

ORACLE®



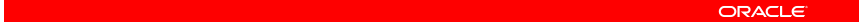
ORACLE®

Data Security in the Cloud

Luc Wijns
Chief Technologist Systems Benelux



The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



NIST Definition of Cloud Computing



Cloud computing is a model for enabling 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.

This cloud model promotes availability and is composed of:

- | | | |
|--|--|---|
| <u>5 Essential Characteristics</u> | <u>3 Service Models</u> | <u>4 Deployment Models</u> |
| <ul style="list-style-type: none">• On-demand self-service• Resource pooling• Rapid elasticity• Measured service• Broad network access | <ul style="list-style-type: none">• SaaS• PaaS• IaaS | <ul style="list-style-type: none">• Public Cloud• Private Cloud• Community Cloud• Hybrid Cloud |

Fear, Uncertainty & Doubt: FUD

- ..."Cloud Computing is not Secure"... ?
- Can Cloud Computing be as Secure as on-premises Data Centers ?
- Can Cloud Computing be Compliant ?
- What About: "Cloud Computing cannot meet the Common Needs Because Customers won't let their Data leave their Country." ?
- "We must move all to the Clouds or we won't be competitive anymore..."?!?
-etc

ORACLE

© 2011 Oracle Corporation

5

In the Cloud Threats do not Change

Security guru Bruce Schneier says that whatever cloud computing is, the security issues and conversations around it are nothing new. The key, he says, always comes down to **trust** and **transparency**.



By Dahna McConnachie
Technology & Business
March 31, 2009
<http://www.schneier.com/news-083.html>

ORACLE

© 2011 Oracle Corporation

6

Security Concerns Don't Change



© 2011 Oracle Corporation

7

ORACLE

Which is "Best" for which Context ?

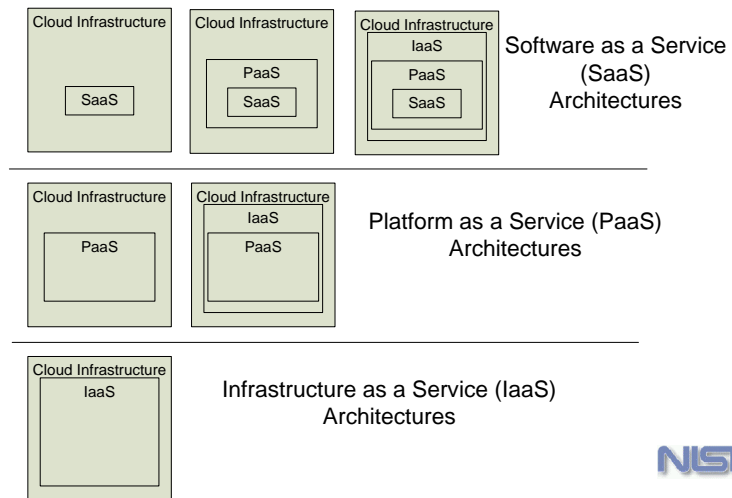


© 2011 Oracle Corporation

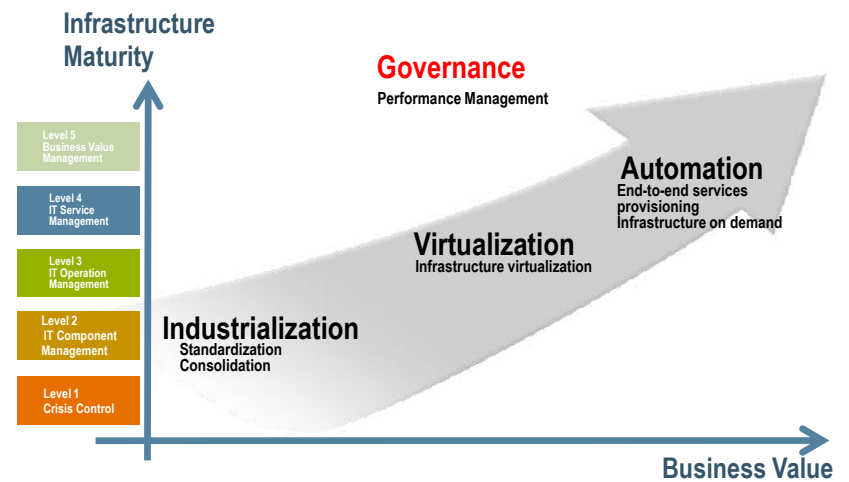
8

ORACLE

Service Models and Transparency



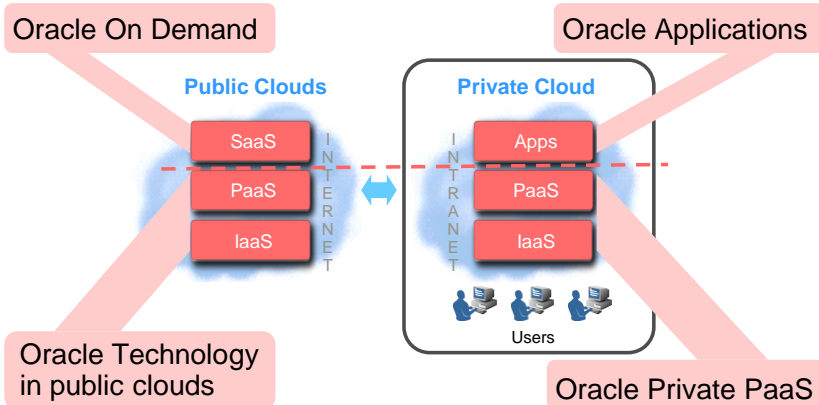
Road To Security Maturity



Oracle Cloud Computing Strategy

Our objectives:

- Ensure that cloud computing is fully enterprise grade
- Support both public and private cloud computing – give customers choice



ORACLE

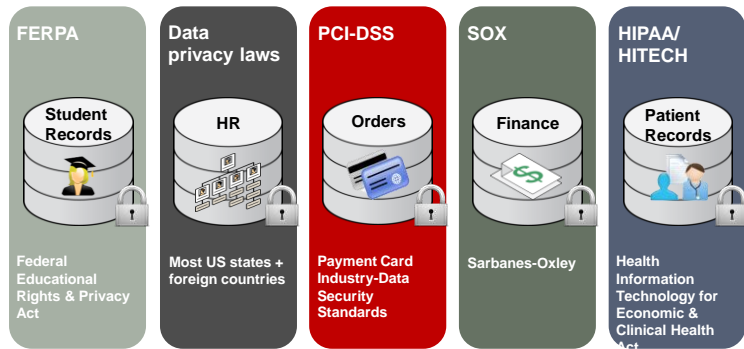
Oracle On Demand – Security (SaaS)

- Compliance Rules are implemented Everywhere
- Example: HIPAA Service Provider for Healthcare
- Compliant with the Technical, Physical and Administrative Safeguards
- HITECH Requires Business Associates (Services Providers) to be Compliant
- ISO27000 Certificate 1/2

ORACLE
ON DEMAND

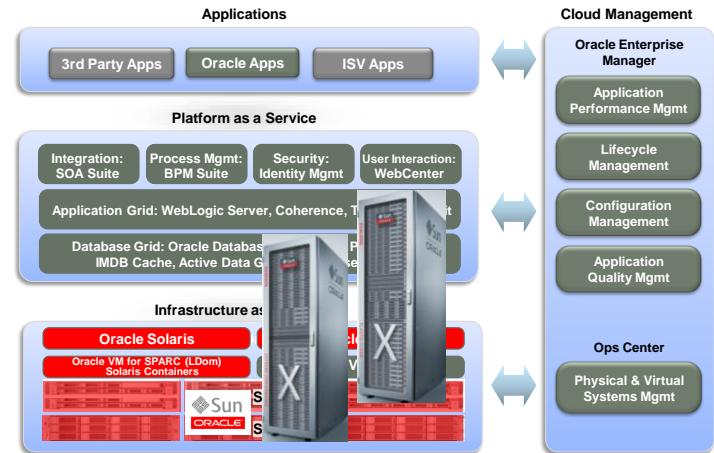
ORACLE

Compliance Requirements



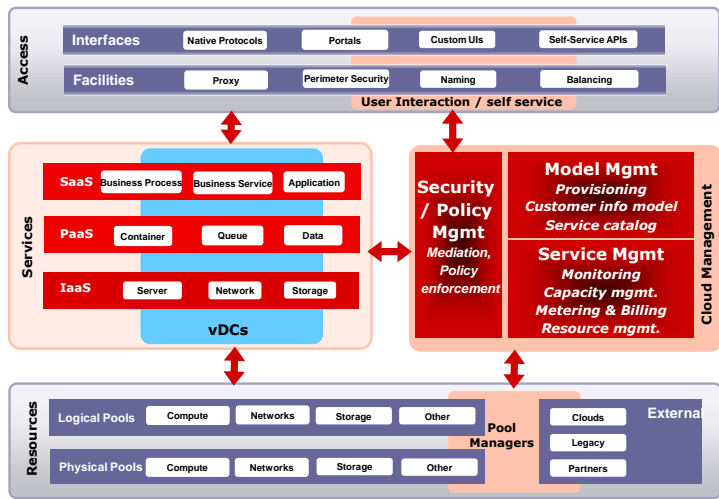
ORACLE

Oracle Private Cloud Solution



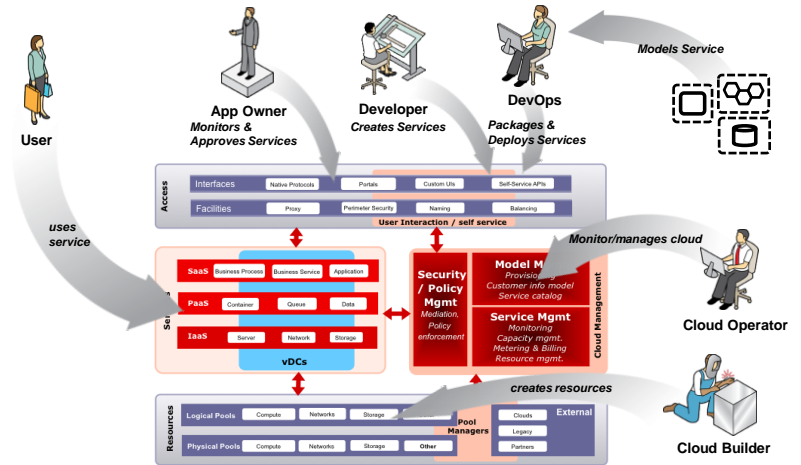
ORACLE

Cloud Architecture – Logical View



ORACLE

Identify Roles and Interactions Cloud Implies Changes in IT Roles



ORACLE

Oracle Defense-in-Depth



Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control

- Oracle Database Vault
- Oracle Label Security

Auditing and Tracking

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Blocking and Monitoring

- Oracle Database Firewall

ORACLE

© 2011 Oracle Corporation

17

Oracle Security Inside Out



Infrastructure Security

- Hardware Accelerated Encryption
- Secure Key Management and Storage
- Strong Workload Isolation
- Secure Service Delivery Platforms

Database Security

- Encryption and Masking
- Privileged User Controls
- Multi-Factor Authorization
- Activity Monitoring and Audit
- Secure Configuration
- Monitor and Block

Middleware

- User and Role Management
- Access Management
- Virtual Directories
- Rights Management
- Identity Governance

Applications

- Comprehensive Compliance Mgmt.
- Centralized Policy Administration
- Access Management
- Track and Audit Content and Usage

ORACLE

© 2011 Oracle Corporation

1 18

Bringing Infrastructure Security



**Secure
Infrastructure
Matters !**

ORACLE

Infrastructure Security Foundation



**OPERATING
SYSTEMS**

Secure Workload Isolation
Role-based Access Control
Process Rights Management

ORACLE
SOLARIS

Unified Cryptographic Infrastructure
Fine-Grained Auditing
Trusted Extensions

VIRTUALIZATION

Secure Data Protection



Secure Workload Isolation



SERVERS

Cryptographic Acceleration



Secure Key Storage



STORAGE

Encrypted Tape Storage



Encrypted Disk Storage



Key Management



ORACLE

Infrastructure and Cryptography



OPERATING SYSTEMS

Secure Workload Isolation Role-based Access Control Process Rights Management	ORACLE SOLARIS	Unified Cryptographic Infrastructure Fine-Grained Auditing Trusted Extensions
---	--------------------------	---

VIRTUALIZATION

Secure Data Protection Sun VDI	Secure Workload Isolation ORACLE VM
-----------------------------------	---

SERVERS

Cryptographic Acceleration ULTRASPARC	Secure Key Storage intel Xeon
--	----------------------------------

STORAGE

Encrypted Tape Storage	Encrypted Disk Storage	Key Management
------------------------	------------------------	----------------

ORACLE

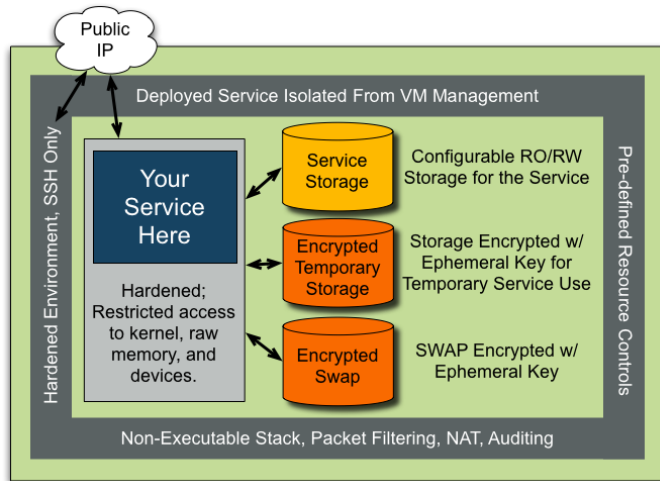
Solaris Security



- Secure Service Containers
- User and Process Rights Management
- Secure Network Access
- Cryptographic Framework
- Comprehensive Auditing
- Solaris Trusted Extensions
- Common Criteria Evaluated (EAL4+)

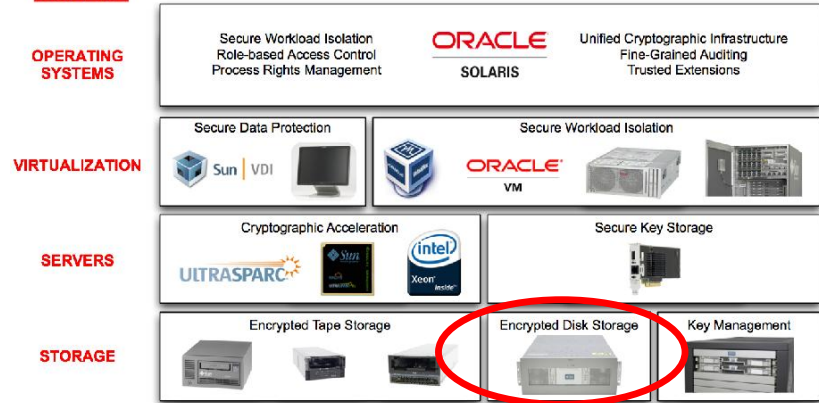
ORACLE

Solaris Zones: Immutable Service Containers



ORACLE

Infrastructure and Cryptography



ORACLE

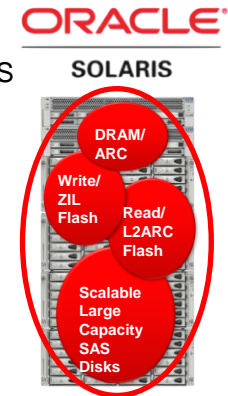
How to Destroy Data in a Hurry

- Delete File: **No**
- Over writing the data: **No**
- Shoot the drive: **No**
- Security Erase: **No**
- De-Gaussing: **No or at High Cost**
- Melting : **No or at High Cost**
- Shredding : **No or at High Cost**

ZFS Hybrid Storage Pool Encryption

Solaris 11 Express brings Encryption to ZFS Hybrid Storage Pools

- DRAM/ARC is not Encrypted
 - But you can protect swapped out pages (encrypted swap ZVOL)
- L2ARC is always encrypted (ephemeral keys)
- ZIL is always encrypted (on-disk or on-SSD)
- On Disk data is always encrypted



Full Disk Encryption (FDE)?



- Almost 100% transparent to the User
 - You will probably to enter a password at boot time
- 0% performance impact if encrypt/decrypt in firmware
- Hardware is filesystem agnostic



- No Access to Ciphertext
- Is it really encrypted ?
- No known versions with data encryption key change
- Same keylen/algorithm/mode for complete disk
 - A lot of data with same key
 - Need HW change to change algorithm
- No Enterprise SSD doing Crypto
- Not aware of Raid Volumes

ORACLE

© 2011 Oracle Corporation

27

ZFS Filesystem & Dataset Encryption



- More Flexibility in Software
- Easiest for Key Management
- Single multi-disk pool or per dataset wrapping keys
- Keys are agnostic of Raid config
- Wrapping and Data encryption change
- Algorithm/keylen/mode change

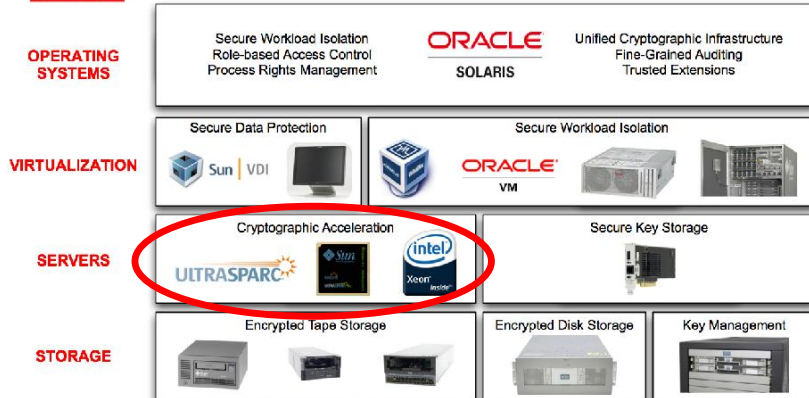
- Integrate with SSDs (HSP)
- Ciphertext is visible
- Encrypt Snapshot and Clones
- Compression, encryption, & deduplication work together
- Integrating with the host & operating system crypto infrastructure (SW and HW)

ORACLE

© 2010 Oracle Corporation. All Rights Reserved. Proprietary and Confidential

28

Infrastructure and Cryptography



ORACLE

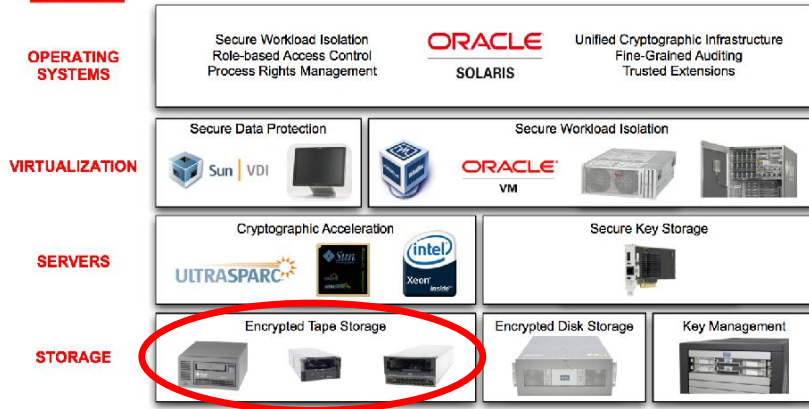
Cryptographic Capabilities and Algorithms T3 Processor



Cryptographic Capabilities	UltraSPARC T3 Supported Algorithms
<ul style="list-style-type: none"> Public Key Encryption 	<ul style="list-style-type: none"> RSA (Up to 2048-bit) DSA ECC (ECDSA, ECDH) DH (Up to 2048-bit)
<ul style="list-style-type: none"> Symmetric Key Encryption 	<ul style="list-style-type: none"> AES (128,192,256 bits) with ECB, CBC, CTR, CFB, GCM 3DES/DES with (ECB, CBC)
<ul style="list-style-type: none"> Message Digests 	<ul style="list-style-type: none"> MD5 SHA-1 SHA-256, SHA-384, SHA-512 HMAC
<ul style="list-style-type: none"> API support 	<ul style="list-style-type: none"> PKCS#11 (Via Solaris Crypto Framework)

ORACLE
ORACLE

Infrastructure and Cryptography



Three Key Elements Needed for Data Encryption on Removable Media



Key Takeways

- Public and Private Clouds share the same Security Requirements
- “Cloud Thinking” wrt/Security
 - Increases security concerns from day one
 - Involves all the stakeholders from day one
- Investing in “Cloud Technologies” Requires to Shift Minds and Impacts the “Complete Stack”
- Whatever you think to do with “Cloud”, Infrastructure Always Matter

ORACLE

© 2011 Oracle Corporation

33

Oracle Security is Complete



ORACLE

© 2011 Oracle Corporation

34



The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

ORACLE®

Trust in Cloud Computing with Transparent Security

- Governance, Information Security and Transparency are inter-related concepts
- Security Governance: can rely on an ISMS based (iso27001/2)
- Transparency is related the disclosure of governance frameworks between cloud SP and users.



Sources:

<http://blogs.barrons.com/ecbtradedaily/>
<http://blog.talkingidentity.com>

ORACLE



Data Encryption Matters

- The Best Way to Destroy Data in a Hurry is: **Encrypt Your Data and Destroy Only the Key**
- The Best Way to Protect Data Efficiently is: **Encrypt Your Data and Protect Only the Key**
- Data in Creation, Data in Transit, Data at Rest
- At All Layers of the Stack

ORACLE