



Securing Sensitive Data in the Cloud

Dan Sarel, VP Product

Where are we today?

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



Technically - we're there

The screenshot shows the Amazon Machine Images (AMIs) page for Oracle. The page is part of the AWS Management Console, with navigation links for AWS, Products, Developers, Community, Support, and Account. The main content area is titled "Amazon Machine Images (AMIs)" and shows a list of 31 results, sorted by Title - A to Z. The list includes several Oracle AMIs, such as Oracle BPM 11gR1 Patchset 2, Oracle Data Mining 11g Release 2 - 32Bit, Oracle Database 10g Release 2 Express Edition - 32 Bit, Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 32 Bit, Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 64 Bit, Oracle Database 11g Release 1 (11.1.0.6) Standard Edition/Standard Edition One - 64 Bit, Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 32 Bit, and Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 64 Bit. The page also features a "Browse By Category" sidebar with filters for Providers, Operating System, and Region, as well as "Developer Resources" and "Share Your AMI" sections.

amazon web services | Sign in to the AWS Management Console | Create an AWS Account | English

▼ AWS | ▼ Products | ▼ Developers | ▼ Community | ▼ Support | ▼ Account

Browse By Category

Providers

- Amazon Web Services
- Community
- IBM
- Oracle**
- Sun Microsystems
- Novell

Operating System

- Linux
- Microsoft Windows

Region

- Asia Pacific
- Europe
- United States (East)
- United States (West)

Developer Resources

- Articles & Tutorials
- Customer Apps
- Developer Tools
- Documentation
- Public Data Sets
- Release Notes
- Sample Code & Libraries
- Security Center
- Videos & Webinars

Share Your AMI

Submit an Amazon Machine Image (AMI) that can be used throughout the AWS community.

> Submit an AMI

Amazon Machine Images (AMIs)
Amazon Machine Images (AMIs) > Oracle

Showing 1-31 of 31 results. Sort by: Title - A to Z

Oracle BPM 11gR1 Patchset 2
The new Oracle BPM 11gR1, including the latest Oracle SOA Suite 11gR1 Patchset-2 is now available as an Amazon Machine Image (AMI). This is a fully configured image which requires absolutely no installation and lets you get hands on experience with the software within minutes.
Last Modified: Aug 10, 2010 18:46 PM GMT

Oracle Data Mining 11g Release 2 - 32Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 4 and Oracle Database 11g Release 2 (11.2.0.1) Enterprise Edition - 32 Bit with Oracle Data Mining.
Last Modified: Feb 26, 2010 10:25 PM GMT

Oracle Database 10g Release 2 Express Edition - 32 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 10g Release 2 Express Edition - 32 Bit.
Last Modified: Jan 3, 2009 23:00 PM GMT

Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 32 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 32 Bit.
Last Modified: Sep 14, 2009 23:06 PM GMT

Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 64 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 11g Release 1 (11.1.0.6) Enterprise Edition - 64 Bit.
Last Modified: Sep 14, 2009 23:05 PM GMT

Oracle Database 11g Release 1 (11.1.0.6) Standard Edition/Standard Edition One - 64 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 11g Release 1 (11.1.0.6) Standard Edition/Standard Edition One - 64 Bit.
Last Modified: Sep 14, 2009 23:06 PM GMT

Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 32 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 32 Bit.
Last Modified: Sep 16, 2009 17:16 PM GMT

Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 64 Bit
This is an Oracle Corporation supplied and publicly available AMI that includes Oracle Enterprise Linux Release 5 Update 1 and Oracle Database 11g Release 1 (11.1.0.7) Enterprise Edition - 64 Bit.



Even I almost got it running...

The screenshot displays the AWS Management Console interface for the 'My Instances' page. The region is set to 'US East'. The navigation pane on the left includes sections for INSTANCES (Instances, Spot Requests), IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), and NETWORKING & SECURITY (Elastic IPs, Security Groups, Placement Groups, Load Balancers, Key Pairs). The main content area shows a table of instances with columns for Name, Instance ID, AMI ID, Root Device, Type, Status, Security Groups, Key Pair Name, Monitoring, Virtualization, and Placement Group. Two instances are listed: 'i-9cfa64f1' (AMI: ami-3c649055, Type: m1.small, Status: running) and 'i-2a86747' (AMI: ami-3c649055, Type: m1.small, Status: running). Below the table, a detailed view for the selected instance 'i-9cfa64f1' is shown, including fields for AMI ID, Security Groups, Status, Zone, Type, and Owner.

Name	Instance	AMI ID	Root Device	Type	Status	Security Groups	Key Pair Name	Monitoring	Virtualization	Placement Group
<input checked="" type="checkbox"/>	i-9cfa64f1	ami-3c649055	ebs	m1.small	running	default	oracle	disabled	hvm	
<input type="checkbox"/>	empty	i-2a86747	ebs	m1.small	running	default		disabled	hvm	

1 EC2 Instance selected

EC2 Instance: i-9cfa64f1

Description		Monitoring		Tags	
AMI ID:	ami-3c649055	Zone:	us-east-1c		
Security Groups:	default	Type:	m1.small		
Status:	running	Owner:	480380597395		

© 2008 - 2010, Amazon Web Services LLC or its affiliates. All right reserved. [Feedback](#) [Support](#) [Privacy Policy](#) [Terms of Use](#) An [amazon.com](#) company

Show all downloads...



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)

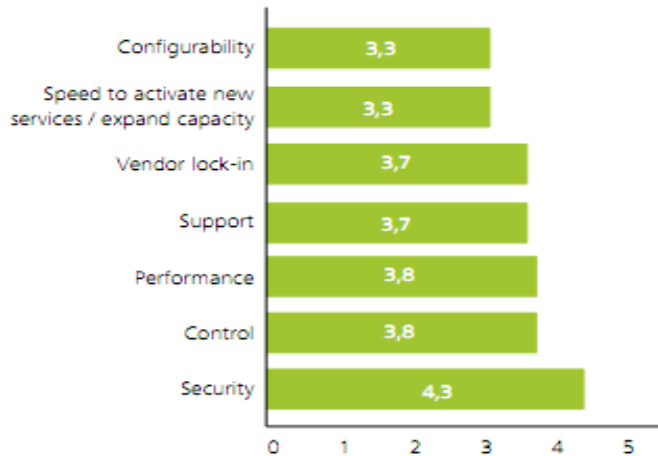
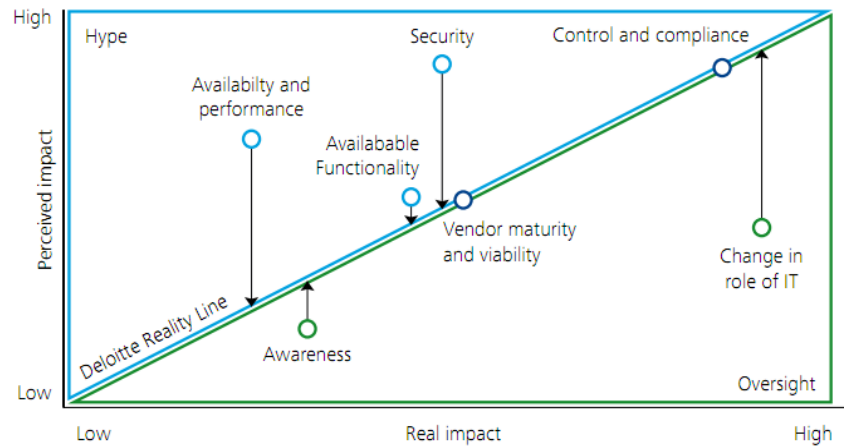


Figure 13 - Deloitte perspective on perceived and real impact of Cloud inhibitors



Source: Deloitte / Information Week



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.)



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



Standard Approaches Might Fail

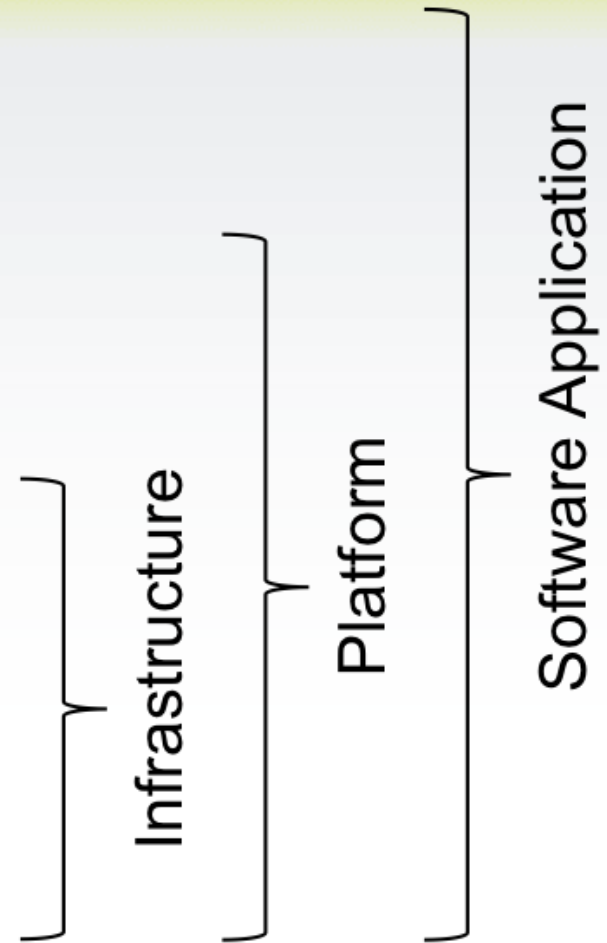
- Authentication and Authorization
- Secure configuration
- Hardening
- Patching
- Vulnerability assessment
- Encryption
- Masking
- Monitoring
- Audit



Focus On Deploying DBs to IaaS

Application

OS + App Server Stack



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



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?



Challenges with DB Monitoring in the Cloud

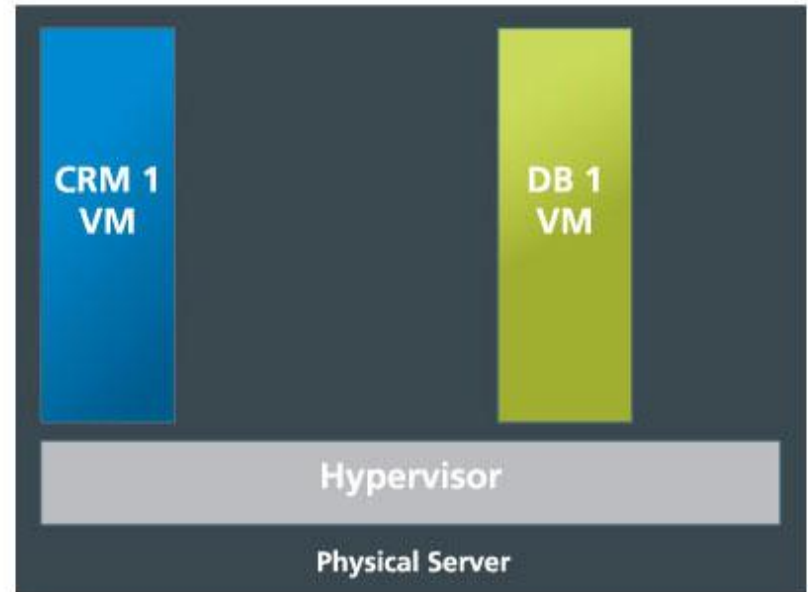
- **Dynamic Systems Environment**
 - Servers are provisioned, moved, and de-provisioned constantly
 - Re-configuration to reflect system/network changes can't keep up
- **VM-to-VM Traffic**
 - Traffic never hits the network
 - Inefficient to send off-host for analysis
- **Distributed WAN Topology**
 - 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



Dynamic Systems Environment

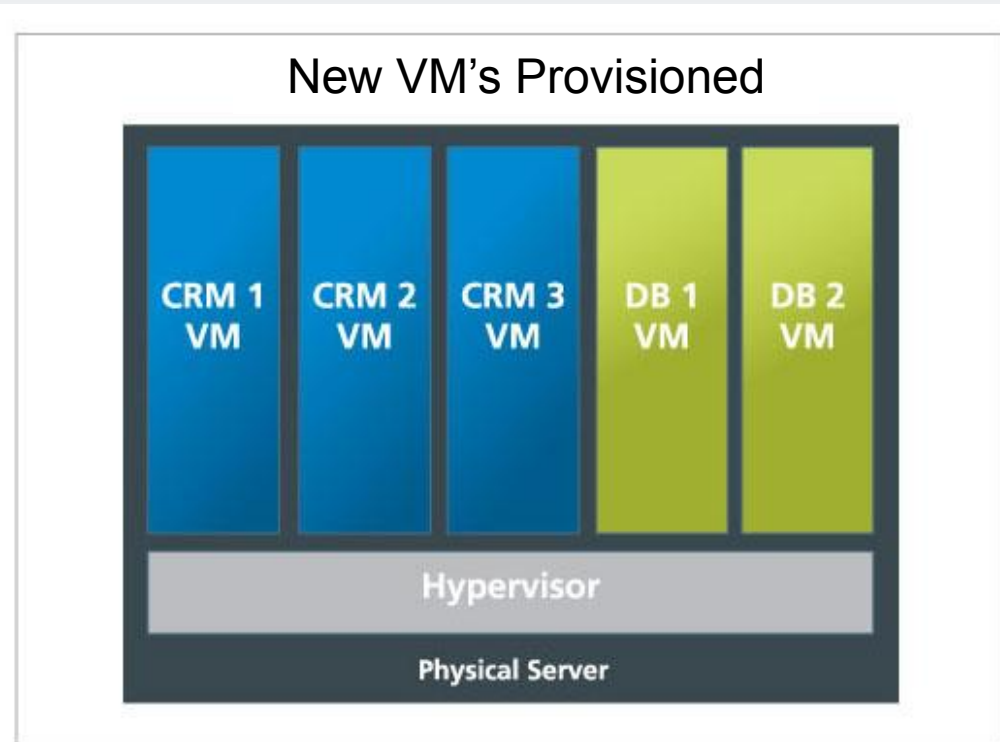
- Servers come up / down
 - provisioning
 - configuration

VM's provisioned as Needed



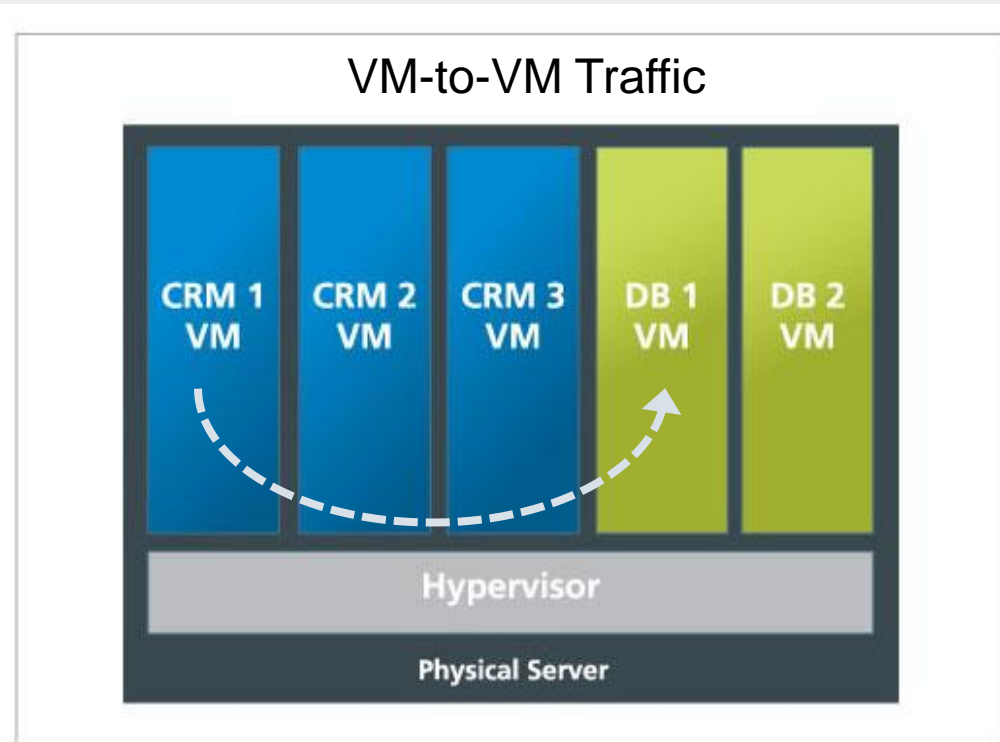
Dynamic Systems Environment

- Servers come up / down
 - provisioning
 - configuration

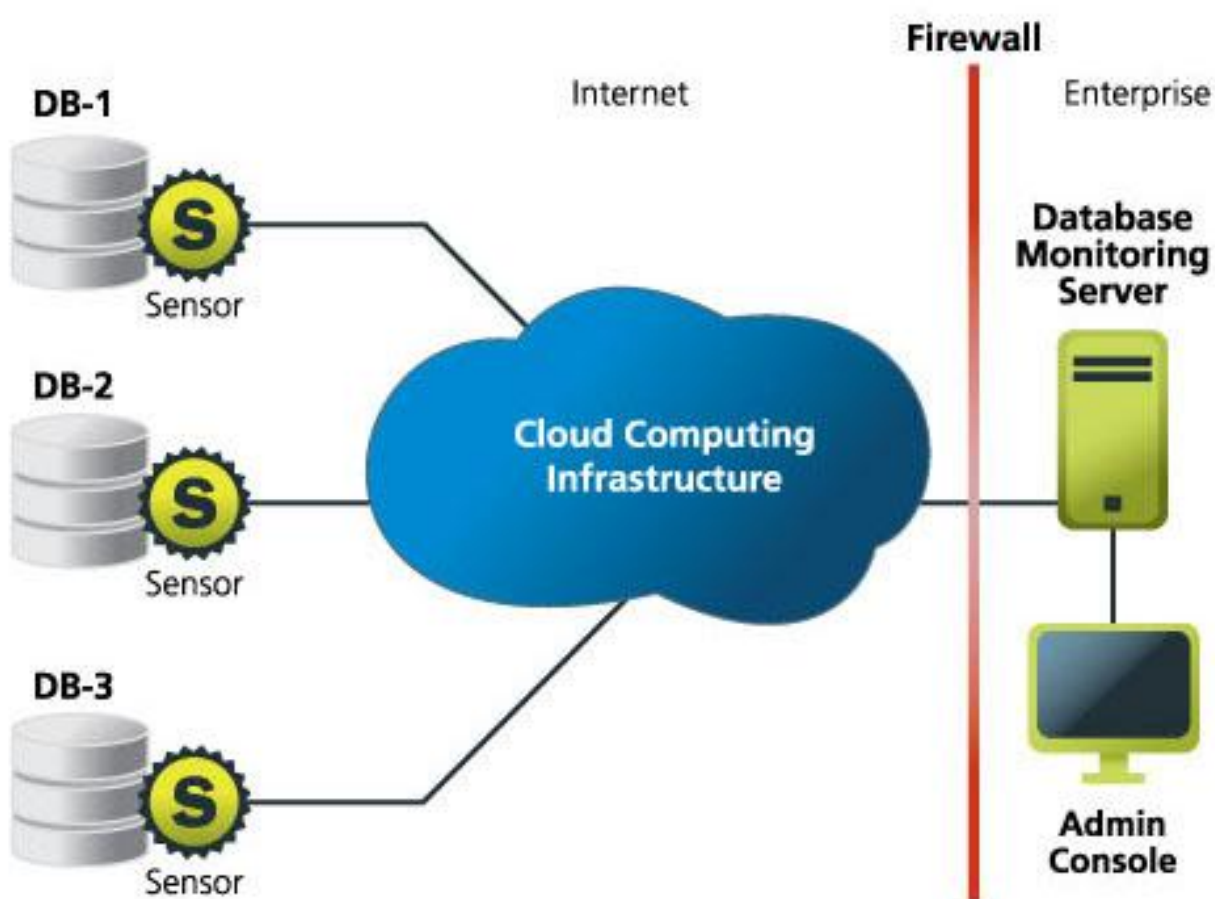


VM-to-VM Traffic

- 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



Dealing With WAN Topologies



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



“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



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



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

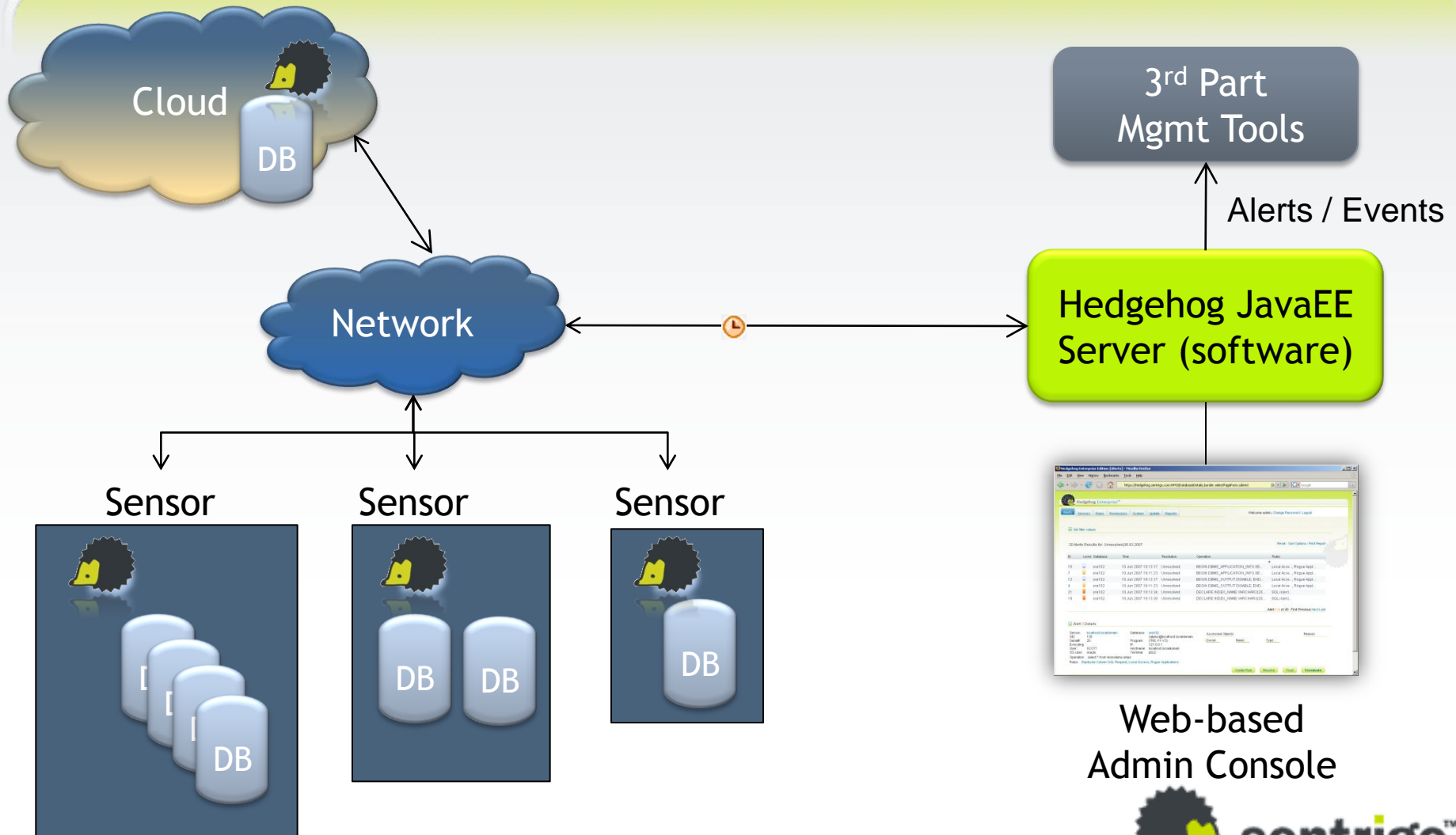


Other approaches

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



Hedgehog: Enterprise+Cloud deployment example



Web-based
Admin Console



Considering placing your security in the cloud?

The screenshot displays the AWS Management Console interface. A modal window titled "Request Instances Wizard" is open, showing the "CHOOSE AN AMI" step. The wizard has tabs for "Quick Start", "My AMIs", and "Community AMIs". The "Viewing" dropdown is set to "All Images", and the search filter is "sentrigo". The table below shows the search results:

AMI ID	Root Device	Manifest	Platform	
ami-6a7d9503	ebs	874042678850/Sentrigo Hedgehog 3.5.2 Server Only	Other Linux	Select
ami-e8658d81	ebs	874042678850/Sentrigo Hedgehog 3.5.2	Windows	Select



Demo

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



Thank You!

