

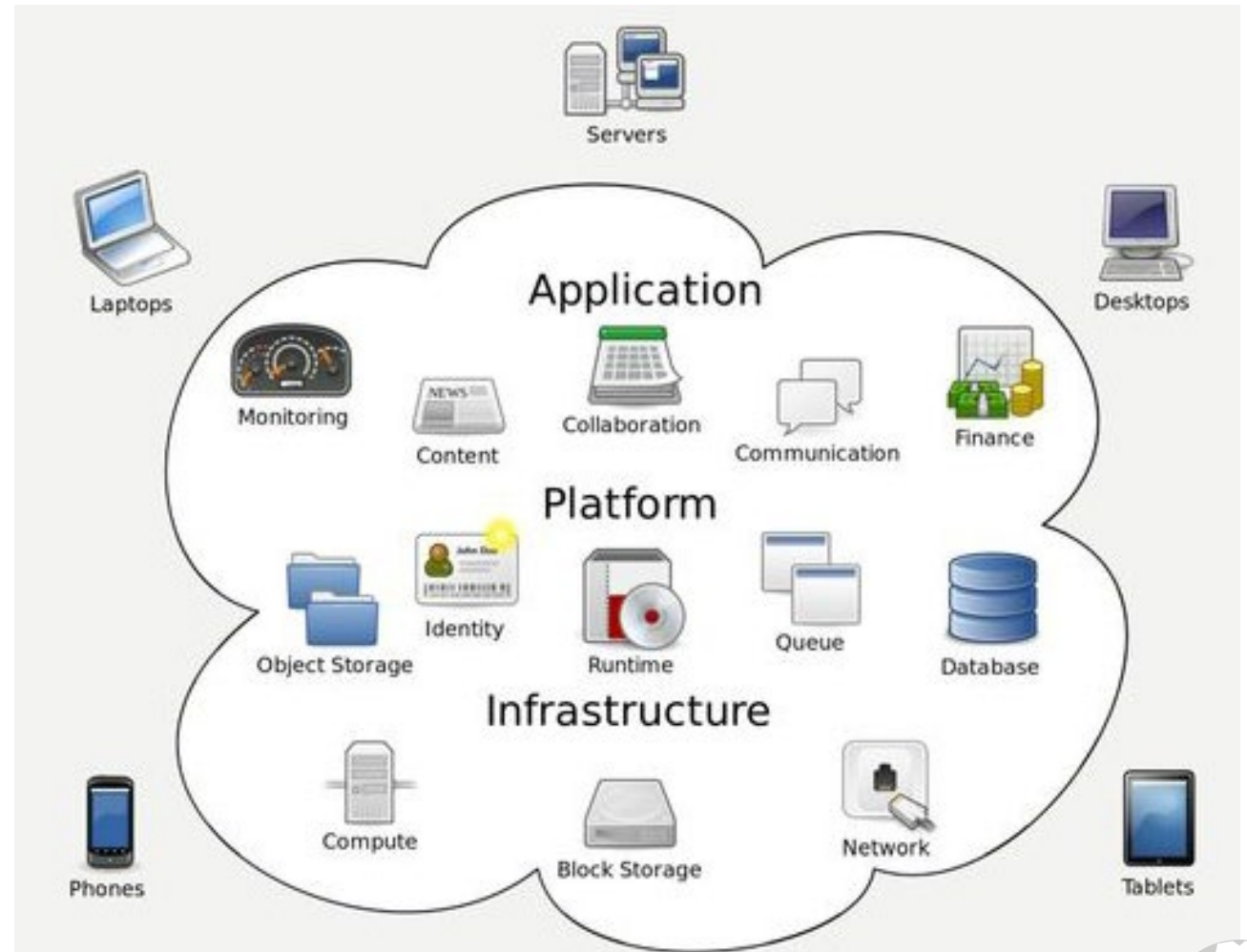
19.1 CLOUD COMPUTING CONCEPTS

- Overview
- Virtualization



WHAT IS CLOUD COMPUTING?

- Virtualization of some or all of your computing and network services
- Offered by a Cloud Services Provider (CSP)



CHARACTERISTICS OF CLOUD COMPUTING

- All functionality is virtualized
- On-demand self-service
 - You buy a general subscription
 - Then use whatever resources you like
 - Only pay for what you use
- Distributed storage
- Rapid elasticity
- Automated management
- Broad network access
 - Wide variety of client types from nearly any location
- Resource pooling



SERVERLESS ARCHITECTURE

- “Serverless” is the most common cloud computing execution model
 - It separates computing functionality from the physical hardware
 - The cloud provider doesn’t allocate a *specific* server to the customer
 - Instead, the provider uses a virtual environment to allocate a *portion* of their server’s CPU time, memory, and disk space to the customer as needed
 - The services and functions are most likely spread across multiple servers in the provider’s datacenter
- The serverless model can automatically:
 - Provision required computing resources on demand
 - Scale those resources up or down as needed
 - Scale resources to zero when the application stops running
- Every leading cloud services provider offers a serverless platform



SERVERLESS ARCHITECTURE EXAMPLE



CLOUD COMPUTING PORTAL EXAMPLE

The screenshot displays the Microsoft Azure portal interface. On the left is a dark navigation sidebar with the 'Microsoft Azure' logo at the top. Below the logo are links for 'Create a resource', 'All services', and a 'FAVORITES' section containing 'Dashboard', 'All resources', 'Resource groups', 'App Services', 'Function Apps', 'SQL databases', 'Azure Cosmos DB', 'Virtual machines', 'Load balancers', 'Storage accounts', 'Virtual networks', 'Azure Active Directory', 'Monitor', and 'Advisor'. The main content area has a top bar with a search box labeled 'Search resources, services, and docs' and icons for navigation, help, notifications, and settings. Below this is a 'Dashboard' header with options to '+ New dashboard', 'Upload', 'Download', 'Edit', 'Share', 'Full screen', 'Clone', and 'Delete'. The dashboard is divided into three columns. The first column, titled 'All resources' with a 'Refresh' button, lists resources under 'All subscriptions': 'chrys123' (Storage account), 'mychrysdbserver' (SQL server), and 'MyChrysSQL' (SQL database). The second column features a 'Getting started' section with a 'Create DevOps Project' button and a 'Quickstarts + tutorials' section listing 'Windows Virtual Machines', 'Linux Virtual Machines', 'App Service', and 'Functions'. The third column contains a 'Microsoft Intune' tile.

Microsoft Azure

Search resources, services, and docs

Dashboard ▾ + New dashboard ↑ Upload ↓ Download ✎ Edit 📁 Share ↗ Full screen 📄 Clone 🗑 Delete

All resources
All subscriptions

Refresh

chrys123	Storage account
mychrysdbserver	SQL server
MyChrysSQL	SQL database

Azure getting started made easy!

Launch an app of your choice on Azure in a few quick steps

Create DevOps Project

Microsoft Intune

Quickstarts + tutorials

Windows Virtual Machines ⓘ
Provision Windows Server, SQL Server, SharePoint VMs

Linux Virtual Machines ⓘ
Provision Ubuntu, Red Hat, CentOS, SUSE, CoreOS VMs

App Service ⓘ
Create Web Apps using .NET, Java, Node.js, Python, PHP

Functions ⓘ
Process events with a serverless code architecture



VIRTUALIZATION

- Virtualization Characteristics
- Virtualization Terminology
- Virtualization Benefits



WHAT IS VIRTUALIZATION?

- A model in which computing functionality is separated from the physical hardware it runs on
- You run computing functionality as an application inside another computer
- A single powerful “host” computer can run entire operating systems and networks as individual applications
- You can also split the various compute functions across multiple hosts



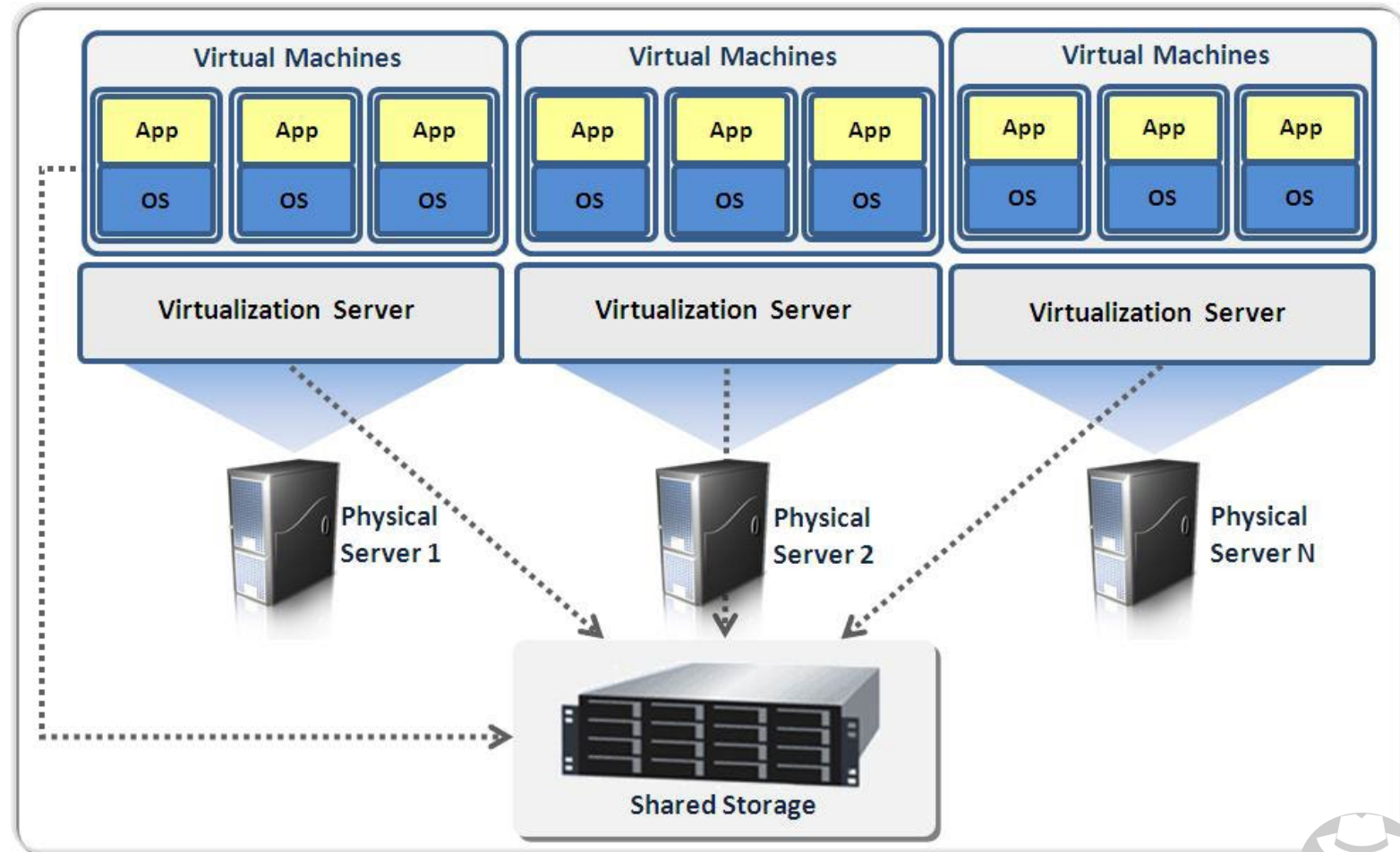
CHARACTERISTICS OF VIRTUALIZATION

- Partitioning
 - Many applications and multiple OSes in a single physical system
- Isolation
 - Each VM is isolated from the host and other VMs
- Encapsulation
 - A virtual hard disk is a single file



VIRTUALIZATION

- VMs run as apps on a host OS
- A hypervisor allows the VMs and host OS to share resources
- Common items that are virtualized:
 - OS
 - Apps
 - Network devices
 - Network connections
 - Storage



VIRTUALIZATION TERMINOLOGY

- Virtual desktop infrastructure (VDI)
 - A virtualization implementation that separates the personal computing environment from a user's physical computer
 - The user's desktop runs as a VM in a datacenter
 - The user's PC connects to the VM across a network
- Virtual private cloud (VPC)
 - A private network segment made available to a single cloud consumer on a public cloud
- Virtual private network (VPN)
 - A secure tunnel created between two endpoints connected via an insecure network, typically the Internet
- User and entity behavior analytics (UEBA)
 - A system that can provide an automated identification of suspicious activity by user accounts and computer hosts.



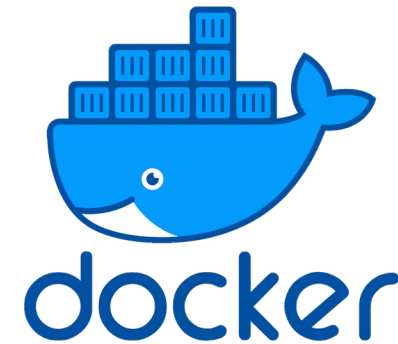
BENEFITS OF VIRTUALIZATION

- Improved business continuity during disaster recovery
 - Just “stand up” (enable) a backup copy of the virtual machine
- Reduced infrastructure cost
 - More efficiently use compute resources, floor space, and electrical power
- Improved delivery of services and IT management
- Improved operational efficiency
- Reduced system administration required
- Improved data protection and backup
- Improved service levels and service positioning
- Improved control and compliance
- “Anywhere” access
- Minimal hardware investment and maintenance

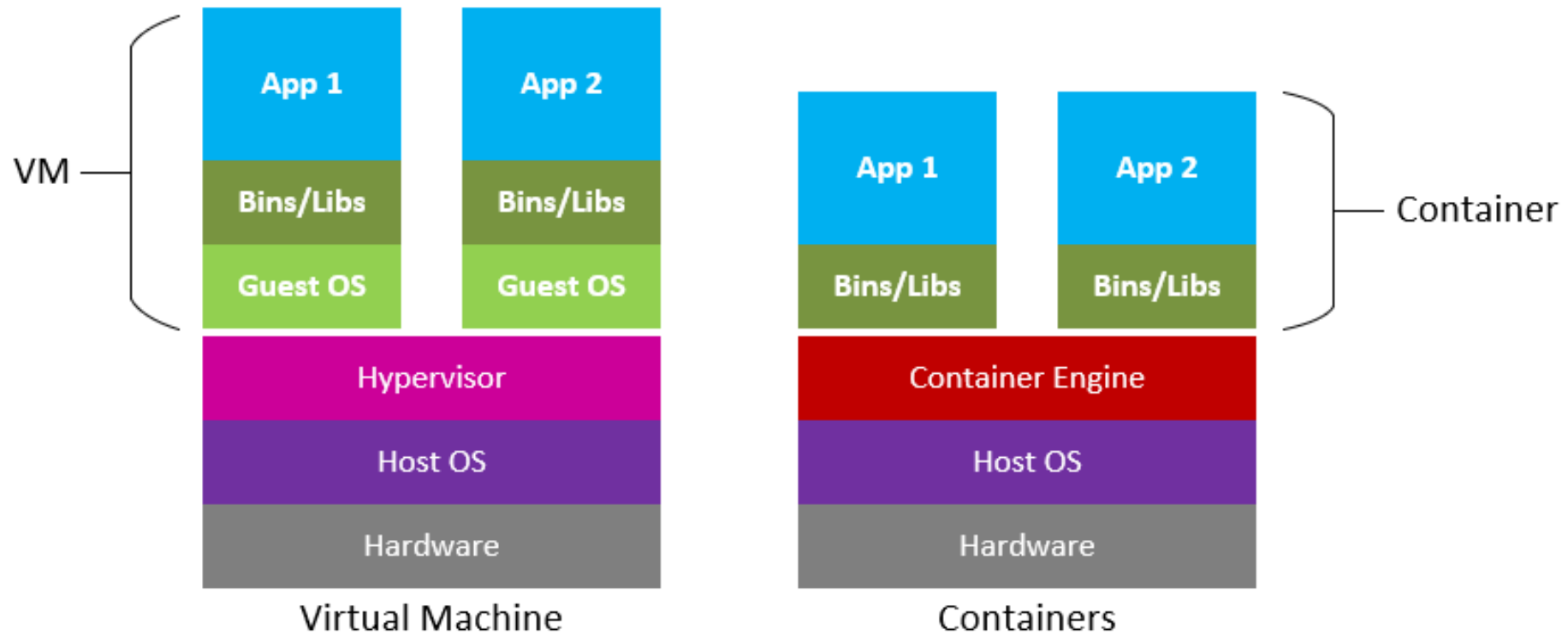


CONTAINERS

- A lightweight “VM” for a single app
- More efficient than traditional virtual machine
 - Does not have its own OS
 - Borrows functionality from the host OS
- Has everything needed to run an single application:
 - Code
 - Runtime
 - System tools
 - System libraries
- Examples include Docker, Kubernetes, Podman, OpenVZ and others
- Cloud-based container services have become very popular



VIRTUAL MACHINE VS CONTAINER



19.2 CLOUD TYPES

- Cloud Service Models
- Cloud Deployment Models
- Fog Computing

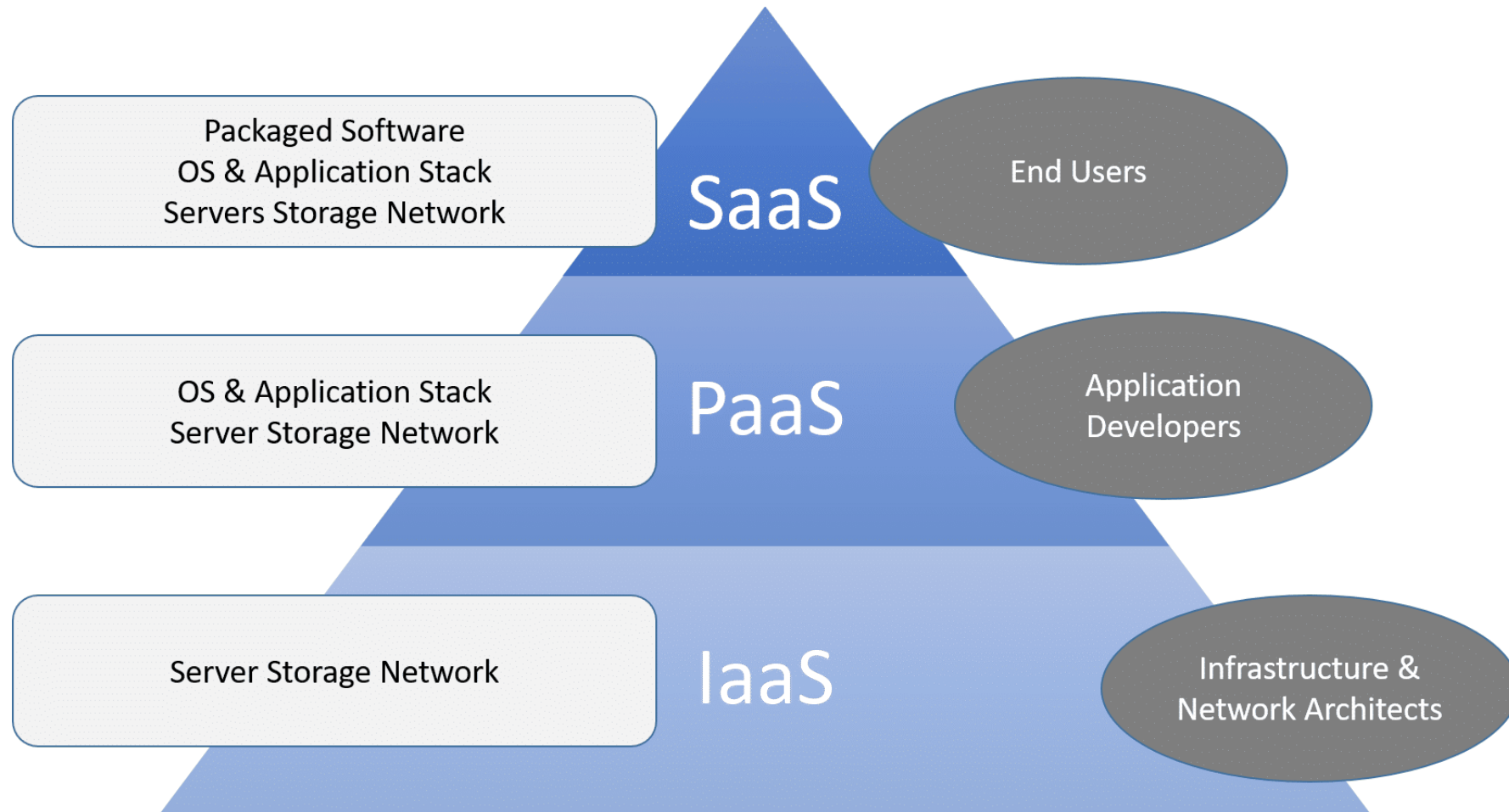


CLOUD SERVICE MODELS

- SaaS
 - Software-as-a-Service
- PaaS
 - Platform-as-a-Service
 - Provides the end-user with a development environment and/or generic computers without all the hassle of configuring and installing it themselves
 - If you want to develop a customized or specialized program, PaaS helps reduce the development time and overall costs by providing a ready to use platform
- IaaS
 - Infrastructure-as-a-Service
 - Focused on the replacement of physical hardware at a customer's location with cloud-based resources
 - Place your entire network in the cloud: subnets, routers, switches, servers, firewalls, WAN links, etc.



CLOUD SERVICE MODELS



SAAS EXAMPLE

Home > SQL databases > MyChrysSQL

SQL databases

TBH Consulting

+ Add Edit columns More

Filter by name...

NAME ↑↓

MyChrysSQL

MyChrysSQL

SQL database

Search (Ctrl+ /)

Copy Restore Export Set server firewall

Resource group (change) [MyChrysResourceGroup](#) S

Status E

Online N

Location C

East US S

Subscription (change) [Pay-As-You-Go](#) P

Subscription ID C

89ee8358-31b4-4ebd-9353-f1ef75bf0058 2

Tags (change) [Click here to add tags](#)

Resource utilization (MyChrysSQL)

1 hour 2

100%

90%

80%

70%

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Quick start
- Query editor (preview)
- Settings
 - Configure
 - Geo-Replication
 - Connection strings
 - Sync to other databases
 - Add Azure Search



PAAS EXAMPLE

AWS Management Console

Services Edit Paris ARAU N. Virginia Help

EC2 Dashboard

- Events
- Tags
- Reports
- Limits

INSTANCES

- Instances
- Spot Requests
- Reserved Instances

IMAGES

- AMIs
- Bundle Tasks

ELASTIC BLOCK STORE

- Volumes
- Snapshots

NETWORK & SECURITY

- Security Groups
- Elastic IPs
- Placement Groups
- Load Balancers
- Key Pairs
- Network Interfaces

AUTO SCALING

- Launch Configurations
- Auto Scaling Groups

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) region.

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
1 Key Pair	0 Load Balancers
0 Placement Groups	3 Security Groups

Easily deploy and operate applications - use Chef recipes, manage SSH users, and more. [Try OpsWorks now](#) Hide

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the US East (N. Virginia) region.

Service Health

Service Status:

- US East (N. Virginia)
This service is operating normally

Availability Zone Status:

- us-east-1a
Availability zone is operating normally
- us-east-1b
Availability zone is operating normally
- us-east-1d
Availability zone is operating normally

[Service Health Dashboard](#)

Scheduled Events

US East (N. Virginia):

- No events

Account Attributes

Supported Platforms

- VPC

Default VPC

- vpc-6e76a30b

Additional Information

- [Getting Started Guide](#)
- [Documentation](#)
- [All EC2 Resources](#)
- [Forums](#)
- [Pricing](#)
- [Contact Us](#)

AWS Marketplace


Find **free software trial** products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these popular AMIs

- [Vyatta Virtual Router/Firewall/VPN](#)
Provided by Vyatta, Inc.
Rating ★★★★★
Pay by the hour for software and AWS usage
[View all Networking Software](#)
- [Alert Logic Threat Manager for AWS](#)
Provided by Alert Logic
Rating ★★★★★
Pay by the hour for software and AWS usage
[View all Security Software](#)

© 2008 - 2014, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)








IAAS EXAMPLE





 **Services** ▾ **Edit** ▾

Amazon Web Services





Compute & Networking

-  **Direct Connect**
Dedicated Network Connection to AWS
-  **EC2**
Virtual Servers in the Cloud
-  **Elastic MapReduce**
Managed Hadoop Framework
-  **Route 53**
Scalable Domain Name System
-  **VPC**
Isolated Cloud Resources







Storage & Content Delivery

-  **CloudFront**
Global Content Delivery Network
-  **Glacier**
Archive Storage in the Cloud
-  **S3**
Scalable Storage in the Cloud
-  **Storage Gateway**
Integrates On-Premises IT Environments with Cloud Storage







Database

-  **DynamoDB**
Predictable and Scalable NoSQL Data Store
-  **ElastiCache**
In-Memory Cache
-  **RDS**
Managed Relational Database Service
-  **Redshift** **NEW**
Managed Petabyte-Scale Data Warehouse Service

Deployment & Management

-  **CloudFormation**
Templated AWS Resource Creation
-  **CloudWatch**
Resource and Application Monitoring
-  **Data Pipeline**
Orchestration for Data-Driven Workflows
-  **Elastic Beanstalk**
AWS Application Container
-  **IAM**
Secure AWS Access Control
-  **OpsWorks** **NEW**
DevOps Application Management Service

App Services

-  **CloudSearch**
Managed Search Service
-  **Elastic Transcoder** **NEW**
Easy-to-use Scalable Media Transcoding
-  **SES**
Email Sending Service
-  **SNS**
Push Notification Service
-  **SQS**
Message Queue Service
-  **SWF**
Workflow Service for Coordinating Application Components



CLOUD DEPLOYMENT MODELS

- **Private Cloud:**
 - Single organization use, typically on-premises
- **Public Cloud:**
 - Open for public use
 - In SaaS, different companies might share the same application
 - Their data will be kept separate
 - Typical in small business such as a doctor's office
- **Community Cloud:**
 - Used by multiple organizations with the same configuration or security requirements
 - Example: different bureaus within the same government agency
- **Hybrid Cloud:**
 - Combination of two or more types of cloud
 - Can also refer to an extension of the on-premises datacenter into the cloud
 - Users can connect to either
 - The on-prem facility treats the cloud as additional servers
 - On-prem and cloud servers replicate to each other
 - An "always on" VPN connects the two



SEPARATION OF RESPONSIBILITIES IN THE CLOUD

- On-premises:
 - Customer is responsible for everything
- IaaS:
 - Customer is responsible for applications, data, runtime, middleware, O/S
 - Service provider is responsible for virtualization, servers, storage, networking
- PaaS:
 - Customer is responsible for applications, data
 - Service is provider responsible for runtime, middleware, O/S, virtualization, servers, storage, networking
- SaaS:
 - Service provider is responsible for (nearly) everything
- Check your contract and SLA for exact provider and customer division of responsibilities



FOG COMPUTING

- Fog
- Fog Benefits
- Fog Layers

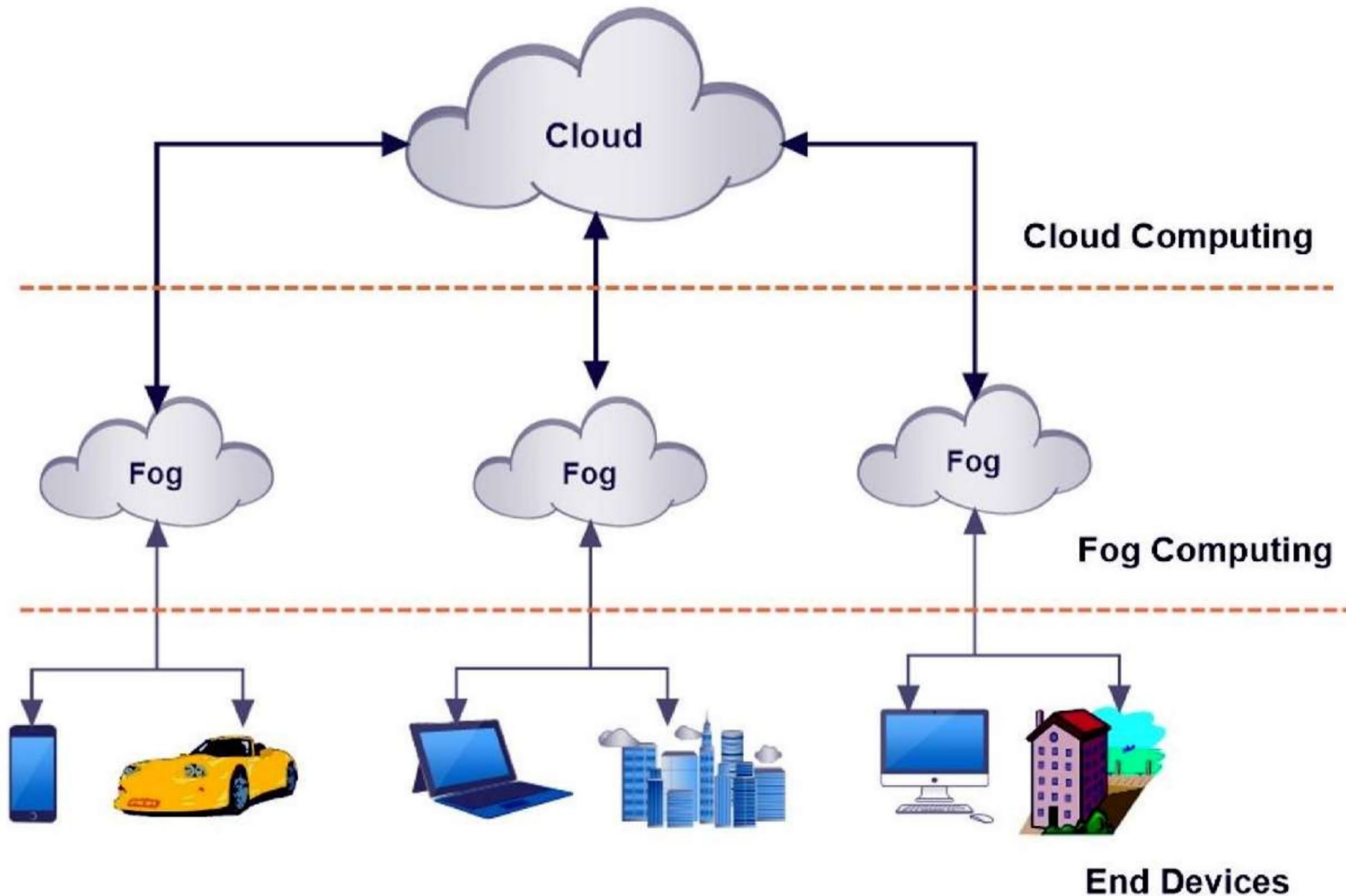


FOG (EDGE) COMPUTING

- The “Fog” is an extension of cloud-based computing
 - Extends the cloud to an enterprise’s network edge
 - Coined by Cisco because “fog” is a cloud close to the ground
- A horizontal, system-level architecture
- Computing, storage, control and networking functions are brought closer to users along a cloud-to-thing continuum
- Decentralizes IoT devices
 - Runs cloud applications and services right at the “edge”
 - They have immediate or direct connection to the Internet while being close to people
 - They can process data in real-time with no latency
 - They don’t have to rely on information being sent to the cloud, then back down again



FOG COMPUTING EXAMPLE



FOG COMPUTING BENEFITS

- Addresses the biggest challenges for IoT:
 - Bandwidth
 - Latency
- Ensures QoS
- Reduces energy consumption / improve battery life
- Provides faster data processing and transfer between IoT systems
- Processes data privately (locally) / improves data security
- Fog enables us to build solutions around:
 - Location awareness
 - Mobility
 - Wide geographical distribution
 - Low latency between devices
 - Wireless access



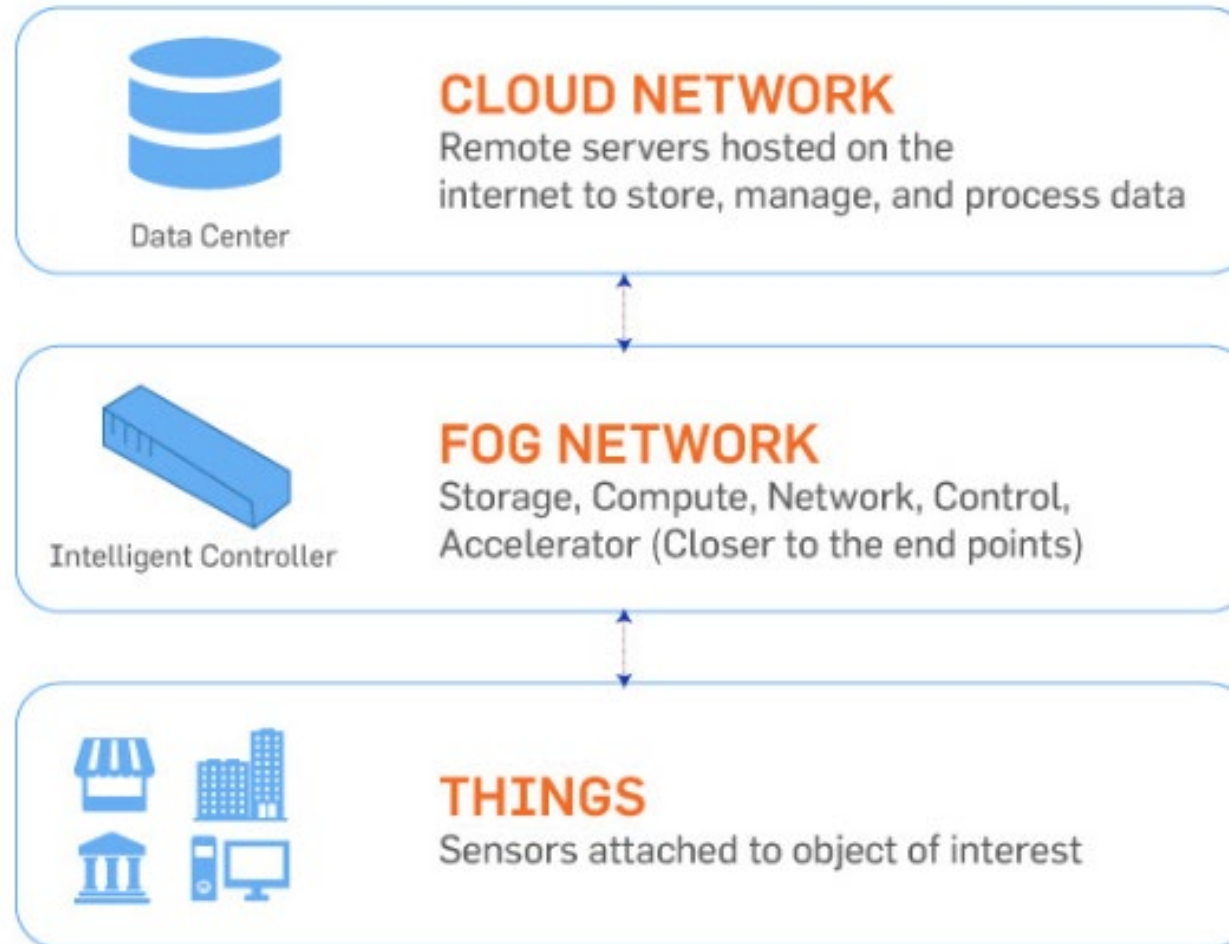
FOG: ENABLER FOR SMART IOT DEVICES

Provides new capabilities such as:

- Sharing resources from one device to another
- Making real-time decisions
- Contextual data (available locally) for customized intelligence
 - Enhances user experience
- Autonomous networks that operate locally
 - Can make decisions such as saving energy and network bandwidth, improving data security, reducing latency, etc.
- Streamline online-to-offline processes
 - Leverage the physical proximity of the customer
 - Better authentication and cross-sell opportunities



FOG COMPUTING LAYERS



THE FOG LAYER

- Fog layer includes “Fog nodes”
 - Devices such as routers, gateways, access points, base stations, specific fog servers, etc.,
- Fog nodes are located at the edge of a network
 - Can be a hop distance from the end device
 - Fog nodes are situated between end devices and cloud data centers
- Fog nodes can be:
 - static, e.g., located in a bus terminal or coffee shop
 - moving, e.g., fitted inside in a moving vehicle
- Fog nodes ensure services to end devices
 - Fog nodes can compute, transfer and store the data temporarily.
- Fog nodes use TCP/IP to connect to a datacenter in the cloud



FOG IN THE CLOUD INFRASTRUCTURE



19.3 CLOUD BENEFITS AND CONSIDERATIONS

- Pros of Cloud Computing
- Cons and Considerations
- Shared Security
- Cloud Forensics

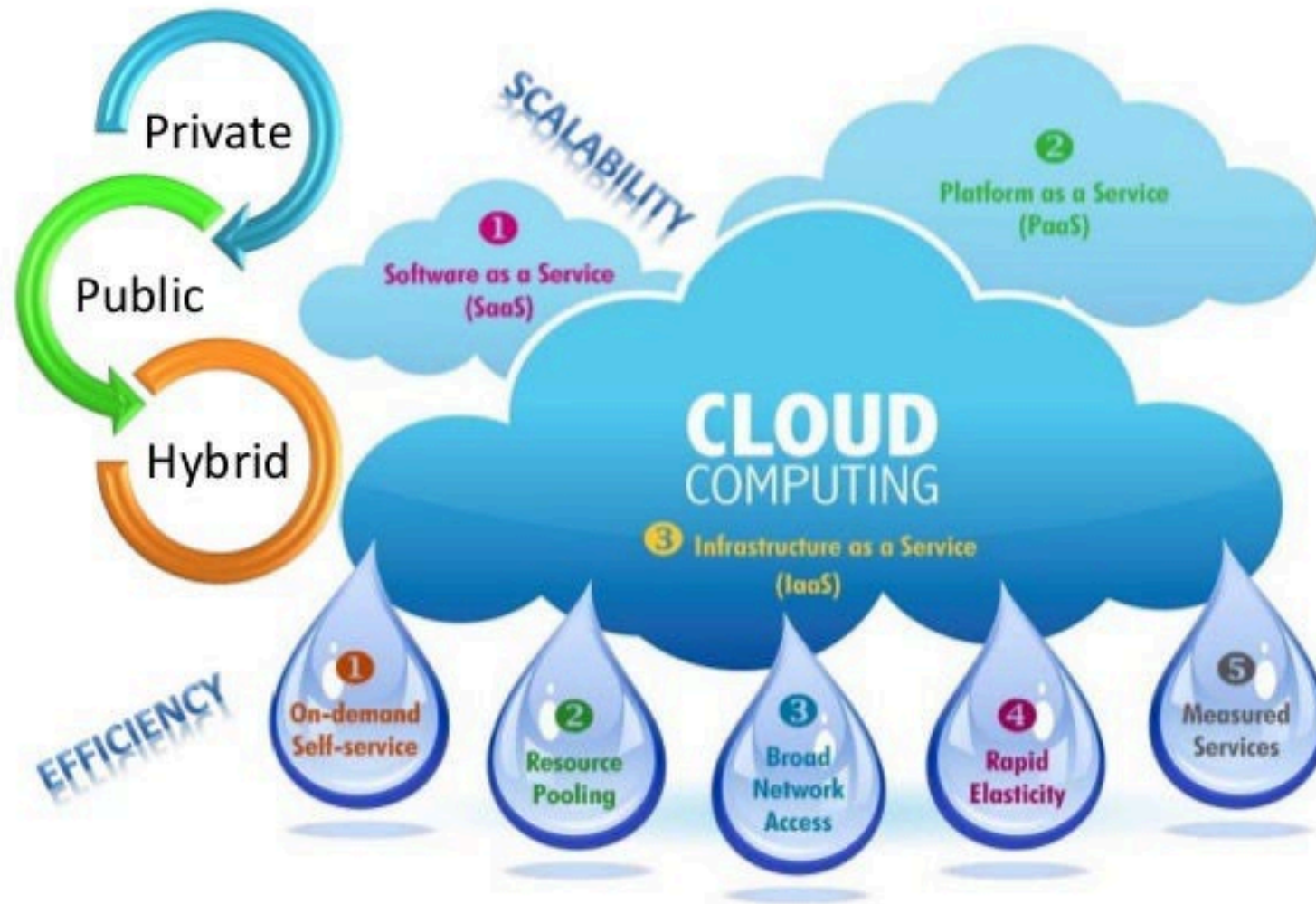


PROS OF CLOUD COMPUTING

- Only pay for what you use
 - Minimal investment in hardware
 - You need good connectivity and end user devices
- Rapid scalability/agility/flexibility
- If you implement SaaS, you don't need much technical expertise
- Most providers have considerably more fault tolerance/disaster recovery capability than the average customer has
- Nearly all on-premises functionality can be moved to the cloud
 - Your users just need to be able to securely connect
- Cloud providers typically have more capabilities than on-premises datacenters including big data analytics, artificial intelligence integration, large scale parallel computing



CLOUD BENEFITS



CONS/CONSIDERATIONS OF CLOUD COMPUTING

- The customer is dependent on the cloud provider to provide the necessary levels of service for their application
 - The customer does not manage the back-end infrastructure
 - The cloud provider is responsible for all back-end tasks such as provisioning, scheduling, scaling and patching
 - Make sure YOUR security policy covers any gaps in the provider's security policy
- Customer end-point devices that connect to the cloud must still have their own security (firewall, anti-virus, etc.)
- You might have to utilize the provider's existing vendor testing and audits in place of normal penetration testing procedures
 - Most SaaS providers will not allow customers to conduct their own port scans or vulnerability scans against the SaaS service



CONS/CONSIDERATIONS OF CLOUD COMPUTING (CONT'D)

- Customization may cost more
 - Be very careful of hidden costs
 - Even if you have shut down VMs, they are still “running” and incurring cost
 - You will also have costs for storage, advanced support, infrastructure services, etc.
- You're at risk of not purchasing the solution you actually need
 - Work with the provider on your use case
- For PaaS and IaaS, you **STILL** need to implement all the same security controls that you would in an on-premises environment
 - You will have to pay for fault-tolerance, load-balancing, and the facilities and features necessary for disaster recovery

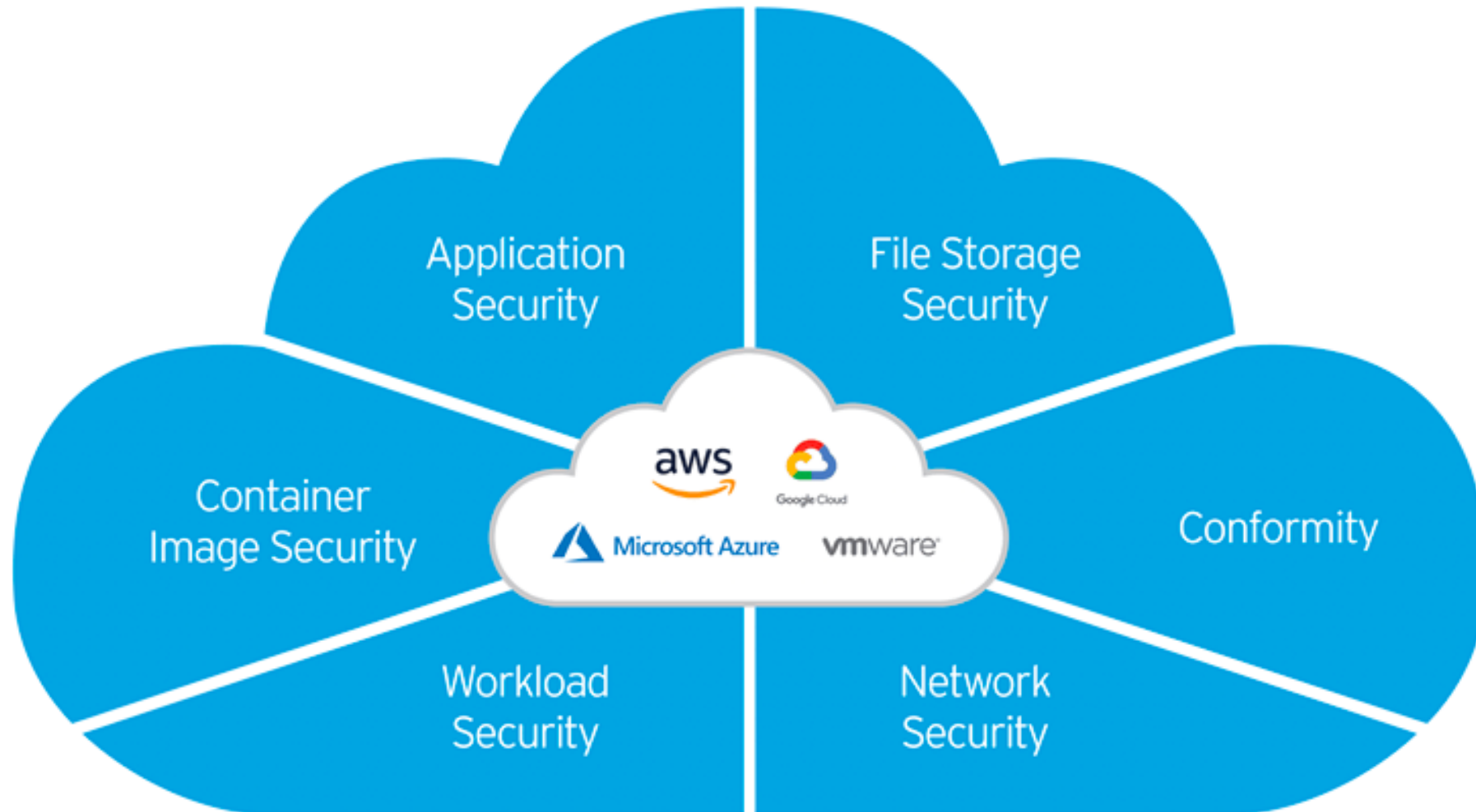


CONS/CONSIDERATIONS OF CLOUD COMPUTING (CONT'D)

- The customer is dependent on the provider to:
 - Maintain adequate security
 - Be able to meet SLAs
- Legal or regulatory requirements may prevent you from moving data to the cloud
 - Cloud datacenter locations are often trans-national
 - You may be required to keep data physically within your national borders
- Your contract might get you “locked in” to a single provider



CLOUD CONSIDERATIONS



CLOUD SHARED SECURITY RESPONSIBILITY

- In a SaaS model, the customer has to ensure that the endpoints being used to access the cloud are secure
 - Since the consumer owns the endpoint (laptop, desktop, tablet, smartphone, etc.), they are responsible for securing it
 - The provider will ensure that the back-end infrastructure performs properly and is hardened against security risks
- In a PaaS model, any applications that the customer develops are the customer's responsibility to secure
- In an IaaS model, the customer must secure all aspects of the deployed virtual infrastructure as if it was a physical infrastructure on their own premises



CLOUD FORENSICS

- Performing digital forensics on cloud assets is particularly challenging
 - The on-demand nature of cloud services means that instances are often created and destroyed again
 - There is no real opportunity for forensic recovery of any data
- Cloud providers can mitigate this to some extent by using extensive logging and monitoring options
 - A CSP might also provide an option to generate a file system and memory snapshots from containers and VMs in response to an alert condition generated by a SIEM
- Employee workstations are often the easiest to conduct forensics on
 - They are a single-user environment for the most part
- Mobile devices have some unique challenges due to their operating systems
 - Good forensic tool suites are available to ease the forensic acquisition and analysis of mobile devices
- On-premise servers are more challenging than a workstation to analyze
 - But they do not suffer from the same issues as cloud-based services and servers



CLOUD SCENARIO

- Which of the following are valid concerns when migrating to a serverless architecture?
- **Dependency on the cloud service provider**
- **Protection of endpoint security**
- Limited disaster recovery options will NOT be an issue



CLOUD SCENARIO #2

- Your company has recently been embarrassed by several high profile data breaches.
- The CIO proposes improving the company's cybersecurity posture by migrating images of all the current servers and infrastructure into a cloud-based environment.
- What, if any, is the flaw in moving forward with this approach?
- **This approach only changes the location of the network and not the attack surface of it**
- A poorly implemented security model at a physical location will still be a poorly implemented security model in a virtual location.
- Unless the fundamental causes of the security issues that caused the previous data breaches have been understood, mitigated, and remediated, then migrating the current images into the cloud will change where the processing occurs without improving the network's security.



19.4 CLOUD RISKS AND VULNERABILITIES

- Provider-related Risks
- Tenant-created Risks
- Cloud Vulnerabilities



CLOUD VULNERABILITIES

- Similar to on-premises
- But...
 - Datacenter is remote
 - Run by someone else
 - Shared with other customers
 - Easily accessed from anywhere



PROVIDER-RELATED RISKS

- Failure of network management
- Compromised management interface
- Risks posed by changes in jurisdiction
- Acquisition of cloud provider
- Computer equipment theft
- Malicious insiders



PROVIDER-RELATED RISKS (CONT'D)

- Failure or termination of cloud services
- Modification or loss of backed up data
- Improper or illegal data handling
- Improper or incomplete data disposal
- Risks associated with compliance
 - You might be at risk if CSP cannot provide evidence of their compliance
- Inadequate infrastructure design and planning by the CSP
 - Might not be able to meet agreed service levels and performance/latency requirements



TENANT-CREATED RISKS

- Data breach/loss
 - Data or keys are illegally accessed, lost, erased, misused
 - Loss of encryption keys
- Shadow IT
 - IT systems or solutions that are developed to handle an issue but aren't sent through the proper approval chain
- Risks with licensing
 - Client might incur huge fees if software is charged on a per-instance basis
- Abuse of cloud services
 - Attackers create anonymous access to cloud services
 - Perform all of the attacks previously studied
- Insufficient Due Diligence
 - Ignorance of the CSP's environment could cause contractual and responsibility gaps



TENANT-CREATED RISKS (CONT'D)

- Insufficient infrastructure planning and design
 - You might not really understand what a cloud deployment entails
 - Your subscription might include services you don't really need, or might be missing services you really do need
- Undetermined risk profiles
 - Clients are unable to get a clear picture of the CSP's internal security procedures, compliance, system hardening, auditing, etc
- E-discovery and subpoena
- Loss of governance
 - Client gives up control to the CSP
- Lock-in
 - Inability of client to migrate to another CSP or in-house systems due to lack of tools or standard data formats



CLOUD ADOPTION RISKS

- Economic Denial of Sustainability (EDOS)
 - A hacker might use up your compute power, causing you to be charged for usage due to their activity
- Loss of security and operational logs
 - Under-provisioning of storage for logs
 - Unsynchronized System Clocks that negatively affect automated tasks or cause time stamp mismatches
- Conflict between cloud environment and hardening procedures
 - Client procedures may conflict with the CSP's environment, negating implementation



CLOUD VULNERABILITIES

- **Server misconfigurations**
 - The most common cloud vulnerability today
 - Improper permissions, not encrypting the data, and failing to differentiate between private and public data
 - Failing to properly configure cloud-based storage such as AWS S3 buckets leads to data breaches
- **Insecure APIs**
 - Improper use of HTTP methods like PUT, POST, DELETE in APIs can allow hackers to upload malware on your server or delete data.
 - Circumvent user defined policies
 - Breach in logging and monitoring
 - Unknown API dependencies
 - Reusable passwords/tokens
 - Insufficient input data validation
 - Improper access control and lack of input sanitization are also main causes of API compromise



CLOUD VULNERABILITIES (CONT'D)

- Lack of Multi-factor Authentication
 - Weak authentication makes it easier for malicious actors to access your cloud services
- Insider Threats
 - Misconfiguration allows accidental security incidents
 - Former employees/vendors/partners still have access
- DDoS Attacks
 - Prefer a cloud vendor that offers DDoS protection features
 - Engage the services of a third party (CrowdStrike, CloudFlare) that specializes in DDoS protection
- Lack of Visibility
 - Companies can end up using thousands of instances of cloud services
 - It's easy to lose track of what you have running



CLOUD VULNERABILITIES (CONT'D)

- Poor Coding Practices (on your part)
 - Security is typically a low priority or afterthought in application development
 - With a push to get customized cloud applications online as quickly as possible, software often contains bugs like SQLi, XSS, CSRF
 - These vulnerabilities are the root cause for the majority of cloud web services being compromised.
- Issues with shared technology
 - Most underlying cloud components (GPU, CPU caches) do not offer strong isolation



19.5 CLOUD THREATS AND COUNTER- MEASURES

- Using the Cloud as a Hacking Tool
- Threats and Countermeasures



USING THE CLOUD AS A HACKING TOOL

- Host malicious content in S3 buckets or other blob storage
- Quickly stand up a high-performing hacking workspace
- Use elastic / distributed cloud compute resources for intensive tasks such as brute forcing
- Leverage greater bandwidth provided by cloud services
- Launch attacks from systems that are physically/logically closer to the target
- Use distributed cloud infrastructure to manage botnets

The Cloud can be both hacker and hacked!



CLOUD THREATS AND COUNTERMEASURES

Threat	Countermeasure
Sniffing	Require encrypted transmissions in the cloud and to the cloud
Port Scanning	Implement firewalls
Browser security misconfigurations	Require TLS, use XML encryption of SOAP messages
Virus/Malware injection	<ul style="list-style-type: none">• Create a whitelist of acceptable requests• Store clean hashes of requests so incoming requests can be hashed and compared



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threat	Countermeasure
<ul style="list-style-type: none">• Account or Service Hijacking via Social Engineering Attacks• Attacker can treat cloud login like any other website login page• Create fake login page/phish to capture credentials	<ul style="list-style-type: none">• Implement input sanitization on all web apps• Scan web apps for vulnerabilities and apply recommendations
Service Hijacking via Network Sniffing	<ul style="list-style-type: none">• Be sure to encrypt all data before transmission• Scan for promiscuous mode NICs
<ul style="list-style-type: none">• Session Hijacking via XSS Attacks<ul style="list-style-type: none">• Could steal cookies and authentication tokens	Use SSL, firewalls, antivirus to help



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threat	Countermeasure
<ul style="list-style-type: none">• Session Hijacking via Session Riding (CSRF)• Attacker uses your session to connect to your cloud	<ul style="list-style-type: none">• Do not allow browsers/websites to save login details• Disallow HTTP referrals
<ul style="list-style-type: none">• Domain Name System (DNS) Attacks• DNS poisoning• Cybersquatting, domain hijacking, domain snipping (registering an elapsed domain name)	<ul style="list-style-type: none">• Implement DNSSEC• Configure DNS server to protect against cache pollution• Patch and update DNS servers• Use an active check that validates the source of DNS responses• Buy domains that are variations of your company name• Trademark your company name to prove in court that you have a legitimate case over a cybersquatter



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threat	Countermeasure
SQL Injection Attacks	<ul style="list-style-type: none">Sanitize and validate input, update and patch, use DB monitoring and IPS, Web app firewall
Cryptanalysis Attacks	Use random number generation to add robustness to SSH keys and DNSSEC
<ul style="list-style-type: none">Wrapping Attacks<ul style="list-style-type: none">Attackers duplicate the body of a SOAP message and send it to the server as if from a legitimate user	Make sure the browser signs XML document



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threat	Countermeasure
<p>Cloud Hopping</p> <ul style="list-style-type: none">• Attack against Managed Service Provider (MSP) infrastructure to gain access to tenants' sensitive data• Attacker can leverage the cloud to hop between customer networks	<p>Provider:</p> <ul style="list-style-type: none">• Implement a proactive incident response measures <p>IT/system administrators:</p> <ul style="list-style-type: none">• Employ data categorization<ul style="list-style-type: none">• Mitigates the damage of a breach / protects the company's core data in case data are exposed• Network segmentation can help<ul style="list-style-type: none">• Limit privileges and access to sensitive data and corporate networks• Makes lateral movement more difficult for attackers



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threat	Countermeasure
<p>Escalation of privileges due to mistake in access allocation</p> <ul style="list-style-type: none">• Illegal access to cloud systems acquired• Weak authentication/authorization	<p>Patch systems, apply least privilege to users and services</p>
<p>Failure of supply chain</p> <ul style="list-style-type: none">• Cloud security is directly proportional to security of each link	<p>Ensure you and your CSP have backup plans and alternate suppliers</p>
<p>DoS and DDoS Attacks</p>	<ul style="list-style-type: none">• Implement fault tolerance and load balancing on services and network links• Apply least privilege principle to all users that connect to your cloud



CLOUD THREATS AND COUNTERMEASURES (CONT'D)

Threats	Countermeasure
<ul style="list-style-type: none">• Hardware/infrastructure/environment failures• Natural disasters• War, civil disturbance, terrorist activity• “Acts of God”	<ul style="list-style-type: none">• Ensure your SLA specifically covers these issues• Ensure your SLA contains enforcement mechanisms
<p>VM Escape</p> <ul style="list-style-type: none">• VM escape refers to malware running on a guest OS jumping to another guest or the host.• VM escape is the biggest threat to virtualized systems.	<p>As with any other software type, it is vital to keep the hypervisor code up-to-date with patches for critical vulnerabilities</p>



SIDE CHANNEL/CROSS-GUEST VM BREACH

- **Malicious co-tenants** might look for/attempt the following:
 - Timing variations, data remanence, acoustic cryptanalysis, power monitoring, differential fault analysis
- **Countermeasures:**
 - Implement virtual firewall on the back end
 - Use random encryption algorithms to avoid predictability
 - Check for repeated access attempts to local memory, hypervisor, or shared hardware cache
 - You'll have to tune process monitoring data and logs to collect this
 - Code your apps to access shared resources such as memory cache in a consistent and predictable way
 - Thus offering less information to attackers on timing statistics or behavioral attributes



MAN-IN-THE-CLOUD (MITC) ATTACKS

- Advanced version of MITM
- Done by abusing cloud file synch services like Google Drive or DropBox
- Hackers intercept and reconfigure cloud services by exploiting vulnerabilities in the synchronization token system
- During the next synchronization with the cloud, the synchronization token is replaced with a new one that provides access to the attackers
- Users may never know that their accounts have been hacked
- An attacker can put back the original synchronization tokens at any time
- There's also risk that compromised accounts will never be recovered



MITC COUNTERMEASURES

- Implement a Cloud Access Security Broker (CASB)
 - The CASB will monitor cloud traffic for account anomalies generated by an MITC attack
- A CASB is a cloud-delivered cybersecurity service
 - It ensures the safe use of cloud computing applications and services to prevent accidental (or intentional) leakage of sensitive data, malware infection, regulatory noncompliance, and lack of visibility.
 - It secures cloud applications, whether they are hosted in public clouds (IaaS), private clouds, or as software-as-a-service (SaaS) applications.
 - It also exposes the use of shadow IT—unsanctioned applications being used without the IT team's knowledge and approval



APTS AND NEW THREATS

- Advanced Persistent Threats (APTs)
- New threats such as Spectre and Meltdown
 - Both attacks break the isolation between applications and host OS
 - Attackers can read information from the OS kernel
 - Not all cloud users install the latest security patches
- VM-level attacks
 - Emerging threats to virtualization technologies



APT AND NEW THREAT COUNTERMEASURES

- Install a Firewall
 - Choosing a firewall is an essential first layer of defense against APT attacks
- Enable a Web Application Firewall
- Keep antivirus updated on all systems
- Implement Intrusion Prevention Systems
- Create a Sandbox/Sheepdip environment to check software before deployment
- Consider engaging a provider that specializes in threat analytics and APT defense



SCENARIO

- The Moo Cows, a professional hacker team, targeted your organization's cloud services
- They infiltrated the target's provider by sending spear-phishing emails
 - They distributed custom-made malware to compromise user accounts and gain remote access to the cloud service
 - Further, they accessed the target customer profiles with their MSP account, compressed the customer data, and stored them in the MSP.
 - Then, they used this information to launch further attacks on the target organization.
- What type of cloud attack did The Moo Cows perform?
- A Cloud Hopping Attack



19.6 CLOUD SECURITY TOOLS AND BEST PRACTICES

- Tools
- Best Practices



CLOUD PENTESTING TOOLS

- **AWS Inspector**
 - A customized security solution for AWS
 - It can be used as a basic minimum or preliminary testing tool.
- **S3Scanner**
 - An open-source tool to scan S3 buckets for misconfigurations and dump their data.
- **MicroBurst**
 - A collection of PowerShell scripts to scan Azure services for security issues
 - Requires PowerShell
- **Azucar**
 - Another popular PowerShell-based Azure scanning tool
- **AZ PowerShell Module**
 - PowerShell cmdlets for Azure Cloud enumeration

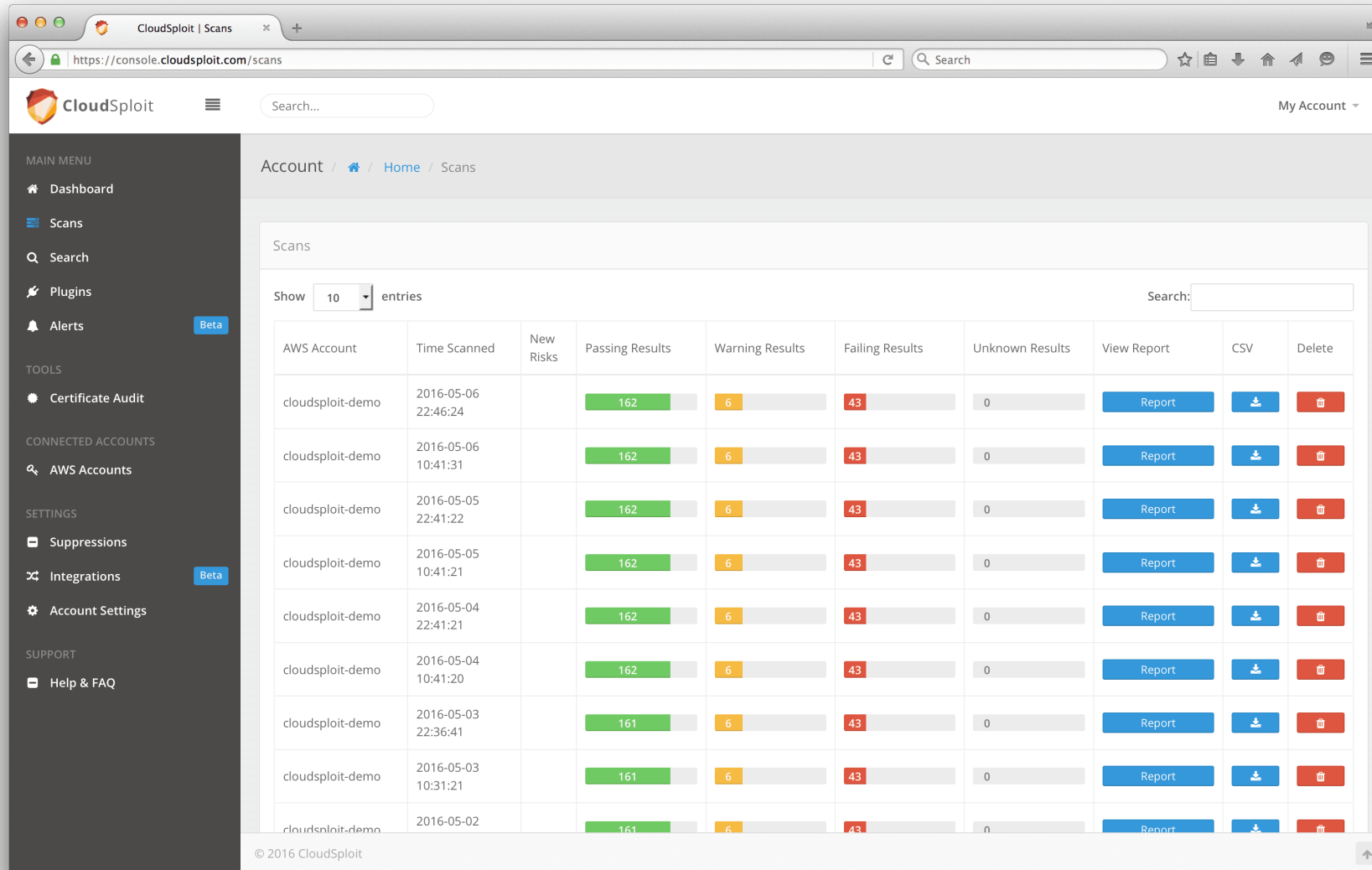


CLOUD PENTESTING TOOLS (CONT'D)

- Cloudsploit
 - A popular open-source tool that can scan multiple types of cloud service providers like Azure, AWS, GCP, OCI, etc.
- ScoutSuite
 - Audits instances and policies created on multi-cloud platforms
- Prowler
 - An AWS auditor
- Pacu
 - An exploitation framework for testing AWS account security
- Core CloudInspect
 - Pen-testing application for AWS EC2 users



CLOUDSPLOIT EXAMPLE



The screenshot displays the CloudSploit web interface. The left sidebar contains a 'MAIN MENU' with links to Dashboard, Scans, Search, Plugins, and Alerts (marked as Beta). Below this is a 'TOOLS' section with 'Certificate Audit' and a 'CONNECTED ACCOUNTS' section with 'AWS Accounts'. The 'SETTINGS' section includes 'Suppressions', 'Integrations' (marked as Beta), and 'Account Settings'. The 'SUPPORT' section has a 'Help & FAQ' link. The main content area is titled 'Scans' and shows a table of scan results. The table has columns for 'AWS Account', 'Time Scanned', 'New Risks', 'Passing Results', 'Warning Results', 'Failing Results', 'Unknown Results', 'View Report', 'CSV', and 'Delete'. The data rows show scans for 'cloudsploit-demo' with various timestamps and results. The footer indicates '© 2016 CloudSploit'.

CloudSploit | Scans

https://console.cloudsploit.com/scans

CloudSploit

Search...

My Account

Account / Home / Scans

Scans

Show 10 entries

Search:

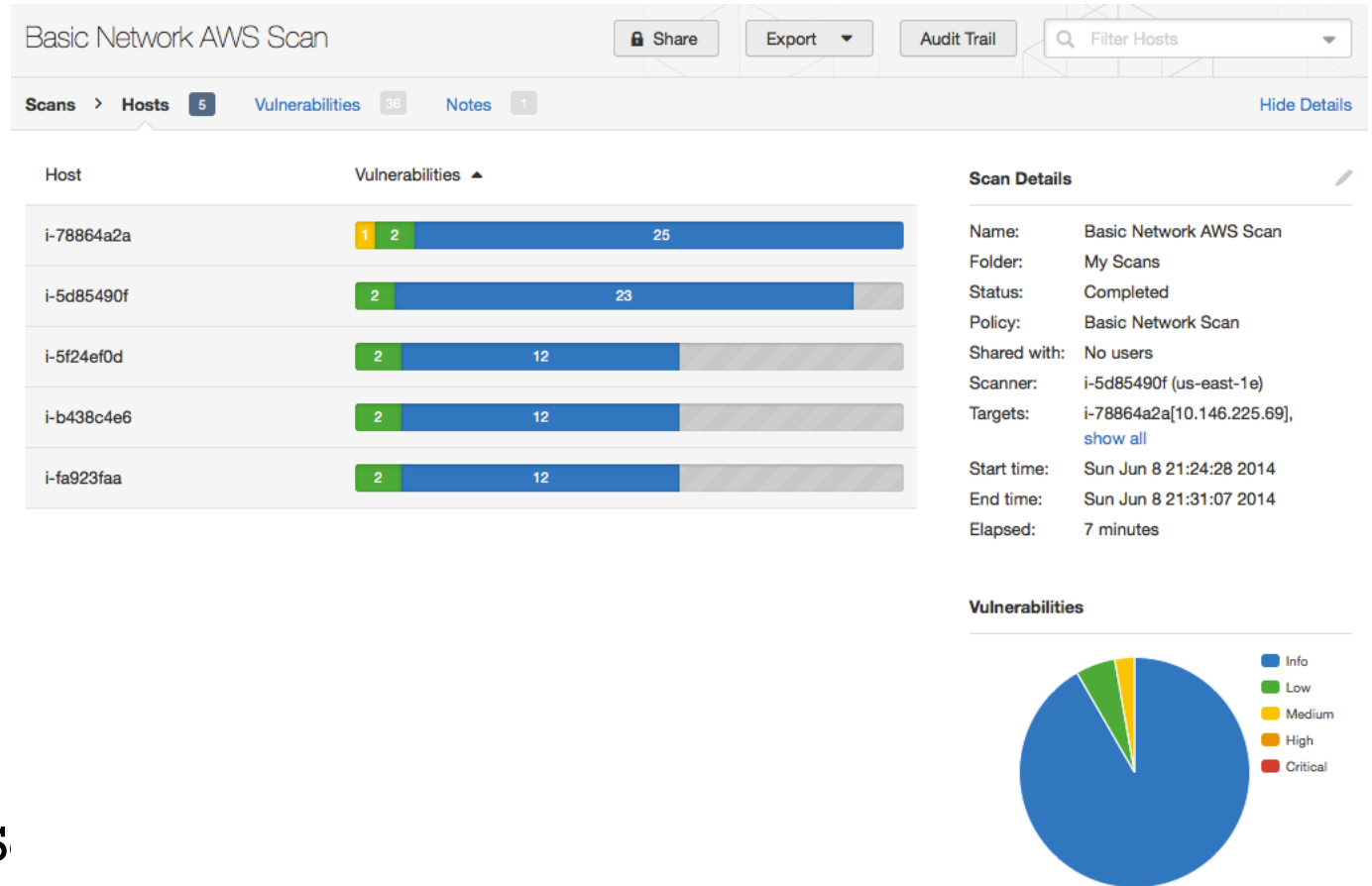
AWS Account	Time Scanned	New Risks	Passing Results	Warning Results	Failing Results	Unknown Results	View Report	CSV	Delete
cloudsploit-demo	2016-05-06 22:46:24		162	6	43	0	Report		
cloudsploit-demo	2016-05-06 10:41:31		162	6	43	0	Report		
cloudsploit-demo	2016-05-05 22:41:22		162	6	43	0	Report		
cloudsploit-demo	2016-05-05 10:41:21		162	6	43	0	Report		
cloudsploit-demo	2016-05-04 22:41:21		162	6	43	0	Report		
cloudsploit-demo	2016-05-04 10:41:20		162	6	43	0	Report		
cloudsploit-demo	2016-05-03 22:36:41		161	6	43	0	Report		
cloudsploit-demo	2016-05-03 10:31:21		161	6	43	0	Report		
cloudsploit-demo	2016-05-02		161	6	43	0	Report		

© 2016 CloudSploit



CLOUD SECURITY TOOLS

- Core CloudInspect
- Alert Logic
- Dell Cloud Manager
- Qualys Cloud Platform
- Symantec O3
- Cloud Application Visibility
- Proticor
- Panda Cloud Office Protection
- CloudPassage Halo
- SecludIT
- Nessus Enterprise for AWS
- Trend Micro Instant-On Cloud S



CLOUD SECURITY BEST PRACTICES

- NIST Recommendations
- Working with the CSP
- End User Connections
- Encryption and Key Management
- Microservices and Containerization



NIST RECOMMENDATIONS FOR SECURING THE CLOUD

- Assessment of risk to client data, infrastructure, and software
- Determining appropriate deployment model
- Ensuring audit procedures are in place
- Renewing SLAs to guard against security gaps
- Establishment of adequate incident detection and reporting mechanisms
- Analysis of organization's security objectives
- Determining who is responsible for data privacy and security issues



WORKING WITH THE CLOUD SERVICES PROVIDER

- Be very clear on responsibilities and duties between CSP and client
- Specify HR requirements as part of legal contracts, against possible malicious CSP insiders
- Require transparency from the CSP and good breach notification processes
- Extensively research the CSP's due diligence
- Have your own robust security policy and gap analysis with regard to the CSP
 - You must make up for any security gaps that you need but the provider does not cover
- Have your own Business Continuity Plan (BCP) and Disaster Recovery (DR) that is not wholly dependent on the CSP
- Ensure your SLA permits vulnerability scanning and pentesting



END USER CONNECTIONS

- Monitor client traffic for malicious activities
- Implement secure authentication and access controls
- Prevent users from sharing credentials
- Enforce acceptable use and employee behavior per policy and legal contracts
- Enforce least privilege on all end users
- Use a VPN to connect to the cloud



ENCRYPTION AND KEY MANAGEMENT

- Encrypt data before sending to cloud
- Encrypt data in transit
- Implement strong key generation, storage, and management
 - Do NOT store your private key in the cloud
 - You can store the data encryption key in the cloud
 - But then use a public key to encrypt the data encryption key
 - Keep the private key on premises/with you



MICROSERVICES AND CONTAINERIZATION

- If you use a microservices or containerization architecture:
 - Check for data protection at both design and runtime
 - Implement robust registration and validation of cloud services
 - Understand the dependency chain associated with CSP APIs



CLOUD OUTAGE - 4-STEP DEFENSE MODEL

- Load balancing:
 - It is essential to have a carefully planned, pre-engineered mechanism for load balancing to distribute client requests across cluster nodes evenly.
 - You must specify the failover procedure in the load balancing mechanism.
- Data scalability:
 - Cloud applications must be designed to auto-scale, so more instances can be brought up or taken down as needed.
 - One solution is to use a central database and provide it with high availability through replication or partitioning.
 - Another option is to make sure each application instance has its own data storage.
- Geographical diversity:
 - Cloud providers have data centers all over the world.
 - Using a provider with multiple data centers can ensure that your applications and data are hosted in more than one location.
 - In addition, this approach can help prevent outages caused by natural disasters or other events that might affect a single data center.
- Backup and recovery:
 - It is essential to have a backup and recovery plan in place for your cloud-hosted applications and data.
 - This should include regular backups stored in a different location than the primary data and a tested disaster recovery plan.



SCENARIO

- Your organization has recently migrated to a SaaS provider for its enterprise resource planning (ERP) software.
- Before this migration, a weekly port scan was conducted to help validate the on-premise systems' security.
- Which of the following actions should you take to validate the security of the cloud-based solution?
- You might have to utilize the provider's existing vendor testing and audits
- Most SaaS providers will not allow customers to conduct their own port scans or vulnerability scans against the SaaS service.
- This means you cannot scan using a VPN connection, utilize different scanning tools, or hire a third-party contractor to scan on your behalf.



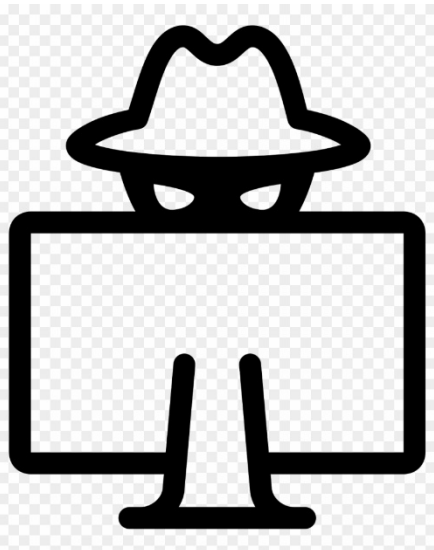
19.7 CLOUD COMPUTING REVIEW

- Review

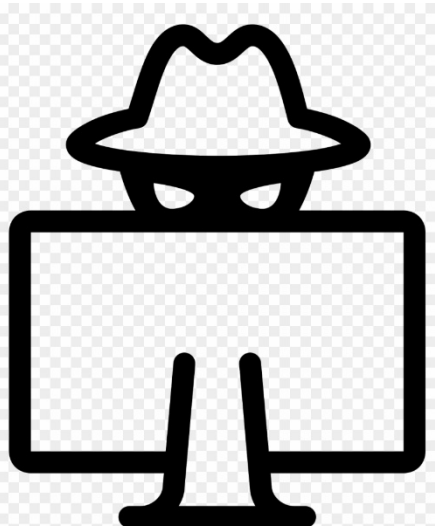


CLOUD COMPUTING REVIEW

- Cloud computing is on-demand delivery of IT capabilities as a metered service
- Serverless architecture uses virtualization to separate compute functionality from the physical hardware it runs on
 - The customer can pay for specific functions they require and no more
- Three categories of cloud services:
 - IaaS - The customer is responsible for the security of all features they use
 - PaaS - The customer is responsible for the security of the platform or app they create
 - SaaS - The provider is responsible for pretty much everything, though the customer must not abuse the service
- The cloud deployment models are: Public, Private, Community, Hybrid



CLOUD COMPUTING REVIEW (CONT'D)

- Attackers gain access to cloud services using various types of attacks
 - Cloud services are vulnerable to both traditional on-premises attacks, web app attacks such as XSS and CSRF, and cloud-specific attacks such as cloud hopping and wrapping
 - Cloud providers can offer dramatically more compute power, fault tolerance, and disaster recovery than traditional on-premises can
-
- 
- The cloud customer is dependent on the Cloud Service Provider for some aspects of security
 - Depending on the type of service you subscribe to, there is a shared responsibility for configuration and security
 - You may have to depend on using the CSP's vendor tests and audits as part of your penetration test
 - Make sure your own security plan covers any gaps in the provider's plan
 - You are also responsible for protecting your own end devices and making sure they can connect securely to the cloud

