Information Security Decisions

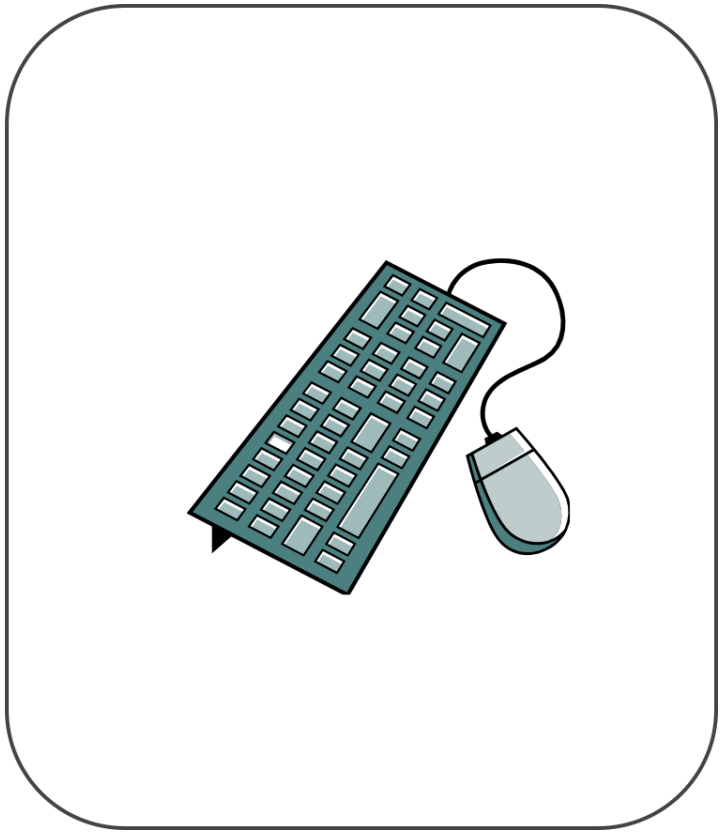
TechTarget

Data Security for Cloud Computing

Rich Mogull, Analyst & CEO, Securosis, LLC
@rmogull

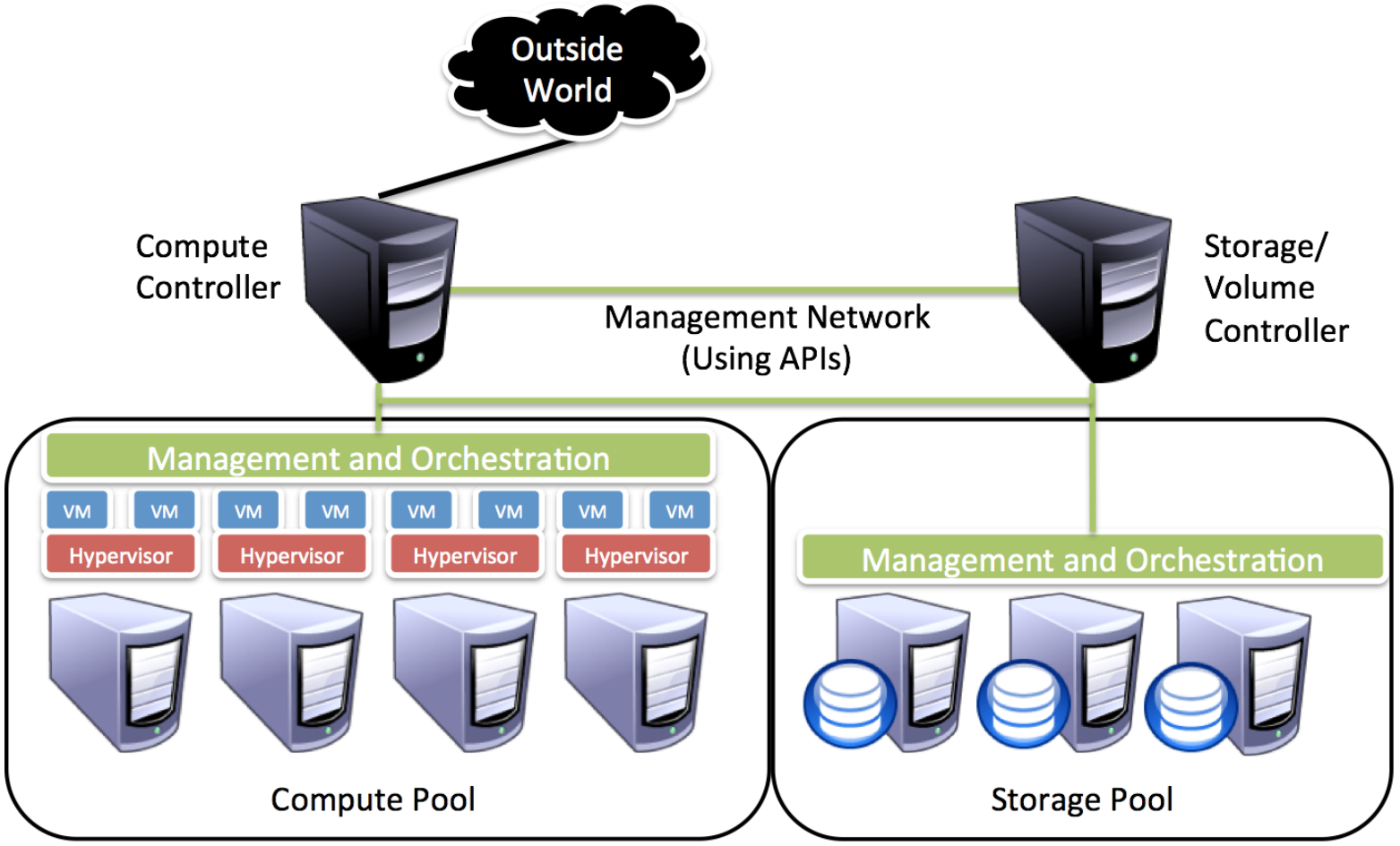
To Steal a Data Center

Old School



Cloud School

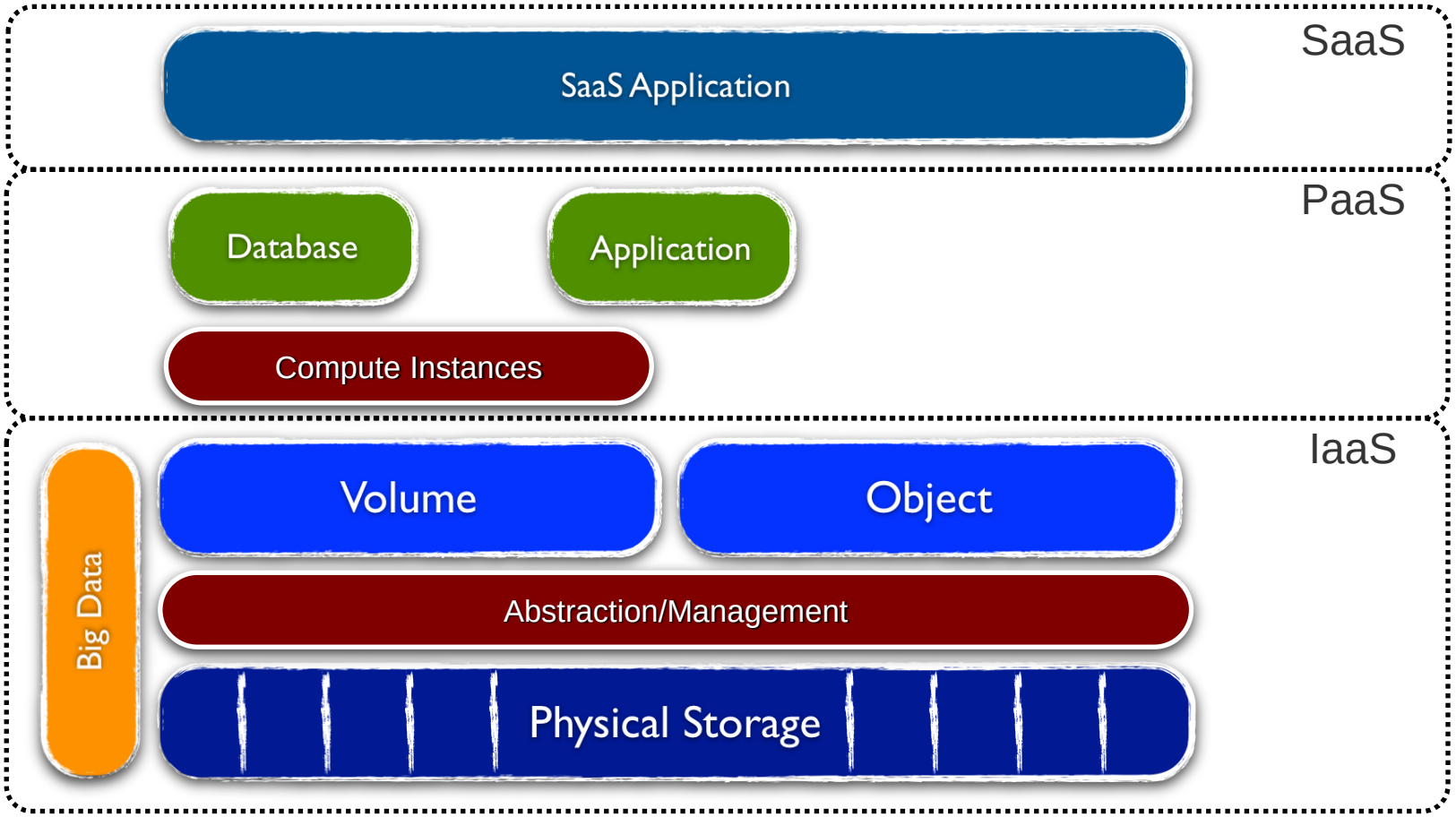
How IaaS Works



TechTarget

How Clouds Store Data

Cloud Data Architectures



Cloud vs. Trad

- Pooled physical storage
- Management by API
- Slower read/write, faster snapshot/migration
- Multitenancy

Photo by richiejarvisuk - http://flic.kr/p/7azb6u

TechTarget

Data Dispersion

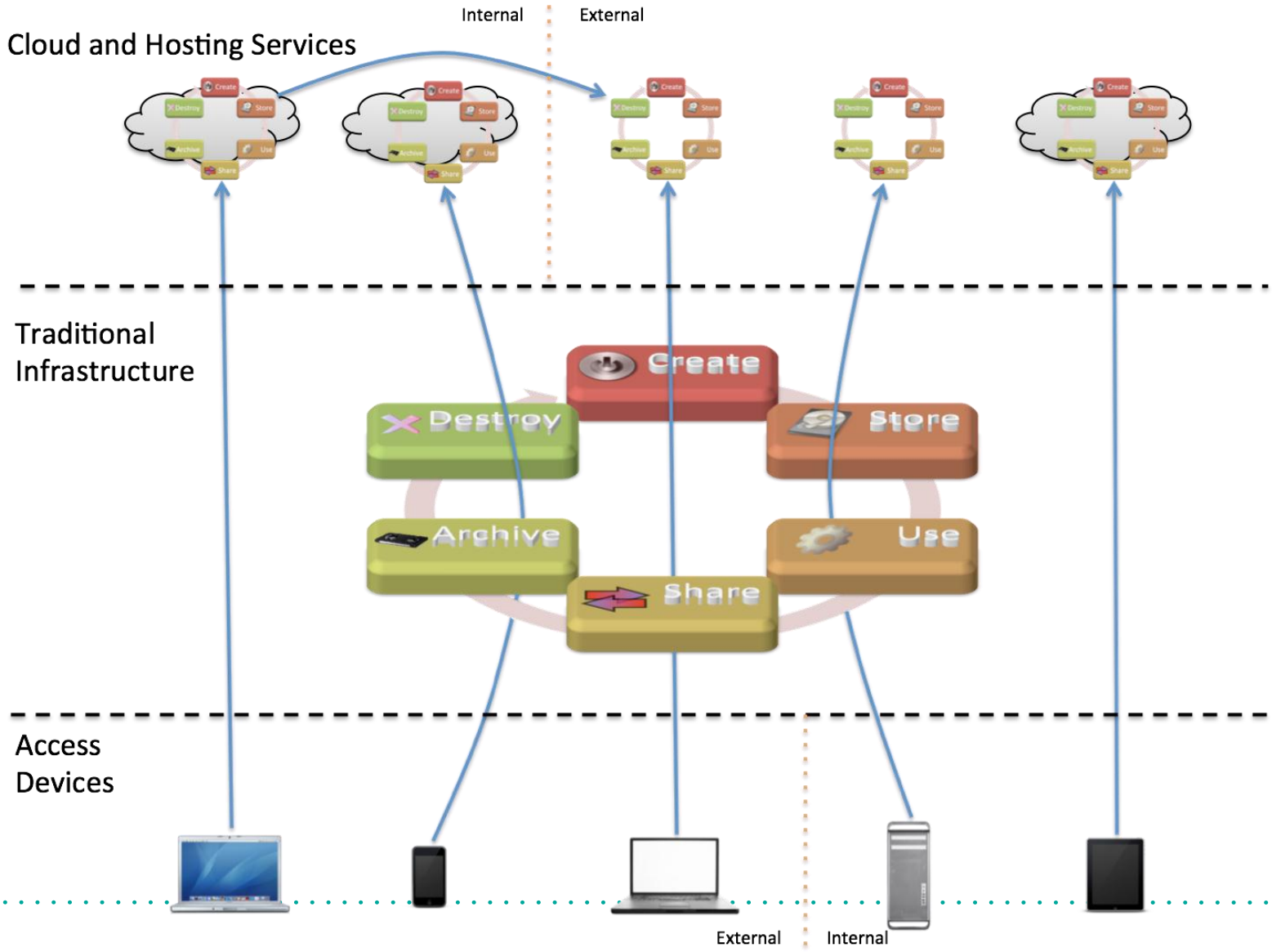
TechTarget

The Pragmatic Process


Assess
Manage Cloud Migrations
Secure Transfers
Encrypt
Monitor

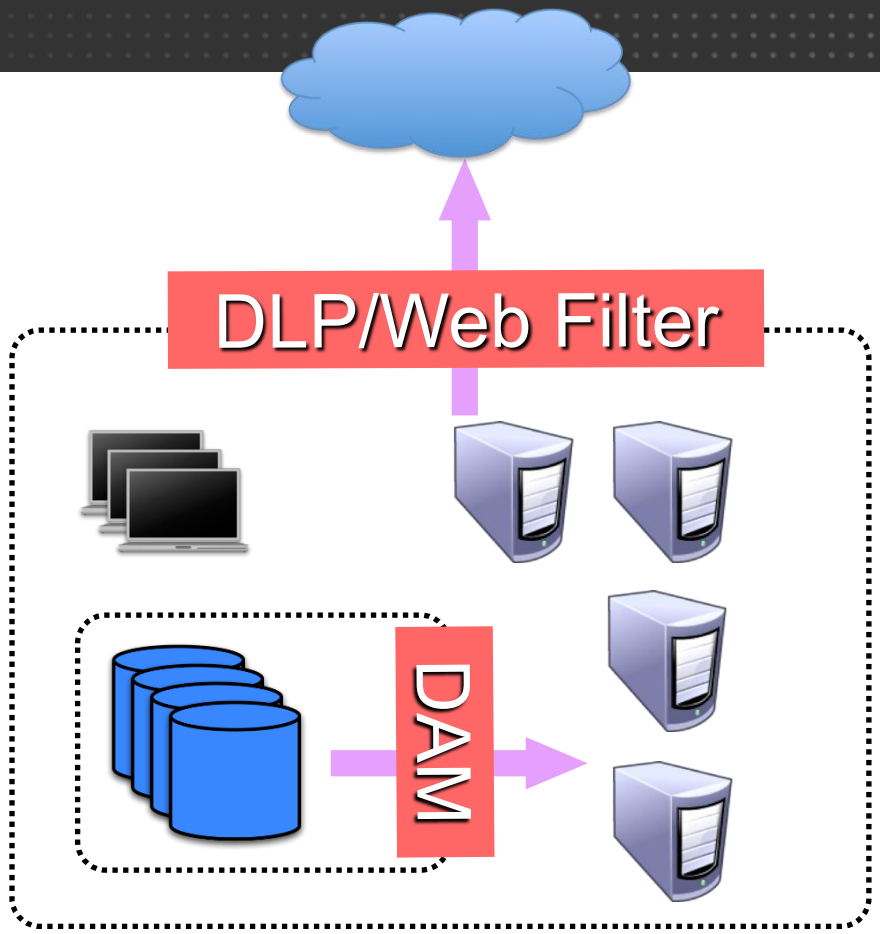
TechTarget

Assess


Internal
External
Cloud and Hosting Services
Traditional
Infrastructure
Create
Destroy
Store
Archive
Use
Share
Access
Devices
External
Internal

TechTarget

Manage Cloud Migrations


DLP/Web Filter
DAM

TechTarget

Secure Transfers

Encryption

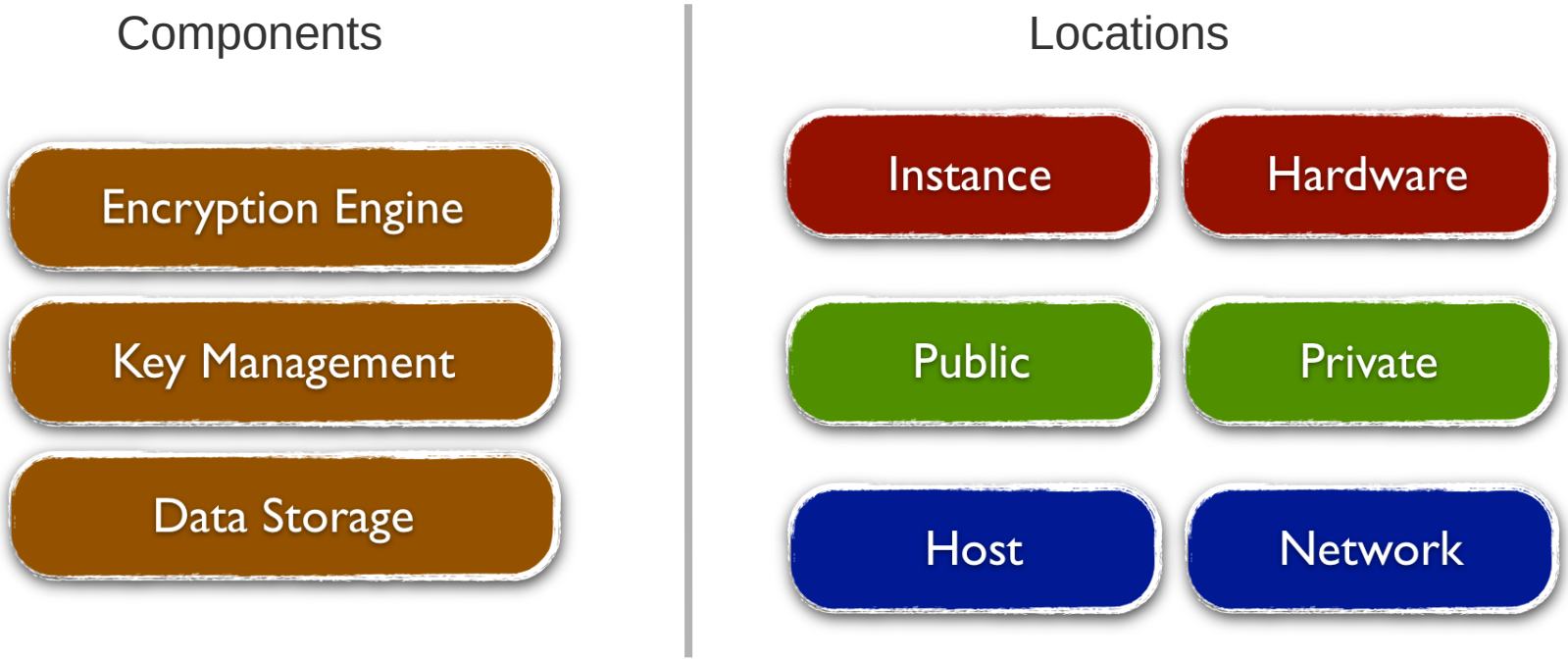
- Link/Network
- Client/Application
- Proxy

Photo by mbrand - http://flic.kr/p/61DP51

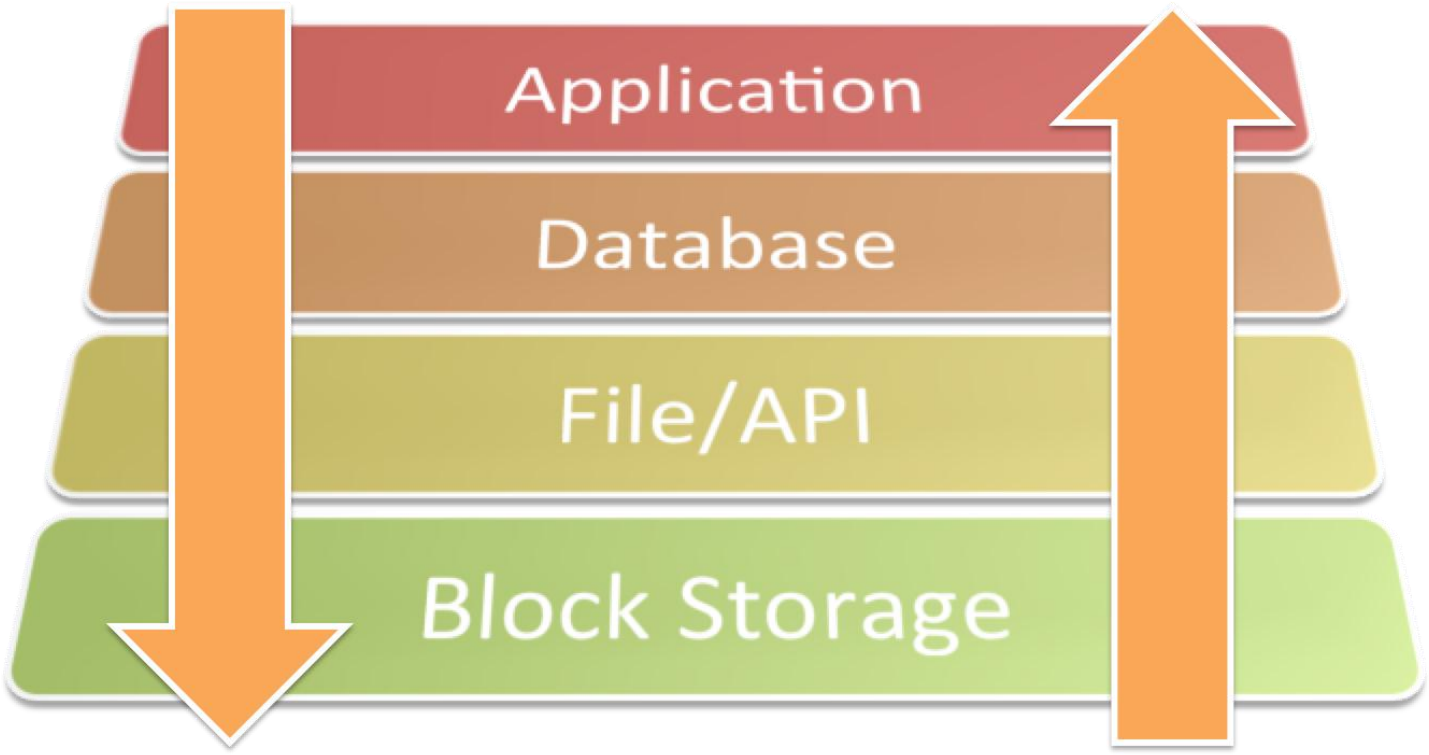
TechTarget

Encrypt

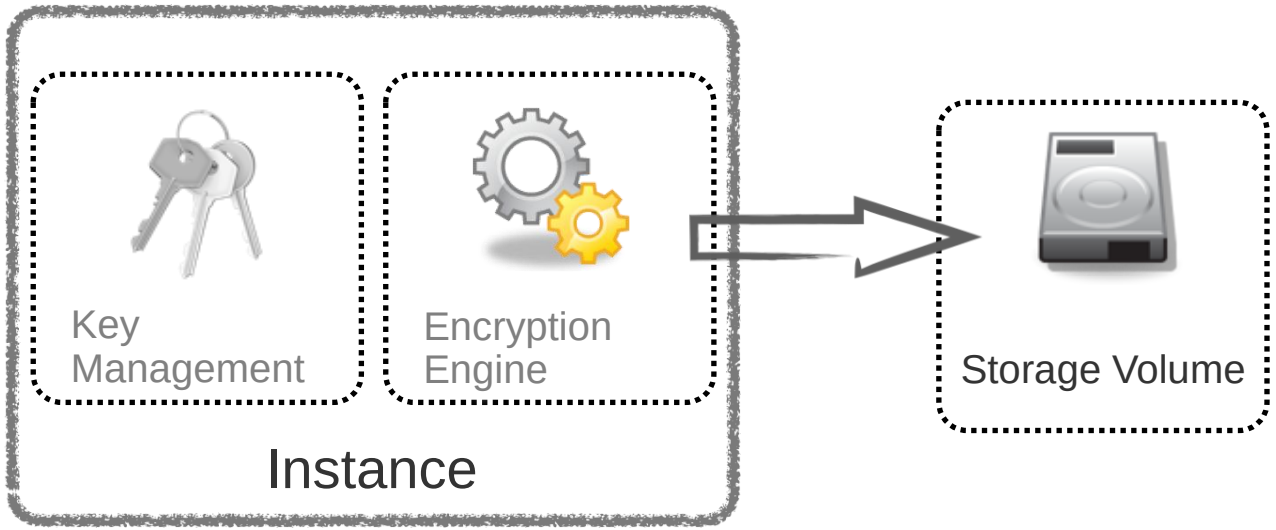
Encryption Matrix



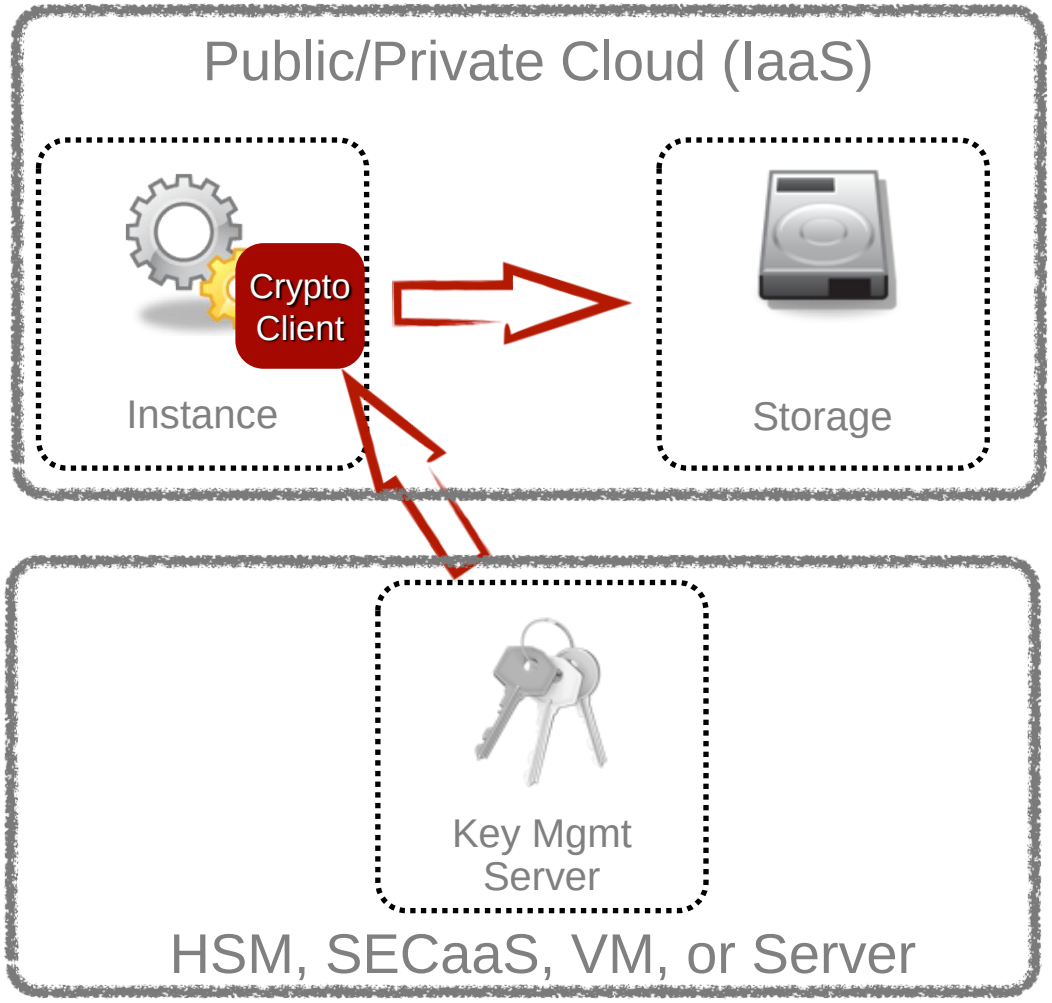
Encryption Layers



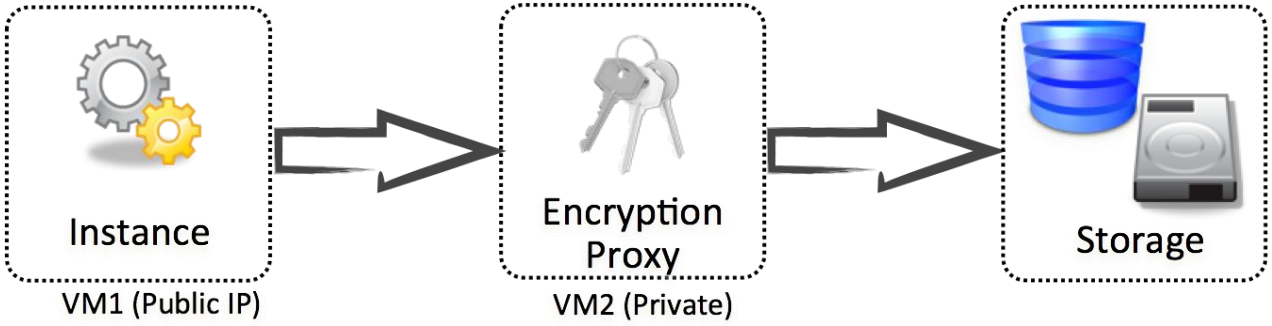
Instance-Managed



External Key Management



Proxy


Instance
VM1 (Public IP)
Encryption
Proxy
VM2 (Private)
Storage

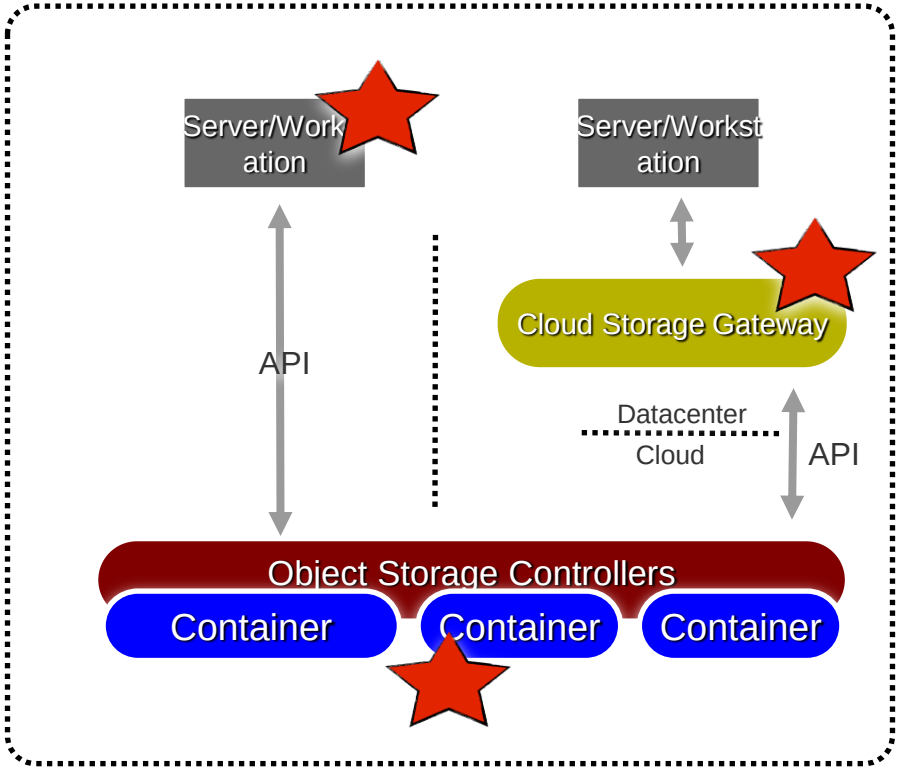
(Proxy)

How to Choose

- Instance is easiest. Built into most operating systems.
- External more secure/flexible; easy to tie to existing infrastructure. Go with agent-based.
- Proxy for databases and more-complex storage situations.

Encrypting Object Storage

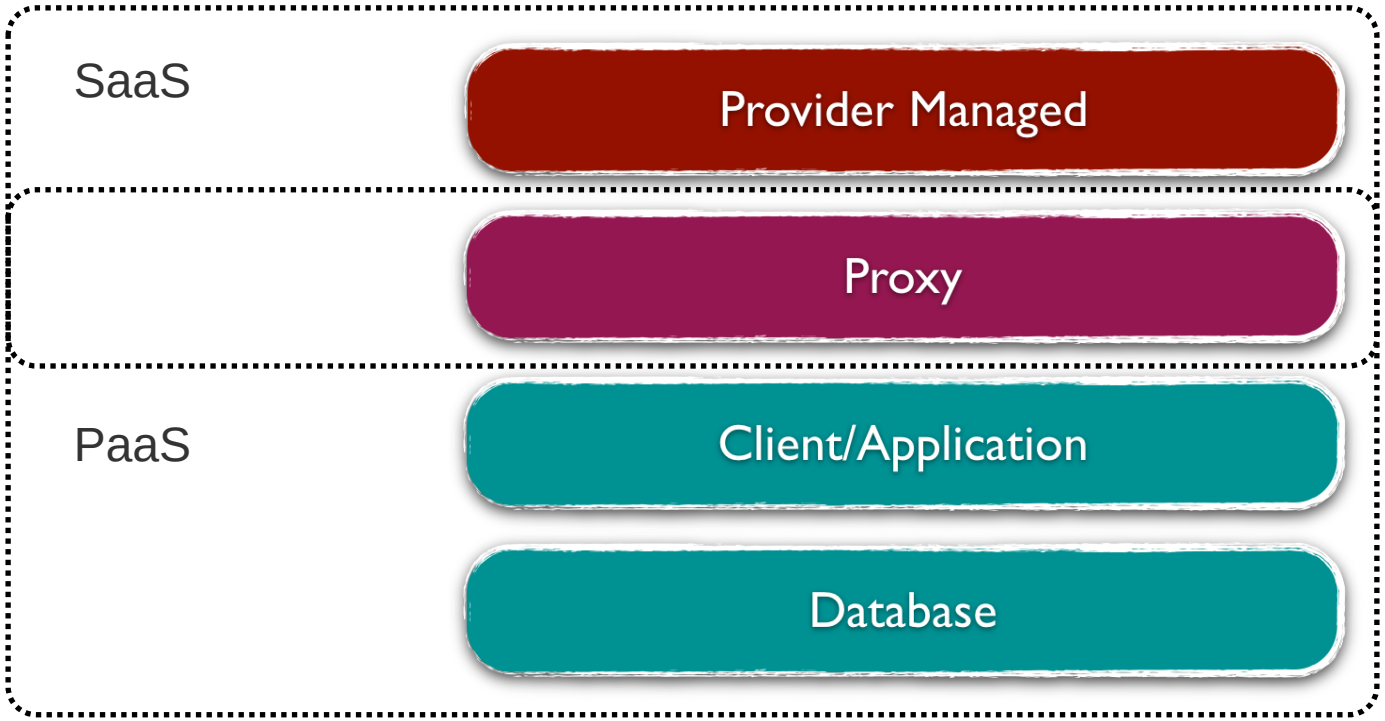
- File/Folder
- Client/Application
- Proxy


Server/Work
ation
Server/Workst
ation
API
Cloud Storage Gateway
Datacenter
Cloud
API
Object Storage Controllers
Container
Container
Container

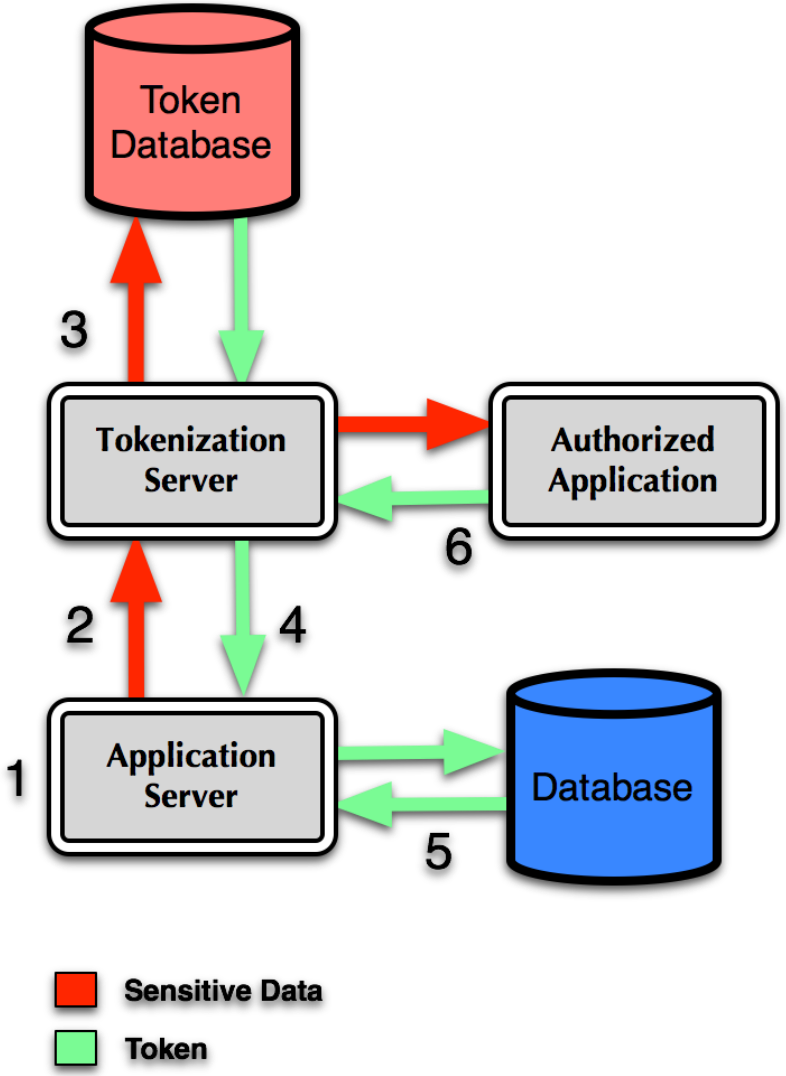
How to Choose

- Try to find storage services that support encryption in the client.
- Use file/folder for public cloud object storage (e.g. DropBox, box.net, S3), or when extra protection needed in private cloud.
- Consider proxy for server-to-object sync.

Encrypting PaaS/SaaS



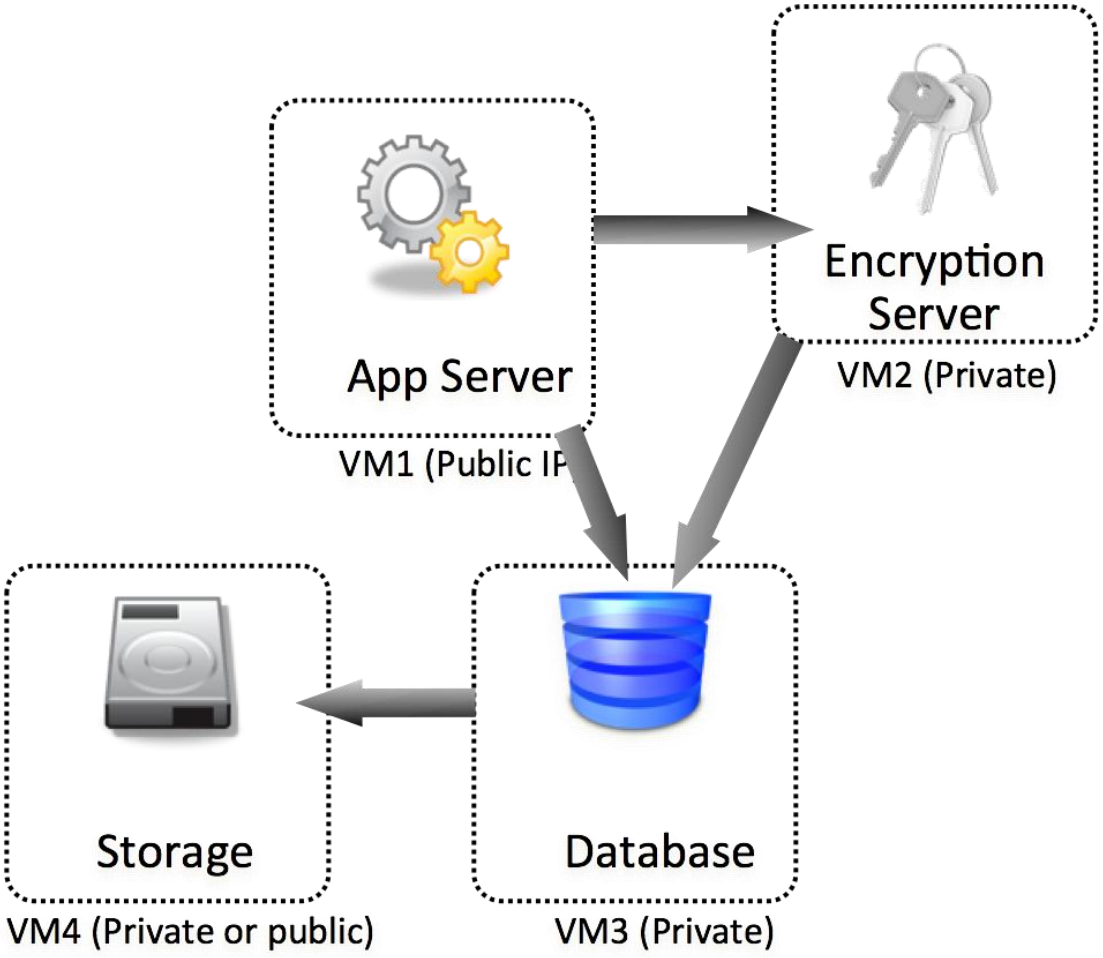
Tokenization



How to Choose

- PaaS is freaking hard to get right. Code into your application if you can. Use a proxy if you can’t. Watch the key management.
- Prefer a SaaS provider you trust.
- Proxy (encryption or tokenization) for SaaS if you have to, but keep it simple.

Application Encryption Architecture



TechTarget

Monitor

Content Discovery

- DLP
- DAM
- Cloud awareness and limitations

Photo by ...-Wink-... - http://flic.kr/p/6hTHYH

Data Loss Prevention

- Agent or hypervisor-based for private cloud.
- Good for content discovery, less good for in-cloud monitoring.
- SaaS for discovery should be available soon.

Database Activity Monitoring

- Must be agent based.
- Physical server okay for private, not good for public.
- Virtual appliance for public.
- Watch that performance.

Digital Rights Management?

- Maybe for consumer.
- Enterprise DRM complex beyond workgroups, never mind cloud.
- It will happen... maybe in 5-10 years.

What We Skipped

- Hardening the management plane.
- Internal segregations for private cloud.
- Authentication and Authorization.
- All the little details- encrypting an IaaS volume is easy; encrypting a distributed cloud application is hard.
- The future.

What to Do

- Control data migrations with DLP, DAM, and FAM.
- Use the lifecycle to define your controls.
- Spend most of your cloud data security time on getting encryption right.

Thank You!

- Rich Mogull
- Analyst/CEO
- nexus.securosis.com
- rmogull@securosis.com
- @rmogull