Security and Forensics from a Cloud Provider’s Perspective

SECURING THE CLOUD

About me. About this talk.

Introduction

About TMRK and me

- Terremark, a Verizon Company
  - Full stack of services: colo, hosting, cloud, security
  - Strong Federal/Public Sector business
- Secure Information Services
  - History with IR against TAGs
  - Analytics is the operational piece
  - Years of eating our own dog food

Federal Datacenter Consolidation

- Improve efficiencies in government IT
  - Express goal of reducing number of datacenters, amount of square feet, and number of servers
  - Shared services (multi-tenancy) is a core concept
- Cloud is the leading approach
  - Many agencies have already moved key processing to the cloud
  - As successful deployments add up, the rate of adoption is accelerating
- Perceived concerns around security and forensics
  - There are good answers!

Cloud Infrastructure is different

- Cloud technologies bring new possibilities
  - Data/image acquisition techniques
  - In situ analysis
- They also brings challenges
  - Privacy & secure data separation
  - Implications for operational continuity
- Vague models and mismatched expectations
  - Who's responsible for the security of what?

Cloud Infrastructure is not magic

- Cloud infrastructure is still infrastructure
  - Providers manage at least a hypervisor farm and back-end equipment (IaaS)
  - PaaS and SaaS control more and more of the underlying platforms
- I'll be talking mostly about IaaS
  - PaaS and SaaS looks more like a specific application
    - Integrated into a larger customer environment
    - Forensics are more specialized, out of scope for this talk
  - **But** PaaS and SaaS providers usually run IaaS environments under the hood, so much of this applies.

How are clouds built? Managed? Secured?

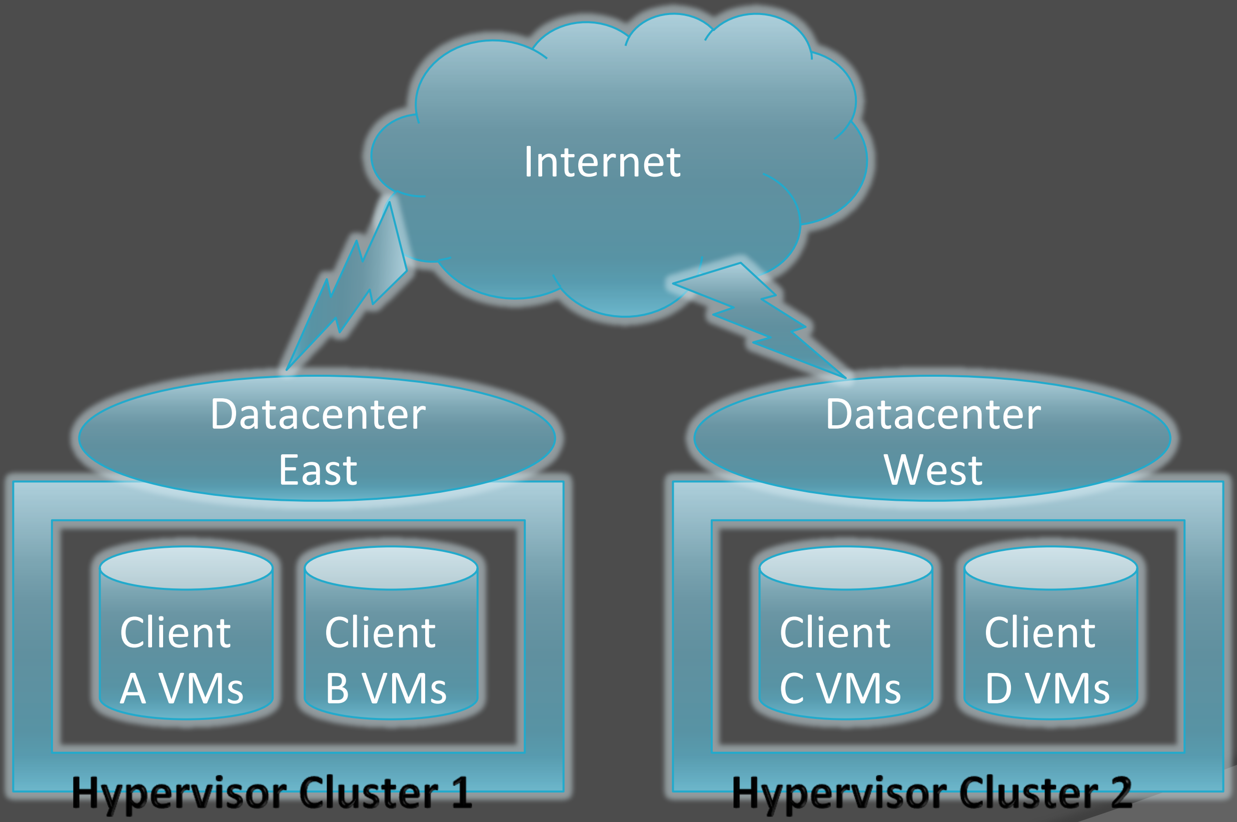
What’s different, from a forensics point of view?

Overview of Cloud Operations

Infrastructure is (mostly) the same

- Cloud providers build big clusters
  - Racks of compute
  - Racks of storage
- Value-add is in the multi-tenancy
  - Front-end software for users
  - Back-end software for support staff
- Differentiation is in add-ons and services
  - Integrated security, back-up, and other services
  - Better plumbing, support, and overall flexibility

Ye Olde Cloud Architecture



Internet

Datacenter East

Datacenter West

Client A VMs

Client B VMs

Client C VMs

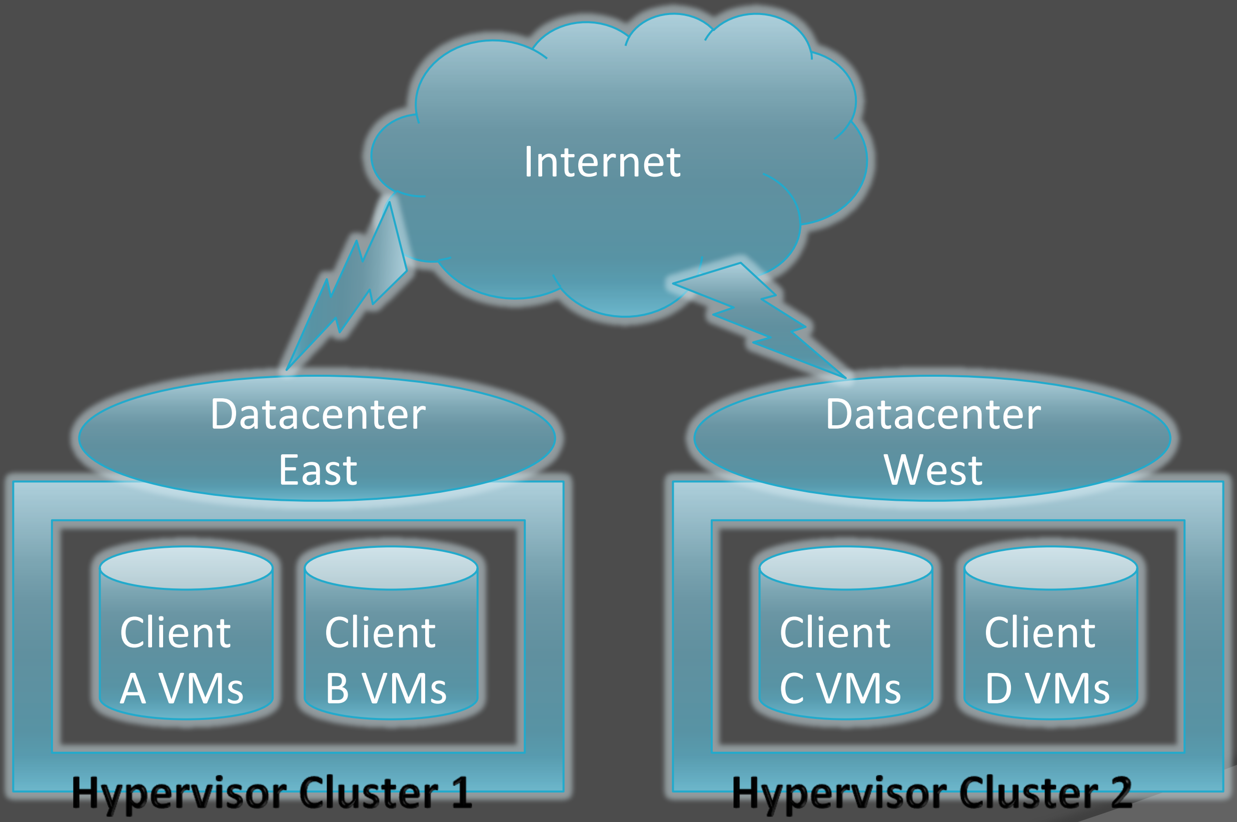
Client D VMs

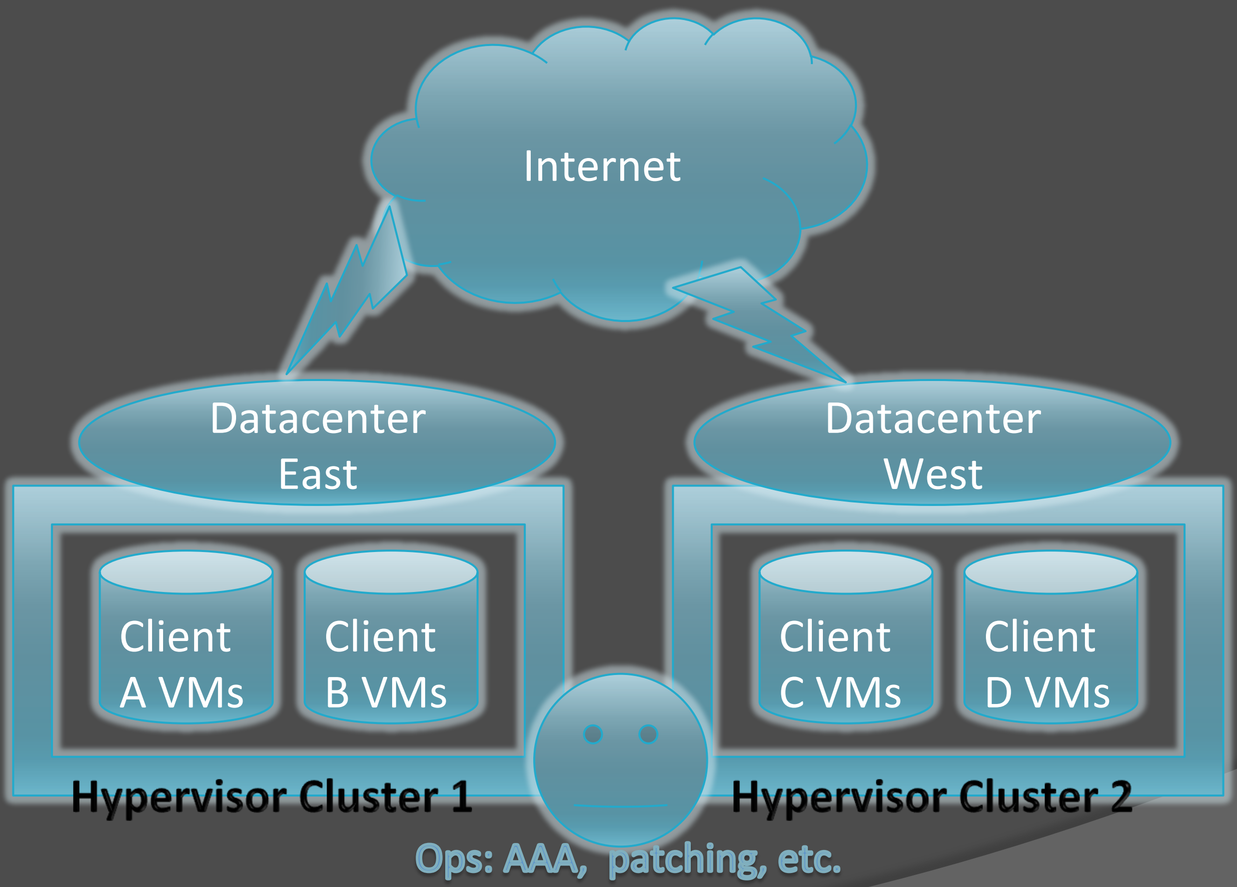
Hypervisor Cluster 1

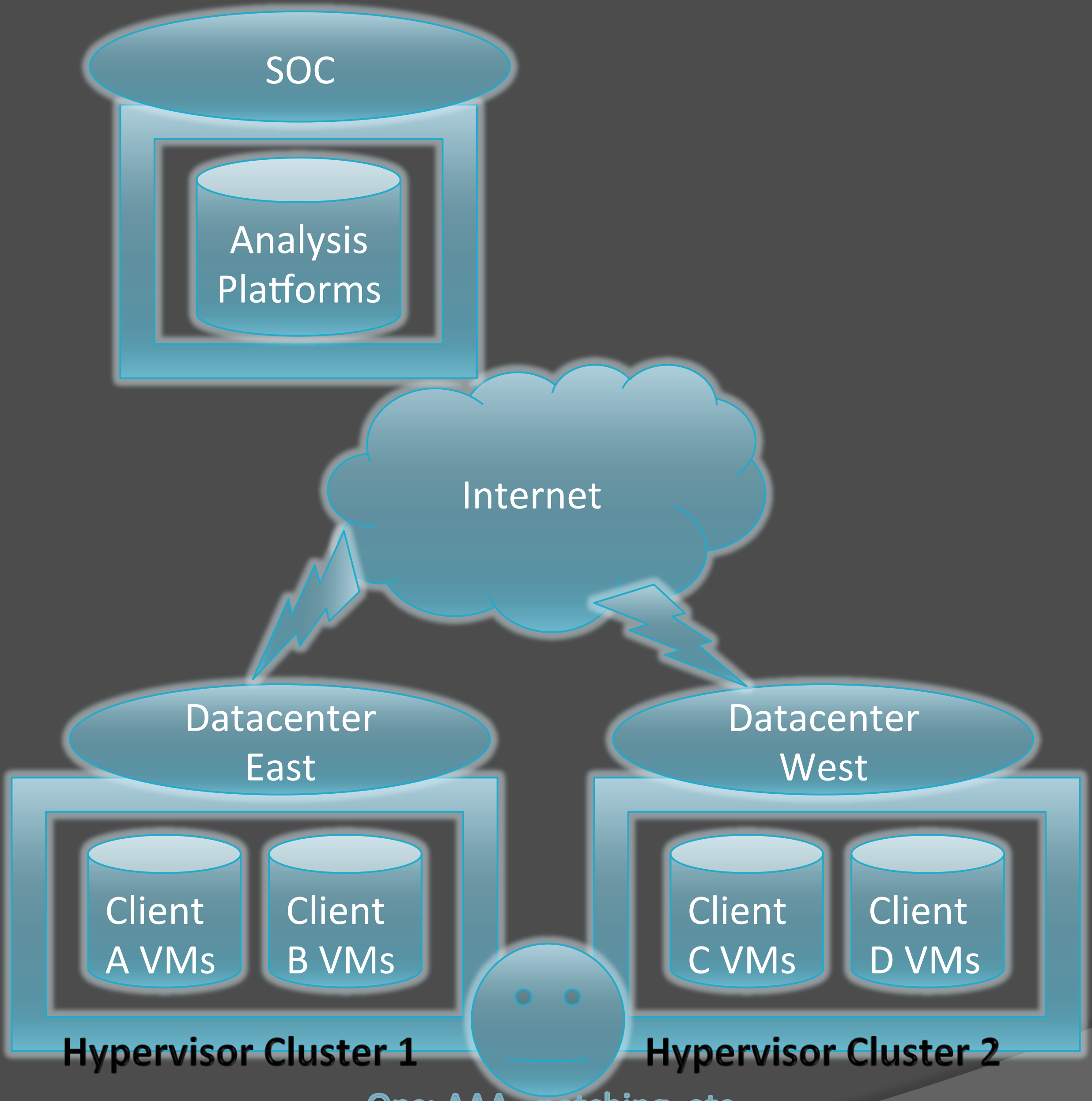
Hypervisor Cluster 2

Cloud Security is (mostly) security

- Providers still need to solve the classical problems
- At a high level: Visibility, instrumentation, staffing, operational integration
- Specific examples: Patching, firewalls, IDS, A/V
- Here again, multi-tenancy is the heart of the Cloud difference
    - Shared instrumentation for greater ROI
    - Analysis across multiple customers for enhanced situational awareness


Internet
Datacenter East
Datacenter West
Client A VMs
Client B VMs
Client C VMs
Client D VMs
Hypervisor Cluster 1
Hypervisor Cluster 2


Internet
Datacenter East
Datacenter West
Client A VMs
Client B VMs
Client C VMs
Client D VMs
Hypervisor Cluster 1
Hypervisor Cluster 2
Ops: AAA, patching, etc.



SOC

Analysis Platforms

Internet

Datacenter East

Datacenter West

Client A VMs

Client B VMs

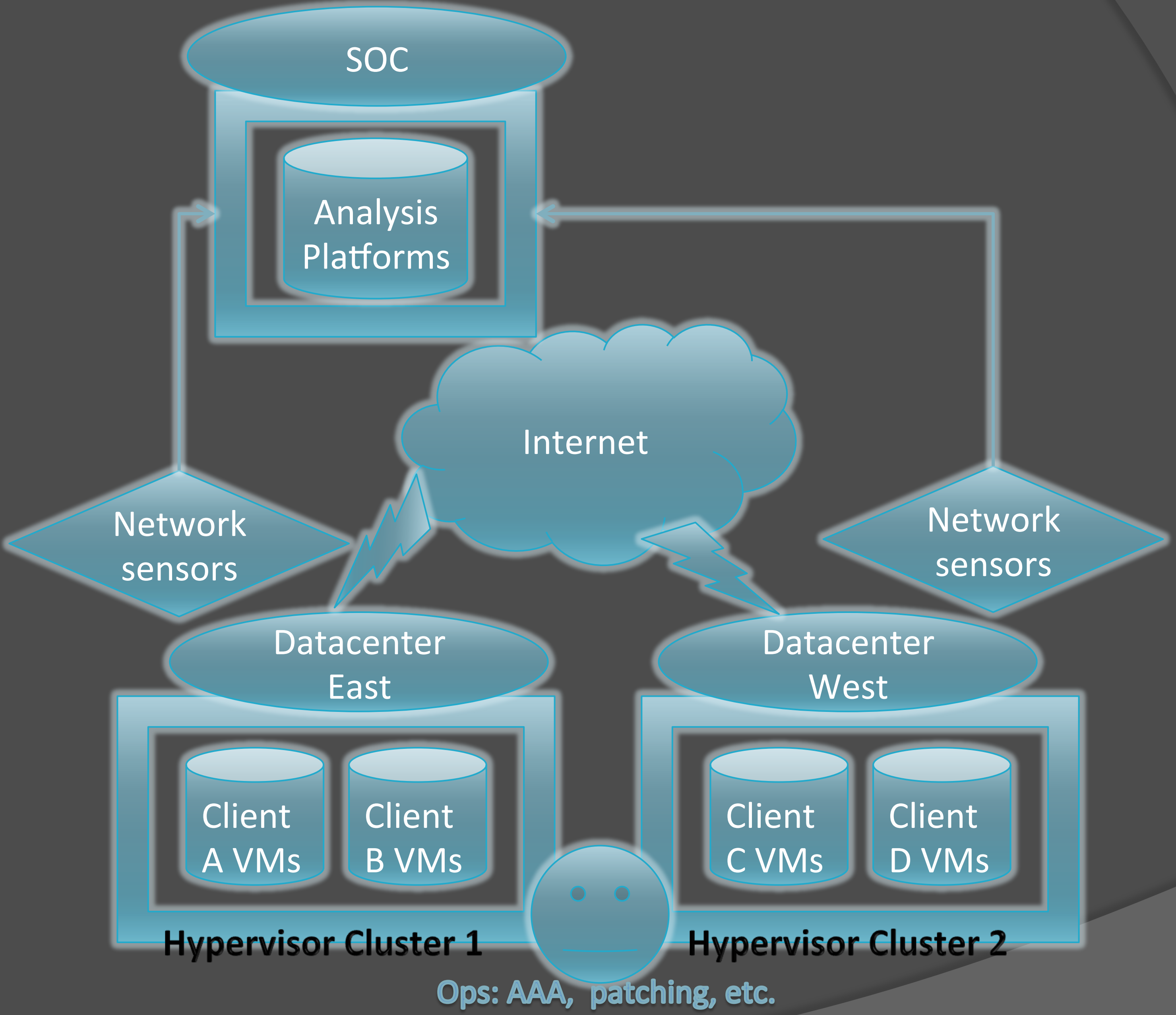
Client C VMs

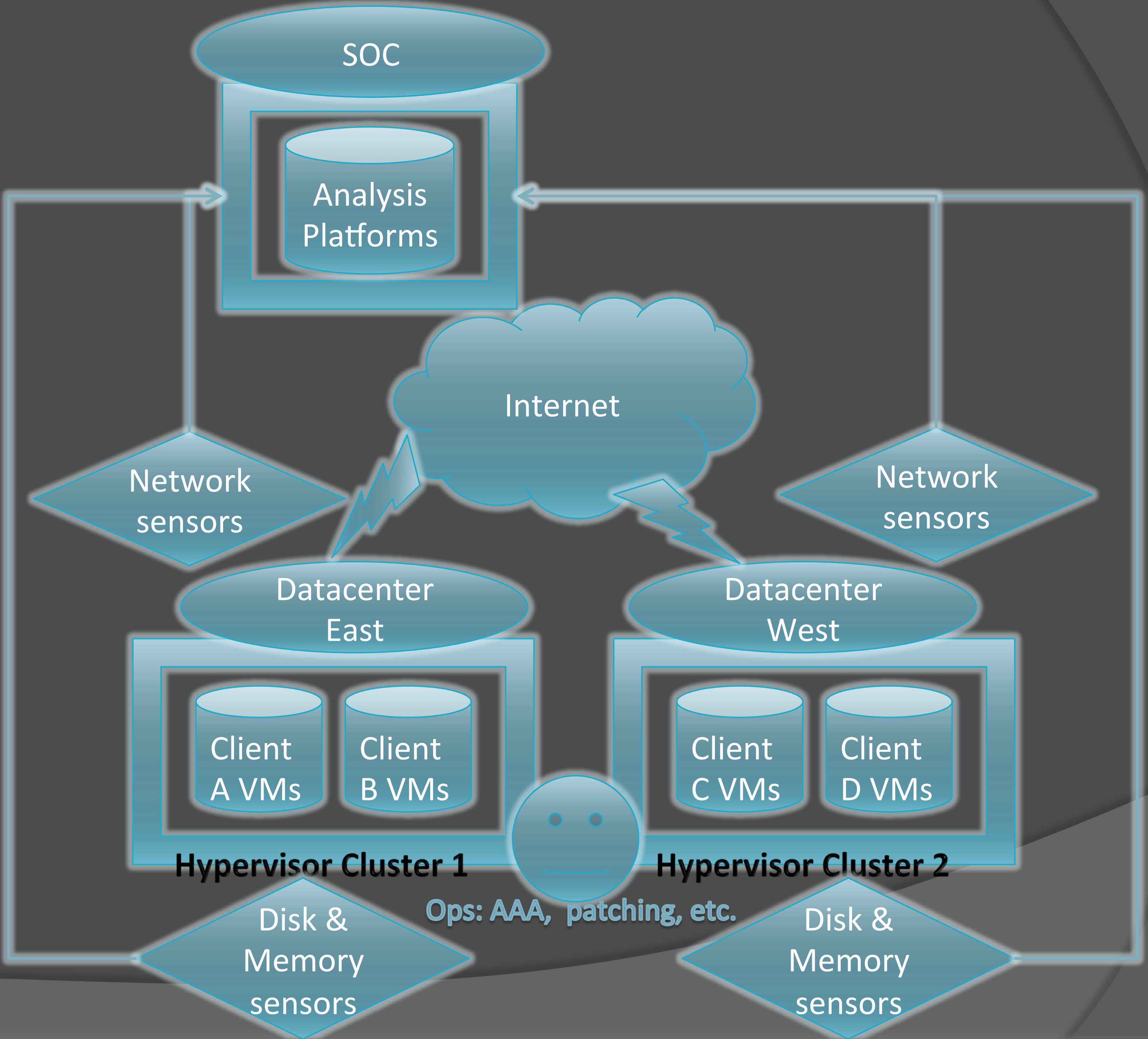
Client D VMs

Hypervisor Cluster 1

Hypervisor Cluster 2

Ops: AAA, patching, etc.


SOC
Analysis Platforms
Internet
Network sensors
Network sensors
Datacenter East
Datacenter West
Client A VMs
Client B VMs
Client C VMs
Client D VMs
Hypervisor Cluster 1
Hypervisor Cluster 2
Ops: AAA, patching, etc.


SOC
Analysis Platforms
Internet
Network sensors
Network sensors
Datacenter East
Datacenter West
Client A VMs
Client B VMs
Client C VMs
Client D VMs
Hypervisor Cluster 1
Hypervisor Cluster 2
Ops: AAA, patching, etc.
Disk & Memory sensors
Disk & Memory sensors

Cloud Forensics is (mostly) the same

- It all rests on solid fundamentals:
  - Identifying relevant data
  - Forensically sound acquisition and analysis
- I.e., disk and log data, as well as memory forensics and other emerging disciplines
- Multi-tenancy is one big difference
  - Implications of a shared environment
  - Side-effects matter, too: centralized log aggregation, integrated backup data available, etc.
- Ubiquitous virtualization is another
  - Whole world of TTPs become available
  - E.g., snapshots are always possible

Cloud as a kind of outsourcing

- Consider classical approaches to full-service outsourcing
  - Outside firm (EDS, GDIT, etc.)
  - Contractual guarantees for performance and security
  - Benefits include reduced cost, better access to expertise
  - Challenges include clear priorities and responsibilities
- Cloud is fundamentally similar
  - Ubiquitous virtualization is core enabler
  - Lower entry barrier for providers, so more vendors, feature sets, and price points

Full vs. Partial resource allocation.

Virtual-only vs. Physical instrumentation.

Practical Application in Popular Operating Models

Full Resource Allocation

- Capacity to run all customers at 100%
  - Excess capacity can be used for “burst”
  - Guaranteed minimum performance
- Tend to be more robust infrastructures
  - Target market values uptime and security
  - More investment in instrumentation, etc.
- Tend to be more full-service providers
  - Managed services layered over base cloud

Partial Resource Allocation

- More optimized use of physical resources
  - Less wasted infrastructure == lower cost
  - Ad-hoc resource allocation == complex data isolation
- Cost-sensitive target market
  - Developers, startups, incubators, etc.
  - Quick PoC deployments
- More of a Wild West feel
  - Bad guys fit the target market description

Physical Instrumentation

- Psst! There's a physical infrastructure here!
  - Visibility resolution depends on details
  - Lots of COTS instrumentation available
  - Easier to guarantee no impact from sensors
- More precisely: non-virtualization-aware
  - Leverage the same stack for cloud and non-cloud
  - Instrument hosts at the OS level: very doable

Virtual-only Instrumentation

- Leverage hypervisor for visibility
  - Network, memory, disk visibility possible
  - Access methods are varied and ever-changing
- Growing number of “virtual appliances”
  - Many of these are non-virtualization-aware!

Privacy and data separation. Isolating operational impacts. Dealing with well-meaning but uninformed courts and LE.

Challenges Unique to the Cloud

Privacy and data separation

- Multi-tenancy implies logical, rather than physical data separation
- Configuration management is critical
  - For cloud providers performing IR or forensics
  - Need multiple logical control layers to compensate
  - Still, sometimes a small difference in control configuration is the only barrier
- IR or forensics often done by other party
  - Thorough work would uncover any data leakage from other customer environments…

Isolating operational impact

- Various ways a single customer can impact performance
  - Malicious activity or compromised environment
  - Normal operation of non-optimized application
  - During IR/subpoena/etc: forensic activity is IO-intensive
- No room for operational fragility
  - Robust workload distribution
  - Consider impacts of specialized activities

Collaborating with courts and LE

- Courts and agencies often optimized to deal with non-Cloud environments
  - E.g., with physical disk imaging tools, etc.
- Often don't understand the impact of their requests
  - Overly-specific subpoenas may specify actual steps to be taken
  - More effective and efficient techniques may be available
- Providers should nurture relationships with local, state and federal LE

Solid infrastructure foundations. Tools for customer-specific visibility and control. Processes for graceful degradation.

Solutions to Cloud-Specific Challenges

Prerequisite: solid foundations

- Controls
  - Part of a robust cloud architecture
  - Layered and tightly managed
- Documentation
  - Transparency can validate TTPs
- Skill sets
  - Deep collaboration among specialist teams
  - Network, OS, compute, storage, security, …

Fraud Detection

- Technological
  - Anomalous environment configurations
  - Learn patterns of fraudulent behavior
- Contractual
  - E.g., require up-front payments
  - Impactful to legitimate small customers
- Operational
  - E.g., verify contact information

Resource constraints

- Technological
  - Robust performance monitoring
  - Graceful performance degradation
- Contractual
  - Allow flexibility in case of performance impacts
  - Dedicated resources makes this easy
- Operational
  - Disciplined capacity planning

Comfort level for LE

- Technological
  - Graceful degradation and isolation for acquisition
  - Compatibility with tools common in LE use
- Contractual
  - Notification and transparency requirements
  - Reduced SLAs during subpoenas or etc.
- Operational
  - Explicitly plan for likely LEO interactions

Chops == Chops. Prepare for the operational differences.

Conclusions

Lean on the Fundamentals

- Take care about multi-tenancy
  - Respect customer privacy
  - Isolate operational impacts
- Several unique benefits
  - Snapshots and related techniques are a godsend
  - Prepare for in situ analysis to avoid data transfer
- Most of the forensic problem is very similar
  - Your non-cloud experience will serve you well

Prepare for the differences

- Get access to multiple cloud environments
  - Individual providers as well as mash-ups
  - Set up forensic scenarios to work through
- Make a cloud-specific toolkit
  - Most in situ analysis requires a tooled-up VM
  - Have tools to deal with various snapshot formats
- Contact cloud providers
  - They can give you valuable insight for when your next case involves their infrastructure

Thank you!   Questions?