Mitigating Information Security Risks of Cloud Computing

Peter Rajnak
Business Development Director for Security Solutions
Oracle OFM APAC
Everyone Is Talking About Cloud

How Cloud Computing Will Change Business

IBM, Qualcomm, Nokia, and other major companies, along with startups, are preparing to cash in on new technology. Not that it will be easy.

- Slide Show: Cloud Computing Meets the Smartphone

How Clouds Can Change Management

Jeremy Burton overhauled Serena Software's IT computing—and transformed the management of the company.

Cloud Computing: Quality

OptumHealth's eSync system assembles medical and drug records in one place and sends out alerts if it detects a potential problem.

Genentech's Cloud Cover

At the time, selling software to large companies was sometimes likened to drug dealing, because once a firm installed a piece of software, it had to pay a stream of licence fees for upgrades, security patches and technical support. Switching to a rival product was difficult and expensive. But with open-source software there was much less of a lock-in. There are no licence fees, and the file formats and data structures are open. Open-source software gained ground during the dotcom boom and even more so afterwards, as a way to cut costs.

Microsoft, the world's biggest software company, went from laughing at the idea to fighting it, giving warning that there might be legal risks associated with using open-source software and even calling it a "cancer" that threatened to harm the industry. Yet the popularity of open-source programs such as the Linux operating system continued to grow. The fact that Google, the industry's new giant, is on a
Cloud Is at the Peak of the Hype Curve

Source: Gartner "Hype Cycle for Cloud Computing, 2009" Research Note G00168780
Public Clouds and Private Clouds

**Public Clouds**
- Used by multiple tenants on a shared basis
- Hosted and managed by cloud service provider
- Limited variety of offerings
- SaaS
- PaaS
- IaaS

**Private Cloud**
- Exclusively used by a single organization
- Controlled and managed by in-house IT
- Limited variety of offerings
- Exclusively used by a single organization
- Controlled and managed by in-house IT
- Large number of applications
- SaaS
- PaaS
- IaaS

**Both offer:**
- High efficiency
- High availability
- Elastic capacity

**Public Clouds:**
- Lower *upfront* costs
- Economies of scale
- Simpler to manage OpEx

**Private Cloud:**
- Lower *total* costs
- Greater control over security, compliance & quality of service
- Easier integration CapEx & OpEx
44% of Large Enterprises Are Interested In Building An Internal Cloud

"What is your company’s highest level of awareness or interest in building and operating an internal “cloud” or pool of pay-per-use virtual servers?"

Enterprise (1,000+ employees)
- 4% already implemented
- 13% interested and planning budget for it
- 23% implementing in the next 12 months
- 33% interested but no budget for it
- 23% not aware (includes “don’t know”)

Mid-market (100-999 employees)
- 1% already implemented
- 4% interested and planning budget for it
- 12% implementing in the next 12 months
- 21% interested but no budget for it
- 38% not aware (includes “don’t know”)

VSE (2-99 employees)
- 1% already implemented
- 1% interested and planning budget for it
- 12% implementing in the next 12 months
- 41% interested but no budget for it
- 39% not aware (includes “don’t know”)

Base: North American and European hardware decision-makers at enterprises, mid-market, and very small businesses

Why Are Enterprises Interested in Cloud? What Are the Challenges Enterprises Face?

Benefits

- **Speed**
  - Easy/fast to deploy: 63.9%
  - Pay only for what you use: 61.5%
  - Less in-house IT staff, costs: 57.0%
  - Low monthly payments: 53.3%
  - Offers the latest functionality: 50.0%
  - Encourages more standard IT: 46.3%
  - Sharing systems/information simpler: 43.4%
  - It's the way of the future: 29.1%

Challenges/Issues

- **Security**
  - Performance: 63.1%
  - Availability: 63.1%
  - Hard to integrate with in-house IT: 61.1%
- **QoS**
  - Not enough ability to customize: 55.8%
  - Worried on-demand will cost more: 50.4%
  - Bringing back in-house may be difficult: 50.0%
  - Regulatory requirements prohibit cloud: 49.2%
- **Fit**
  - Not enough major suppliers yet: 44.3%

The Reality of Cloud Computing

Salesforce staff speared by phishers
By Tom Espiner, ZDNet UK
08 November 2007 09:21 AM
Tags: salesforce.com, social, phishing, messagebots, hack, attack, phisher, customer

Salesforce.com has revealed few details about a security breach caused by a phishing attack against an employee that surrendered internal customer database details.

Details of Salesforce.com’s customers were stolen as a result of the password being surrendered, the CRM services company admitted to customers on Monday.

Webhost hack wipes out data for 100,000 sites
Vaserv suspects zero-day virtualization vuln
By Dan Goodin in San Francisco • Get more from this author
Posted in Small Biz, 8th June 2009 20:02 GMT
Free whitepaper — Vulnerability management buyer’s checklist

A large internet service provider said data for as many as 100,000 websites was destroyed by attackers who targeted a zero-day vulnerability in a widely-used virtualization application.

Technicians at UK-based Vaserv.com were still scrambling to recover data on Monday evening UK time, more than 24 hours after unknown hackers were able to gain root access to the company’s system, Rus Foster, the company’s director told The Register. He said the attackers were able to penetrate his servers by exploiting a critical vulnerability in HyperVM, a virtualization application made by a company called LXT Labs.

Google Privacy Blunder Shares Your Docs Without Permission
by Jason Kincaid on March 7, 2009
253 Comments

In a privacy error that underscores some of the biggest problems surrounding cloud-based services, Google has sent a notice to a number of users of its Document and Spreadsheets products stating that it may have inadvertently shared some of their documents with contacts who were never granted access to them.

According to the notice, this sharing was limited to people “with whom you, or a collaborator with sharing rights, had previously shared a document” — a vague statement that sounds like it could add up to quite a few people. The notice states that only text documents and presentations are affected, not spreadsheets, and provides links to each of the user’s documents that may have been shared in error.

Hackers Plan to Clobber the Cloud, Spy on Blackberries
A new era of computing is on the rise and viruses, spies and malware developers are tagging along for the ride.

By Dan Nystedt
October 05, 2009 — IDG News Service — A new era of computing is on the rise and viruses, spies and malware developers are tagging along for the ride.

The new playground for hackers is the cloud, the term for computer applications and services hosted on the Internet. Some of the devices making the cloud more popular these days are BlackBerrys and other smartphones.

“The focus, or the lack of it, is definitely moving towards the cloud and to the security of embedded devices (Android, iPhone) to more advanced client-side attacks which leverage on Web 2.0 technologies, such as attacks on Facebook, Twitter and other popular sites,” said Dilshan Andrew Kannamaharan, host and organizer of the Hack in The Box (HITB) security conference in Kuala Lumpur, Malaysia this week.
Key Barriers to Cloud Computing

74% rate cloud security issues as “very significant”
Source: IDC

- Security
- Compliance
- Control
Cloud Security Challenges

- IT agility
- B2B collaboration
- Access control complexity
- Privileged user access

- Interoperability
- User experience
- Workload portability

- Data breaches
- Multi-tenancy
- Data location
- Compliance
SaaS, PaaS and IaaS

**Software as a Service**

Applications delivered as a service to end-users over the Internet

**Platform as a Service**

App development & deployment platform delivered as a service

**Infrastructure as a Service**

Server, storage and network hardware and associated software delivered as a service
Security with Oracle Cloud Platform

Platform as a Service

Shared Services
- Integration: SOA Suite
- Process Mgmt: BPM Suite
- Security: Identity Mgmt
- User Interaction: WebCenter

Application Grid: WebLogic Server, Coherence, Tuxedo, JRockit

Database Grid: Oracle Database, RAC, ASM, Partitioning, IMDB Cache, Active Data Guard, Database Security

Infrastructure as a Service

Operating Systems: Oracle Enterprise Linux

Virtualization: Oracle VM
- Servers
- Storage

Cloud Management

Oracle Enterprise Manager
- Configuration Mgmt: Assembly Builder, Capacity & Consolidation Planning
- Lifecycle Automation: Self-Service Provisioning, Policy-Based Resource Scheduling, Metering
- Application Performance Management: RUEI, SLA Management, Monitoring, Diagnostics
- Application Quality Management: Testing, Patch Management
Confidential documents and emails are moderately secure while stored (unused) within folders, inboxes and repositories.

But when used, thousands of copies are stored on desktops, laptops, wireless devices, USB drives, CDs/DVDs, CLOUD – inside and outside your organization!

How do you
- Secure all the copies, and audit access to them?
- Prevent copies being forwarded (or edited) inappropriately?
- Protect your confidential information within your customers, partners and suppliers?
- Revoke access to confidential information, when projects end or employees leave?
Managing Information Rights

• “Sealing” (encrypting) documents and emails protects them everywhere they go
  – Regardless of how many copies are made, and where those copies are stored and used
  – Including copies of documents and emails that leave your network!
• Oracle IRM Server centrally manages access rights, and audits usage
  – Even when users offline and IRM Server unreachable (via automatic synchronization)
Cloud Data Management

- Privileged database and OS user/admin abuse
- Lost backups containing sensitive data or PII
- Network eavesdropping malware
- Application exploits
- Application by-pass
- Regulatory infractions
Database Security Defense-In-Depth

- Encryption & Masking
  - Advanced Security
  - Secure Backup
  - Data Masking

- Access Control
  - Database Vault
  - Label Security

- Monitoring
  - Audit Vault
  - Configuration Management
  - Total Recall

- User/Role Management
  - Oracle Identity Management

© 2009 Oracle – Proprietary and Confidential
Oracle Advanced Security
Comprehensive Standards-Based Encryption

- Transparent data at rest encryption
- Data stays encrypted when backed up
- Encryption for data in transit
- Strong authentication of users and servers
Oracle Database Vault
Privileged User Access Control and Multi-Factor Authorization

- Keep privileged database users from abusing their powers
- Address Separation of Duties requirements
- Enforce security policies and block unauthorized database activities
- Prevent application by-pass to protect application data

select * from finance.customers
Oracle Audit Vault
Automated Activity Monitoring & Audit Reporting

- Automated Oracle and non-Oracle database activity monitoring
- Detect and alert on suspicious activities
- Out-of-the-box compliance reports
- Custom forensic reports

© 2009 Oracle – Proprietary and Confidential
Oracle Configuration Management

Vulnerability Assessment & Secure Configuration

- Database discovery
- Continuous scanning against 375+ best practices and industry standards, extensible
- Detect and prevent unauthorized configuration changes
- Change management compliance reports
Identity Management Challenges in the Cloud

The cloud model requires an identity infrastructure that is:

- Service-oriented
- Standards-based
- Loosely coupled
- Modular
Service-Oriented Security
Identity Services for the Cloud

Oracle Identity Management

- Identity Administration
- Role Management
- Directory Services
- Authentication
- Authorization
- Federation

Web Services

Oracle Apps

3rd Party/Custom Apps

Cloud Service Providers

- Discrete, easily consumable security services
- Rapid application security, improved IT agility
- Security seamlessly woven into applications

© 2009 Oracle – Proprietary and Confidential

21
Definition - Identity as a Service

- Refers to implementing identity, access and compliance management functionality predominantly as services in a service oriented architecture within the cloud or enterprise
  - Either cloud provider or cloud consumer, or both, offer identity services
  - The core platform is known as the Identity Services Platform
- Various lines of business applications, policy management applications, devices, and other services then leverage these services either autonomously or in an choreographed manner
Effective Cloud Computing requires all participants to have inter-operable identity services.

Every participant can be both the service provider and service consumer.
Design Considerations
Identity Services Platform

- Identity Hub
- Identity Assurance
- Identity Authorization
- Identity Administration
- Identity Audit
Identity Hub
Oracle IDM Point of View

- Accounts for Identity Storage and Repository Administration, Synchronization and Virtualization
  - Identity profile services with privacy controls (IGF)
  - Secure Storage of Credentials
  - Support for Cryptography through XML-Sig, XML-Enc etc
  - Out of the box plugins that offer connectivity to multiple repositories for OVD for true Identity Publishing
  - Common Virtualization layer at the J2EE Platform layer that can be adopted by any application
Identity Assurance
Oracle IDM Point of View

- Accounts for Authentication, (including MFA), Fraud Prevention, Identity Proofing and Single Sign-On
  - JAAS based Login modules offered through OAM
    - Support for traditional authentication schemes including LDAP, Certificate etc.
    - Support for newer authentication means including OTP etc in OAAM
  - Support for SAML, Kerberos, SPNEGO as well internet identity (OpenID, InfoCard etc) tokens in OIF
  - Interoperability across trusted domains through OIF
  - Exposed webservices in OAAM for risk forensics, that can tie into existing authentication engines, as well as identity proofing services
Identity Authorization
Oracle IDM Point of View

• Accounts for policy definition, enforcement and management
  • Exposed XACML-based policy engine in OES
  • JAAS based permissions and RBAC via OPSS
  • Data security – row, column and attribute level security by means of integration with Oracle VPD
  • Shared Authorization service at the Platform layer, adopted by OAM, OIM etc
  • Integrated Policy model which becomes the foundation for J2EE/.NET, Webservice based applications
Identity Administration
Oracle IDM Point of View

- Accounts for user and role lifecycle management, provisioning, and credential management
  - Expose all OIM Inbound & Outbound APIs as Web Services
  - Expand/Extend Inbound & Outbound SPML Web Services to support distributed architectures
  - Support various authentication and authorization policies for OIM SPML and other web services calls using Oracle Web Services Manager
  - Support for multiple inbound gateways and outbound agents – one per tenant for tenant specific security enforcement
Identity Audit
Oracle IDM Point of View

- Accounts for identity auditing, compliance reporting and analytics
  - Common audit framework delivered at the J2EE Platform Layer
  - Centralized Identity Warehouse that supports ETLs from various repositories both Oracle and non-Oracle
    - ETLs driven through Oracle Data Integrator
  - Offer support for pre-built reports for existing component areas, delivered through BI Publisher
  - Deliver Attestation Service through exposed webservices on the Identity Warehouses data
The Identity Services Platform

Systems and Operational Management

- Identity Audit
- Identity Administration
- Identity Authorization
- Identity Assurance
- Identity Hub
Summary: Identity Services Framework

- **Identity Provider**
- **Provisioning**
- **Authentication**
- **Virtualization & User Store**
- **Federation & Trust**
- **Policy & Orchestration**
- **Audit Connectors, Agents**

**Service Interfaces**
- **WS-*, SPML, SAML, XACML, IGF**

**Legacy Interfaces**
- **Connectors, Agents**

**Identity Services**
- **Authentication Authorization**
- **Provisioning Administration**
- **Identity Provider Role Provider**
- **Audit Federation & Trust**

**Enterprise Identity Management Infrastructure**
- **Policy & Orchestration**
- **Virtualization & User Store**
Regulatory Considerations for Cloud Security

- **Enforce Controls**
  - Segregation of duties
  - Access control

- **Monitor Controls**
  - Who accessed what?
  - Who changed what?

- **Streamline Processes**
  - Attestation / Recertification

- **Automate Reporting**
  - Out-of-the-box compliance reports
  - Customized reports
Case Study

Oracle IT
Evolution to Cloud
Oracle IT: Oracle Development
Self-Service Private Cloud

• Implementation Overview:
  – Scope/Scale - Over 2600 physical servers with over 6000 Virtual Servers used by over 3500 developers
  – Activations – Processing over 70 jobs per day, this translates into over 45,000 jobs processed supporting production and test requirements.
  – Utilization – Rates on these servers averages 80% 7 days a week and can reach 90% during peak times.

• Results/Benefits:
  – Increase in development productivity
  – Self-Service system for creation of development environments
  – Cleaner code lines as environments are created quickly for more thorough testing/validation.
  – Physical Server/Environmental Reduction by 75%
  – Server/Apps Deployment reduced by 80%
Oracle IT: Oracle University
Dynamic Provisioning with Grid Computing

- Education Services
- 2,300 environments automatically provisioned weekly
- 1/10th the hardware
- CPU utilization increased from 7% to 73%
- Floor space reduced 50%
- Power consumption reduced 40%
- Servers: Administrator ratio increased 10X
- Revenue/Server increased 10X
Cloud Security with Oracle Security Solutions
Real World Examples

- Offers managed identity services including managed fraud prevention and identity verification services
- Federated provisioning deployment spans hosted PeopleSoft hosted and on-premise apps
- Federated user provisioning to Microsoft Live
- Offers Oracle Identity Management Suite to partners as a hosted/managed service
For More Information

search.oracle.com

Search for: security solutions
In the section: All

or

oracle.com/security
ORACLE IS THE INFORMATION COMPANY