Covering my IaaS: Security and Extending the Datacenter

Brian Bourne
Tadd Axon
• Tadd Axon - Holds a Bachelor of Business Administration with a minor in Spanish from Wilfrid Laurier University. Went to school with every intention of becoming an accountant (CMA, if you’re curious)

• Brian Bourne – A management guy still trying to be technical.
Cloud Basics
Applications delivered to the consumer running from the provider’s infrastructure.
Used by business users for email, office automation, CRM, ERP, etc.
IDC Numbers: $993M in 2013 growing to $2.04B in 2017

Software as a Service – SaaS

A computing platform typically including operating system, programming language execution environment, database and web services.
Used by developers and application providers.
IDC Numbers: $105M in 2013 growing to $554M in 2017

Platform as a Service - PaaS

The provisioning of processing, storage, networks or other fundamental computer resources where the consumer can run arbitrary software
Used by IT administrators
IDC Numbers: $62M in 2013 growing to $372M in 2017

Infrastructure as a Service - IaaS

* Also note that private hosted solutions were $170M in 2013 growing to $554M in 2017
Cloud Defined

Public: Shared services or resources provided by a third party and available to many participants or tenants.
- Community Cloud – Participation limited to specific demographic.

Private: Cloud computing resources open to just the owner. Can be hosted on-premise or off.

Hybrid: Cloud computer resources spread between your own systems and a third party’s resources.
Infrastructure as a Service Detailed

IAAS is three building blocks

- Storage
- Network
- Compute

- All IaaS services fit into one of these buckets
- Operational SLAs backed by contract
- Certain levels of regulatory compliance and security backed by contract
**Typical IaaS Deployment Scenarios**

- **Bottomless storage** (NetApp, StorSimple, etc)
- **Backup** (CommVault, Veeam, etc)
- **DR Plans** (Hot-Hot, Hot-Cold, HyperV Recover Manager, VMWare vCloud Hybrid Service)
- **Extended Datacenter**
  - Treat the cloud provider like another one of your own datacenters
Network
Networks are all virtual (Software Defined)

- Optional MPLS-like connectivity
- VPN Connectivity:
  - Site to Cloud
  - Multi-Site to Cloud
  - Point to Cloud
  - Cloud to Cloud (Within Cloud and Cross-Provider)
- Load Balancing
- Traffic Management
- Content Delivery Network *
Security Considerations

- Traditional “data in transit” concerns
- Traditional “end point attack vector” concerns
- Egress Monitoring
- Traditional security zones that you have in your current DC are not simple to implement in cloud
  - Getting progressively simpler
- Short list of supported on premise hardware for VPN scenarios
  - Can always be made to work but you better understand IKE proposals and possibly BGP
Security Mitigations

• Manual ACLs on host or network layers as supported
• Host-based controls such as IPS and local firewall
• Network isolation (varies by provider)
• Protect data in transit (VPN or host IPSec rules)
• Pick your algorithms carefully
• Careful management of cloud to Internet gateways and endpoint mapping
Storage
Storage Architecture

Bottomless pit of storage
- How much do you want to spend (this billing cycle)?

Highly Available Storage
- Great for availability (varying degrees of redundancy)
- Marginally increased attack surface

At rest protection:
- Base physical layer crypto by cloud provider
- Managed destruction

“All your storage are belong to API”

- Encryption of your data (file, blob, VHD, whatever) is another matter
Security Considerations

- Access to tenant = (usually) unfettered access to storage
- Data sovereignty / regulatory requirements
  - Spoiler: Really a BC only problem
  - Contract wording and commitments
- Data remnants, replicas and backups (who knows where they go)
Mitigations

• Management of API keys and certs is paramount
• Role based access control models are evolving
• “Third Party” products and services to encrypt workload data
• Volume-level Crypto
  • Leveraging O/S features or vendor specific toolkits
• Item Level Crypto
  • Traditional encryption options
  • Digital rights management solutions
• Application Containerization
• Worry about:
  • Who has access to keys (on premise or in cloud)
Compute
• Virtual machines
  • Multiple OSes available
  • Some with pre-loaded software
    • DBMS, ERP, Configuration Management…
  • “Official” and “Community” contributed images
  • Bring/Brew your own image

• Virtual appliances
  • Load balancers, application proxies, firewall

• Available in (nearly) any flavour and any size
Compute Considerations

• Who built that image?
• Who manages patch level?
• Traditional firewall solutions will not work
• Multiple network connections can be difficult or impossible
• VM to VM attacks and Hypervisor to VM attacks
• “Normal” considerations for any internet connected machine
• Provider side attacks
  • Provider initiated
  • Fallout from a provider hack
Compute Mitigations

- “Normal” protections (AV, HIDS/HIPS, etc)
- Host hardening is critical
- Domain isolation and network isolation
- Careful care of image management for VMs
- Service-level ACLs on VM endpoints
- End point monitoring
- Single NIC, WAF and reverse proxy solutions
Control Plane
Control Plane Realities

- Overall lack of granularity of delegation
- Remember the unix “all or nothing” problem?
- Major players are making moves to enable RBAC
- “Maturing”
- Serious degree of trust required for cloud admin
- At the VM level, normal controls for O/S, application platform are still available
Summary
In Summary

- IaaS brings many advantages operationally
- IaaS also brings some security challenges
  - Some of these are old
  - Some of these are new
- The extended datacenter model makes “traditional” security good practices even more important
- Encryption becomes a more interesting proposition
- Key management practices become more critical
Questions & Answers

Contact Us:
• Tadd Axon
  • @grey_area
  • tadd.axon@softchoice.com

• Brian Bourne
  • @brianbourne
  • brian@sector.ca

THE END