Datacastle


Automatic PC Backup and Recovery


At Rest Encryption


Remote Data Deletion


Port Access Control


Device Trace

IT Security Automation Conference 2009

"Endpoint Data Protection (EDP) In The Cloud"

Gary Sumner
Founder & CTO
Datacastle Corporation

garysu@datacastlecorp.com

Top ~~10~~ 8 Lessons Learned

#1 Means to an end, not end in itself

#2 Automated key management is, well, key

#3 Keep control at the top where it belongs

#4 Multi-tenant everything

#5 Client deduplication over encrypted data

#6 Web access, be careful what you ask for

#7 Expect and plan for failures

#8 Deployment flexibility

#1: Means to an end, not end in itself

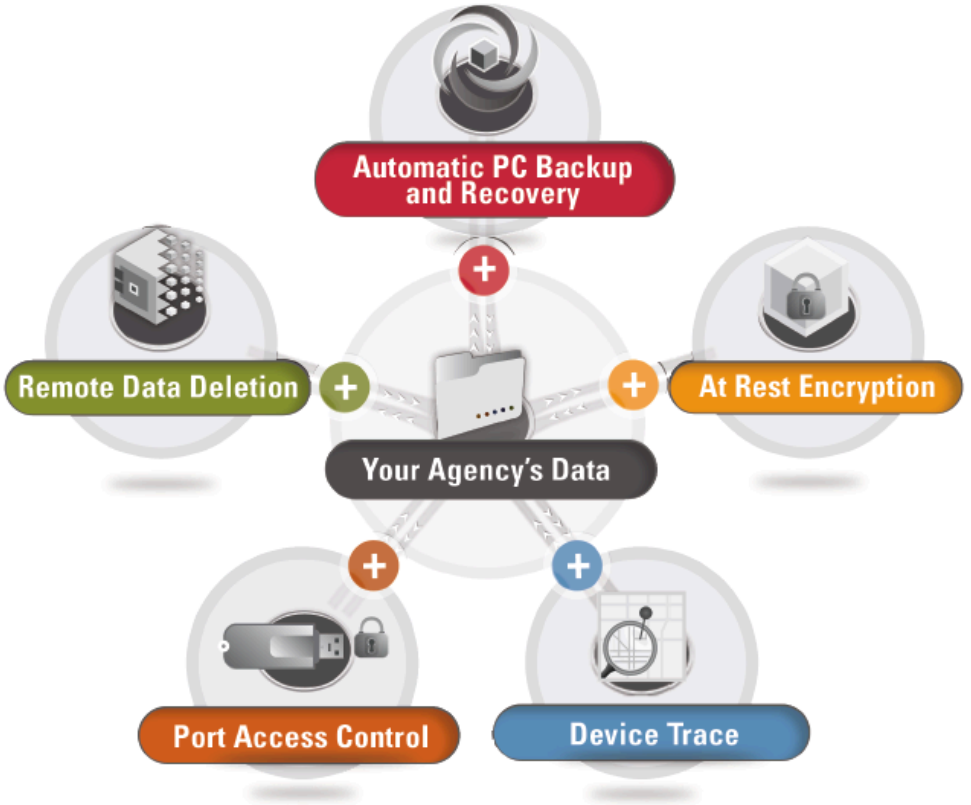
Anti Virus != EDP

Data Loss Prevention != EDP

Why even run any of these tools?

Your data is “valuable”

EDP needs to be multi-faceted



#2: Automated key management is, well, key

Cryptographically random keys required

Manual key management doesn't scale past more than a handful of keys

Hard to get right, so most solutions push problem to end user
- Password derived keys significantly weaken effective key strength
- Easy for hackers to crack with regular cracking tools

Not just about initial key generation and key management
- complete key life cycle management
- policy driven, automated key rotation

#3: Keep control at the top where it belongs*

Can't rely on end user behavior

All aspects of client agent functionality needs to be able to be policy driven
- What, Where, When, How Often, How Long

Policy changes should auto-propagate within defined window

Ideally end user doesn't even know they are being protected
- Silent install, auto-activation, policy configured

* Name the movie featuring a young Matthew Broderick that this line was unashamedly lifted from?

#4: Multi-tenant everything

Cloud services = shared infrastructure

Security and privacy shouldn't be compromised

Management portal needs granular delegated permissions

Hierarchical policy inheritance

Storage deduplication based on arbitrary logical separation

Tenant requirements may dictate physical separation of storage

#5: Client deduplication over encrypted data

Encrypted data and data deduplication work totally against each other

Encrypt in transport, deduplicate on server, then encrypt in storage

For client side deduplication, server side needs to control, or at least have access to keys

Keys need to be shared and passed around

Datacastle has designed and built a system that allows for client side deduplication of encrypted data without decrypting it first or sharing of encryption keys.

#6: Web access, be careful what you ask for

This one goes hand-in-hand with #2 around key management

Web portal where protected data can be accessed from anywhere

Great convenience, but at what cost

- Privacy and security are now compromised
- File system metadata stored in the clear
- If not, server needs to know your encryption key
- Password based key needed
- Server administrator can now easily get to your data

#7: Expect and plan for failures

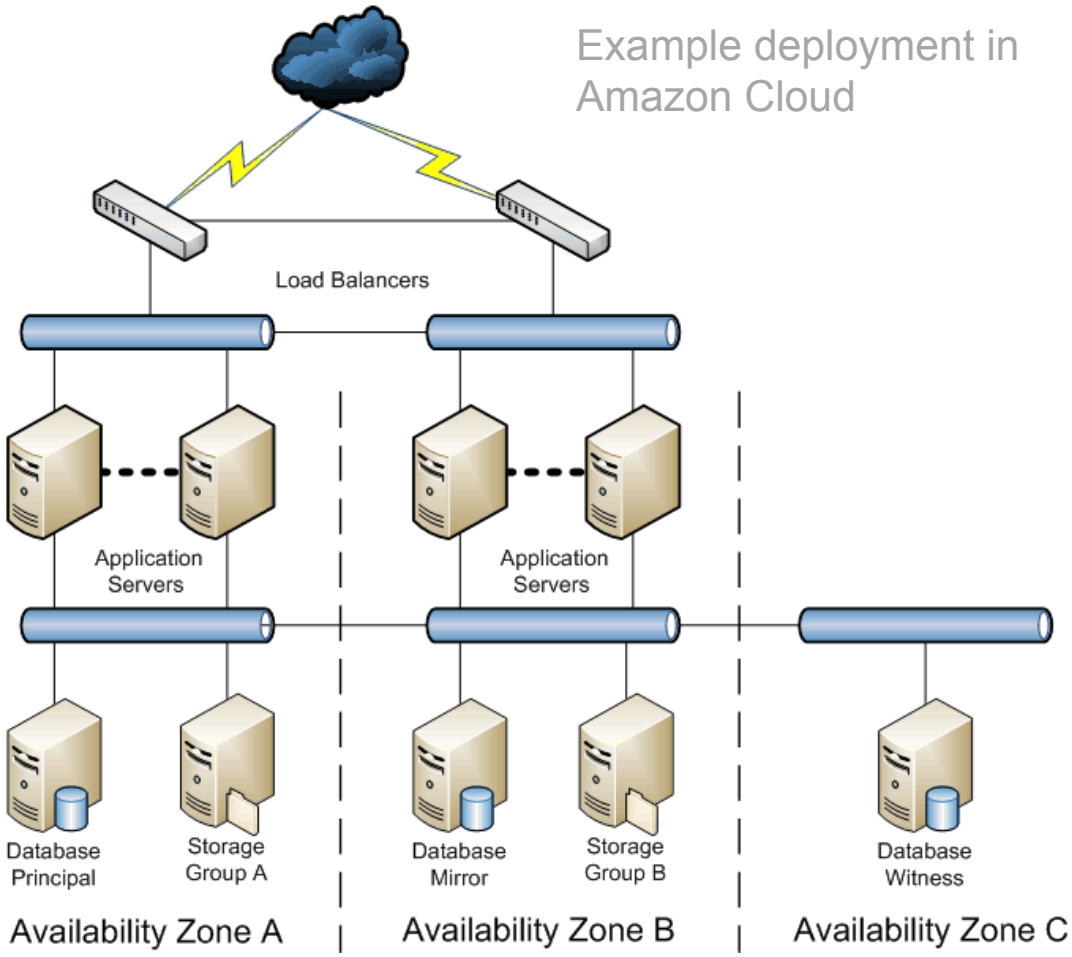
The downside of scale

Use commodity components

Stateless application tier

Fail gracefully
- Allow clients to work offline
- Support reverting database

Example deployment in Amazon Cloud



#8: Deployment flexibility

Internal IT model really no different than external 3rd party multi-tenant model

Client deployment model differences

- Silent deployment
- IT need to be able to recover device
- Auto activation synched with internal domain

All communication should go over HTTPS

Support deployment to internal IT data center, 3rd party partners data center or via the cloud without changing software.

Datacastle


Automatic PC Backup and Recovery


At Rest Encryption


Remote Data Deletion


Port Access Control


Device Trace

OK, just one marketing slide

Support for running on Windows in FIPS mode utilizing FIPS validated crypto libraries (Dec 09)

Automated encryption key rotation by policy (1H10)

Secure Web Access (2H10)

Available on Apps.Gov today via a partner delivering a cloud service from a "Designated Homeland Security Critical Infrastructure Facility"

Datacastle

Automatic PC Backup and Recovery

At Rest Encryption

Remote Data Deletion

Port Access Control

Device Trace