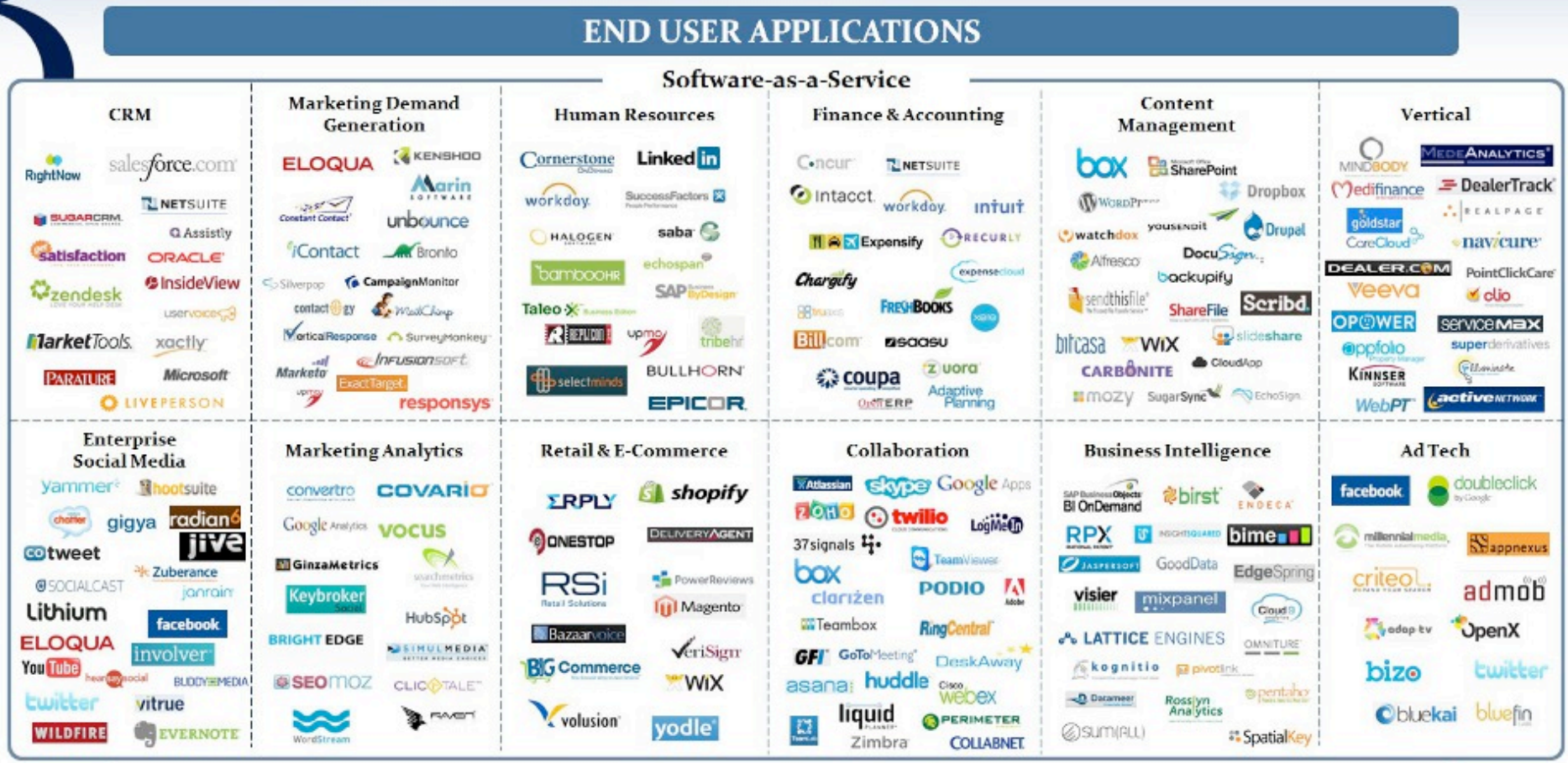
- Elastic Services
- Pay as you go
- Utility Computing
- No capital expenditure

- Offsite Storage
- Disaster Recovery App Replication
- Mobility applications
  - **BYOD Support**

# CLOUD COMPUTING OFFERINGS

- **Infrastructure as a Service** (Sometimes Hardware as a Service HAAS)
  - Outsourcing of equipment to SP - Examples are Storage, Processing, "Elastic Computing"
- **Platform as a Service**
  - 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**
  - Complete application outsourced (WP, SF.com, etc.)
-

# Bessemer Venture Partners Cloudscape




BESSEMER VENTURE PARTNERS

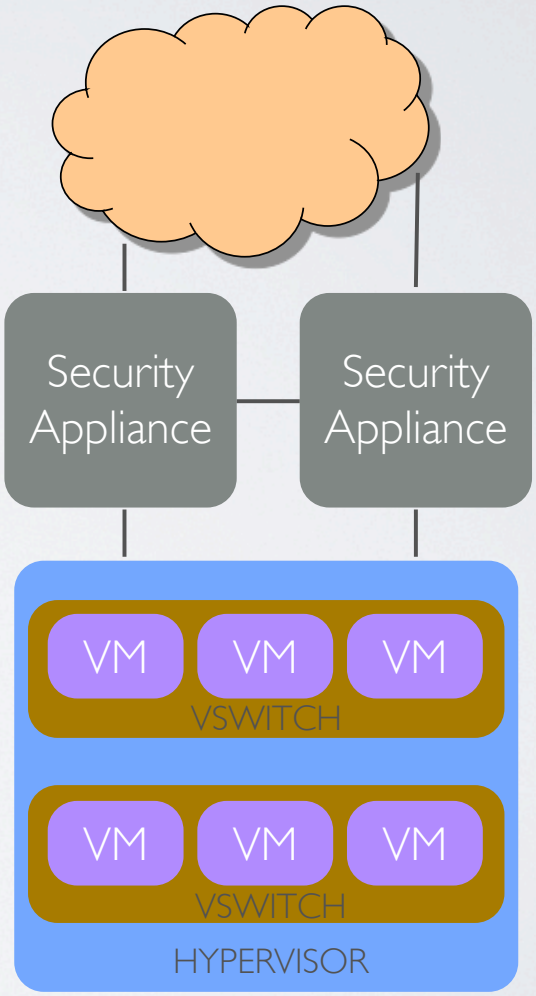
# SECURING CLOUD APPLICATIONS

- Most cloud applications are virtualized
- Hypervisor is a fundamental component
  - Hypervisor is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. However, the hypervisor is actually controlling the host processor and resources, allocating what is needed to each operating system in turn and making sure that the guest operating systems (called virtual machines) cannot disrupt each other. *
- Three primary methods of securing cloud apps
  - Extra-Hypervisor
  - Intra-Hypervisor
  - Host

*thanks techtarget

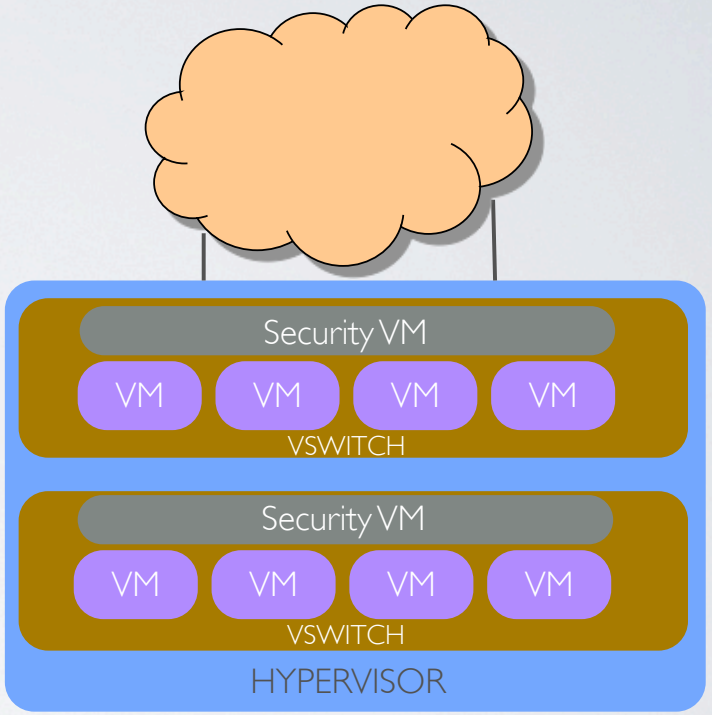
# EXTRA-HYPERVISOR SECURITY

- Outside the VM platform
- Typically an appliance
- Pros: Fast / Mature
- Cons: Lack of Visibility into VM space



# INTRA-HYPERVISOR SECURITY

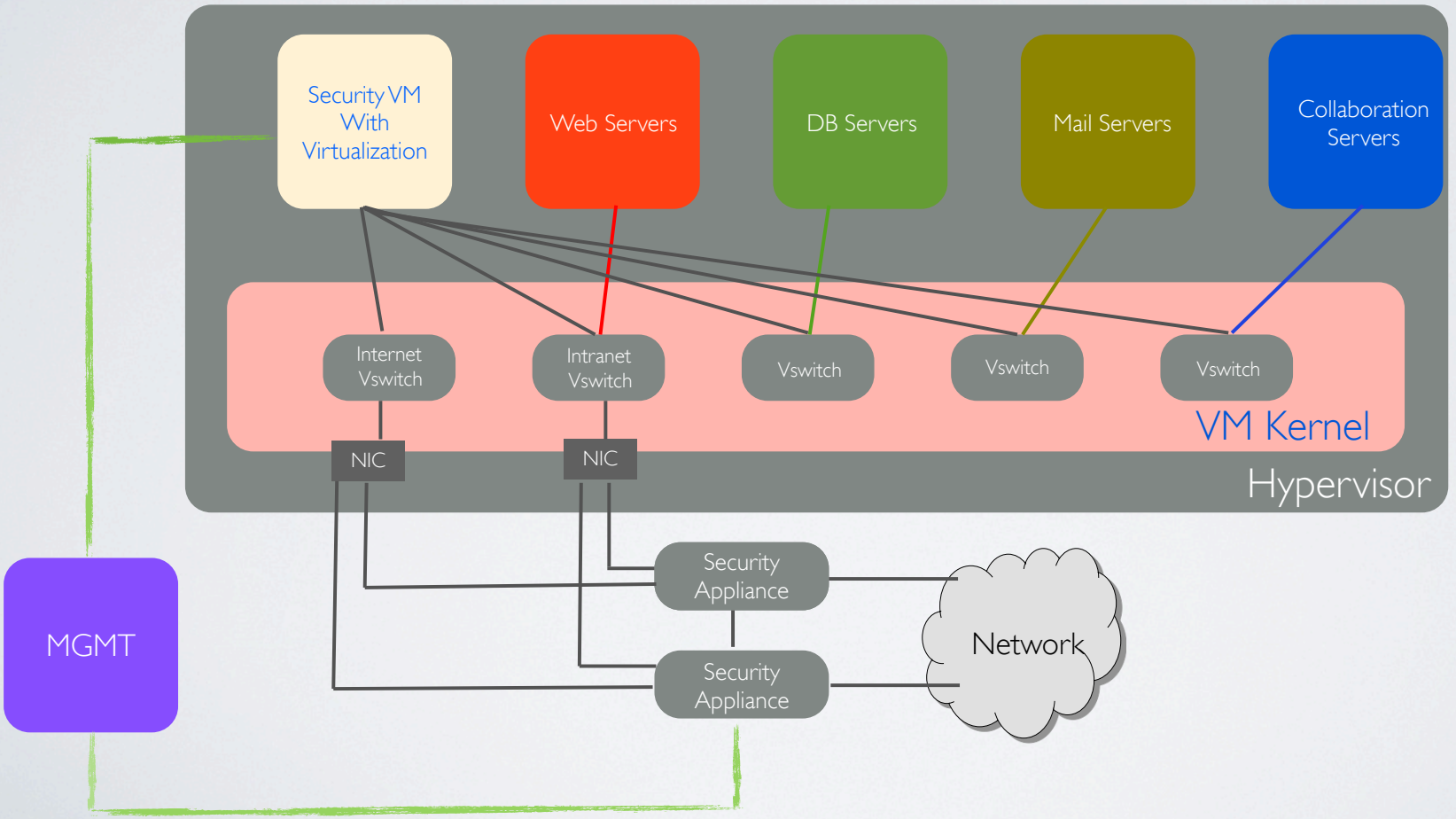
- VM based
- Typically leverages API for integration with the hypervisor
- Pros: Visibility to intra-VM communication
- Cons: Takes CPU from VM



# THE VM SECURITY PROBLEM

- VSwitch is not a switch
- Hypervisor vendors have limited APIs
- High Availability is more complicated
- Takes Resources from VM application operations
- *Easy* to create new applications!

# COMBINED ARCHITECTURE



# ADDITIONAL SECURITY CONCERNS

# DO YOU *TRUST* YOUR PROVIDER?

- Multi-tenant Data Stores...what does that mean?
- Cross contamination
  - If another cloud customer is compromised, can it spread?
  - Is the Hypervisor hardened?
  - How is log data handled/stored?
    - Forensics / Incident Response

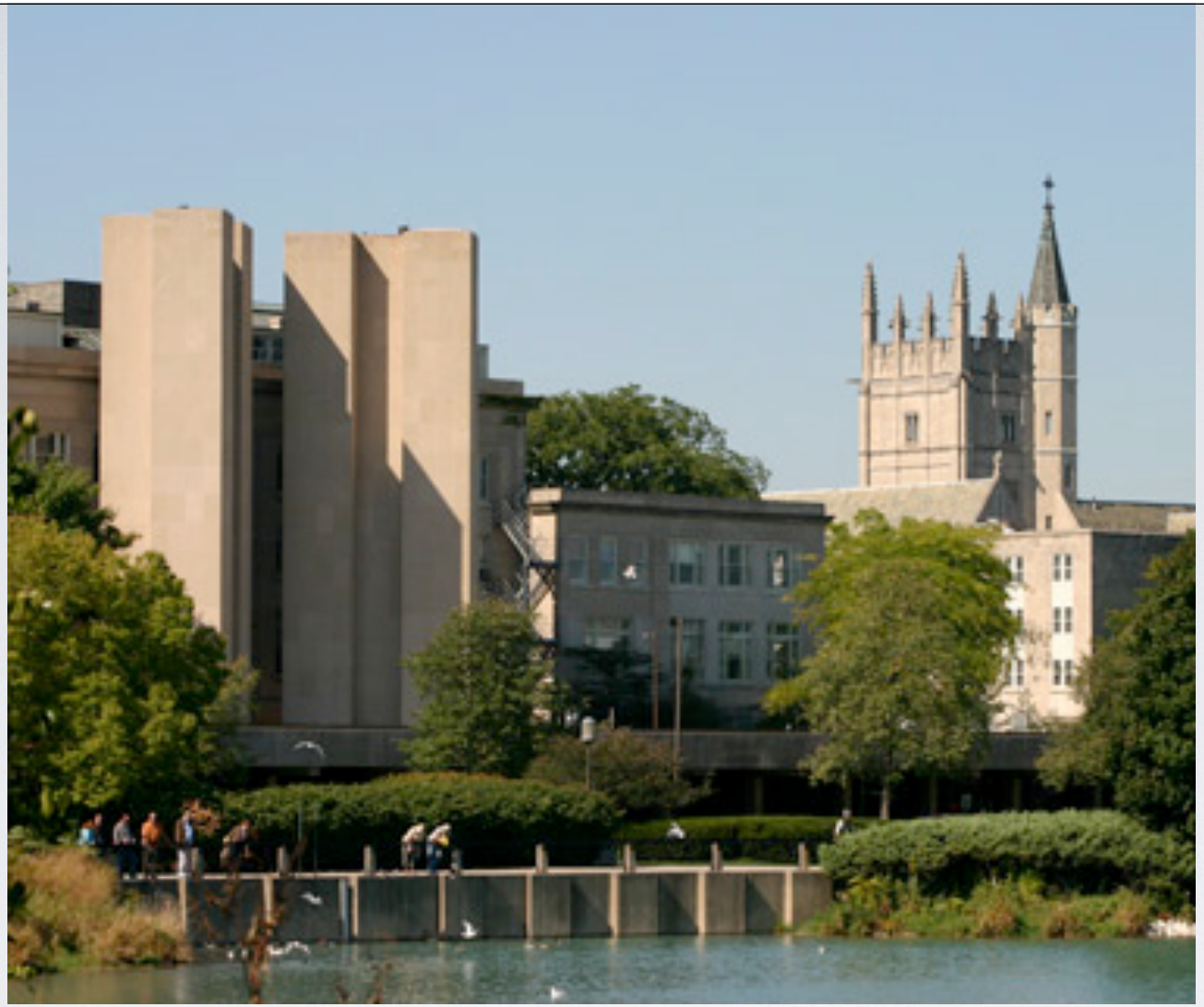
# DO YOU TRUST YOUR ANALYSTS?

- How do you control how many cloud apps are spun up and why?
- How do you keep employees from violating policy in the cloud?

amazon web services™

# 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?



# CLOUD SECURITY ALLIANCE AND NIST

# 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 (CSA)

- 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

# 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

# CSA STAR

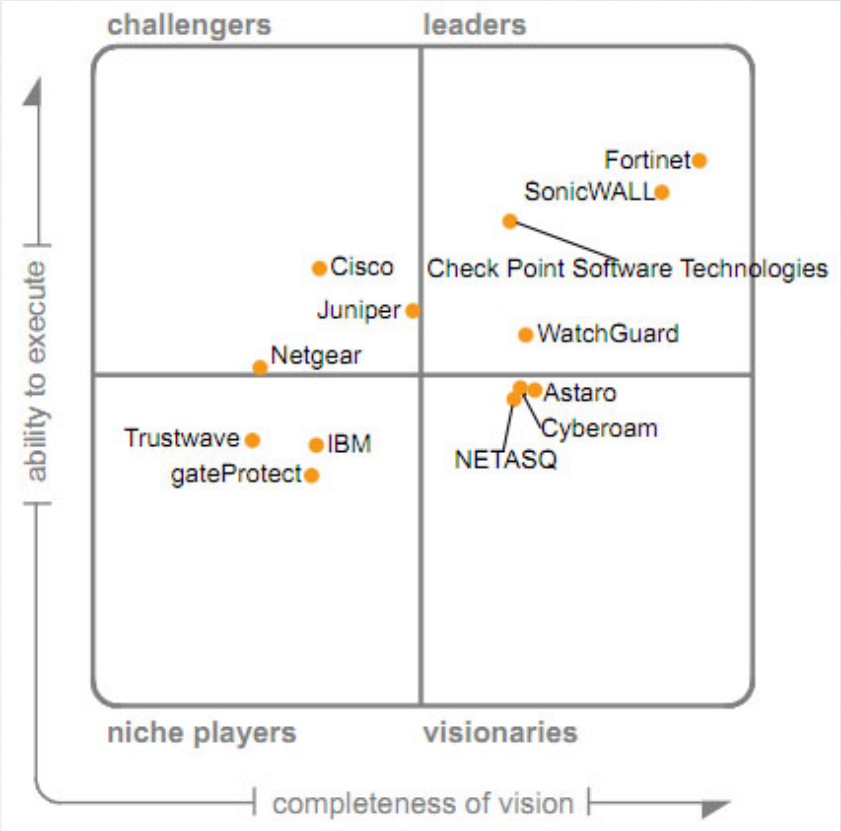
- STAR = CSA SECURITY, TRUST AND ASSURANCE REGISTRY
  - Cloud providers self assess their security
  - Launched in Q4 of 2011
  - https://cloudsecurityalliance.org/star/faq/

# CONCLUDING

- Business finance objectives pushing enterprises to the cloud
- Managed Services / Utility and Cloud Security offers a viable alternative to self managed
- Evolution of physical to virtual driving security architecture in new directions
- Policy, Process must be automated to ensure proper compliance and protection for virtual assets
- The legal and audit standards have not caught up to cloud adoption

# I WORK @ FTNT

- Founded in 2000
- Nasdaq Listed FTNT
- ~2000 Employees
- Over 1M units shipped
- Over 100k customers



# THANK YOU!

- Questions?
- Need to reach me?
- Kurtis Minder - kurtis@kurtisminder.com - 847-902-3325 (m)
- kurtisminder (Skype)