Infrastructure Security for Cloud Computing

Module 2

63

Module Structure

MODULE 2 //
Infrastructure Security For Cloud
Maps to the following domains in the Security Guidance:

DOMAIN 6 // Management Plane and Business Continuity

DOMAIN 7 // Infrastructure Security

DOMAIN 8 // Virtualization and Containers

Also maps to CAIQ and CCM, and ENISA
Covers the following subject areas:
Securing base infrastructure
Management plane security
Securing virtual hosts and networks
IaaS, PaaS, SaaS security

CSA cloud security alliance®

64

INSTRUCTOR LOGO HERE
Change img on all slide masters.

64

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Structure

Unit 1 // Module Introduction

Unit 2 // Introduction to Infrastructure Security for Cloud Computing

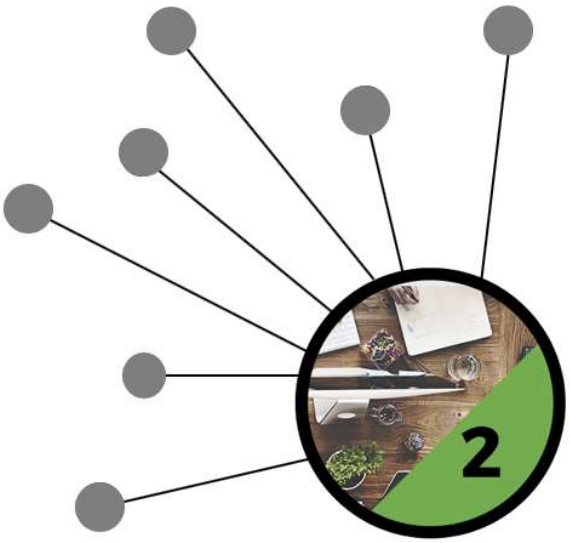
Unit 3 // Software Defined Network

Unit 4 // Cloud Network Security

Unit 5 // Securing Compute Workloads

Unit 6 // Management Plane Security

Unit 7 // BCDR



65

INSTRUCTOR LOGO HERE
Change img on all slide masters.

65

Objectives

Understand the components of cloud infrastructure.

Assess the security implications of virtual networks and workloads.

Learn the security advantages and disadvantages of working with cloud infrastructure.

Evaluate how to secure the cloud management plane.

Learn how to manage business continuity for cloud computing.

66

INSTRUCTOR LOGO HERE
Change img on all slide masters.

66

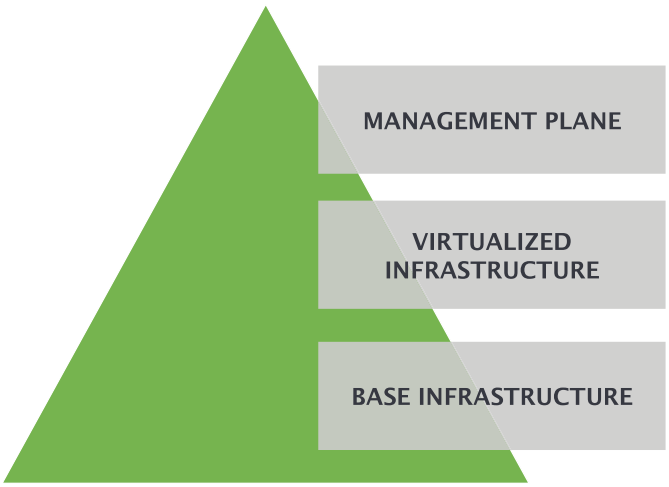
Copyright 2019 Cloud Security Alliance and Securosis, LLC

Intro to Infrastructure Security for Cloud Computing

Module 2 // Unit 2

67

Macro Layers



CSA cloud security alliance®

68

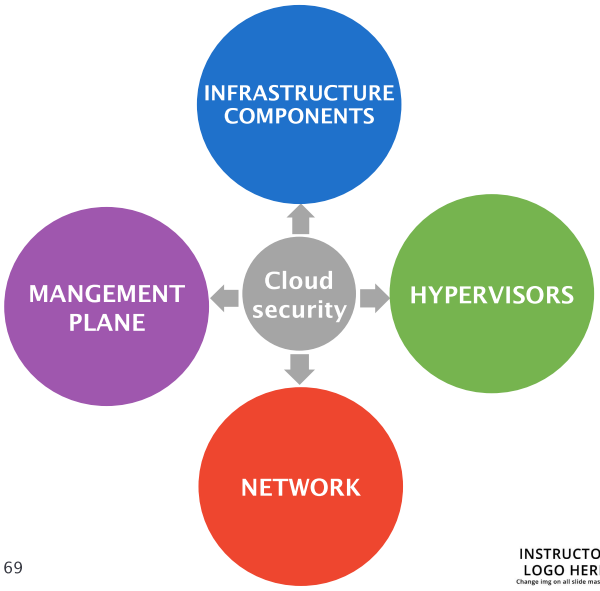
INSTRUCTOR LOGO HERE
Change img on all slide masters.

68

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Infrastructure Security Overview

- No capital expenditures (using public cloud)
- More agility
- Unbounded scale
- Improved resource utilization
- Customer-controlled migration
- Resilience
- Pay for use



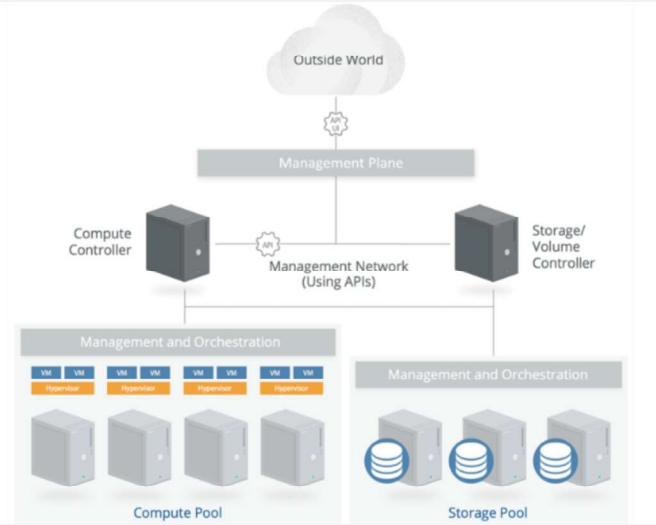
CSA cloud security alliance®

69

INSTRUCTOR LOGO HERE
Change img on all slide masters.

69

Example // How IaaS Works



CSA cloud security alliance®

70

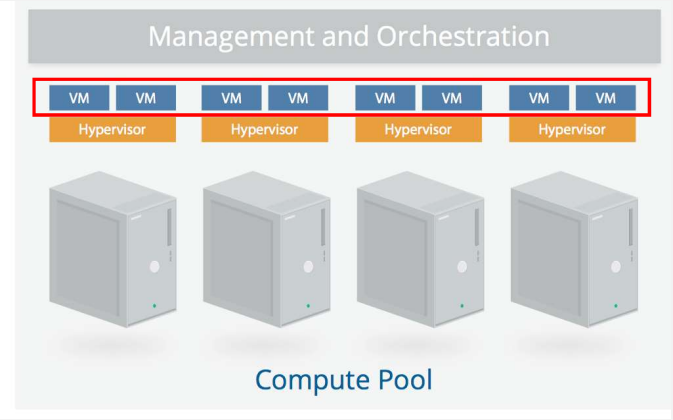
INSTRUCTOR LOGO HERE
Change img on all slide masters.

70

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Public vs. Private

In public cloud, you only control what you consume, plus a little management.



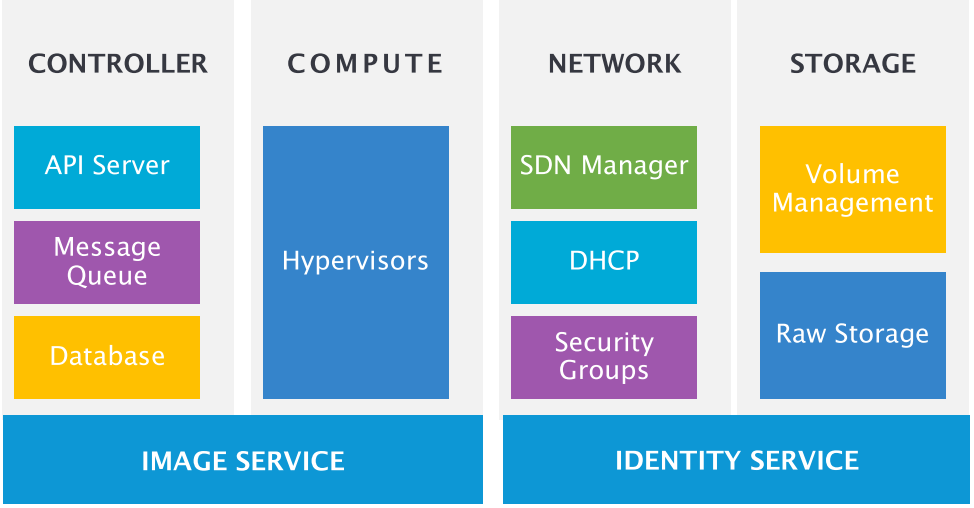
CSA cloud security alliance®

71

INSTRUCTOR LOGO HERE
Change img on all slide masters.

71

Simplified Infrastructure Components



CSA cloud security alliance®

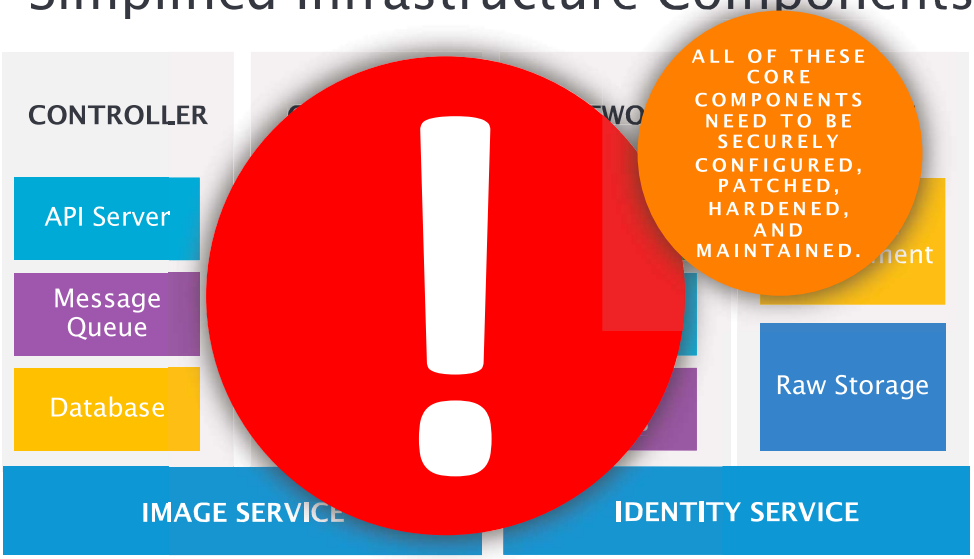
72

INSTRUCTOR LOGO HERE
Change img on all slide masters.

72

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Simplified Infrastructure Components



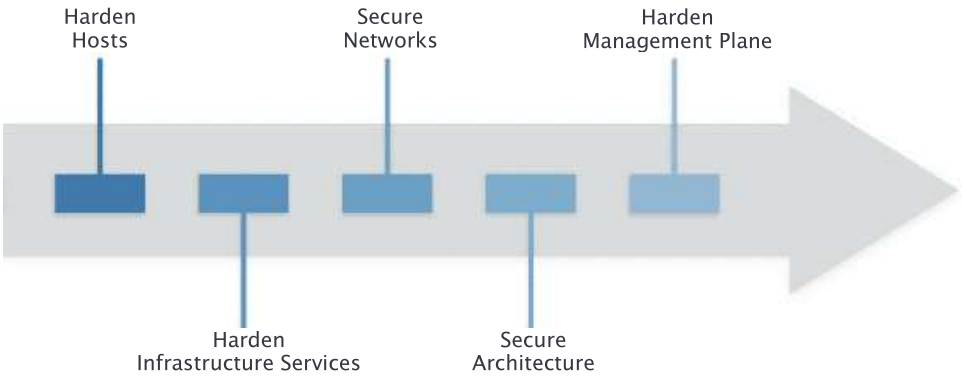
cloud security alliance

73

INSTRUCTOR LOGO HERE
Change img on all slide masters.

73

Securing Cloud Infrastructure



cloud security alliance

74

INSTRUCTOR LOGO HERE
Change img on all slide masters.

74

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Infrastructure security includes all the underlying physical resources and the software, like operating systems, that runs on them.
2. With private cloud you are responsible for securing all the hardware and software that makes up the cloud platform. With public cloud you are only responsible for what you deploy in the cloud.
3. Cloud platforms, especially private cloud, are often built using common components including operating systems, message queues, and databases. All these need to be properly secured.
4. Securing cloud infrastructure starts with proper design, then hardening of the base systems and various services. Lastly, providers must lock down the management plane.

cloud security alliance

75

INSTRUCTOR LOGO HERE
Change img on all slide masters.

75

76

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Underlying IaaS Networks

Management	• Management plane to nodes
Storage	• Storage nodes (volumes) to compute nodes (instances)
Service	• Internet to compute nodes • Instances to instance

CSA cloud security alliance®

77

INSTRUCTOR LOGO HERE
Change img on all slide masters.

77

Building Underlying Networks for Cloud

Use Separate Physical Networks.

- Don't rely on VLANs.
- SDN may be a good option but depends on the version and the hardware you use… *physical separation is still preferred, as much for performance as security.*

Isolate the Cloud Networks From the LAN.

- There should be only 2 outside connections:
  - The network manager to route Internet traffic.
  - The management and web and API server.

CSA cloud security alliance®

78

INSTRUCTOR LOGO HERE
Change img on all slide masters.

78

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Virtual Networks

VIRTUAL NETWORKS AND SECURITY

- Virtual networks are subject to the same security concerns of a physical network.
- Virtual networks always run on a physical network.

VIRTUAL NETWORKS MAY PROVIDE A SIMPLER STACK TO BUILD THE PRIVATE CLOUD.

- Greater control is afforded through SDN.

VIRTUAL NETWORKS MAY include inherent security capabilities.

CSA cloud security alliance®

79

INSTRUCTOR LOGO HERE
Change img on all slide masters.

79

Major Virtual Network Types

VLAN:

- Leverage existing technology available in essentially all networks
- Designed for network segregation, not isolation, in single-tenant environments
- Not effective as a security barrier
- Have performance and address space limitations at cloud scale

SDN

- Software Defined Networks decouple the network control plane from the underlying hardware
- Abstracts virtual networking from traditional LAN limitations
- Extremely flexible (e.g. overlapping IP address ranges on same physical hardware)
- Multiple implementations, both standard and proprietary
- Can create effective security barriers

CSA cloud security alliance®

80

INSTRUCTOR LOGO HERE
Change img on all slide masters.

80

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Software - Defined Networking

- Provides a decoupled control plane that is (potentially) easier to secure.
- OpenFlow is an example of an SDN.
- Remote access is controlled by the Administrator.
- Different flavors support different capabilities, but generally they can couple tightly with the cloud platform and possibly security tools.
- Nearly all implementations are API-enabled.
- While they may look like a regular network to the cloud consumer, they function VERY differently.
- Rely heavily on *packet encapsulation*.

CSA cloud security alliance®

81

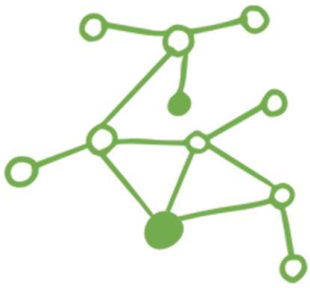
INSTRUCTOR LOGO HERE
Change img on all slide masters.

81

SDN Security Benefits

EASIER ISOLATION

TOPOLOGOLOGY NOT LIMITED TO PHYSICAL STRUCUTRE
- E.g., you can put multiple overlapping virtual networks, even with the same address ranges, on the same physical network



SDN FIREWALLS / SECURITY GROUPS
- Default Deny
- Orchestrated
- Granularity of host firewall with manageability of a network appliance

SECURITY POLICIES AND CONTROLS ON TAGS AND OTHER CONTEXT

CSA cloud security alliance®

82

INSTRUCTOR LOGO HERE
Change img on all slide masters.

82

Copyright 2019 Cloud Security Alliance and Securosis, LLC

SDN Firewalls / Security Groups

POLICY-BASED

- Not necessarily tied to IP addresses
- Can include context/tagging and other intelligence

NO ADDITIONAL HARDWARE OR SOFTWARE TO DEPLOY

TYPICALLY DEFAULT-DENY

- Even assets in the same security group can't communicate

APPLY ON A PER-ASSET LEVEL (INSTANCE OR PaaS OBJECT)

- But managed outside that asset. For example, if a virtual machine is compromised that can't be used to disable the firewall

INTEGRATED INTO CORE SDN LOGIC

- Traffic/packets simply dropped if they don't match the policy's rules
- Tightly coupled with the cloud orchestration so fully capable of keeping up with high velocity changes

CSA cloud security alliance®

83

INSTRUCTOR LOGO HERE
Change img on all slide masters.

83

Review

1. Cloud platforms typically rely on three physical networks (at a minimum). One for management, one for storage, and one for traffic between resources.
2. The two most common virtual networking technologies used in cloud are VLANs and Software Defined Networks. For security, SDNs are preferred since they provide better isolation and security.
3. SDNs decouple the control plane from the underlying physical network and provide tremendous flexibility. They are capable, for example, of deploying the same IP address range across isolated networks on the same physical hardware.
4. Security Groups are the common name for the firewalling built into SDNs. They can provide the manageability of a network firewall with the granularity of a host firewall.

CSA cloud security alliance®

84

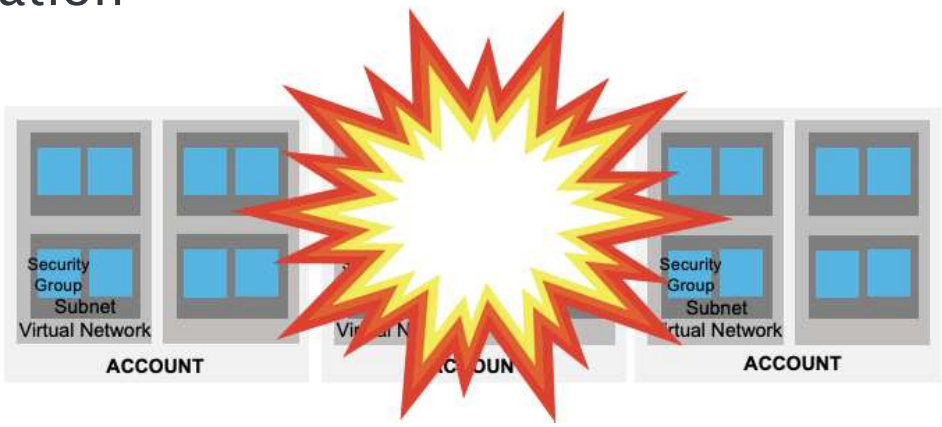
INSTRUCTOR LOGO HERE
Change img on all slide masters.

84

Copyright 2019 Cloud Security Alliance and Securosis, LLC

85

Controlling Blast Radius with Virtual Networks & Cloud Account / Subaccount / Subscription Isolation



cloud security alliance

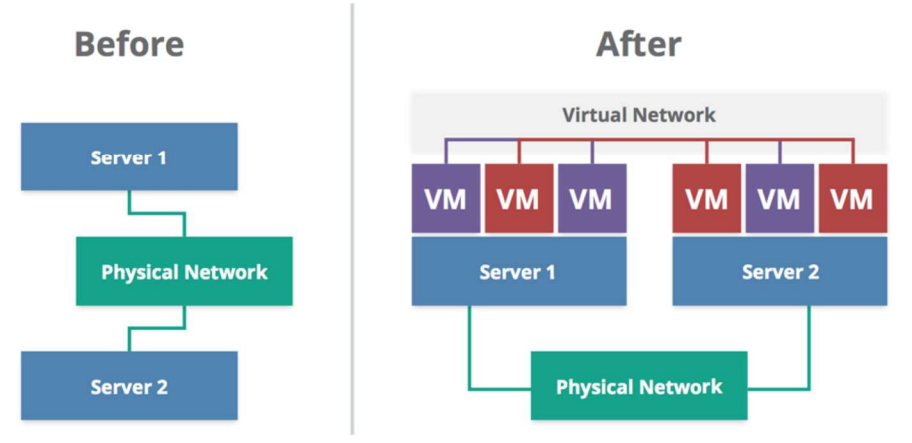
86

INSTRUCTOR LOGO HERE
Change img on all slide masters.

86

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Losing Network Visibility



CSA cloud security alliance®

87

INSTRUCTOR LOGO HERE
Change img on all slide masters.

87

3rd-Party Security Tools Advantages & Disadvantages

PHYSICAL APPLIANCE	VIRTUAL APPLIANCE	HOST SOFTWARE
• Unusable in public cloud • Lack visibility into virtual networks • If used, require highly inefficient routing and topologies • Typically incapable of keeping up with cloud rates of change	• Become bottlenecks • May materially increase cloud costs due to resource requirements • Must support autoscaling, elastic pricing, and other cloud native orchestration • Must support high rates of change (e.g., IP address velocity) • Still often least worst option to fill CSP gaps	• Typically better suited to cloud topologies and rates of change • Must be consistently embedded in images/virtual machines • Will add to local resource requirements • Agents should be designed for cloud, lightweight, and cloud-aware • Must communicate and save data externally

CSA cloud security alliance®

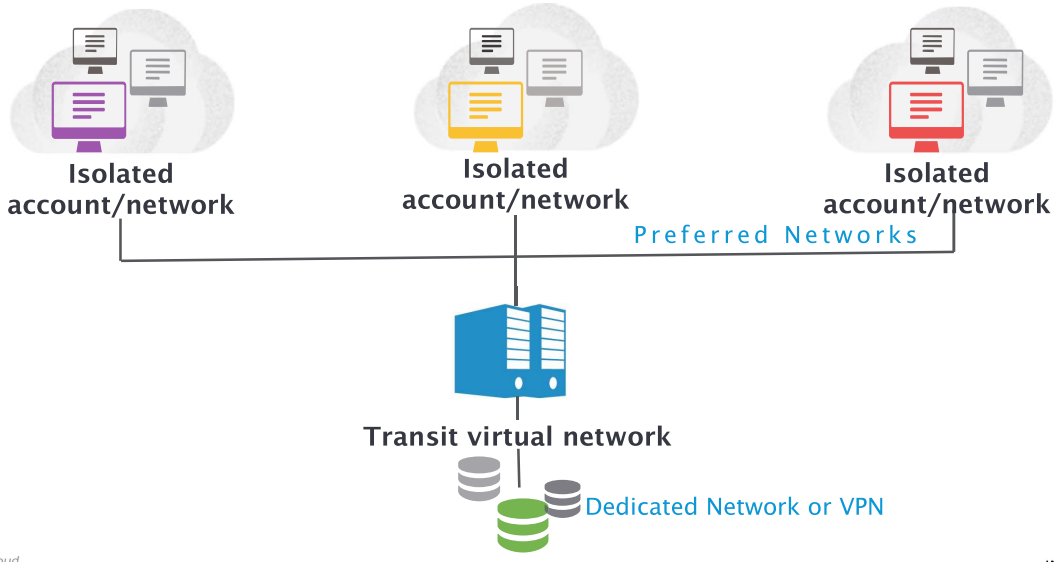
88

INSTRUCTOR LOGO HERE
Change img on all slide masters.

88

Copyright 2019 Cloud Security Alliance and Securosis, LLC

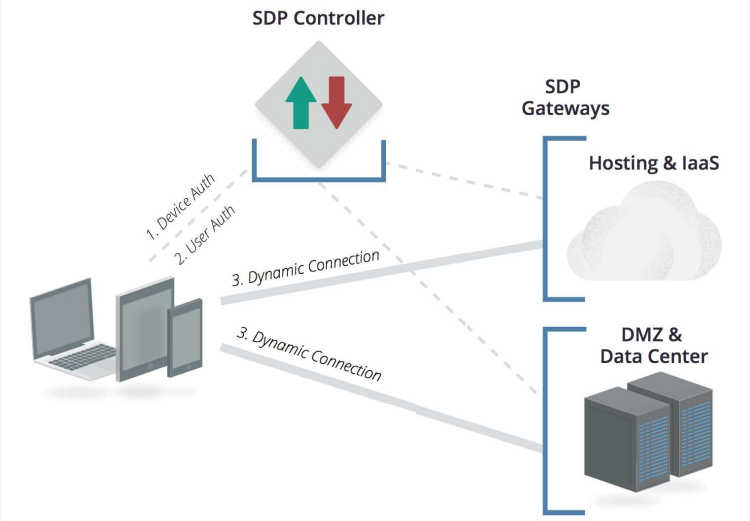
Bastion/Transit Networks / Accounts for Hybrid



89

89

Software Defined Perimeter



90

90

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Provider & Consumer Responsibilities

CONSUMER

- Proper virtual network design
- Implementing virtual security controls (e.g., security groups)
- Securing their portion of the management plane/metastructure (e.g., proper IAM)

PROVIDER

- Security of the virtualization technology
- Exposing security controls (e.g., security groups)
- Disabling attack surface (e.g., packet sniffing)
- Securing the virtual management infrastructure

CSA cloud security alliance®

91

INSTRUCTOR LOGO HERE
Change img on all slide masters.

91

Review

1. Prefer SDN when available.
2. Use SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.
3. Separate accounts and virtual networks dramatically limit blast radius compared to traditional data centers.
4. Implement default deny with cloud firewalls.
5. Apply cloud firewalls on a per-workload basis as opposed to a per-network basis.
6. Always restrict traffic between workloads in the same virtual subnet using a cloud firewall (security group) policy whenever possible.

CSA cloud security alliance®

92

INSTRUCTOR LOGO HERE
Change img on all slide masters.

92

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Securing Compute Workloads

Module 2 // Unit 5

93

Workloads are More than Virtual Machines…

Security Controls Will Vary, But In General:

- Configure the environment/features securely
- Application security fundamentals still apply, but may need to be implemented at a different layer (e.g., within the code/workload)
- Monitoring/logging will change significantly

CSA cloud security alliance®

94

INSTRUCTOR LOGO HERE
Change img on all slide masters.

94

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Controls

- May not be able to run agents (E.g., AV)
- "Traditional" agents may not work properly in cloud or will impede performance
- Agents must be cloud aware
  - E.g., not rely on static IP addresses and capable of communicating across virtual network boundaries
- Agents should be lightweight and support auto-scaling and auto-registration
- Agents should not increase attack surface
  - E.g., require ports to be open for management

Monitoring

- Network addresses are not sufficient to identify a workload in the cloud
- Logs should be offloaded quickly due to more-ephemeral nature of cloud workloads
- Logging architectures should be redesigned to account for cloud topology and variable costs of different storage tiers
  - Cascading log collection is generally preferred. Collect locally in object storage and use filtering tools to migrate security-sensitive logs to central collection and management

Assessment

- Providers often limit vulnerability assessment
- Default deny networks may further limit network assessment effectiveness
- Host assessments (agents) are often preferable
- Assess images rather than instances when using immutable

95

Immutable Workloads Enable Security

IMMUTABLE

- Based on images and automatically deployed (e.g. by an auto scale group)
- Login disabled since changes won't propagate to other instances
- You replace with new versions instead of patching/updating old versions
- Very easy to harden for security (e.g. disable SSH)

AUTOMATED CONFIGURATION MANAGEMENT

- The virtual machine is automatically configured using a template/policy based tool (e.g. Chef / Puppet / Ansible / Salt)
- It changes, but manual changes disabled since the automation would overwrite

STANDARD/LONG RUNNING

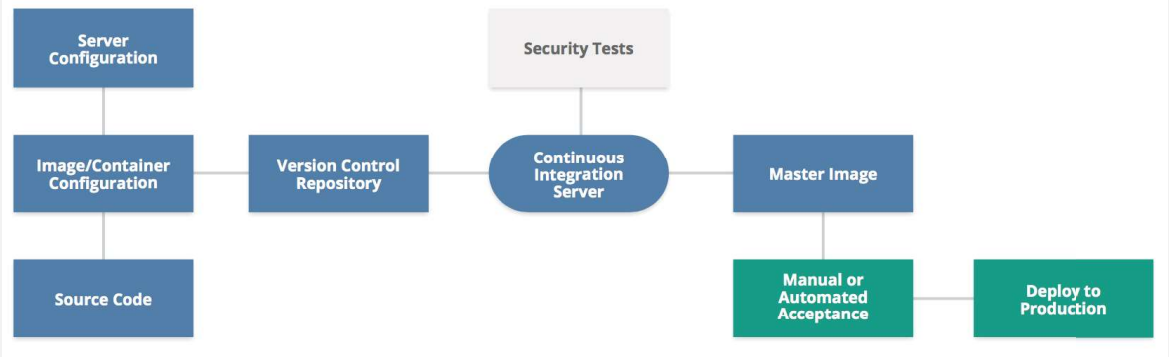
- Managed just like traditional servers

RELATIVE SECURITY

96

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Creating Immutable Images with Deployment Pipelines



CSA cloud security alliance®

97

INSTRUCTOR LOGO HERE
Change img on all slide masters.

97

Provider & Consumer Responsibilities

CONSUMER

- Security settings
- Monitoring and logging
- Image asset management
- Use dedicated hosting if needed and available
- All in-workload security controls (e.g., patching virtual machines)

PROVIDER

- Workload isolation
- Underlying infrastructure security
- Securing the virtualization technology
- Providing consumers adequate security controls
- Protecting volatile memory

CSA cloud security alliance®

98

INSTRUCTOR LOGO HERE
Change img on all slide masters.

98

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Compute Security Recommendations

Leverage immutable workloads whenever possible.

- Disable remote access.
- Integrate security testing into image creation.
- Alarm with file integrity monitoring.
- Patch by updating images, not patching running instances.
- Choose security agents that are cloud-aware and minimize performance impact, if needed.

Maintain security controls for long-running workloads but **use tools that are cloud aware**.

Store **logs external** to workloads.

Understand and comply with cloud provider **limitations on vulnerability assessments and penetration testing**.

cloud security alliance®

99

INSTRUCTOR LOGO HERE
Change img on all slide masters.

99

Review

1. Disable remote access.
2. Integrate security testing into image creation.
3. Alarm with file integrity monitoring.
4. Patch by updating images, not patching running instances.
5. Apply cloud firewalls on a per-workload basis as opposed to a per-network basis.
6. Choose security agents that are cloud-aware and minimize performance impact, if needed.
7. Maintain security controls for long-running workloads but use tools that are cloud aware.
8. Store logs external to workloads.
9. Understand and comply with cloud provider limitations on vulnerability assessments and penetration testing.

cloud security alliance®

100

INSTRUCTOR LOGO HERE
Change img on all slide masters.

100

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Management Plane Security

Module 2 // Unit 6

101

The Management Plane

KEY FUNCTIONS

- Provisioning resources
- Starting/stopping/terminating
- Configuring resources

SECURITY CONSIDERATIONS

- Authentication
- Access Control
- Logging/Monitoring

THE MANAGEMENT PLANE IS THE LITERAL KEY TO YOUR PRIVATE CLOUD. PROTECT IT WISELY.

ACCESS METHODS

WEB

API
(Usually REST)

CSA cloud security alliance®

102

INSTRUCTOR LOGO HERE
Change img on all slide masters.

102

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Management Plane Access & Credentials

DIFFERENT PROVIDERS / PLATFORMS USE DIFFERENT AUTHENTICATION OPTIONS

- We cover some of these in more depth in the Identity Management section

WEB CONSOLE LOGINS ARE TYPICALLY LIKE LOGGING INTO ANY OTHER WEB SERVICE

- Username and password
- Maybe MFA

APIs USE MULTIPLE TECHNIQUES THAT MAY OR MAY NOT HAVE CEDENTIALS DIFFERENT FROM THE WEB CONSOLE

- HTTP request signing (crypto using keys)
- Tokens
- Oauth/SAML

ALL CONNECTIONS SHOULD ALWAYS USE TLS

CSA cloud security alliance®

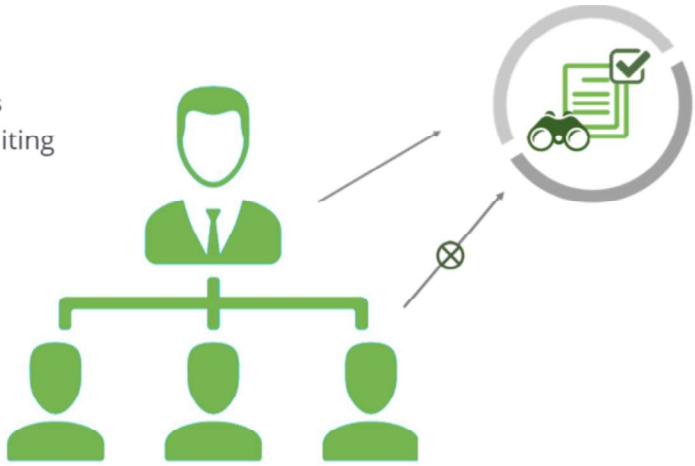
103

INSTRUCTOR LOGO HERE
Change img on all slide masters.

103

Management Plane Security

- Secure root account
- Manage Non-Root Users
- Enable Monitoring / Auditing



CSA cloud security alliance®

104

INSTRUCTOR LOGO HERE
Change img on all slide masters.

104

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Root/Master Account Security

ENABLE HARDWARE MULTI-FACTOR AUTHENTICATION (MFA)

- Store in a locked, central location

USE ISOLATED CREDENTIALS (A DESIGNATED EMAIL OR USER ACCOUNT NOT USED FOR ANYTHING ELSE)

- Use a name with a random seed if possible to reduce phishing

IF AVAILABLE, USE ACCOUNT SECURITY QUESTIONS

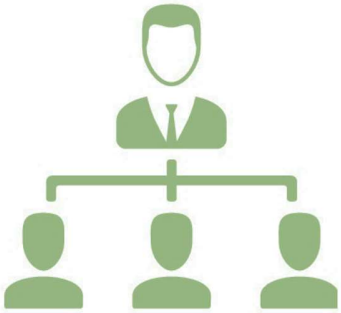
- Record and store securely

NEVER USE ACCOUNT EXCEPT FOR EMERGENCIES

105

Cloud Management IAM

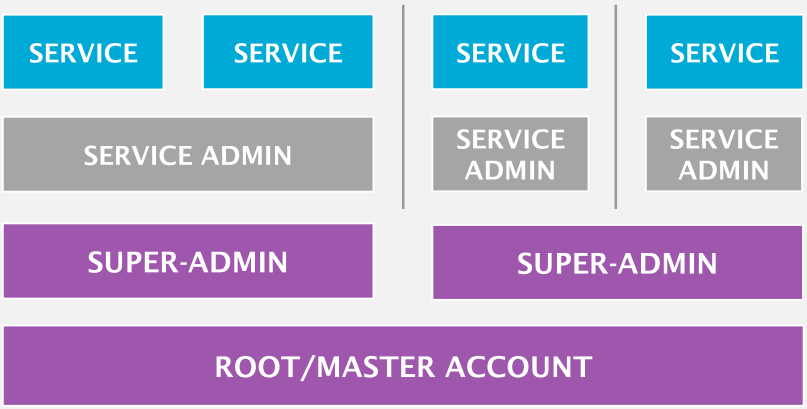
- Role-Based Access Control (RBAC)
- Variable granularity across providers/platforms
- Variable granularity within product lines
- Look for ability to integrate w/SSO or directory services
- Investigate third-party tools



106

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Privileged Users



107

Monitoring and Auditing

CLOUD SIDE

- Logs all API and internal activity
- Best option when available
- Pull logs to secure, central location

PORTAL / PROXY

- Route users through a portal, they don't have direct credentials
- Misses internal activity or compromised creds
- May be the only option
- CASB tools often used for SaaS (we discuss later) Host / Network Logs

108

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. The management plane is how you manage your cloud deployments. It's the biggest difference from traditional infrastructure security, and the most critical piece to protect.
2. Nearly all clouds support both web console and API management plane access. When running your own cloud it's critical to make sure these are effectively locked down.
3. Management planes support different kinds of credentials, all of which must be managed securely.
4. Always start by securing the root or master account since losing control of that means losing complete control over your cloud deployment.
5. Enforce least privilege when setting up your other privileged users and administrators.
6. Always use multifactor authentication for all cloud accounts, especially privileged users.

cloud security alliance

109

INSTRUCTOR LOGO HERE
Change img on all slide masters.

109

110

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Rule # 1

ARCHITECT FOR FAILURE!

Design for your platform(s) and don't expect existing architectures to lift and shift without compromise

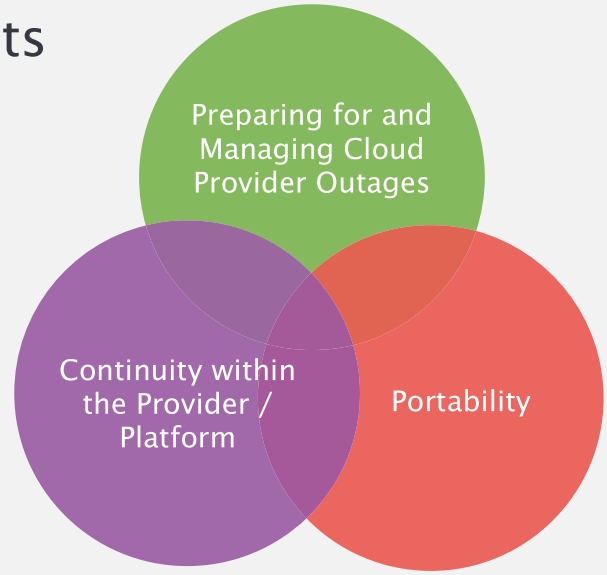
CSA cloud security alliance®

111

INSTRUCTOR LOGO HERE
Change img on all slide masters.

111

Key Aspects



CSA cloud security alliance®

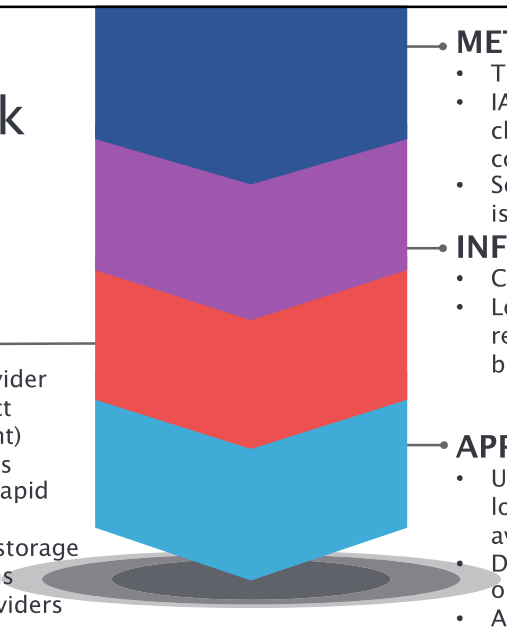
112

INSTRUCTOR LOGO HERE
Change img on all slide masters.

112

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cover the Entire Stack



METASTRUCTURE
- The cloud configuration
- IAM, monitoring, and other in-cloud management controls and compliance artifacts
- Software Defined Infrastructure is a key tool

INFRASTRUCTURE
- Core configuration
- Leverage platform/provider resiliency capabilities rather than building from scratch inside VMs

APPLISTRUCTURE
- Understand PaaS limitations and lock-in, including the historical availability of services
- Downtime is nearly always an option – have realistic standards
- Adopt Chaos Engineering

INFOSTRUCTURE
- Leverage "resilient" provider storage (e.g. most object storage is highly resilient)
- Keep backups/snapshots within the provider for rapid restore
- Always use lowest cost storage and transfer mechanisms within and between providers

CSA cloud security alliance®

113

INSTRUCTOR LOGO HERE
Change img on all slide masters.

113

BC/DR in the Cloud

ARCHITECTURE FOR FAILURE.

TAKE A RISK-BASED APPROACH TO EVERYTHING.
- Even when you assume the worst, it doesn't mean you can afford or need to keep full availability if the worst happens.

DESIGN FOR HIGH AVAILABILITY WITHIN YOUR CLOUD PROVIDER.
- In IaaS and PaaS, this is often easier and more cost effective than the equivalent in traditional infrastructure.
- Take advantage of provider-specific features.
- Understand provider history, capabilities, and limitations.
- Cross-location should always be considered, but beware of costs depending on availability requirements.
- Also ensure things like images and asset IDs are converted to work in the different locations.
- Business continuity for metastructure is as important as that for assets.

CSA cloud security alliance®

114

INSTRUCTOR LOGO HERE
Change img on all slide masters.

114

Copyright 2019 Cloud Security Alliance and Securosis, LLC

BC/DR in the Cloud

PREPARE FOR GRACEFUL FAILURE IN CASE OF A CLOUD PROVIDER OUTAGE.

- This can include plans for interoperability and portability with other cloud providers or a different region with your current provider.

- For super-high-availability applications, start with cross-location BC before attempting cross-provider BC.
- Cloud providers, including private cloud, must provide the highest levels of availability and mechanisms for customers/users to manage aspects of their own availability.

CSA cloud security alliance®

115

INSTRUCTOR LOGO HERE
Change img on all slide masters.

115

Review

1. The first rule of cloud is to architect for failure. Since any individual virtual resource may be less resilient, cloud providers and platforms have built in tools to improve systemic resilience. Fail to use these will make you more likely to experience an outage.
2. The three major areas to focus on are resiliency in your application, resiliency within your cloud provider, then resiliency if your provider goes down. Portability can play a role here but don't get so hung up on it that you become paralyzed and can't use all of the capabilities of your platform or provider.
3. Your BC/DR should cover the entire stack of the logical model- from the metastructure/management plane and infrastructure to your data and application architecture.

CSA cloud security alliance®

116

INSTRUCTOR LOGO HERE
Change img on all slide masters.

116

Copyright 2019 Cloud Security Alliance and Securosis, LLC