sentrigo™

Securing Sensitive Data in the Cloud

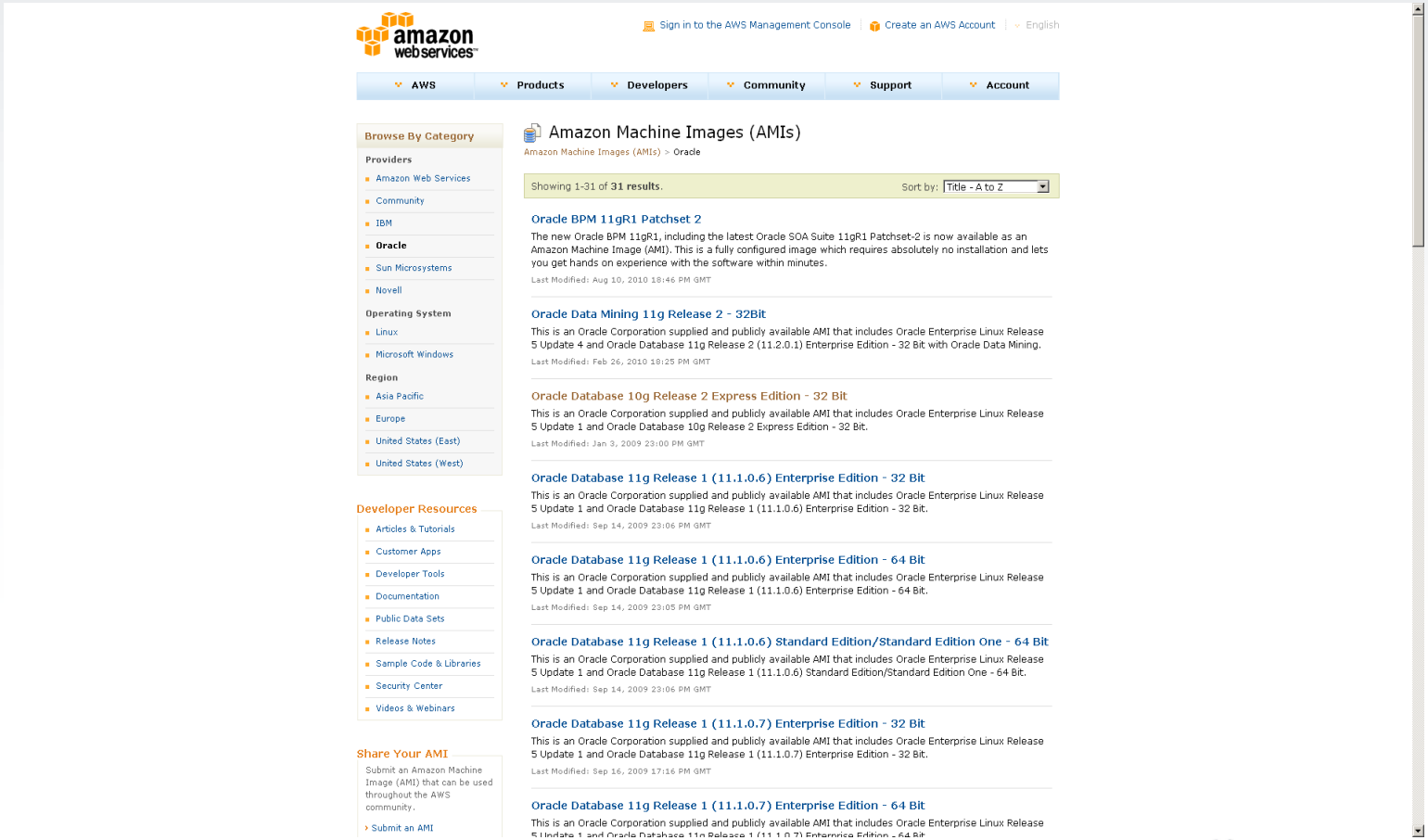
Dan Sarel, VP Product

Where are we today?

- Databases on virtualized servers – yes
- Database on the public cloud?

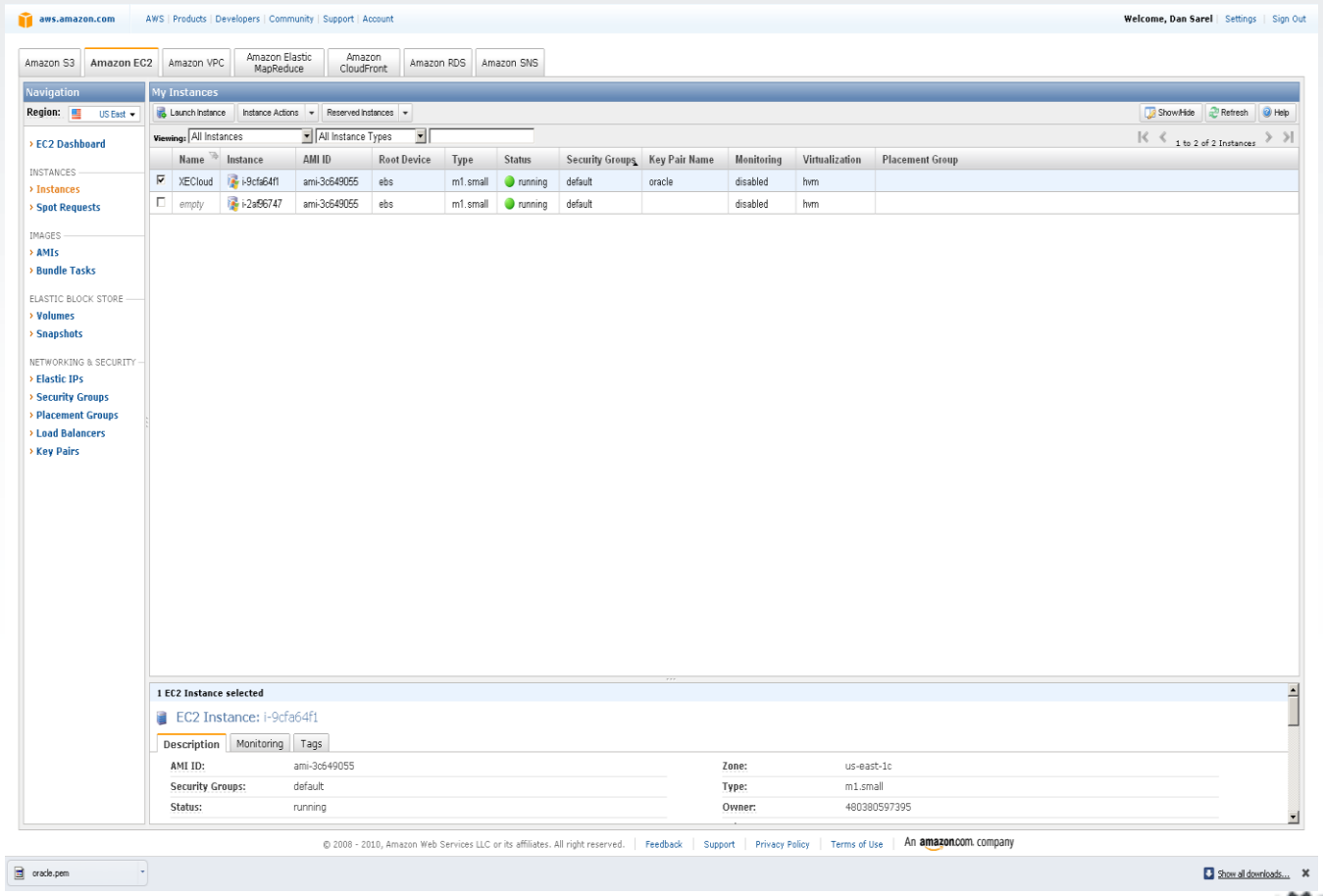
sentrigo™

Technically – we're there



sentrigo™

Even I almost got it running…



sentrigo™

A key reason why users don't go there is security and control

Figure 14: Information week analytics Cloud computing survey, 2009. Respondants were asked: How concerned are you with following issues as they relate to cloud computing? (range from 1 to 5)

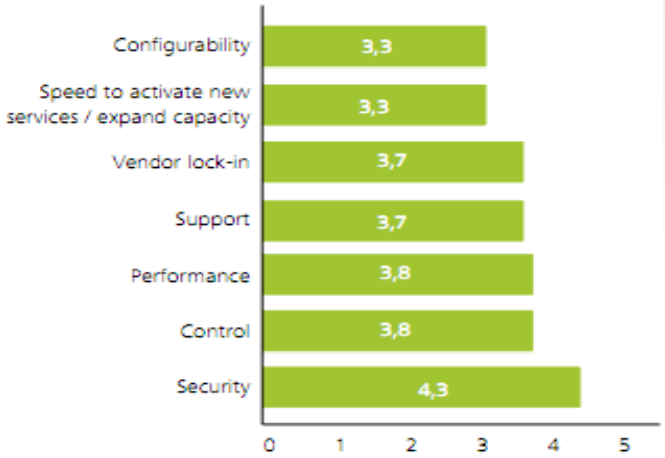
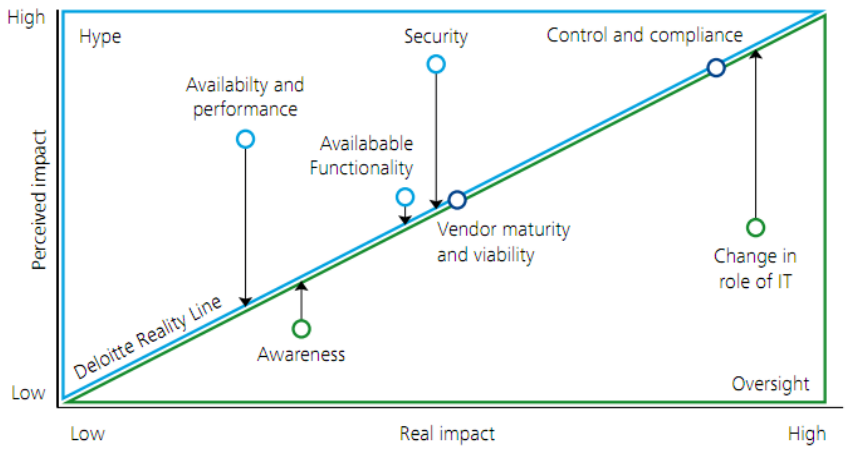


Figure 13 - Deloitte perspective on perceived and real impact of Cloud inhibitors



Source: Deloitte / Information Week

sentrigo™

Regulations

- To move applications to the cloud, you will need to be able to demonstrate compliance
  - Credit cards → PCI DSS
  - Medical Records → HIPAA
  - Financials → Sarbanes-Oxley
  - …and many others
- Some regulations require you to control where data is saved (Swiss banks do not allow data to be saved outside Switzerland, UK data privacy law does the same for the UK, etc.)

sentrigo™

Accept Innovation – But Be Prepared

- Elastic
- Outsourced Administration
- Globally available
- Easy to replicate
- Failover & DR
- Cheap storage

- Less Capital

- Where is my data?
- Who has privileged access to my data?
- Access controls?
- How to protect all copies?
- Is data encrypted?

- Less Control

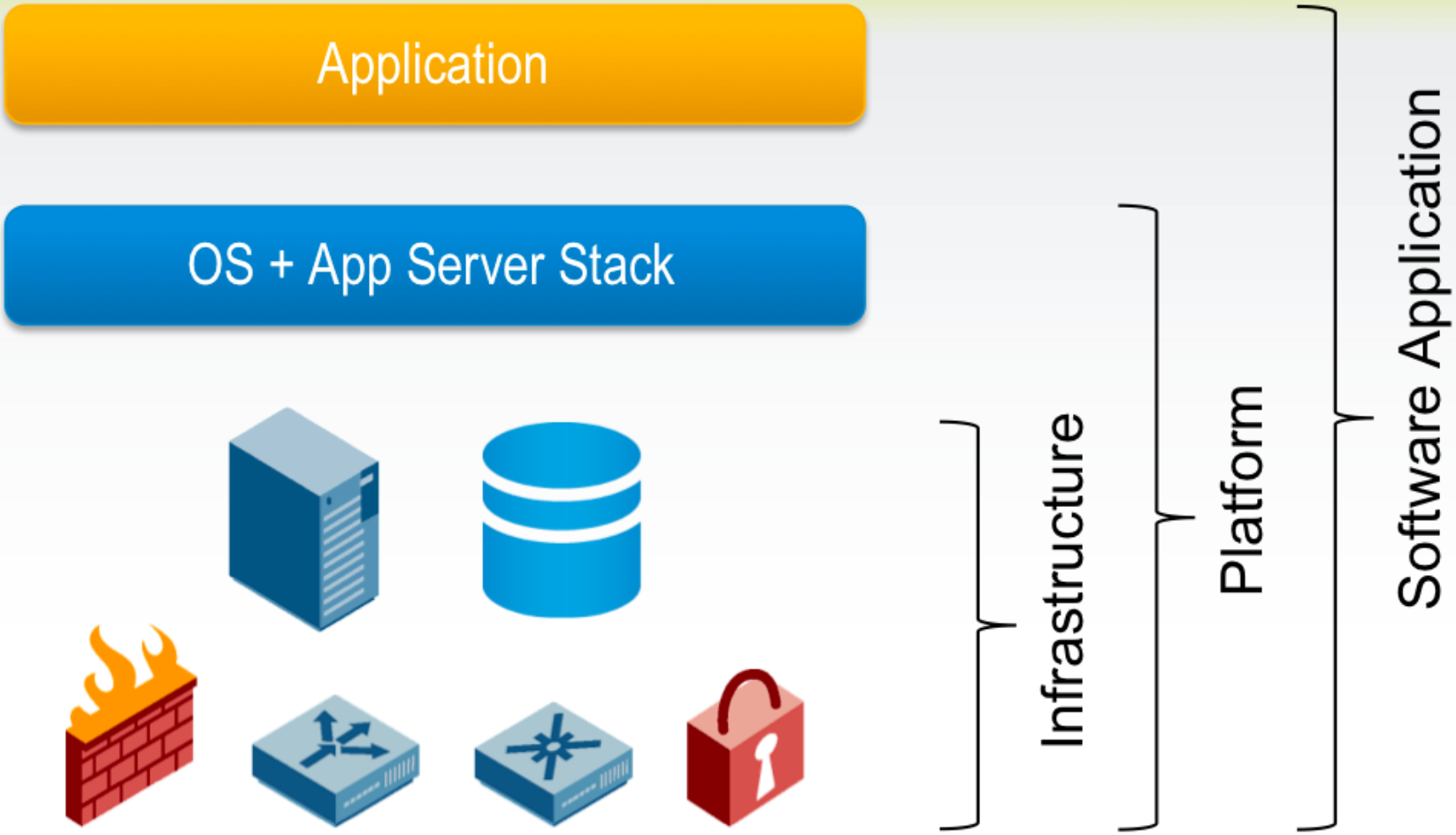
sentrigo™

Standard Approaches Might Fail

- Authentication and Authorization
- Secure configuration
- Hardening
- Patching
- Vulnerability assessment
- Encryption
- Masking
- Monitoring
- Audit

sentrigo™

Focus On Deploying DBs to IaaS



Source: zhen.org

Different Types of Clouds, Have Different Types of Challenges

- Application (ie. Software as a Service)
  - Privilege User Oversight
  - Exploits of Application Vulnerabilities

- Platform (ie. Amazon SimpleDB, Force.com, Google App Engine, MS Azure)
  - Privileged User Oversight
  - Detailed Logging for Compliance

- Infrastructure (Amazon EC2 – Elastic Compute Cloud, Rackspace, etc)
  - All of the Above

Traditional Approaches to DB Security

- Native Audit
  - Easily defeated and tampered with
  - Performance impact
  - Too late (good for forensics)
- Column / Data level encryption
  - Application changes required
  - Where are the keys (and who can get them)?
  - Hardware might no longer be an option
  - Performance implications
  - Indexing, searching encrypted data

sentrigo™

Traditional Approaches (Cont'd)

- TDE (Transparent Data Encryption)
  - A great solution for protecting data on disk (and backups) – definitely should be considered
  - Does not help with access through database interfaces
- Network-based monitoring
  - Where to put the taps… the whole internet?
  - Won't see local access, so won't meet compliance
  - Have you tried giving AWS an appliance to deploy?

sentrigo™

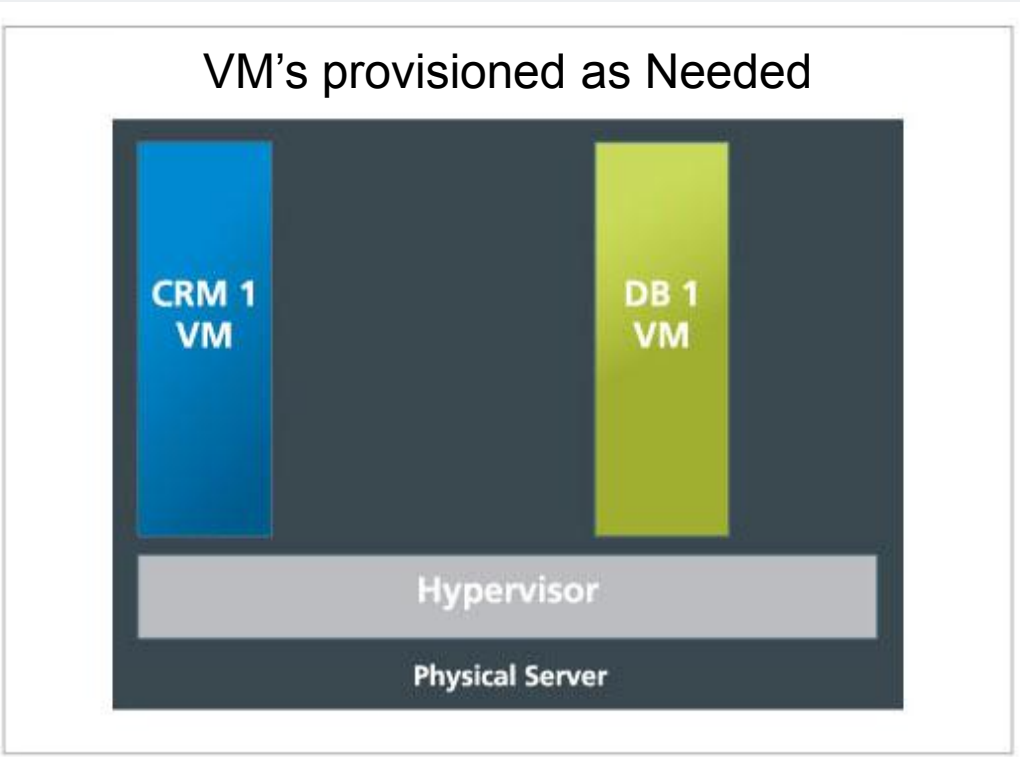
Challenges with DB Monitoring in the Cloud

- **Dynamic Systems Environment**
  - Servers are provisioned, moved, and de-provisioned constantly
  - Re-configuration to reflect system/network changes can't keep up
- **VM-to-VM Traffic**
  - Traffic never hits the network
  - Inefficient to send off-host for analysis
- **Distributed WAN Topology**
  - First generation solutions for DAM architected for local appliances
- **Segregation of Duties**
  - It's one thing to thoroughly vet *your own* staff…
  - … now there are privileged users you don't even know

sentrigo™

Dynamic Systems Environment

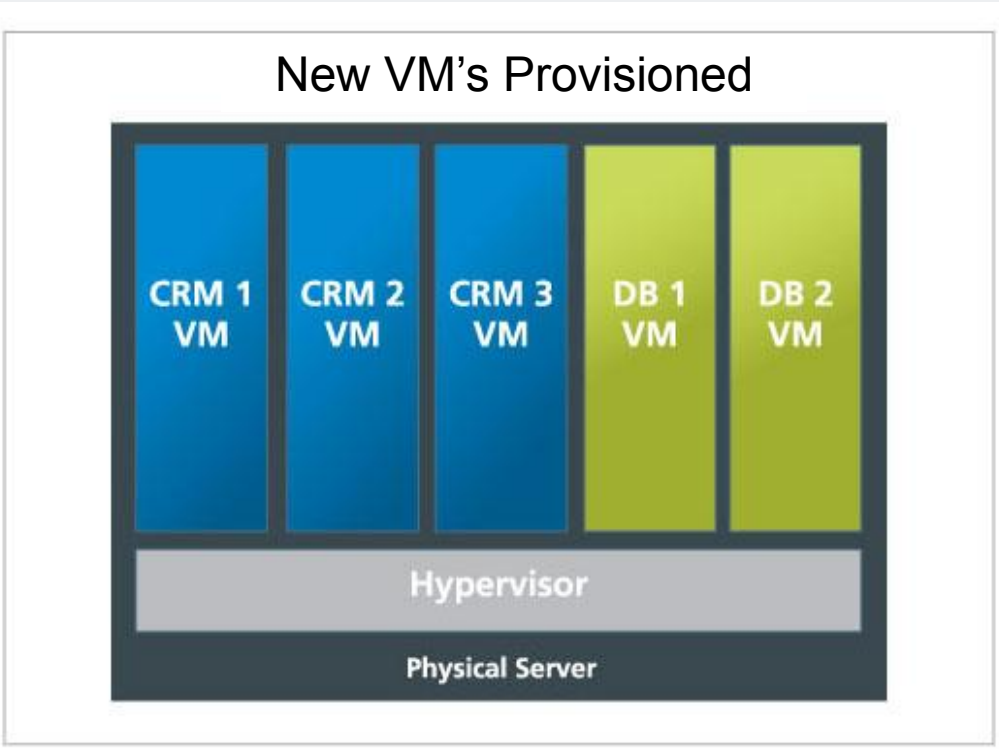
- Servers come up / down
  - provisioning
  - configuration



sentrigo™

Dynamic Systems Environment

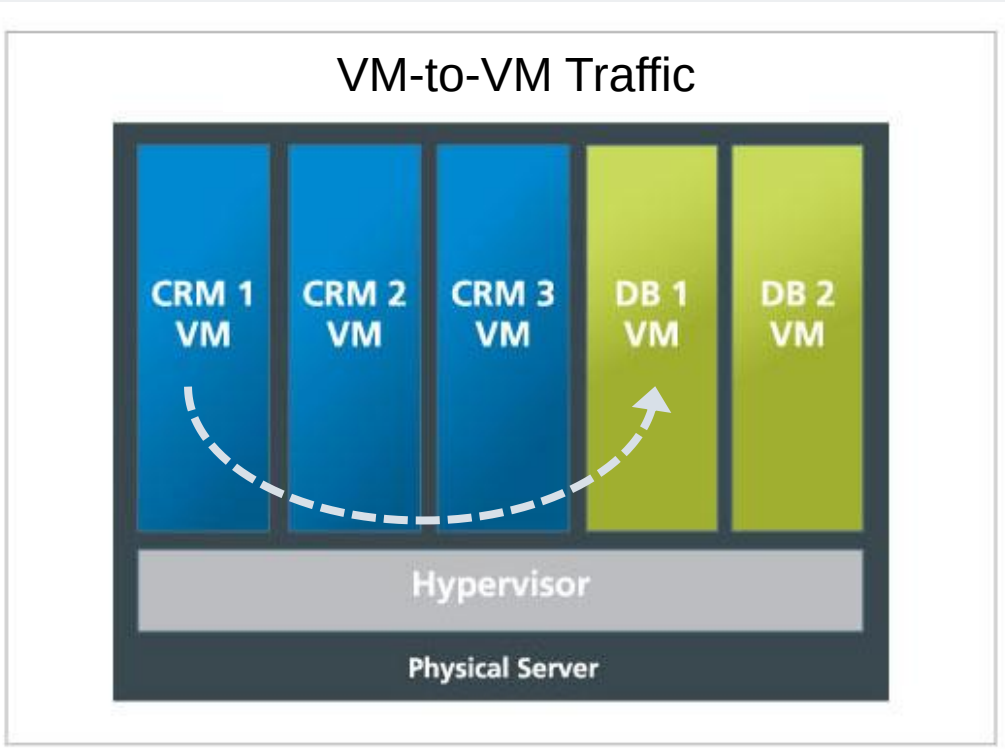
- Servers come up / down
  - provisioning
  - configuration



sentrigo™

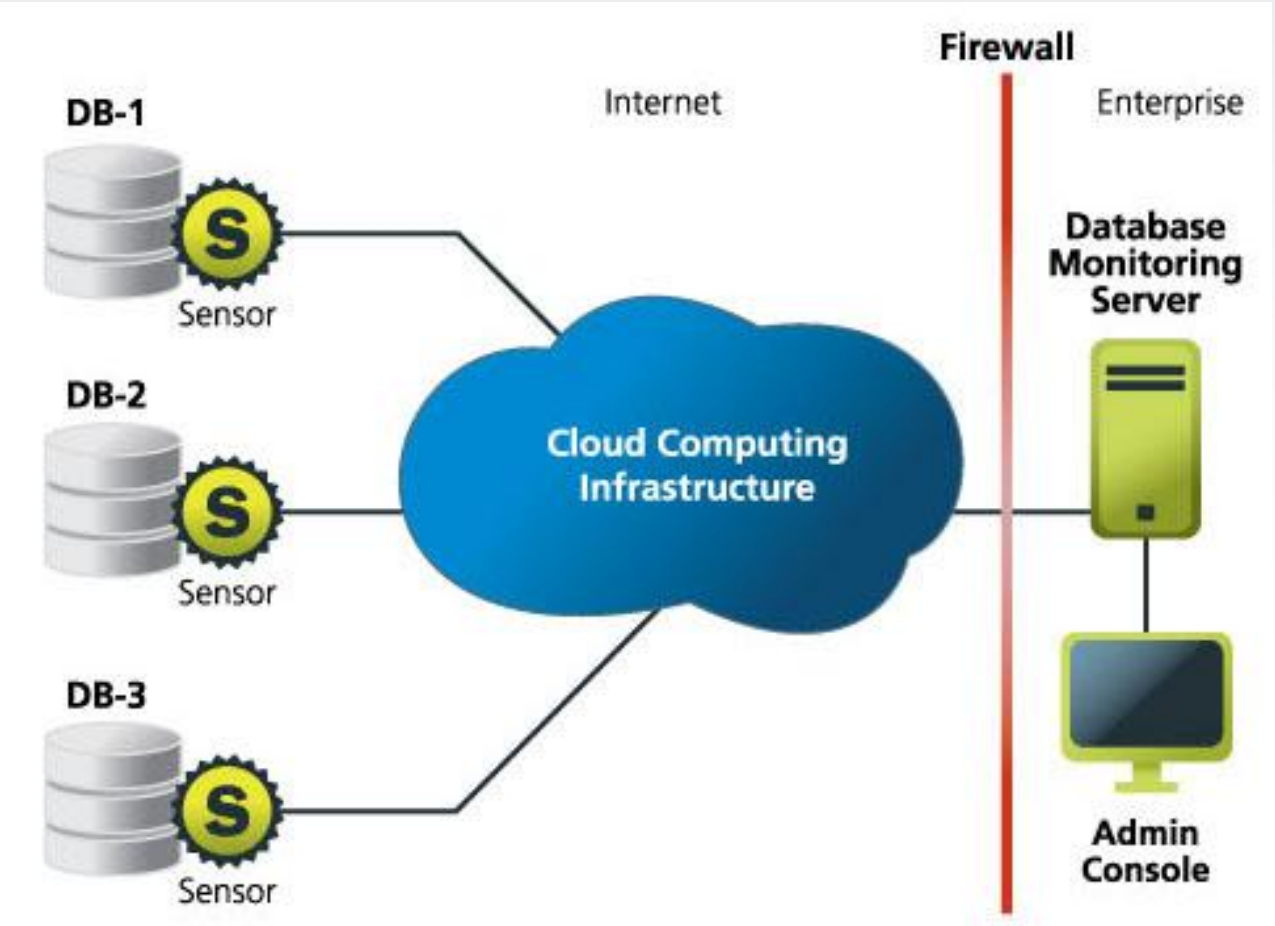
VM-to-VM Traffic

- Application(s) may be on same server as DB
  - Traffic never hits network
  - Traditional “Agent” model will try to send all traffic out for analysis → latency and performance issues



sentrigo™

Dealing With WAN Topologies



- Must work in long latency / low bandwidth (or no bandwidth) environments
  - Secure communications
  - Compression
  - Store & Forward

sentrigo™

“But My Cloud Vendor Says They are SAS-70 Compliant”

- What does that really mean?
  - Great, so they did background checks on their staff
- YOU are on the hook for compliance
  - Tools that tell you what privileged users are up to are required
  - Privileged users are no longer under your supervision, you need to compensate for this

sentrigo™

Local Agents On Each DB Host Can Protect from All Attack Vectors

- Network / Application Users
  - Including web-based attacks
- Host Access
  - Physical or SSH, authorized or not
- Intra-DB
  - Sophisticated attacks based on stored procedures, triggers, views, or encoded SQL

sentrigo™

Agent Deployability and Efficiency

- To Work in the Cloud:
  - Deployment Must Be Non-intrusive
    - Read-only (to minimize risk)
    - No kernel changes or reboot required
    - Automatic re-configuration
  - Distributed Threat Analysis
    - Look for architectures that process locally
    - Sending traffic off-host will degrade performance and be too slow to prevent threats

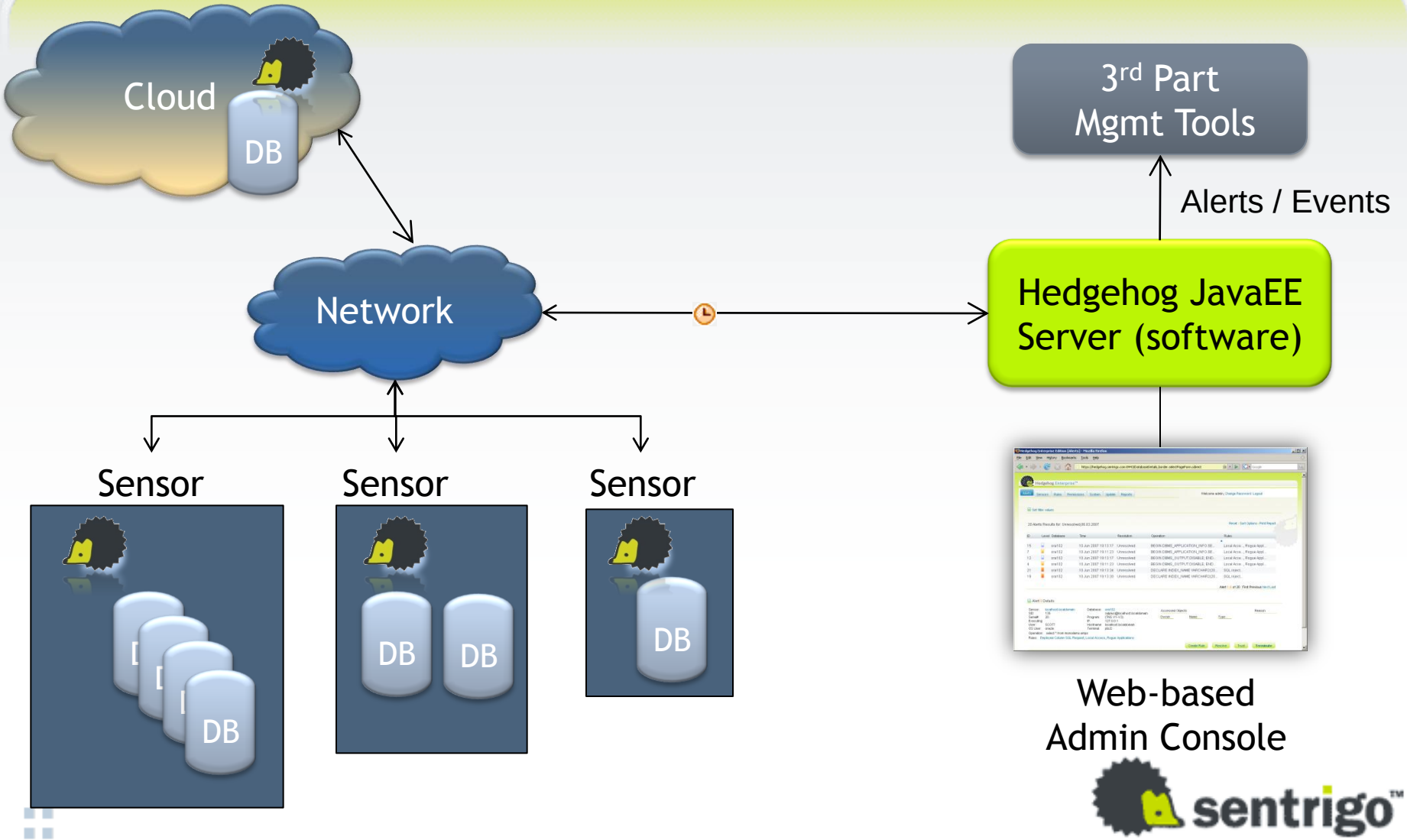
sentrigo™

Other approaches

- Virtual network devices
  - Switches
  - Routers
  - Tap-ports
- Virtual appliances & agents
- Making local agents smarter will be key

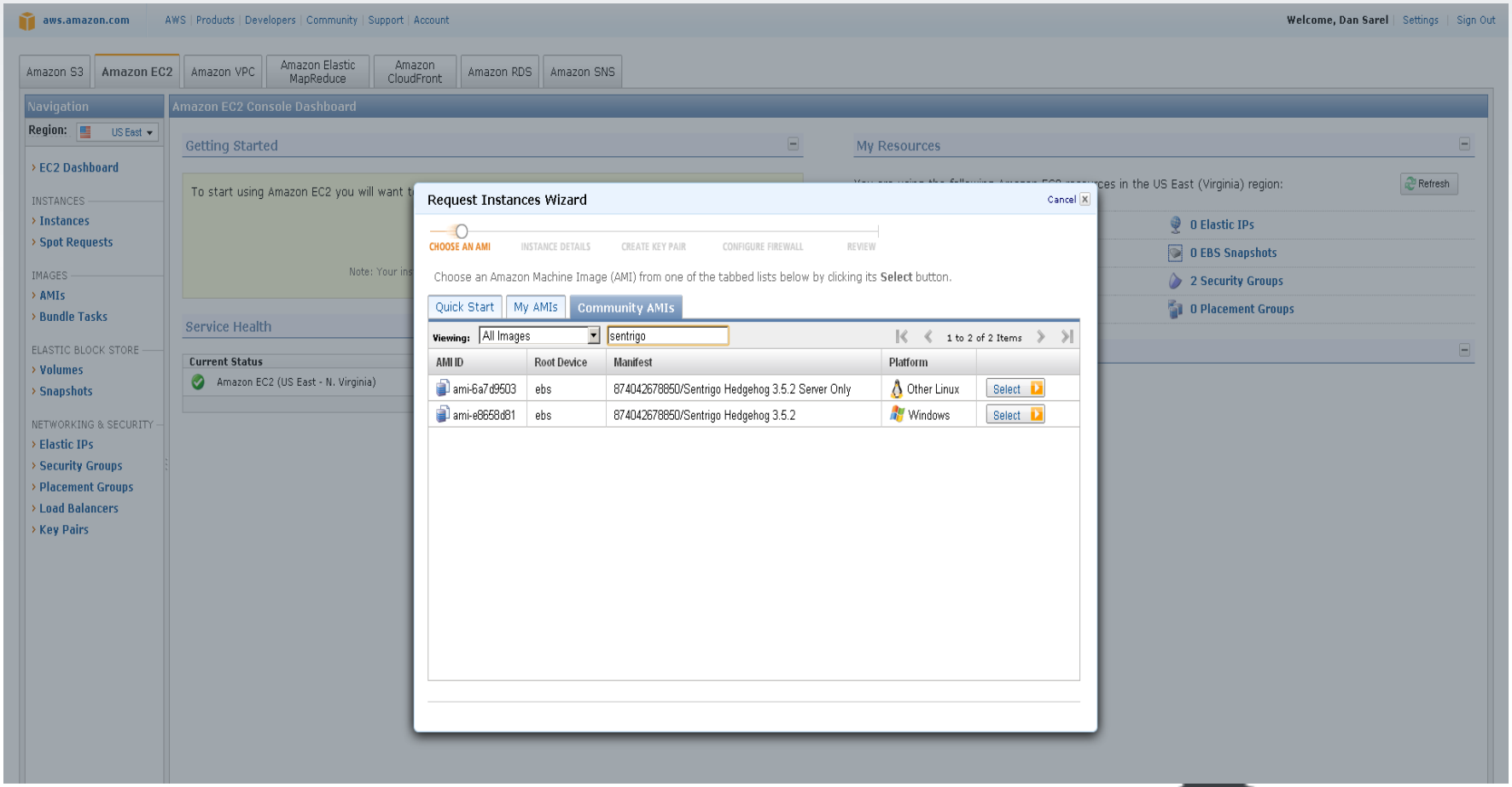
sentrigo™

Hedgehog: Enterprise+Cloud deployment example



sentrigo™

Considering placing your security in the cloud?



sentrigo™

Demo

- Assessing DB security in the cloud
- Monitoring databases in the cloud

sentrigo™

Thank You!

sentrigo™