What Should You Move to the Cloud, and How Do You Protect It?

David Giambruno
Senior VP & CIO
Revlon

Cloud Options

- Currently
  - Internal cloud (Revlon has deployed)
  - External cloud
- Future
  - Hybrid: “Black box” on site that provides processing power and data resides in your environment. Likely attached to your SAN.

Global internal cloud delivering world class performance: 99.99996 uptime. Pretty cloud…

Cloud Value Creation

Definition of "Revlon" Cloud: Internal

- Core
  - Virtualized servers
  - Virtualized network
  - Virtualized SAN
- Secondary
  - Virtualized applications
  - Virtualized desktops
- Tertiary
  - Virtualized databases
  - Virtualized transactions
  - Mobile devices on cloud
  - Delivering applications regardless of platform
- Future
  - Delivering "micro " apps based on device and user
    - Internal "Marketplace" apps

Cloud Security Principles

"Southwest" Model: 1 (One)ness / Common

1. Foundation:
   - Asset Management
     Know what you have and what you don't know
   - One Network:
     Common and logical IP Addressing scheme
     One DNS / DHCP structure
   - Identity Management
     Meta Directory
     Automation in Directory management (One ID per person)
   - One SAN
     Implement ALUA
   - Server and PC images
     Create common image (with overlays)

2. Virtualized everything
   - Servers
   - Network
   - SAN
   - Applications

3. One view of the world (Tool sets)

CLOUD – Why Internal

- External Cloud did not exist when we started
- Operate well before you put it out there. Do not “outsource” problem or unknowns.
  - Risks
    - **Cost Containment**
    - **Rate of change**
- FACT: Everything is on the SAN - ALL DATA, no matter if it is a file or an Operating System.
- Weekly global replication 21 TB of changes to DR.
  - That is 707 TB and $21.M a year if we did nothing
  - Data Reduction: Reduce volume 87% to 91 TB through WAN optimization
  - Second Pass de duplication and thin provisioning reduce storage by another 85% .
  - 91 TB is reduced to 13 TB, which actually has to be "physically" stored.
  - **Numbers are silly, but we go from $21m to $390k for organic growth.**

What worked..

- ABSOLUTE management backing.
  - This is a requirement in this space.
  - Forced adoption is a requirement.
- Technical managers.
  - No other department can be run by a non SME.
  - Generalists don’t close the books or engineer product.
  - Technology in context is important.
- Pressure testing:
  - Exposes problems fast.
  - Fails really big.

What worked (continued)...

- The day of discrete job roles is dying.
  - This model forces everyone to share, learn, and get involved in all aspects of the IT shop.
  - A virtual network is still down and is now everyone's issue.
- SIMPLE. Technology is OWNER implemented and maintained.
  - If you need an army of people to put it in, you may need that army to run it.
  - Sometimes a Casio is better than a Rolex… More dollars does not always get more function.
- Simple storage configuration.
- Global DNS / DHCP Grid
- Any standard (even a less than perfect one is better than a one off)
- Have smart people!

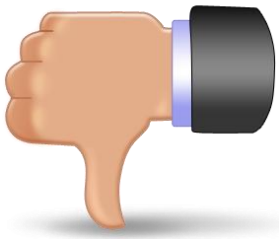
Results

- 531 Applications on internal cloud
- Reduced datacenter power consumption by 72%.
  - Datacenter is a “soccer field”
- Server build went from 12 man hours to 20 minutes
  - Commoditized required skill set – now a Help Desk activity
- “Backups” went from 17 hr 38 min (1058 minutes) to 15 minutes (Replication)
  - Backup is now replication (full replication DR – Data, Application, and OS)
  - Eliminated “back up” network
- Restructured server licensing
  - Decouples cost / server / networking / HVAC / IPKVM / Management

Results (continued)

- Leverage assets: Host to server ratio (free capacity increases)
  - 1 – 7 to 1-16 to 1-28.
  - Projecting 1-35 in 2011
- Storage Utilization
  - Production 86%
  - DR 1500%
- Self Management
  - Capacity Management – Move applications as needed
  - Geographical Management: Auto-build / destroy of servers as needed in the cloud

What NOT to do…



- Underestimate just how badly a 100 user network can be wrecked, but still kind of work.
- SAN provider has tools, understand them. They have individual capabilities.
- Underestimate how old or hacked a server can be and still run.
  - Software raid on old external shelves..Becomes your problem fast.
- Believe anything not photographed.
- “OK, Yes” does not mean “OK” or “yes” as you understand it.
- “Sure we can sell this in country”, not so much.

Mulligans (lets do this differently)

- Test Wide Area File Services: Failure will cause your cloud to implode.
  - Test VPN scenarios.
- Block alignment of P2Ved machines.
- FC vs. NFS
  - Use NFS wherever you can.
- Force a CIFS migration.
  - Everyone is already mad because you messed with “their” network.
  - Might as well go all the way.
- Places you may not want to travel generally have the worst connectivity.
- Implement ALUA. Do not bother with anything else. SAN is god, let it manage the hosts in the cloud.
  - SAN is the epicenter – hosts are immaterial.

Unintended Consequences

- Time
  - Massive reduction in time to do operational work
  - Required re-focusing team
    - Deploy a server anywhere in the world in under 20 minutes with ZERO costs.
- VM Server Sprawl (Who really cares)
  - Server having the same value as a file
- Servers just memory and CPU
  - Have to think about “logical binding”
- Vendors self selecting
  - Lack of Support or competing support means I won’t have you around
  - Automation beats labor arbitrage any day of the week
- Data Change Rate: Way higher than you think it is
- When it fails, it is BIG

Continuing Results

- Reliability
  - Six “9” (99.999906) uptime: Move people from operations to projects
  - Cloud makes ~15,000 AUTOAMTED changes a month with no human intervention.
- Speed
  - 295% increase in number of projects completed since we started this adventure (2008 – 2010). Same budget, way more activity.
- Accuracy
  - 1% failure rate in projects
  - 99.6% accurate on budget and timeline.
- Satisfaction
  - Highly engaged IM team
  - Very happy business units

How much should you do?

- Disclaimer: We make lipstick
- EVERYHTING YOU CAN
- First iteration so compelling we went to “all”
  - Crawl, Walk, Run
    - Phase 1: Start bottom up
      - File, print, etc.
      - Basic applications
    - Phase 2: Mid-Tier application servers
    - Phase 3: Front ends of major applications
    - Phase 4: Databases

Cloud Computing Threats

- Elegant “hacks” are made simpler and obfuscated
- Poor configuration: Self inflicted wounds
- Virtual Machine Wrapping: Machine in a machine in machine. Each has distinct presence.
- Where servers and services go and their policies
  - Wrapping servers & services with policies
- SAN: All of your data is on the SAN. SAN is shared medium.
  - Poor configuration of protocols (iSCSI since it is a virtual initiator as an example)
  - Rate of change and movement of data in SAN makes it hard to see if “badness” is happening.
- Devices (Mobile): The new attack vector
  - Foot in three networks (WWAN, 3G, Bluetooth)
  - Phone as SAN / Storage object

Cloud Security Observations

- Plus
  - Cloud demands homogeneity which, in many ways, makes Security "easier"
    - Testing and deploying patches
    - Testing and scanning applications
  - Much more control of data and applications
    - Virtual PC and Servers: CONTROL what can and can not be sent, printed….etc.
  - Much more fluid but self healing nature means less people touching it.
- Minus
  - Data density and change rate
  - Integrated nature of "cloud components" (secure multi-tenant)
  - Everything on the same wire

Security Policies: Some new, mostly the same

- **Most are the same old problem**
  - **Systems (Everything connected to the network)**
    - Complete asset inventory (computing, users, applications, and devices)
    - Configuration management
    - Deploy security patches within 30 days.
    - Update anti-virus software at least weekly and scan.
    - Vulnerability scan 24 X 7 X 365 (infrastructure and applications).
  - **Access Control**
    - Issue a unique ID to each person with network access.
      - No shared ID's on system (include connected systems / platforms)
      - Change passwords regularly
    - Default deny to data and systems
    - Segment network
  - **DNS / DHCP**
    - Secure DNS & DHCP to prevent hijacking
  - **Social Engineering**

Security Policies: Some New, Mostly the Same (continued)

- **New issues are fluidity and density. Everything is moving fast and more span of control**
  - **Virtual Firewalls**
    - Wrap critical / external servers with virtual firewalls that “follow” as moved in the cloud.
  - **Encryption**
    - Encrypt all sensitive data transitioning borders
    - Encrypt all data at external cloud
  - **Network**
    - Virtual system admins’ do not need network engineer to gain access to network traffic
    - SAN administrators can move data and get around logging
  - **SAN**
    - Secure protocols
  - **Delete**
    - Delete unused assets (review every week)

Short List: Things to Look For

- SAN
  - New object relationships
    - Clones, Mirrors, and “containers” can exist long enough to copy then go away.
  - API Engine: Calls and events
    - Client software used for backup and disk management can initiate relationships. Vendors need better, more intuitive, RBAC and compartmentalization.
    - Common OS exploits can be used to gain highest access to SAN through client software.
  - Protocols: Default Deny
    - Secure iSCSI initiator list.
    - Secure NFS export list with port security.
    - Tie protocols to ports. Short of NFS4, which is not supported by largest VM vendors.

Short List: Things to Look For (continued)

- Network
  - Deep packet inspection of everything leaving your core. Why would a replication protocol be talking to a Desktop, Laptop, or Phone on the edge using CIFS ports?
  - Storage protocols should stay in “reasonable” places.
  - Prune trunks going to VM systems, expose as little as needed.
  - If it really is that important, put it on a secure net.

- Virtual Environment
  - Secure virtual switching (role based access control)
  - Restrict guests from ability to change their mac.
  - Restrict private networks between machines. IE lowsec machine can be on a private net with hisec machine. NICs can be added and removed dynamically from guests.
  - Restrict promiscuous modes.
  - Syslog everything.

Security Issues on the Horizon

- SAN is the new target in cloud computing.
  - Has all the DATA.
  - Moves very fast / change
  - Don’t attack hypervisor attack the San
- Mobile devices
  - Run virtual machines on mobile devices
    - Run “servers” on virtual machines
    - WLAN, 3G, BlueTooth
    - Pump data out any number of ways.

Next Cloud Evolutions

- SAN Transaction Management
  - SAN and Database integration to push transactions (and associated infrastructure / services) out to the edge and mage it back to core.
    - SAN managing record locking
    - Automatically building database and application tiers at the edge to handle transactions.
- Transparent Virtual Application Delivery
  - Trusted WAN: Eliminate the LAN for transparent access for devices to deliver applications via thick, this, virtual.
- Mobile devices
    - Deliver virtual apps to any device
    - Interface and real estate issues
    - Application transformation (Workflow, kPi, Yes /No)

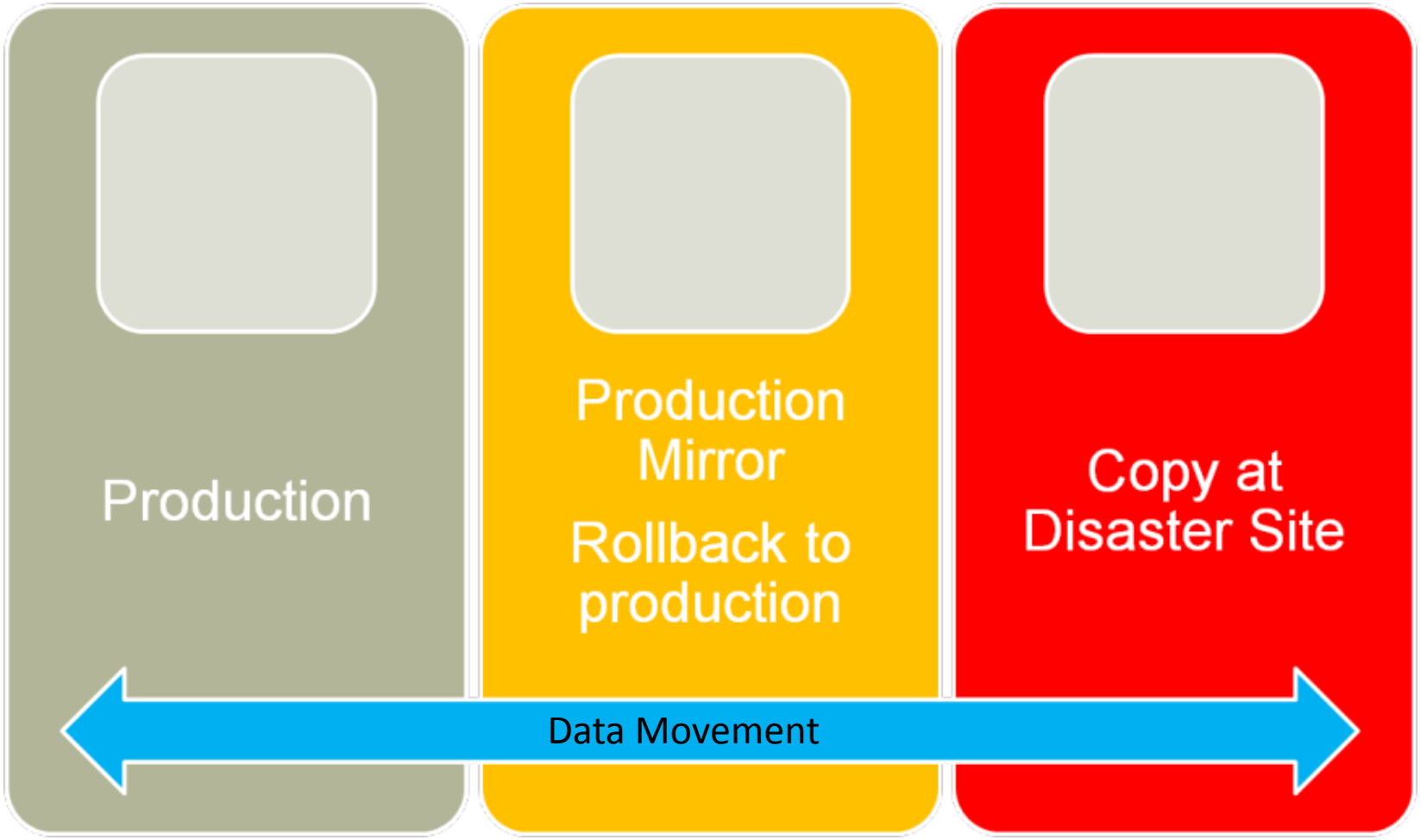
Reference Material

Single Pane of Glass
Global Monitoring of Global Cloud Capacity

Example of an Actual Non U.S. Data Center

All non U.S. data centers replaced with this footprint. Acts as cloud capacity to move applications and services around the planet. Lots of empty rooms….. Fully remotely managed. What we call a DRiB.

Global Cloud Replication and Recovery: Simplify



Change Disaster Recovery Model

- Remove complexity by just copying it all – all means “all”
  - Move towards indiscriminate recovery capability to remove dependency mapping
    - Technology stack enables minimal moving parts
      - Virtualization: Everything is a file, recover OS, application and data
      - SAN: Easy replication, reduced skill sets (WYSIWYG)
  - Falling technology price point enables strategy
  - Simplicity allows for labor reductions

- Scalability
  - Process gets replicated
  - Global management
  - Wide Area File Services (WAFS) allows for over wire backup without linear cost

Thank you!

David Giambruno
Senior VP & CIO
Revlon