Defending Your Cloud with AWS Security Services

MINN MYAT SOE, CISSP, CCSP, CCSK

Co-Founder, NEX4 ICT Solutions

NEX4
ICT Solutions

Today’s Agenda

- Cloud Security
- What are the problems?
- Security Principles
- AWS Security Controls
- Demo
- Tutorials

> whoami

Minn Myat Soe, ***Co-founder***, **NEX4**
twitter: @minnmyatsoe

- Over **a decade of experience** in information security
- Previously worked at **F5 Networks**, as an enterprise engineer for commercial cyber security products.
- Certs & Certifications:

Cloud

What is it?

- NIST Definition of Cloud Computing (800-145)
  - Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

National Institute of Standards and Technology (NIST)

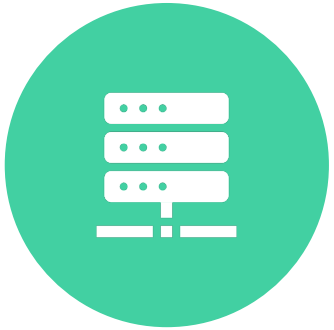
- The **National Institute of Standards and Technology (NIST)** 800-53 security controls are generally applicable to US Federal Information Systems. Federal Information Systems typically must go through a formal assessment and authorization process to ensure sufficient protection of confidentiality, integrity, and availability of information and information systems.
- The NIST Cybersecurity Framework (CSF) is supported by governments and industries worldwide as a recommended baseline for use by any organization, regardless of its sector or size. According to Gartner, in 2015 the CSF was used by approximately 30 percent of US organizations and usage is projected to reach 50 percent by 2020. Since Fiscal Year 2016, federal agency Federal Information Security Modernization Act (FISMA) metrics have been organized around the CSF, and agencies are now required to implement the CSF under the Cybersecurity Executive Order.

Five Essential Characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Service Models

SOFTWARE AS A SERVICE (SAAS)



PLATFORM AS A SERVICE (PAAS)

INFRASTRUCTURE AS A SERVICE (IAAS)

Deployment Models

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud

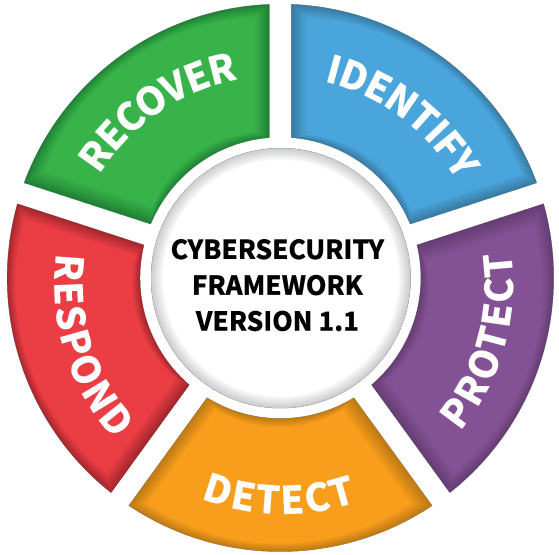
Security

Security Objectives (CIA Triad)

https://www.f5.com/labs/articles/education/what-is-the-cia-triad

The NIST Cybersecurity Framework (CSF)

- **Three Elements:** Core / Tiers / Profiles
  - **Core:** set of cybersecurity practices, outcomes and technical, operational, and managerial security controls that support the **five risk management functions** – **Identify, Protect, Detect, Respond, Recover**
  - **Tiers:** Organization's aptitude and maturity
  - **Profiles:** Organization's "as is" and "to be" cybersecurity postures



Principles and concepts

Least Privilege

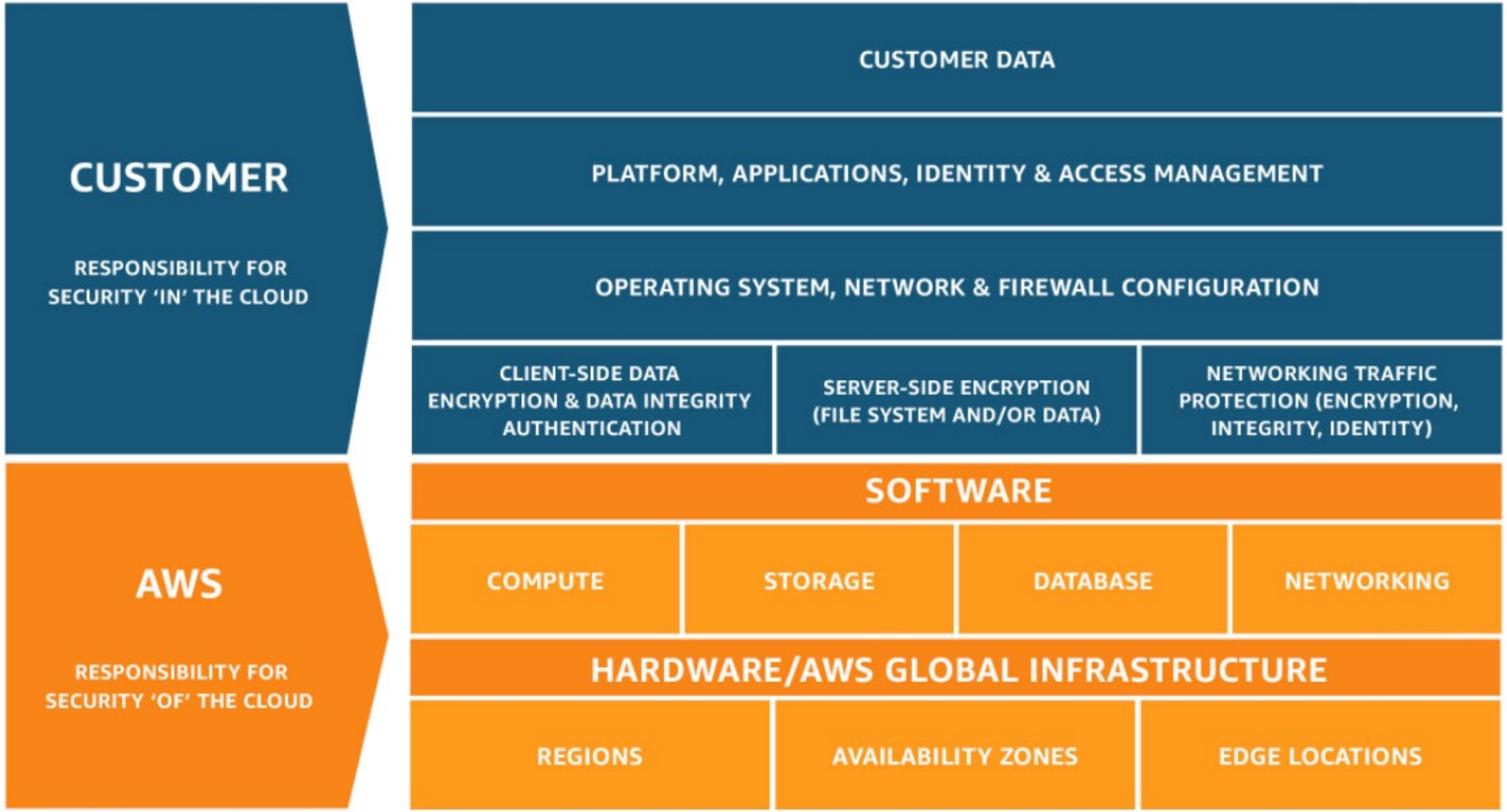
- Access policies *denied by default*
- “How many administrators have access to your cloud console?”

Defense in Depth

- Security control can fail
- Create multiple layers of overlapping security controls
- Pick one of your security control and ask “What if this fails?”

Cloud Security?

Shared Responsibility



AWS Compliance Programs

CSA
Cloud Security Alliance Controls

CyberGRX
Third Party Risk Management

ISO 9001
Global Quality Standard

ISO 27001
Security Management Controls

ISO 27017
Cloud Specific Controls

ISO 27701
Privacy Information Management

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

https://aws.amazon.com/compliance/programs/

What can go wrong?

…in the cloud

Home » Security Bloggers Network » Pfizer Suffers Huge Data Breach on Unsecured Cloud Storage

Pfizer Suffers Huge Data Breach on Unsecured Cloud Storage

by Sonrai Security Marketing on October 22, 2020

Today, we learned that Pfizer suffered a huge data breach because of unsecured cloud storage. The exposed data, including email addresses, home addresses, full names, and other HIPAA related information, was found on a misconfigured Google Cloud storage bucket. It is believed that highly confidential medical information came from automated customer support software that had been stored in the Google database. It is unclear how long this data had been stored or who had access to this information.

Ubiquiti Inc.

January 11, 2021: One of the biggest Internet of Things (IoT) technology vendors, Ubiquiti, Inc., alerted its customers of a data breach caused by unauthorized access to their database through a third-party cloud provider. The email communication advised customers to change passwords and enable multi-factor authentication. The data exposed may include an undisclosed number of customer names, email addresses, hashed and salted passwords, addresses, and phone numbers.

VIPGames

January 26, 2021: VIPGames.com, a free gaming platform, exposed over 23 million records for more than 66,000 desktop and mobile users due to a cloud misconfiguration. The leaked user records include usernames, emails, IP addresses, hashed passwords, Facebook, Twitter and Google IDs, bets and data on players who were banned from the platform.

Common causes of breaches?

… in the cloud

Home » Security Bloggers Network » Pfizer Suffers Huge Data Breach on Unsecured Cloud Storage

Pfizer Suffers Huge Data Breach on Unsecured Cloud Storage

by Sonrai Security Marketing on October 22, 2020

Today, we learned that Pfizer suffered a huge data breach because of unsecured cloud storage. The exposed data, including email addresses, home addresses, full names, and other HIPAA related information, was found on a misconfigured Google Cloud storage bucket. It is believed that highly confidential medical information came from automated customer support software that had been stored in the Google database. It is unclear how long this data had been stored or who had access to this information.

Ubiquiti Inc.

January 11, 2021: One of the biggest Internet of Things (IoT) technology vendors, Ubiquiti, Inc., alerted its customers of a data breach caused by unauthorized access to their database through a third-party cloud provider. The email communication advised customers to change passwords and enable multi-factor authentication. The data exposed may include an undisclosed number of customer names, email addresses, hashed and salted passwords, addresses, and phone numbers.

VIPGames

January 26, 2021: VIPGames.com, a free gaming platform, exposed over 23 million records for more than 66,000 desktop and mobile users due to a cloud misconfiguration. The leaked user records include usernames, emails, IP addresses, hashed passwords, Facebook, Twitter and Google IDs, bets and data on players who were banned from the platform.

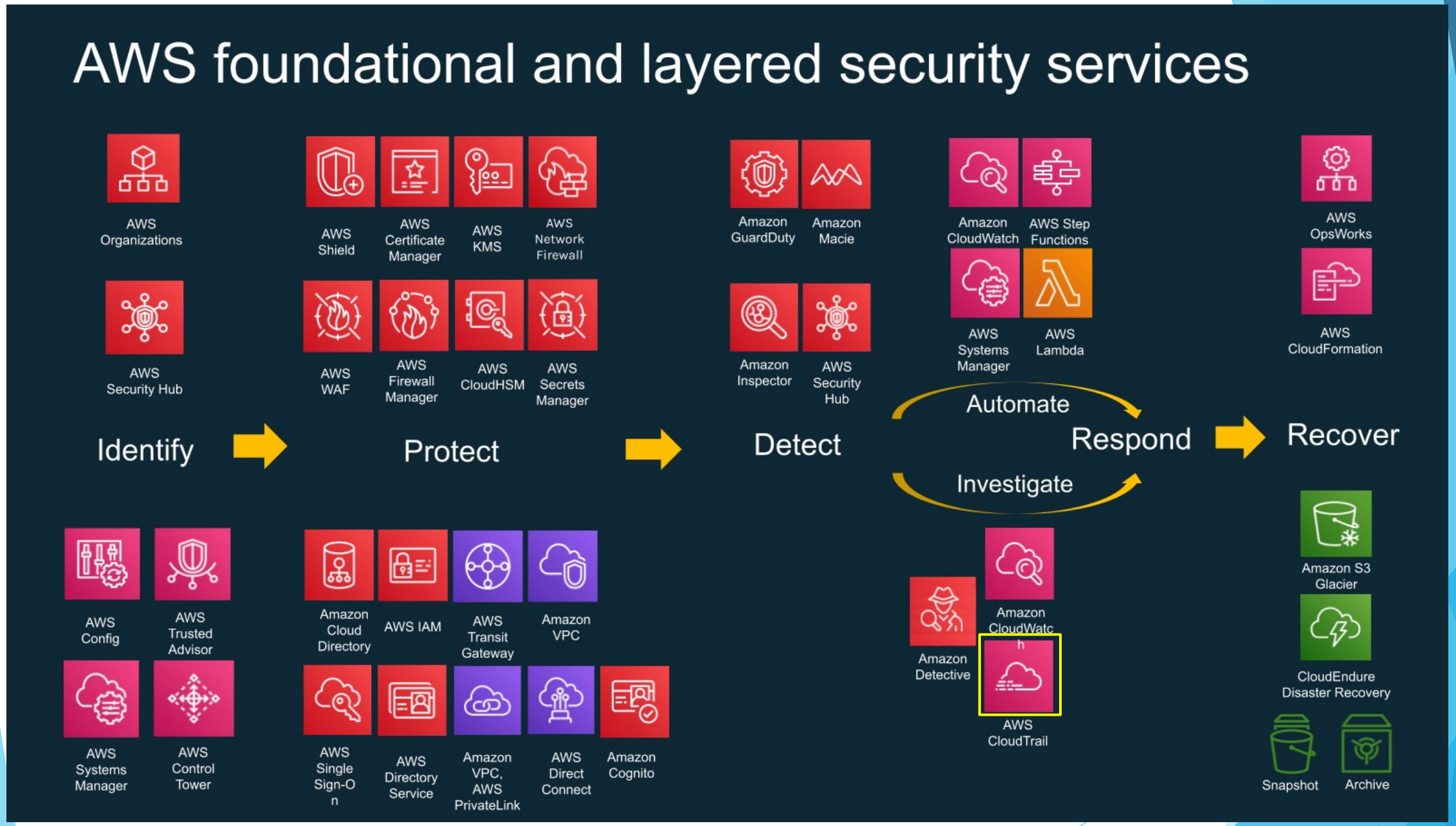
Top Threats to Cloud Computing: Egregious Eleven

- Data Breach
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture and Strategy
- Insufficient Identity, Credential, Access and Key Management
- Account Hijacking
- Insider Threats
- Insecure Interfaces and APIs
- Weak Control Plane
- Metastructure and Applistructure Failures
- Limited Cloud Usage Visibility
- Abuse and Nefarious Use of Cloud Services

https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

What are we going to do about it?

AWS foundational and layered security services



CSF: Identify

- Identifying and managing IT assets is the first step in effective IT governance and security.
- Top #1 and #2 of CIS controls.
- Use of IAM, Roles, Tags
- IT Governance
  - AWS Organizations, AWS Config, AWS Systems Manager – to implement and enforce governance

Identify: Governance (1)

- Supporting business objectives by defining policies and control objectives to manage risk
- Achieve risk management by following a layered approach
- Shared Responsibility is the foundational layer.
- Then, your control objectives - IAM, SSO, Detective Controls, SCP (e.g. limit the regions, or prevent disabling of detective controls)
- Top layer is application security.

Governance (2)

- Control -> to manage risk

Likelihood	Risk Level				
Very Likely	Low	Medium	High	Critical	Critical
Likely	Low	Medium	Medium	High	Critical
Possible	Low	Low	Medium	Medium	High
Unlikely	Low	Low	Medium	Medium	High
Very unlikely	Low	Low		Medium	High
Consequence	Minimal	Low	Medium	High	Severe

AWS Config

- Infrastructure visibility
- Resource inventory
- Compliance checker
- Configuration manager
- Security analysis

AWS Config (Identify): Use Case

- Let's say have this web application:
  - 3-tiered architecture
  - Front-end web servers in public subnet
  - Backend servers with EBS
  - Backend database is RDS
- Security requirements:
  - No SSH login is allowed
  - EBS volumes must be encrypted
  - RDS must have high availability
  - Data on RDS must be encrypted

AWS Config: Sample (1)

EC2 VPC vpc-73ad90

on April 21, 2019 6:32:15 PM (UTC-03:00)

Manage resource

19th April 2019 7:14:21 PM	19th April 2019 9:42:43 PM	21st April 2019 6:28:49 PM	21st April 2019 6:28:50 PM	21st April 2019 6:32:15 PM
1 Change	2 Changes	4 Changes, 3 Events	3 Changes	1 Change

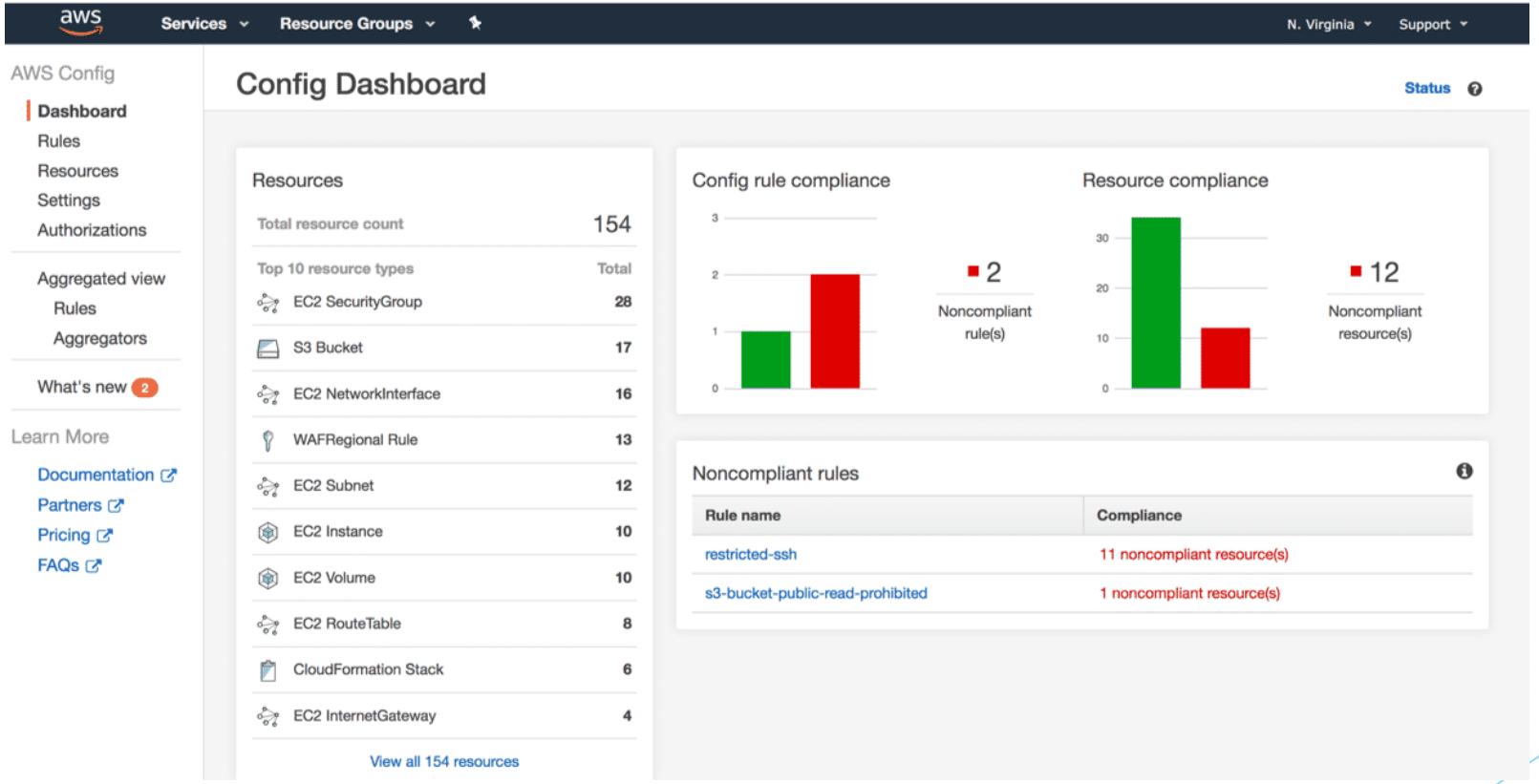
Now

Configuration Details

View Details

Amazon Resource Name	[illegible]	**VPC ID**	vpc-73ad90
Resource type	AWS::EC2::VPC	**State**	available
Resource ID	vpc-73ad90	**VPC CIDR**	172.31.0.0/16
Resource name	*null*	**DHCP Options Set**	dopt-5c2bc
Availability zone	Multiple Availability Zones	**Default VPC**	true
Created on	Not available	**Instance tenancy**	default
Tags (0)			

AWS Config: Sample (2)



AWS IAM

aws

Search in this guide

AWS > Documentation > AWS Identity and Access Management > User Guide

- What is IAM?
- Getting set up
- Getting started
- Tutorials
- Signing in to AWS
- Identities
- Access management
- Security
  - Data protection
  - Logging and monitoring
  - Compliance validation
  - Resilience
  - Infrastructure security
  - Configuration and vulnerability analysis
  - Security best practices and use cases
    - Security best practices

Security best practices in IAM

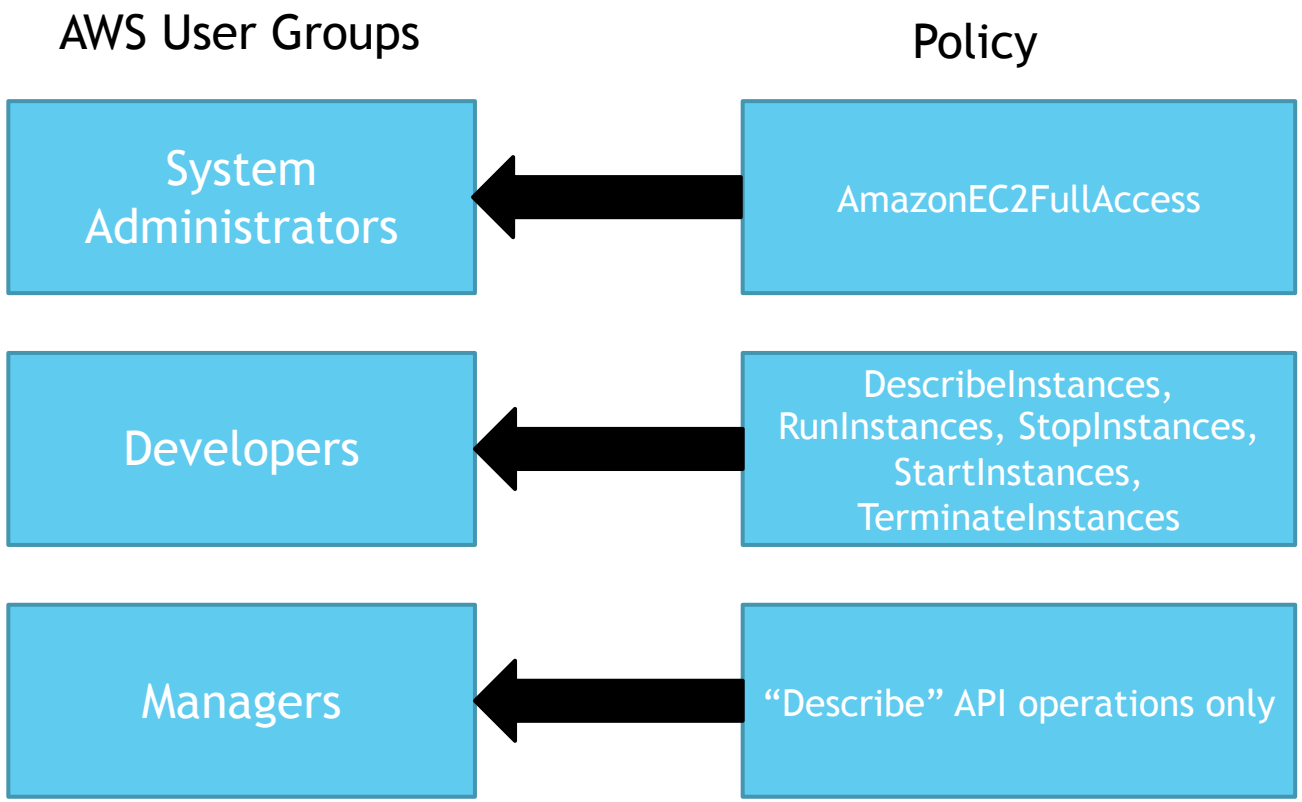
PDF | Kindle | RSS

To help secure your AWS resources, follow these recommendations for the AWS Identity and Access Management (IAM) service.

Topics

- Lock away your AWS account root user access keys
- Use roles to delegate permissions
- Grant least privilege
- Get started using permissions with AWS managed policies
- Validate your policies
- Use customer managed policies instead of inline policies
- Use access levels to review IAM permissions
- Configure a strong password policy for your users
- Enable MFA

AWS IAM – EC2 Use Case

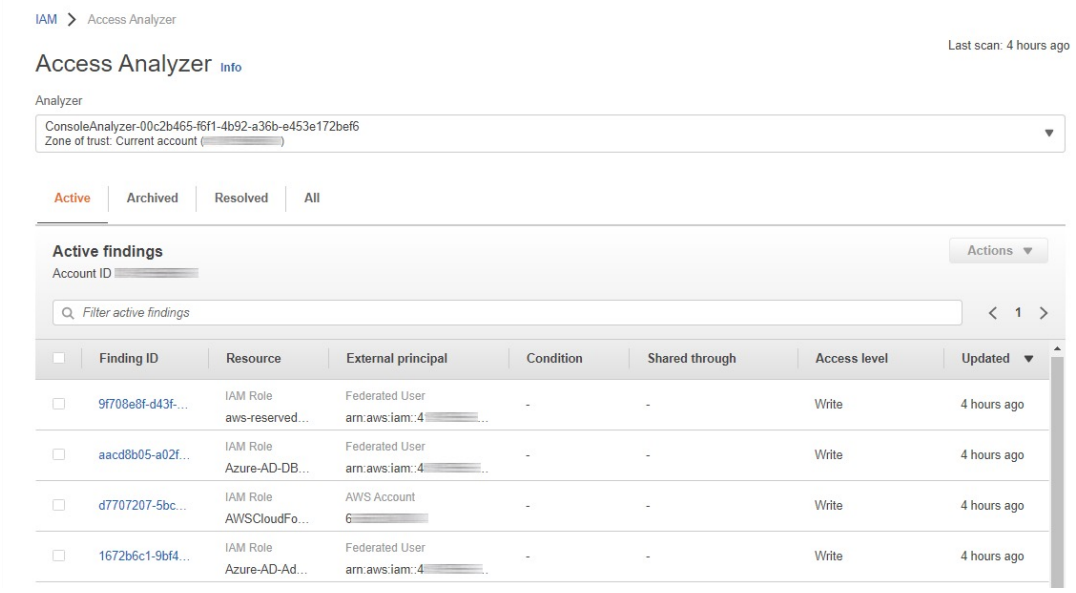


AWS IAM – Identity Management

- Human Identities
  - SSO, Cognito
  - Temporary Credentials by using roles instead of IAM users with long term access keys
- Machine Identities
  - Use IAM roles
  - AWS Secret Manager for programmatic access to stored credentials
- Rotate and audit credentials periodically
  - IAM credential report
  - AWS Config rules

AWS IAM – Permissions Management

- Least Privilege
  - IAM Access Analyzer
  - IAM Access Analyzer can generate policy based on activities in Cloudtrail.



AWS Secrets Manager

- Secrets Manager enables you to replace hardcoded credentials in your code.
- It is done with an API call to Secrets Manager to retrieve the secret programmatically.

Cloudtrail Example


```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "accountId": "123456789012",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:22:54Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StartInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {"instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]}},
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 0,
            "name": "pending"
        },
        "previousState": {
            "code": 80,
            "name": "stopped"
        }
    }]}}
}]}
```

CSF: Protect

- To meet security objectives of Confidentiality, Integrity and Availability
- Confidentiality
  - Encryptions on EBS, S3, TDE on RDS, VPN
  - Protect data at rest, data in motion, data in use
  - KMS, Dedicated HSM
- Integrity
  - AWS Config provides integrity of your AWS environment
  - CloudWatch, CloudTrail
- Availability
  - AWS ALB, Shield

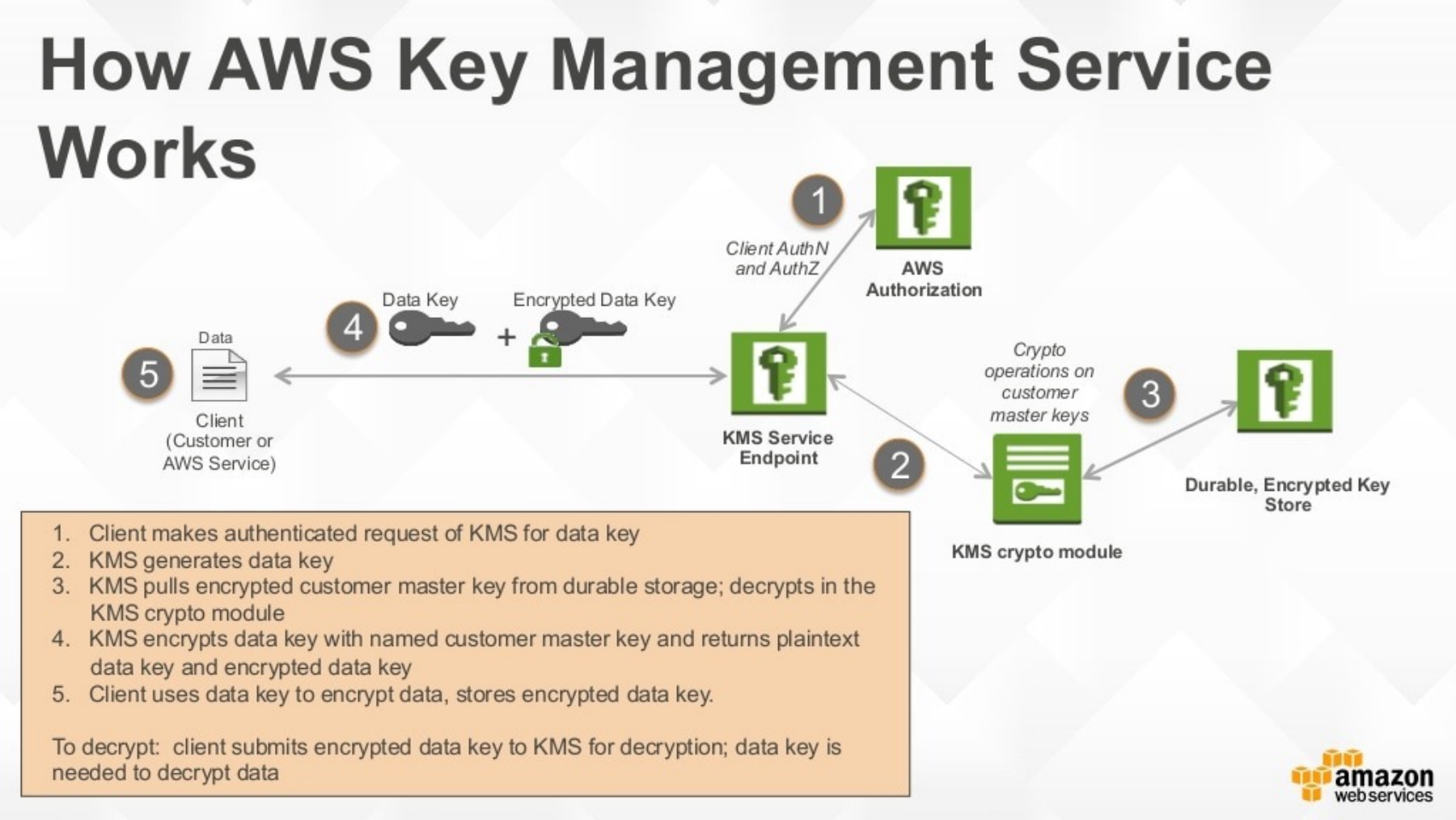
Layered Security

Layer	Controls
Application	WAF, IAM
Operating Systems	Configuration, Vulnerability Scanning, Backups, IAM
Data	Encryption, Backups, DLP
Network	ACL, Security Groups, Routing, DDoS
Hypervisor	Configuration, ACL, etc

AWS VPC

- ACLs
  - What ports are you exposing? Ingress / Egress or both?
- Check Security Groups
  - Is it open to the whole world? 0.0.0.0/0
- Routing
  - Does the systems need to go out to internet?
- Subnets
  - Should the systems in different subnets talk to each other?
- Diagrams would help

AWS KMS


How AWS Key Management Service Works
1
Client AuthN and AuthZ
AWS Authorization
Data Key
Encrypted Data Key
4
+
Data
5
Client (Customer or AWS Service)
KMS Service Endpoint
Crypto operations on customer master keys
3
2
KMS crypto module
Durable, Encrypted Key Store
1. Client makes authenticated request of KMS for data key
2. KMS generates data key
3. KMS pulls encrypted customer master key from durable storage; decrypts in the KMS crypto module
4. KMS encrypts data key with named customer master key and returns plaintext data key and encrypted data key
5. Client uses data key to encrypt data, stores encrypted data key.
To decrypt: client submits encrypted data key to KMS for decryption; data key is needed to decrypt data
amazon web services

CSF: Detect

- Anomalies and Events, Security Continuous Monitoring, Detection Processes
- **AWS CloudTrail** to log all API calls
- **VPC Flow** logs to record network activities to and from VPC
- **AWS CloudWatch** to monitors your AWS environment, and generate alerts based on rules
- **Amazon GuardDuty** to correlate activity within your environment with threat intelligence from multiple sources.

Amazon GuardDuty

- **Amazon GuardDuty** continuously monitors and identifies threats by analyzing several types of activity in your AWS account. GuardDuty uses the following data sources to make its threat findings: **VPC Flow Logs**, **AWS CloudTrail** event logs, and **DNS logs**.

UnauthorizedAccess:EC2/SSHBruteForce

Finding ID: 28b22bbc2f98c08b391f2a9f62f6acb1

34.220.138.155 is performing SSH brute force attacks against i-022423c697ff4ebc1. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity	Region	Count
Low	us-west-2	14
Account ID	**Resource ID**	**Created at**
010055289521	i-022423c697f…	07-01-2018 14…
Updated at		
07-01-2018 16…		

UnauthorizedAccess:EC2/MaliciousIPCaller.Custom	Instance: i-022423c697ff4ebc1	a minute ago
UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-03598253c25a35541	11 minutes a…
UnauthorizedAccess:EC2/SSHBruteForce	Instance: i-022423c697ff4ebc1	15 minutes a…
Recon:EC2/PortProbeUnprotectedPort	Instance: i-03598253c25a35541	20 minutes a…

CSF: Respond

- Human element always involved.
- Tools from AWS can assist to take forensic snapshots, install analysis tools, connect the suspect instance to a forensic workstation.

CSF: Recover

- AWS services provide self-healing and automated recovery:
  - Auto Scaling Groups
  - CloudWatch, Lambda

Final Thoughts

- Security at every layer
- Reused security objects
- Design for failure
- Redundancy
- User awareness and training

Demo Sessions