Demystifying the Cloud

OR

Cloudy with a Chance of Data

D. L. Corbet & Assoc., LLC

thelinuxguy@donet.com

Why 'The Cloud'

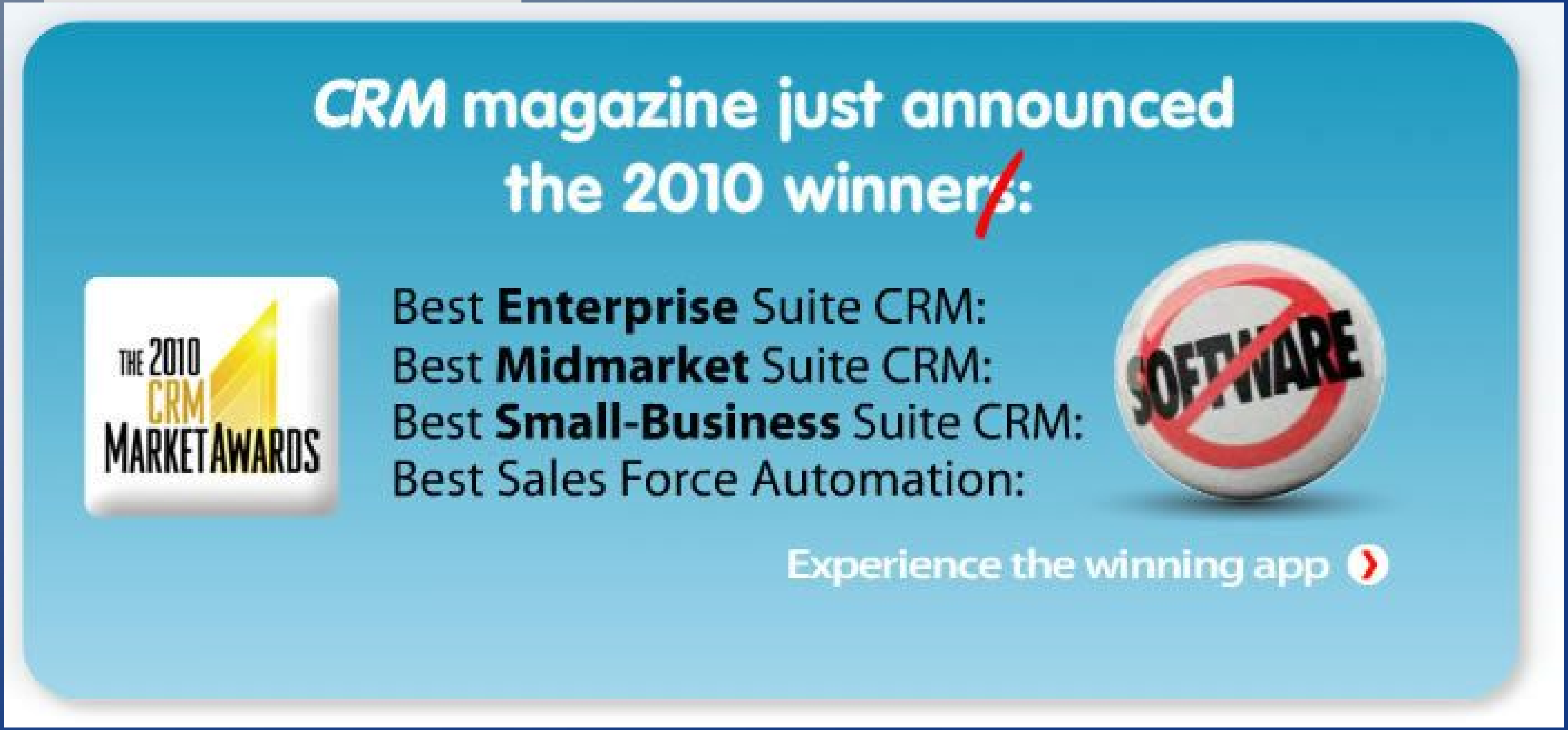
Common Clouds

Considerations and Risk

Why 'The Cloud'

- Distributed
- Very Large / Very Small
- Elastic
- Storage
- Processing

amazon.com®



CRM magazine just announced the 2010 winner~~s~~:

THE 2010 CRM MARKET AWARDS

Best **Enterprise** Suite CRM:
Best **Midmarket** Suite CRM:
Best **Small-Business** Suite CRM:
Best Sales Force Automation:

SOFTWARE

Experience the winning app ❯

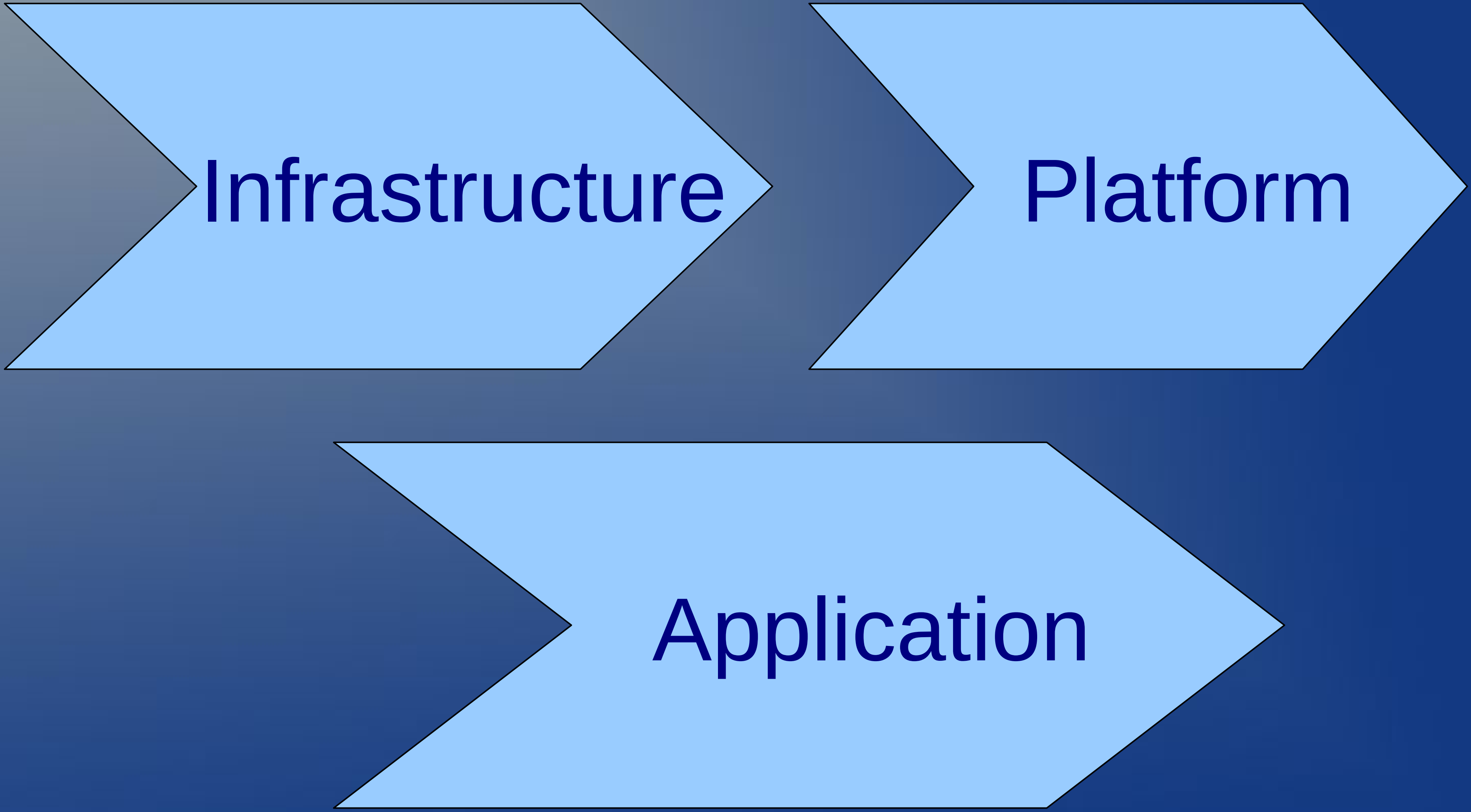
- Security - ssh, key pair (X509), port wrappers
- Cost - > 50% savings in yr 1

  0.10 / hr +
- Scale – CPU, I/O, Storage
- Utility Capacity, like electricity metered service.
- Need for Open Standards

Issues / Considerations

- Where is my data? (copies?!?)
- Civil / Criminal Restrictions
- Embargo / Contractual SLA's
- Who Admins the 'upgrades'
- Who is liable, accountable, and responsible?

Why 'The Cloud'



Infrastructure

Platform

Application

Infrastructure

- Load Balanced HaaS
- Physical vs Virtual
- Private, Public, or Hybrid
- Data Center CoLo

Infrastructure

- Public DNS
- Hypervisor Management
- ssh for CLI
- X for GUI

Platform - PaaS

- Images – Create Apps w/o lock-in
- Utility computing
- Instance Driven – Fedora, Ubuntu, Windows
- HPC / HA model

Application

- SaaS
- Elastic Availability – Released when finished; Auto Re-acquire
- Azure
- Google Apps

Application

- Multi-Tenancy
- Subscription based
- PAYGO
- Plug-ins for UI:
- Java, Ajax, VB, C++

Risk

- ChannelWeb warns to use caution entering 'The Cloud'

- Technology has moved us from computer, to cluster, to cloud and the paradigm is gaining momentum. Putting applications into the cloud and trusting data to be housed somewhere other than on-site introduces certain unknow security threats.

- ChannelWeb reports that the Cloud Security Alliance (CSA) and HP have combined teamed up, demonistrating key threats to cloud computing. They do also make recommendations on how to avoid many of this issues.

- Abuse And Nefarious Use Of Cloud Computing
- Because some cloud computing Infrastructure-as-a-Service (IaaS) providers offer an anonymous registration process, typically requiring little more than a credit card number to get up and running with cloud computing services, the cloud is ripe for spammers, malicious code authors and other criminals to work with relative impunity. This creates concern for possible password and key cracking attacks; distributed denial-of-service (DDoS) attacks; hosting malicious data; and a host of other potential hacks.

- The CSA recommends tighter registration and validation processes; enhanced credit card fraud monitoring and coordination; comprehensive introspection of customer network traffic; and monitoring public blacklists to quell potential nefarious use.

- Insecure Interfaces And APIs
- Since customers use software interfaces and APIs to interact with and manage cloud services, the APIs need to be secure. APIs should feature authentication, access control, encryption and activity monitoring and must be designed to protect against accidental and malicious attempts to circumvent policy. Additionally, as third parties, such as solution providers, build on the interfaces to add services for customers, the risk increases as customer credentials may now be in the hands of those third-parties. Insecure interfaces and APIs can result in unwanted access, improper authorizations, limited monitoring and logging and myriad other issues.

- To combat insecure interfaces and APIs, the CSA recommends users analyze the security model of cloud provider interfaces; ensure strong authentication and access controls are implemented in concert with encryption; and understand the dependency chain associated with the API.

- Malicious Insiders
- Malicious insiders are a constant struggle and in cloud computing environments that's no different. In fact, the CSA notes that the threat of a malicious insider increases in cloud environments. There is a lack of transparency into some cloud provider's processes and procedures means that a provider may not reveal how employees are granted access, how access is monitored or how it analyzes reports or policy compliance. Additionally, end users have little visibility into the hiring practices of their provider, which could open the door for an adversary, hacker or other cloud intruder to steal confidential information or take control of the cloud undetected.

- Protecting against malicious insiders, the CSA said, involves enforcing strict supply chain management and conducting a comprehensive supplier assessment; specifying human resource requirements as part of legal contracts; requiring transparency into overall security and management practices and compliance reporting; and determining a security breach notification process.

- Shared Technology Issues
- Since IaaS vendors offer services in a shared infrastructure to deliver a multi-tenant architecture, hypervisors are used to mediate access between guest operating systems and physical resources. Hypervisors can sometimes enable guest operating systems to gain inappropriate levels of control or influence on the underlying platform. The CSA recommends that strong compartmentalization be employed to ensure individual customers don't impact the operations of other tenants running on the same provider's cloud infrastructure and so others don't have access to another tenant's data or traffic.

- To protect against this, the CSA advises cloud computing users implement security best practices for installation and configuration; monitor the environment for unauthorized changes and activity; promote strong authentication access control for administrative access and operations; enforce service level agreements for patching and vulnerability remediation; and conduct vulnerability scanning and configuration audits.

- Data Loss Or Leakage
- According to the Cloud Security Alliance, the threat of data compromise increases in cloud computing. The cloud creates a new paradigm for possible deletion or alteration of records without backups of the original, or unlinking a record from a larger context to make it unrecoverable. The cloud also opens the door for unauthorized parties to gain access to data. The threat lies in the cloud's architectural characteristics. To thwart potential data loss or leakage the CSA suggests cloud users implement strong API access control; encrypt and protect integrity of data in transit; analyze data protection at both design and run time; and implement strong key generation, storage and management, and destruction practices. Further, users should contractually demand cloud providers wipe persistent media before it's released into the pool and specific provider backup and retention strategies

- According Or Service Hijacking
- A common security threat in any environment, account and service hijacking still exists in the cloud. Actually, the cloud adds a new threat to the landscape. From phishing and fraud scams to vulnerability exploitation, attackers can access credentials and passwords, which, let's be honest, are often reused. If an attacker gets those, they can eavesdrop on user activities and transactions; manipulate data; return falsified information; and redirect clients to illegitimate Web sites.

- While it sounds like common sense, users should prohibit the sharing of account credentials between users and services; leverage two-factor authentication where possible; employ proactive monitoring; and understand cloud provider security policies and SLAs, the CSA said.

- Unknown Risk Profile
- Because cloud computing reduces the amount of hardware and software a company has and also reduces the amount of maintenance, there is a clear financial and operational benefit. However, saving time and money could cause companies to lower their guard as it comes to security. Companies opting for "security by obscurity" may be the hardest hit as it can result in unknown exposures. It could also impair the in-depth analysis required highly controlled or regulated operational areas.

- Prevention starts with disclosure of applicable logs and data; partial or full disclosure of infrastructure details; and monitoring and alerting on necessary information, the CSA suggests.

Risk

Cloud Security Alliance

~ “ nefarious use ... DoS”

~ “ insecure API's”

~ “malicious insiders”

~ “loss and leakage”

~ “ service hijacking”

Must Have:

- HA/HP Elasticity
- Service Metrics
- SELF-Service On Demand
- Location Resource Pooling
- Ubiquitous Network

BYOC?

- Cloudo
- OOS.cc iCUBE
- eyeOS
- Xen Cloud Platform
- RHEV Cloud Foundation

Thank YOU

http://www.thelinuxguy.com/about.htm
http://www.mouseclickstv.com
http://twitter.com/linuxupdates
http://www.linkedin.com/pub/don-corbet/0/4a8/901
http://www.dlcorbet.com
http://www.facebook.com/don.corbet