Review

1. The Cloud Controls Matrix is a list of cloud security controls mapped by domain and aligned to various regulatory frameworks.
2. The CCM is an excellent tool for evaluating your cloud security controls and is useful to both cloud providers and consumers.
3. The Consensus Assessment Initiative Questionnaire is a standard set of security questions for cloud providers. It allows cloud consumers to directly compare providers and allows providers to reduce the need to respond to non-standard RFPs.
4. The Cloud Security Alliance Guidance (which this training is based on) tells you how to implement your controls, while the CCM tells you which controls to implement.
5. The STAR and StarWatch tool serve as central repositories and methods for cloud provider security documentation, including the CAIQ.

189

INSTRUCTOR LOGO HERE
Change img on all slide masters.

189

190

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Content

Content in this module comes from the following domains in CSA's Security Guidance:

- **DOMAIN 5** // Information Governance
- **DOMAIN 6** // Management Plane and Business Continuity
- **DOMAIN 11** // Data Security

Covers the following subject areas:

- Cloud data architectures
- Data security and encryption
- CASB and Data Loss Prevention
- Data governance

Click on the module to the right to view the course objectives.

DOWNLOAD THE LATEST VERSION OF THE CSA SECURITY GUIDANCE.

cloud security alliance®

191

INSTRUCTOR LOGO HERE
Change img on all slide masters.

191

Module Structure

Unit 1 // Module Intro

Unit 2 // Cloud Data Storage and Data Moving to the Cloud

Unit 3 // Access Controls and Entitlements

Unit 4 // Encryption for IaaS

Unit 5 // Encryption for PaaS and SaaS

Unit 6 // Encryption key management

Unit 7 // Other Data Security Options

Unit 8 // Data Security Lifecycle

cloud security alliance®

192

INSTRUCTOR LOGO HERE
Change img on all slide masters.

192

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Objectives

Understand the different cloud storage models

Define security issues for data in the cloud

Assess the role and effectiveness of access controls.

Learn different cloud encryption models.

Understand additional data security options

Introduce data security lifecycle.

cloud security alliance

193

INSTRUCTOR LOGO HERE
Change img on all slide masters.

193

194

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Data Storage Is Different

- All data is eventually stored on a physical device, but cloud platforms use multiple types of data storage virtualization to abstract and build storage pools.
- These are not necessarily off-the-shelf technologies that map to traditional data storage virtualization, like SAN/NAS, that are well known.
- This storage may be expressed/exposed like traditional storage but under the hood is quite different.
- Just like SDN
- Security focuses on access controls, encryption, and proper configuration.

195

Major Cloud Data Storage Types

APPLICATION / PLATFORM
- Everything from a content delivery network to a SaaS application that includes file storage as a feature.

DATABASE
- Includes relational and non-relational.
- Not merely a DB running on an instance.

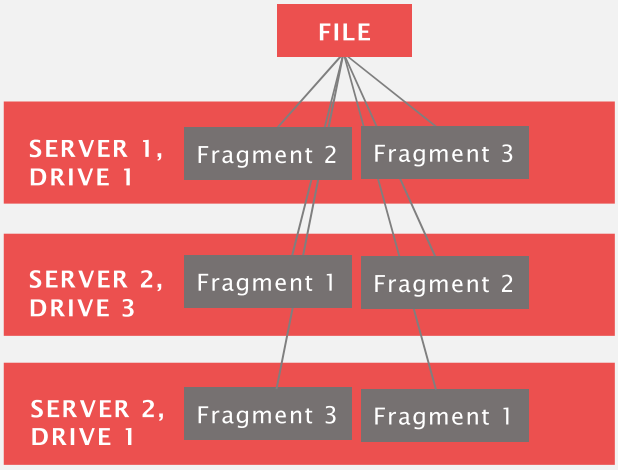
OBJECT
- Resilient file storage via API
- Not normal filesystems. Closer to a "database for files."

VOLUME
- Essentially, virtual hard drives for VMs/Instances.

196

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Data Dispersion (Bit-Splitting)



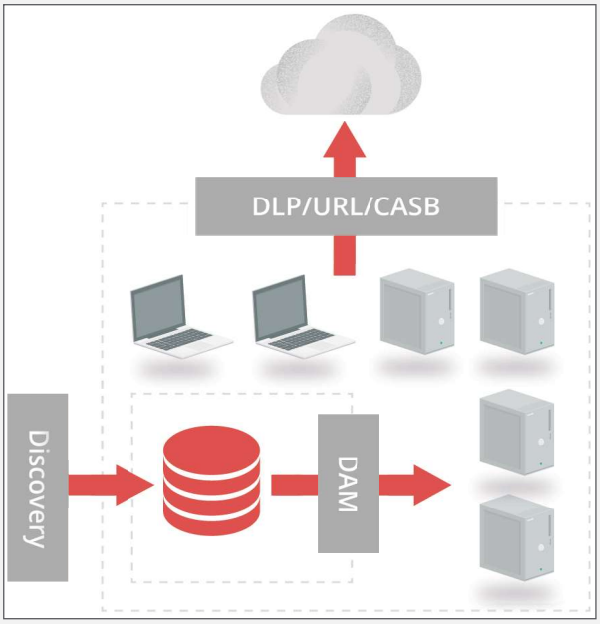
cloud security alliance®

197

INSTRUCTOR LOGO HERE
Change img on all slide masters.

197

Manage Data Migrating To The Cloud



cloud security alliance®

198

INSTRUCTOR LOGO HERE
Change img on all slide masters.

198

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Access Security Brokers (CASB)

Also known as Cloud Security Gateways

DISCOVER | MONITOR | PROTECT

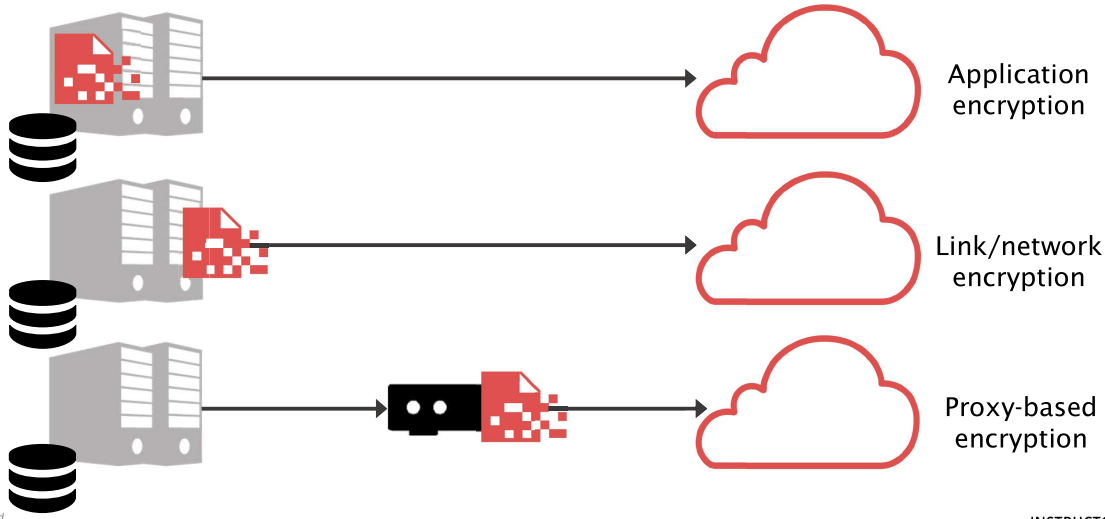
Inline (Local)

Inline (Cloud)

Via API

199

Protecting Data As It Moves



200

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

- Cloud data storage types include object, volume, database and application.
- Cloud providers store data in a multitenant and resilient way
- Migration control tools: CASB, DLP, URL filtering and DAM
- Data in motion can be encrypted client side, on the network, and/or proxy based

cloud security alliance®

201

INSTRUCTOR LOGO HERE
Change img on all slide masters.

201

Access Controls and Entitlements

Module 4 // Unit 3

202

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Access Controls

- Always your first data security control
- Granularity and implementation vary massively between platforms, services, and technologies
- The finer-grained the access controls the better for security, but the harder for manageability
- As with many things they may look the same on the surface but will likely be very different in practice
- It's critical to create platform-specific entitlement matrices

Management plane

Public & internal sharing controls

Application-level controls

203

Building An Entitlement Matrix

ENTITLEMENT	SUPER-ADMIN	SERVICE-ADMIN	STORAGE-ADMIN	DEV	SECURITY-AUDIT	SECURITY-ADMIN
VOLUME DESCRIBE	X	X		X	X	X
OBJECT DESCRIBE	X		X	X	X	X
VOLUME MODIFY	X	X		X		X
READ LOGS	X				X	X

204

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Access controls are the most fundamental security control, even in cloud computing.
2. There is massive variability of available access controls between cloud providers, and cloud storage may offer new categories of controls, such as sharing, beyond those in more-traditional storage.
3. An entitlement matrix is the documentation of authorizations. It defines who should be allowed to not only access data, but what they should be allowed to do with it.

cloud security alliance®

205

INSTRUCTOR LOGO HERE
Change img on all slide masters.

205

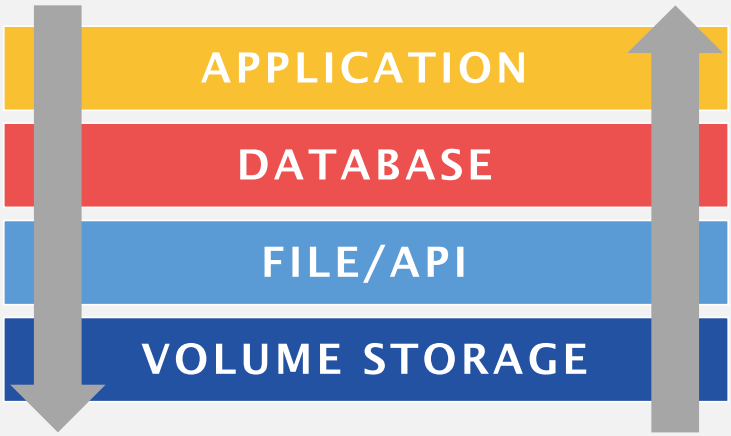
Encryption for IaaS

Module 4 // Unit 4

206

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Data Encryption Layers



cloud security alliance®

207

INSTRUCTOR LOGO HERE
Change img on all slide masters.

207

Cloud Encryption System Matrix

Who owns the components? Where are they? How are they connected?

cloud security alliance®

208

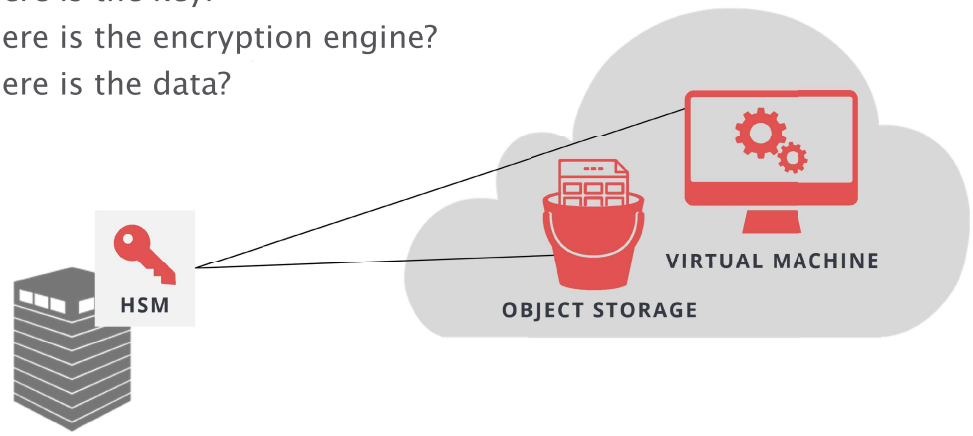
INSTRUCTOR LOGO HERE
Change img on all slide masters.

208

Copyright 2019 Cloud Security Alliance and Securosis, LLC

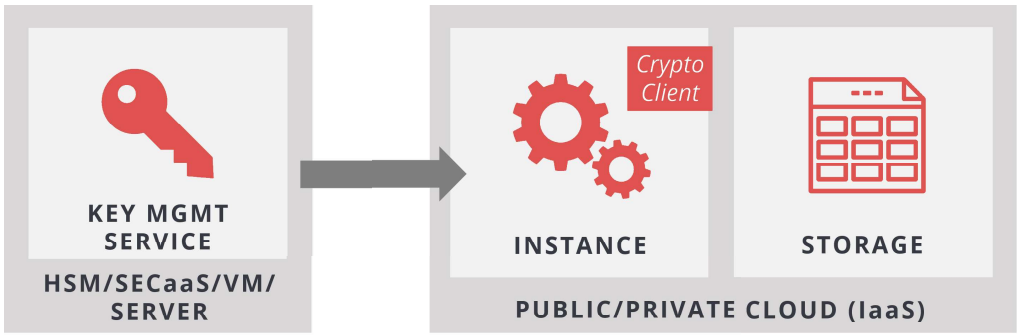
Cloud Encryption System Matrix

- Where is the key?
- Where is the encryption engine?
- Where is the data?



209

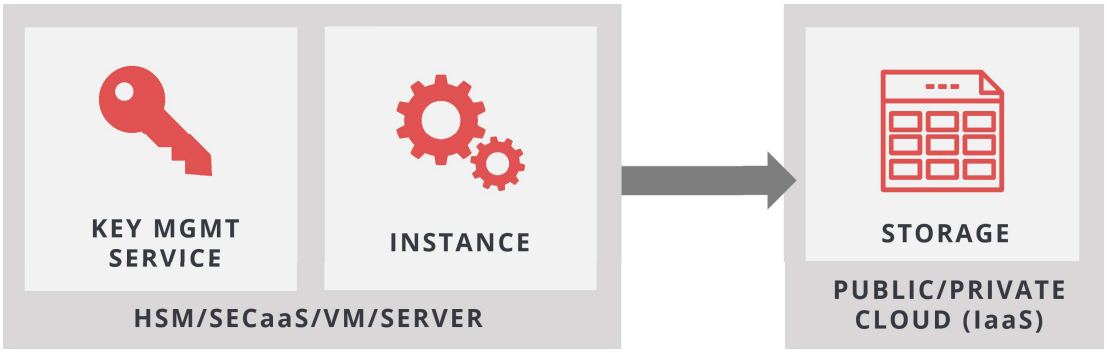
Volume Storage Encryption



210

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Instance-Managed



211

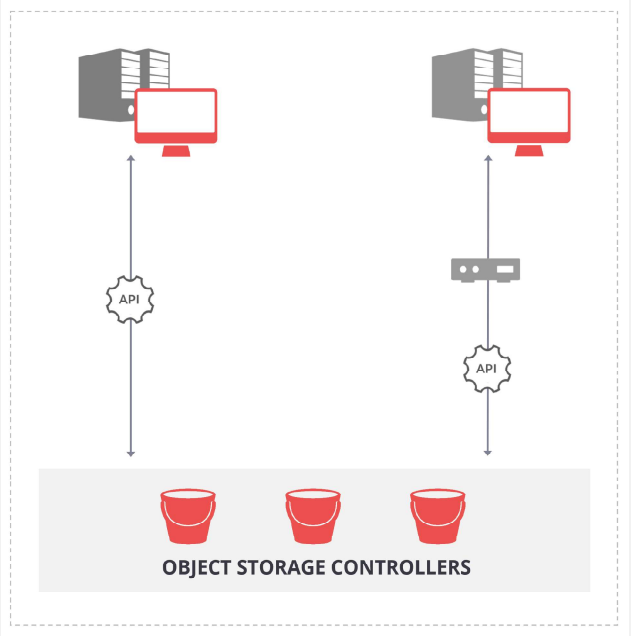
211

Object Storage

CLIENT-SIDE

SERVER-SIDE

PROXY



212

212

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. There are multiple layers where you can encrypt, each with benefits and complications. Encrypting higher in the application stack is often best for discreet data, while lower-level encryption, like volume, is better for bulk data.
2. Encryption systems are composed of the data, the encryption engine, and the key management, Where you place these determines the architecture and affects the security of the system.
3. Whenever possible, you want to separate the encryption key from the data and the encryption engine.
4. For object storage encryption, you can encrypt the data on the client site, the server side (using multiple techniques), or even through storage proxies (which we frequently see used for site backups).

cloud security alliance

213

INSTRUCTOR LOGO HERE
Change img on all slide masters.

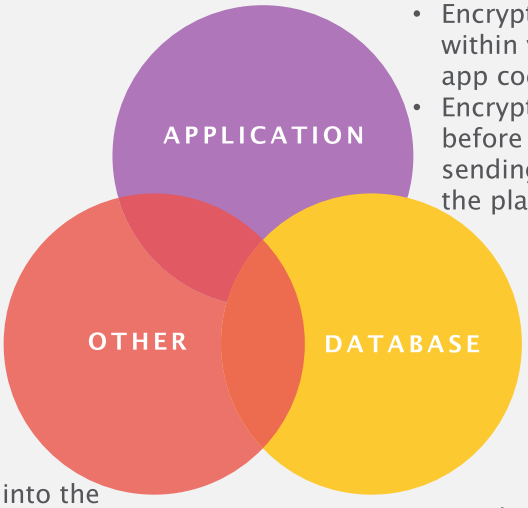
213

214

Copyright 2019 Cloud Security Alliance and Securosis, LLC

ENCRYPTING PaaS

- When you control the code, you can always encrypt there, which is also more portable.
- Volatile memory and swap files may be issues; understand your platform specifics.
- If you are the provider, use per-customer keys as much as possible.



- Encrypt within your app code
- Encrypt before sending to the platform

- Integrated into the provider's platform
- May include customer-managed key options

- Transparent Database Encryption (TDE)
- Field-Level

cloud security alliance®

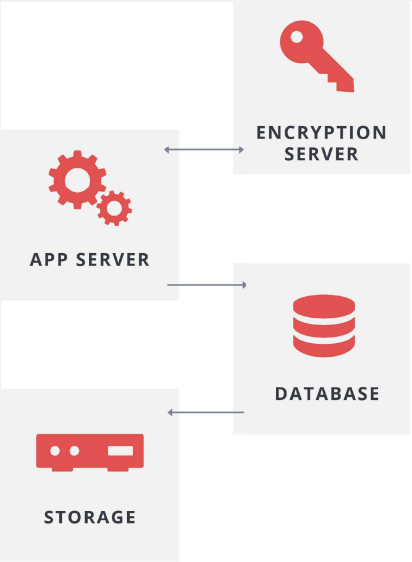
215

INSTRUCTOR LOGO HERE
Change img on all slide masters.

215

Example // Application Encryption Architecture

- Where is the key?
- Where is the data?
- Where is the encryption engine?



cloud security alliance®

216

INSTRUCTOR LOGO HERE
Change img on all slide masters.

216

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SaaS Encryption

Provider Managed

- Provider-managed may offer customer managed keys (we will discuss in a moment)

Customer Managed

- Proxy encryption requires an external tool or service
  - You re-route SaaS traffic to the proxy before it is sent to your SaaS provider
  - This encryption typically breaks SaaS applications, often dramatically reducing capabilities

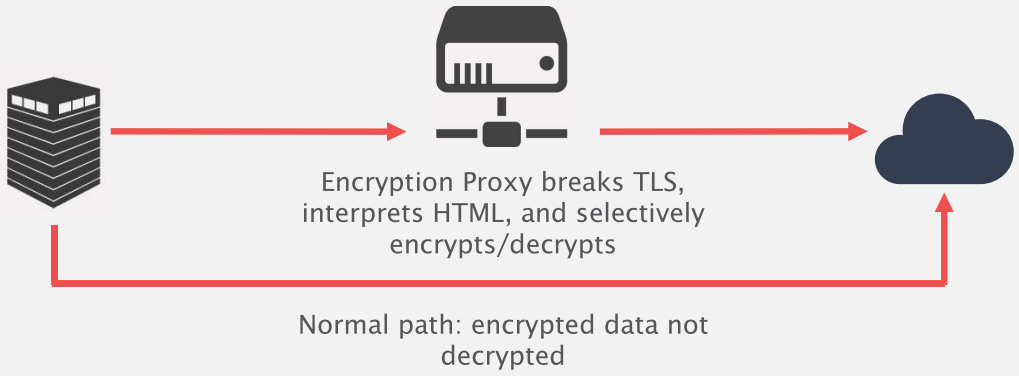
cloud security alliance®

217

INSTRUCTOR LOGO HERE
Change img on all slide masters.

217

PROXY ENCRYPTION FOR SaaS



cloud security alliance®

218

INSTRUCTOR LOGO HERE
Change img on all slide masters.

218

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Platform as a Service (PaaS) encryption will depend almost completely on the kind of platform and options supported by your provider. For workloads though, you can nearly always program your own encryption at the application layer.
2. When encrypting in your application, you can handle the encryption in your own code or hand it off to an external encryption server or service.
3. For Software as a Service you only have two options – rely on your provider's supported encryption or use a third-party encryption proxy that sits as a man in the middle.
4. SaaS encryption proxies may introduce new security concerns due to requiring you to break any network encryption to the cloud provider. They may also break application functionality. However, there are still valid use cases, albeit limited.

cloud security alliance®

219

INSTRUCTOR LOGO HERE
Change img on all slide masters.

219

220

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Key Management Options

HSM / APPLIANCE

VIRTUAL APPLIANCE / SOFTWARE

CLOUD PROVIDER SERVICE

HYBRID

CSA cloud security alliance®

221

INSTRUCTOR LOGO HERE
Change img on all slide masters.

221

Provider Key Management & BYOK

- Some providers build encryption into their platform. By default they typically manage keys for you.
  - E.g., The checkbox to encrypt an S3 bucket, or the default encryption on Box/Dropbox.
- Some providers now allow you to manage your own keys. "Bring your own key" (we also call these customer managed keys).
  - To varying degrees of security. Some are fully under your control, others the provider can technically get to, but they provide separation of duties.

CSA cloud security alliance®

222

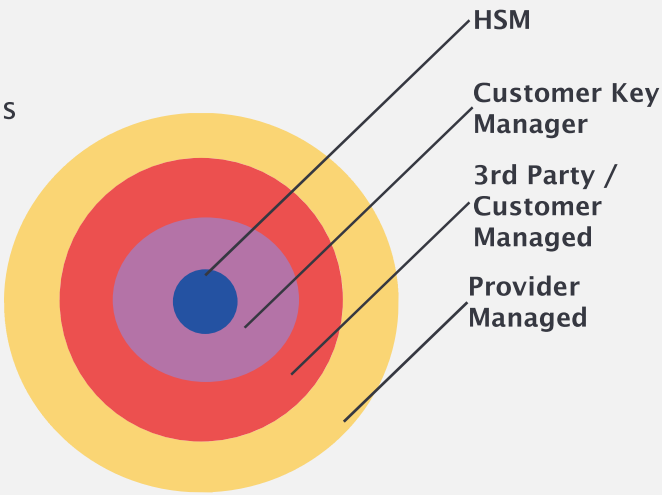
INSTRUCTOR LOGO HERE
Change img on all slide masters.

222

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Key Management Options

- The customer owns the keys, but the provider may manage
- This isn't necessarily insecure it all depends on the provider's security controls
- Providers should be very transparent about these
- Keys always exposed at some level, but typically data encryption keys, not master keys
- Often good option for SaaS and PaaS



CSA cloud security alliance®

223

INSTRUCTOR LOGO HERE
Change img on all slide masters.

223

Review

1. Proper key management is essential to effective encryption.
2. HSMs and physical appliances may be offered by your cloud provider, or you can look at deploying software or virtual appliances in the cloud, connecting to existing hardware over a hybrid connection, or even leverage new options like a key management service from your cloud provider or a third party.
3. Providers offer a range of key management options, from the provider completely managing the keys, to allowing you to manage your own keys in their environment or even provide keys as needed.
4. Bring Your Own Key will work differently on different providers and services, with varying levels of relative security.
5. Once you know the risk you are trying to prevent, you can evaluate the technical options in your provider and platform of choice. Remember, not all data needs the same level of security, so you don't always need to default to the most secure option.

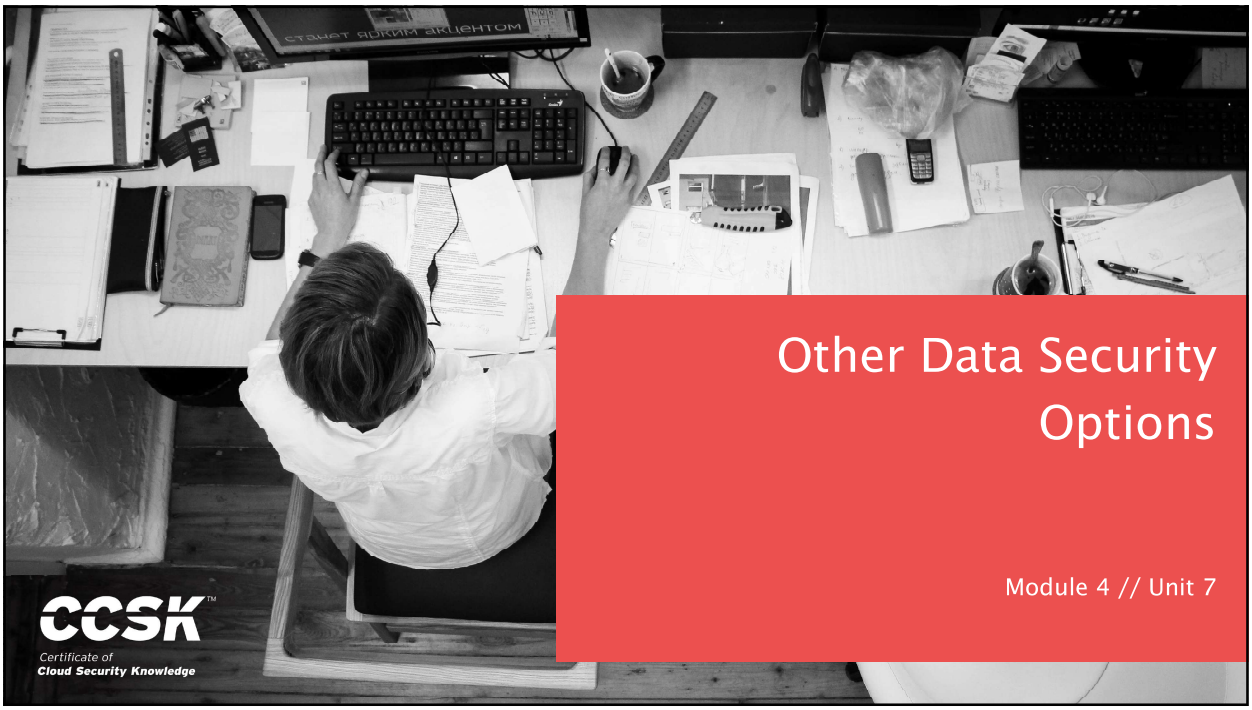
CSA cloud security alliance®

224

INSTRUCTOR LOGO HERE
Change img on all slide masters.

224

Copyright 2019 Cloud Security Alliance and Securosis, LLC



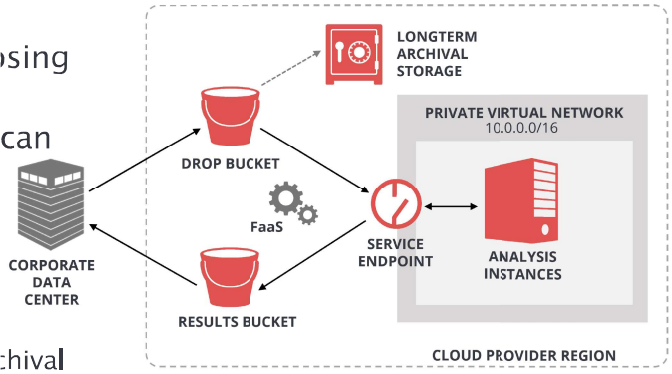
Other Data Security Options

Module 4 // Unit 7

225

Data Security Architecture

- This example shows using a private network for data processing without ever exposing servers to the internet
- Good architectural decisions can optimize security
- Performance advantages:
  - No servers running
  - No instances
  - No virtual machines
  - You only pay for batch jobs, archival storage & object storage
- There's no network attack path



CSA cloud security alliance®

226

INSTRUCTOR LOGO HERE
Change img on all slide masters.

226

Copyright 2019 Cloud Security Alliance and Securosis, LLC

More Than Encryption

Auditing/Monitoring/Alerting

- Collect at the provider / metastructure and the data storage level when possible

Provider Specific Controls

- Various providers and platforms have their own data security controls that may not fit our categories

Data Loss Prevention

- Typically a SaaS (and maybe PaaS) priority, don't see much in IaaS
- CASB often best bet, and may integrate with dedicated DLP tools
- Cloud providers sometimes offer basic DLP in the platform (mostly file collaboration products)

ERM/Digital Rights Management

- Full DRM not often seen and not a cloud-specific issue. Will break most SaaS
- Providers may offer DRM-like capabilities (e.g., user + device + content restrictions)

CSA cloud security alliance®

227

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

227

Data Masking // Dynamic & Test Data Generation

Masking Tool

PRODUCTION

ID	LAST	FIRST	CREDIT CARD PAN
1	Smith	John	1234-5678-9101-1234
2	Doe	Jane	2345-8654-8646-4567

DEV / TEST

ID	LAST	FIRST	CREDIT CARD PAN
1	Jones	John	1234-6824-9854-1234
2	Smith	Jane	2345-8346-1623-4567

Test Data Generation Shown

CSA cloud security alliance®

228

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

228

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Integrating PaaS and other new cloud architectural options into applications and data storage may allow cloud consumers to shift more security burden onto cloud providers and reduce the stack's attack surface.
2. Good activity monitoring and alerting are important to cloud data security, and providers may also support a variety of additional security controls.
3. Data Loss Prevention tends to be more useful for SaaS and may be integrated into CASB tools.
4. Traditional DRM/ERM isn't necessarily useful for cloud, but some SaaS/PaaS services may have "DRM-like" capabilities such as sharing or view controls that provide similar protections.
5. Data masking is critical for test data generation and to ensure production data is not exposed in development environments.

cloud security alliance

229

INSTRUCTOR LOGO HERE
Change img on all slide masters.

229

230

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Data Security Lifecycle

231

How to Use the Lifecycle

- The Data Security Lifecycle is a tool to help you model your security controls.
- Don't get too granular or it will be too complex to model. Focus on the big picture.
- Use the lifecycle to determine where data flows.
- Then use it to map how data *can* be used, and how it *should* be used.
- When you can do something that shouldn't be allowed, that's where you need to insert a security control.

232

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Locations & Access

- The simple data security lifecycle does not address location or how data is accessed
- External use reliant on different controls
- Internal and external access usually have different security policies
- You have *multiple* data security lifecycles

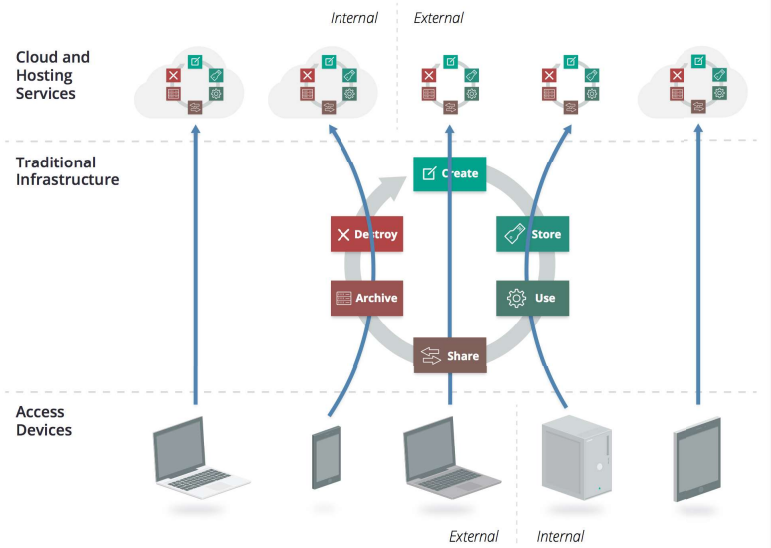
CSA cloud security alliance®

233

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

233

Locations & Access



CSA cloud security alliance®

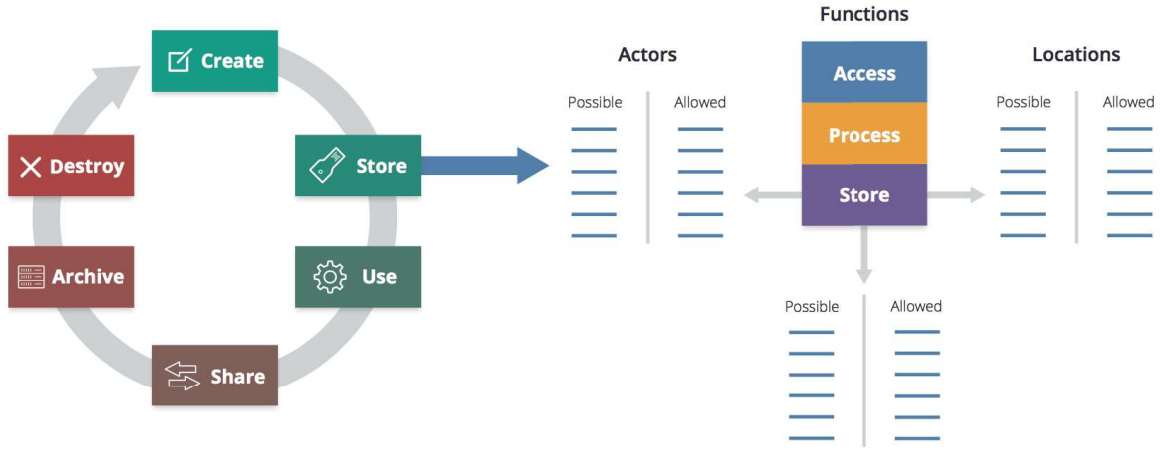
234

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

234

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Mapping The Lifecycle To Functions



235

Functions Possible in Each Data Lifecycle Phase

	Create	Store	Use	Share	Archive	Destroy
Read	X	X	X	X	X	X
Process	X		X			
Store		X			X	

236

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Mapping Controls

Function		Action		Location	
Possible	Allowed	Possible	Allowed	Possible	Allowed
		RW	R		
		RWE	E		
		E			

CSA cloud security alliance®

237

INSTRUCTOR LOGO HERE
Change img on all slide masters.

237

Recommendations

- Understand the specific capabilities of the cloud platform you are using.
- Don't dismiss cloud provider data security. In many cases it is more secure than building your own and comes at a lower cost.
- Create an entitlement matrix for determining access controls. Enforcement will vary based on cloud provider capabilities.
- Consider CASB to monitor data flowing into SaaS. It may still be helpful for some PaaS and IaaS but rely more on existing policies and data repository security for those types of large migrations.
- Use the appropriate encryption option based on the threat model for your data, business, and technical requirements.

CSA cloud security alliance®

238

INSTRUCTOR LOGO HERE
Change img on all slide masters.

238

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Recommendations

- Consider use of provider-managed encryption and storage options. Where possible, use a customer-managed key.
- Leverage architecture to improve data security. Don't rely completely on access controls and encryption.
- Ensure both API and data-level monitoring are in place, and that logs meet compliance and lifecycle policy requirements
- Standards exist to help establish good security and the proper use of encryption and key management techniques and processes. Specifically, NIST SP-800-57, ANSI X9.69 and X9.73.

cloud security alliance

239

INSTRUCTOR LOGO HERE
Change img on all slide masters.

239

Review

1. The Data Security Lifecycle is a tool to help us visualize how our data is used and exposed and can be helpful in determining where to place security controls.
2. The lifecycle itself consists of 6 phases from creation to destruction, but practically speaking data will bounce between all the phases as it is used. However, each phase has a distinct set of potential associated security issues and controls.
3. Data will move between various locations, and be accessed using a variety of devices, users, and services. Mapping these can be useful in designing security controls.
4. Depending on the location, phase, etc., the data will have a set of potential actors, functions, and locations. Our application risk assessment will tell us what we want to allow (e.g. through an entitlement matrix.
5. Mapping these against each other will tell us what additional security controls, such as access controls, we need.

cloud security alliance

240

INSTRUCTOR LOGO HERE
Change img on all slide masters.

240

Copyright 2019 Cloud Security Alliance and Securosis, LLC