Best Practices for Security at Scale

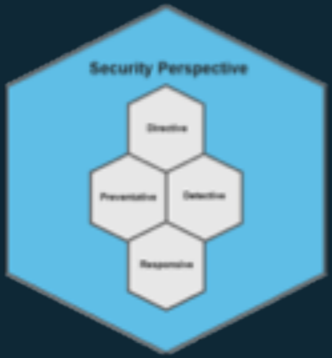
“Best of the Best” tips for Security in the Cloud

Paul Hawkins. Security SA, Amazon Web Services

20 August, 2019

Sources of Best Practices

AWS Cloud Adoption Framework (CAF)



How to move to the cloud securely including the “Core Five Epics”:

- Identity and Access Management
- Logging and Monitoring
- Infrastructure Security
- Data Protection
- Incident Response

AWS Security Best Practices

Whitepaper with 44 best practices including:

- Identity and Access Management (10 best practices)
- Logging and Monitoring (4)
- Infrastructure Security (15)
- Data Protection (15)

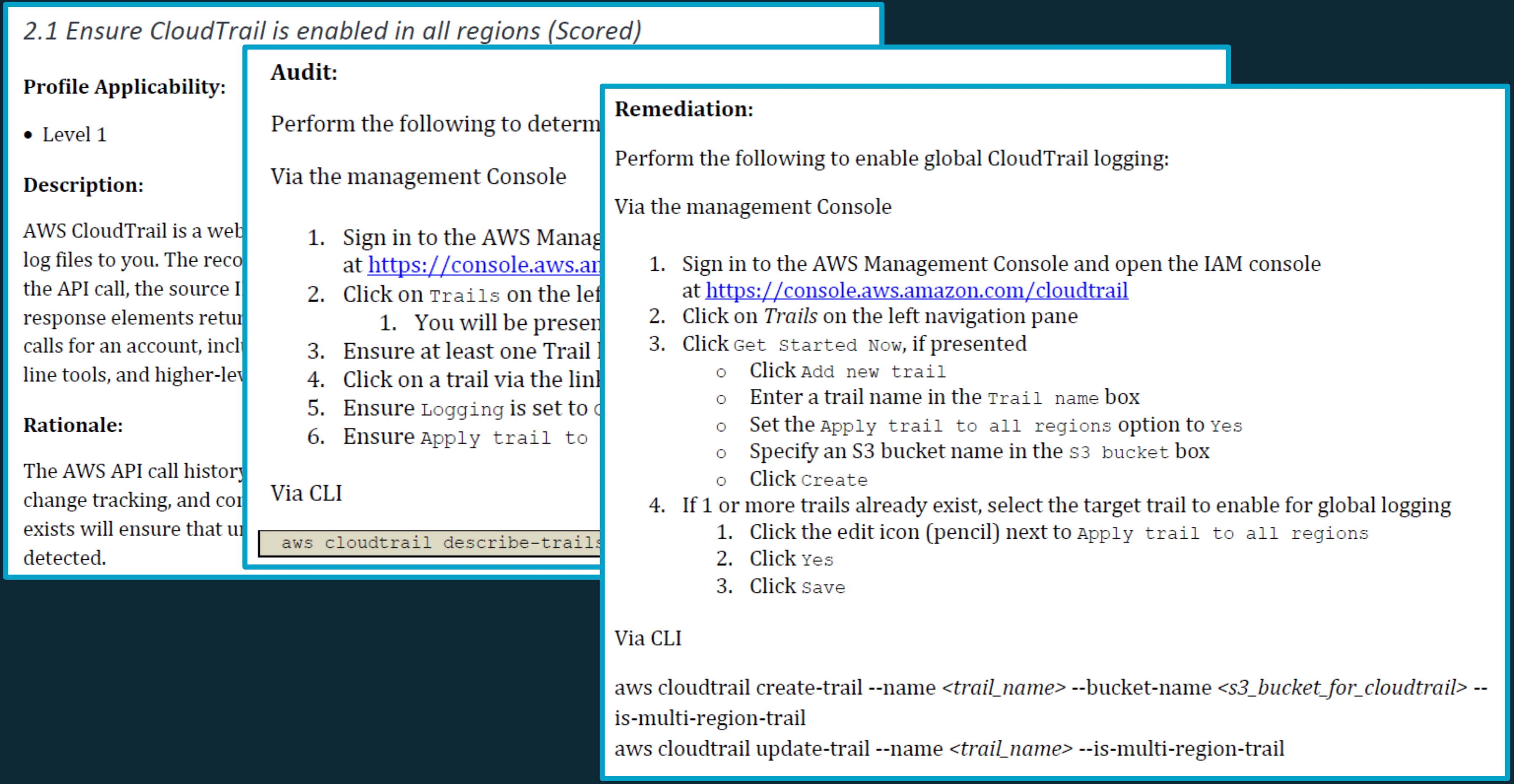
Centre for Internet Security (CIS) Benchmarks

CIS Center for Internet Security

148 detailed recommendations for configuration and auditing covering:

- “AWS Foundations” with 52 checks aligned to AWS Best Practices
- “AWS Three-Tier Web Architecture” with 96 checks for web applications

CIS Benchmarks: What, Why, Check, Fix



2.1 Ensure CloudTrail is enabled in all regions (Scored)

Profile Applicability:

- Level 1

Description:

AWS CloudTrail is a web
log files to you. The reco
the API call, the source I
response elements retur
calls for an account, incl
line tools, and higher-lev

Rationale:

The AWS API call history
change tracking, and co
exists will ensure that u
detected.

Audit:

Perform the following to determ

Via the management Console

1. Sign in to the AWS Manag
   at https://console.aws.a
2. Click on `Trails` on the lef
   1. You will be presen
3. Ensure at least one Trail
4. Click on a trail via the lin
5. Ensure `Logging` is set to
6. Ensure `Apply trail to`

Via CLI

```
aws cloudtrail describe-trails
```

Remediation:

Perform the following to enable global CloudTrail logging:

Via the management Console

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/cloudtrail
2. Click on *Trails* on the left navigation pane
3. Click `Get Started Now`, if presented
   - Click `Add new trail`
   - Enter a trail name in the `Trail name` box
   - Set the `Apply trail to all regions` option to `Yes`
   - Specify an S3 bucket name in the `S3 bucket` box
   - Click `Create`
4. If 1 or more trails already exist, select the target trail to enable for global logging
   1. Click the edit icon (pencil) next to `Apply trail to all regions`
   2. Click `Yes`
   3. Click `Save`

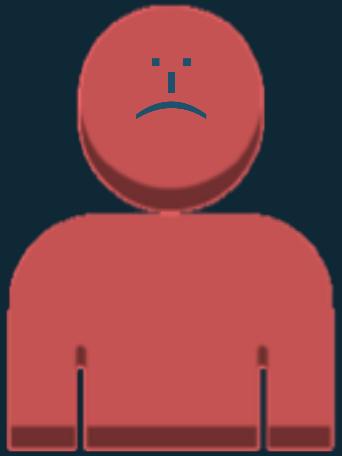
Via CLI

aws cloudtrail create-trail --name <*trail_name*> --bucket-name <*s3_bucket_for_cloudtrail*> --is-multi-region-trail
aws cloudtrail update-trail --name <*trail_name*> --is-multi-region-trail

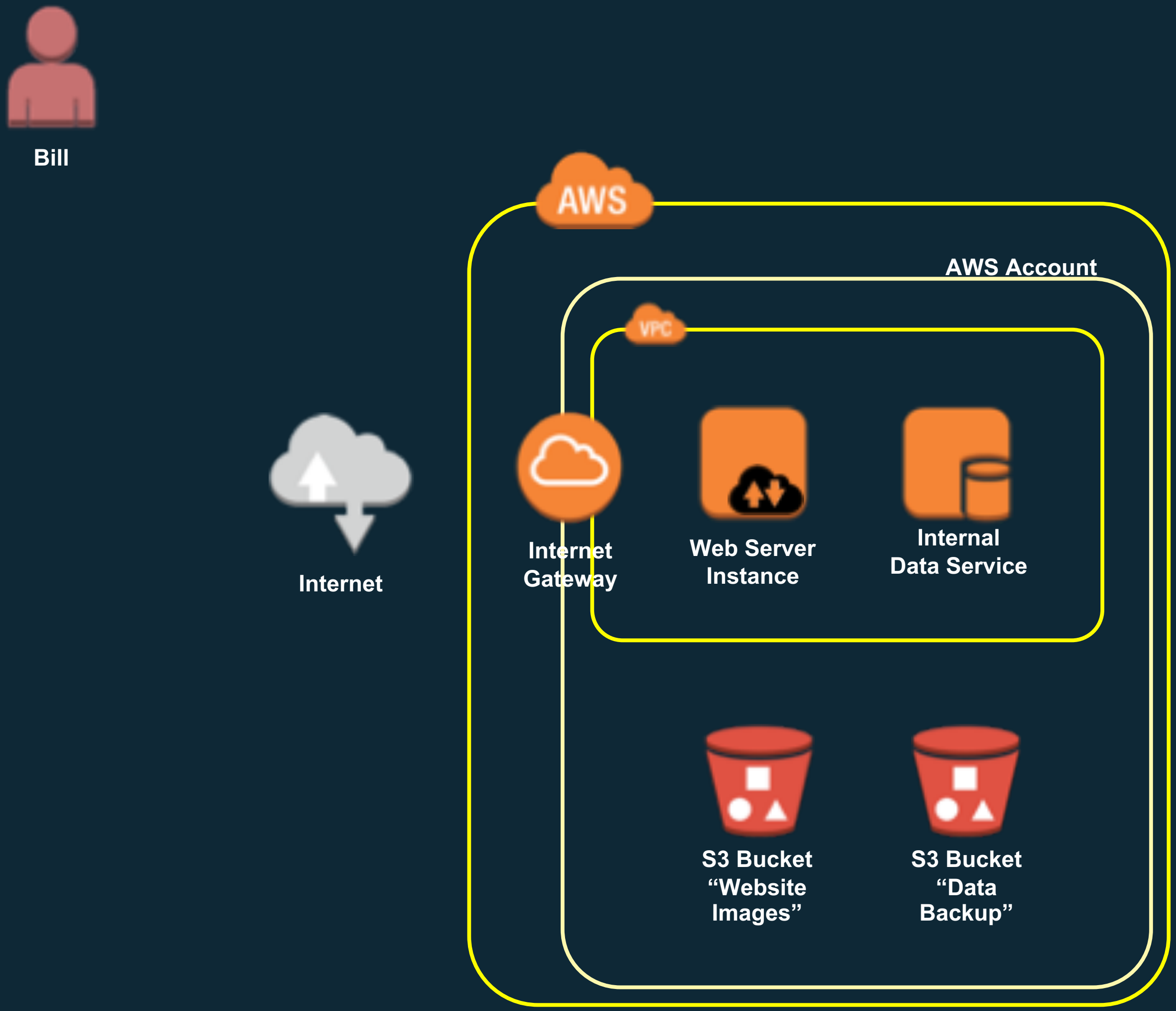
A is for “Alice” and B is for “Bill”

Alice follows best practices

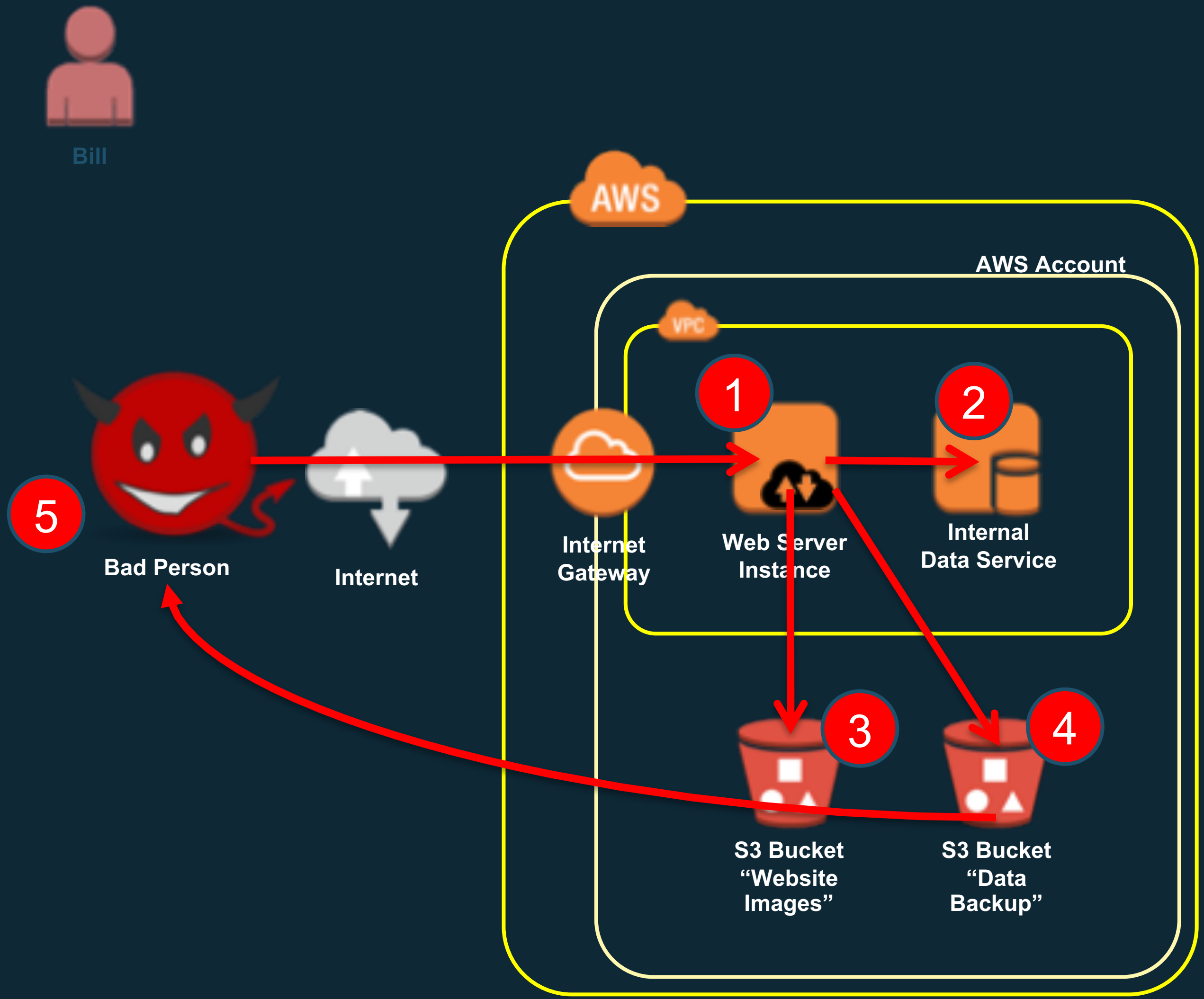
Bill does NOT follow best practices



Bill’s Bad Day



Bill's Bad Day



1 Access the vulnerable web application

2 Pivot to the data service

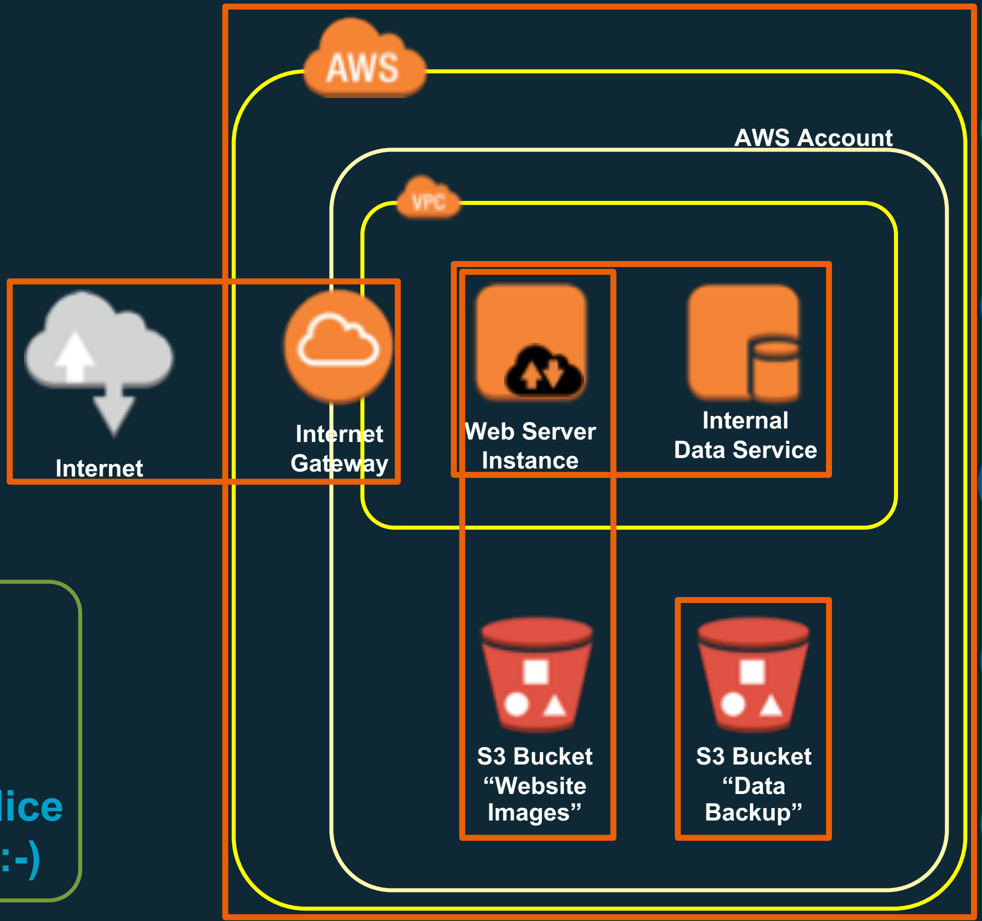
3 Delete the website image files

4 Change permissions to the data backup

5 Download the data backup

Bill's Bad Day

Bill



1. No web application protection
2. No segmentation
3. One account
4. All permissions granted
5. Sensitive data not encrypted
6. No logging, monitoring, alerting

Alice

… now let's help Alice have a great day! :-)

Best of the Best Practices: Identity and Access Mgmt

1) Use **multiple AWS accounts** to reduce blast radius

Production

Staging

AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and types of data classification.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	5	0

2) Use **limited roles** and grant **temporary security credentials**

IAM

IAM Roles

Secrets Manager

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	13	8

3) **Federate** to an existing identity service

IAM

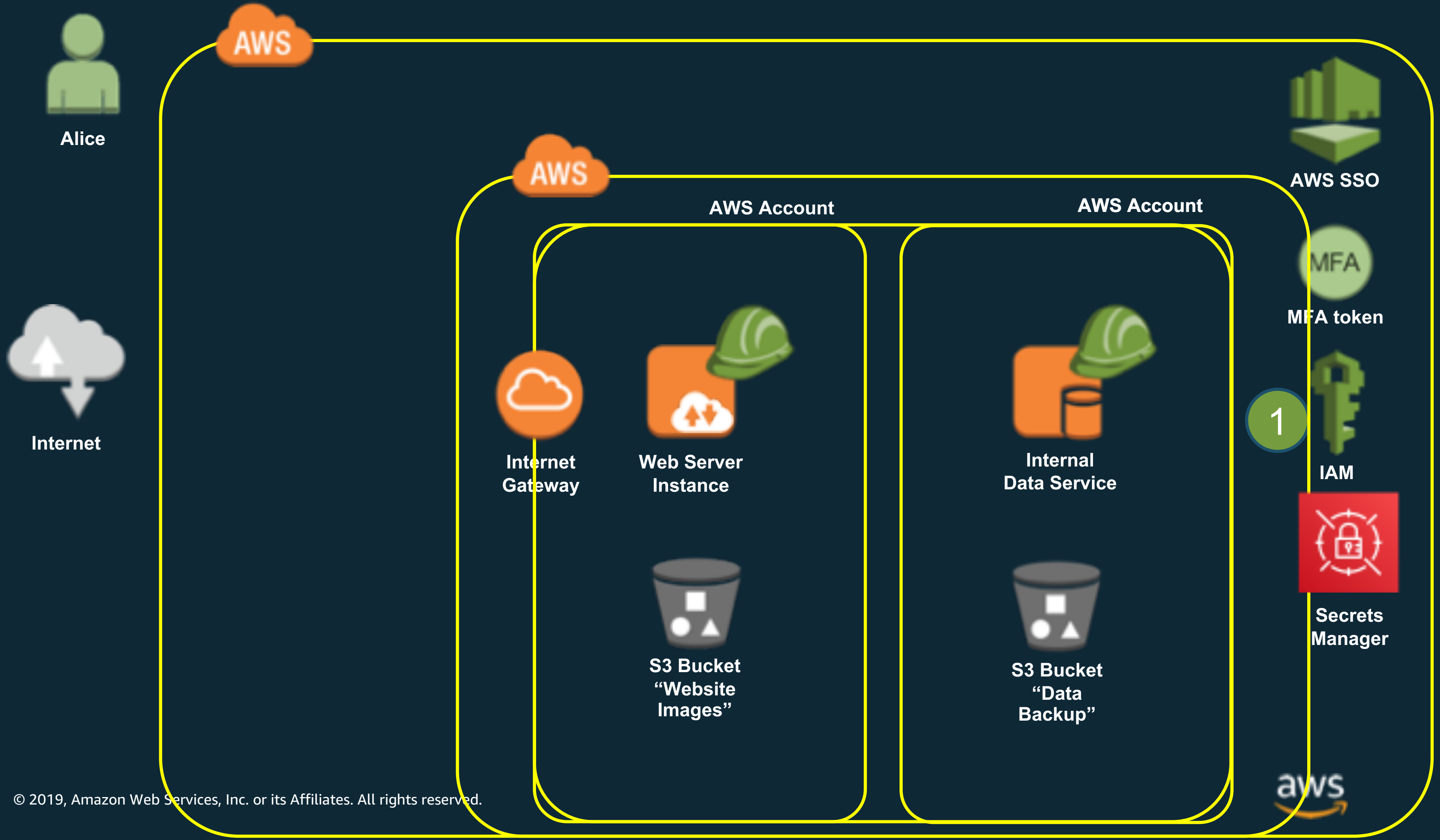
MFA token

AWS SSO

Control access to AWS resources, and manage the authentication and authorisation process without needing to re-create all your corporate users as IAM users.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	0	0

Identity and Access Management



Best of the Best Practices: Logging and Monitoring

4) Turn on logging in all accounts, for all services, in all regions

AWS CloudTrail

Amazon GuardDuty

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence & findings.

✓	8	6
AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark

5) Use the AWS platform’s built-in monitoring and alerting features

Security Hub

AWS Config

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.

✓	15	3
AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark

6) Use a separate AWS account to fetch and store copies of all logs

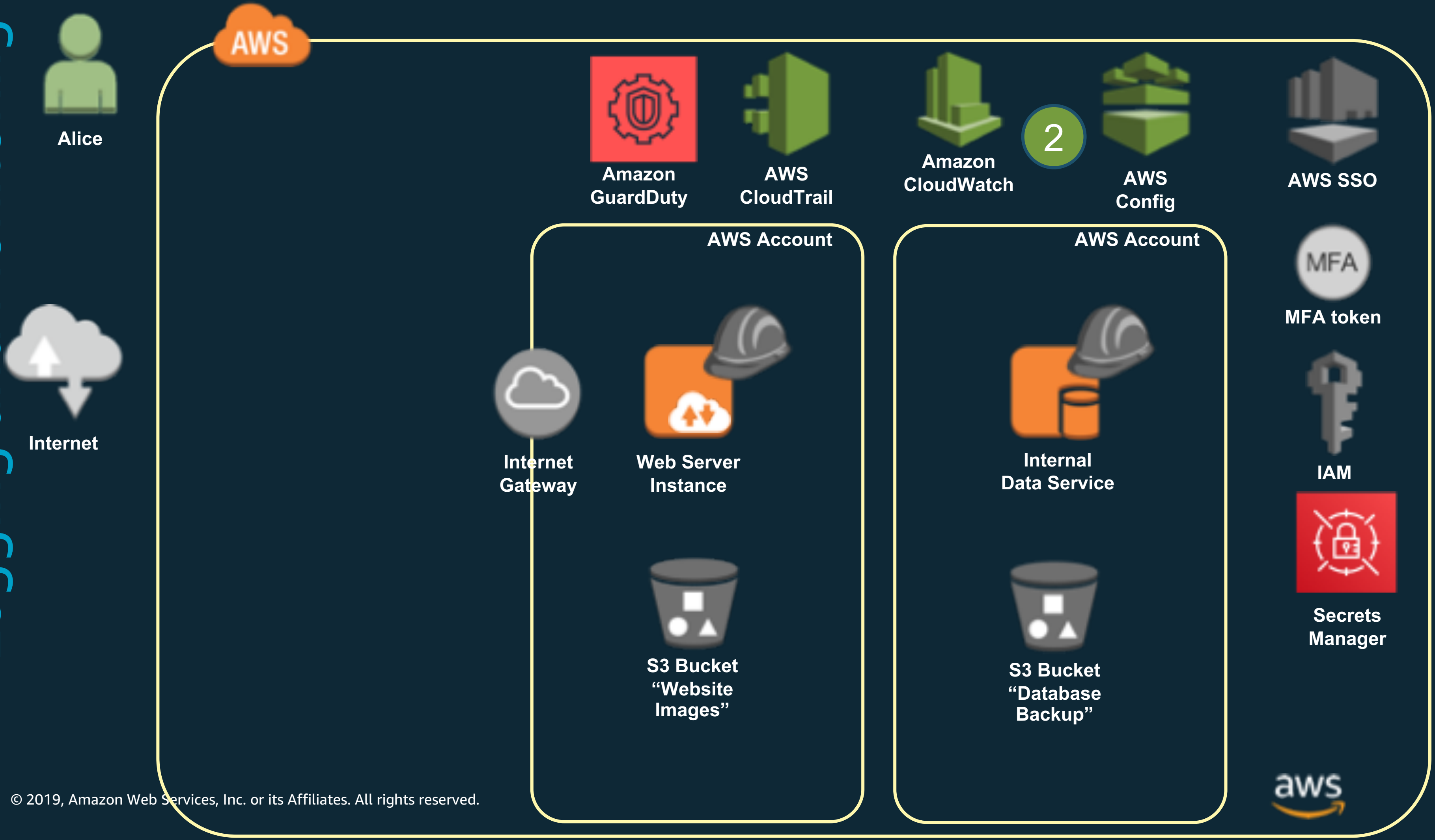
Production

Security

Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.

✓	2	3
AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark

Logging and Monitoring



Alice

Internet

AWS

Amazon GuardDuty

AWS CloudTrail

Amazon CloudWatch

2

AWS Config

AWS SSO

AWS Account

Internet Gateway

Web Server Instance

S3 Bucket “Website Images”

AWS Account

Internal Data Service

S3 Bucket “Database Backup”

MFA

MFA token

IAM

Secrets Manager

aws

Best of the Best Practices: Infrastructure Security

7) Create a **threat prevention layer** using AWS edge services

Amazon CloudFront

AWS Shield

AWS WAF

Use the 100s of worldwide points of presence in the AWS edge network to provide scalability, protect from denial of service attacks, and protect from web application attacks.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	0	5

8) Create **network zones** with Virtual Private Clouds (VPCs) and security groups

VPC

Security Group

Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	5	30

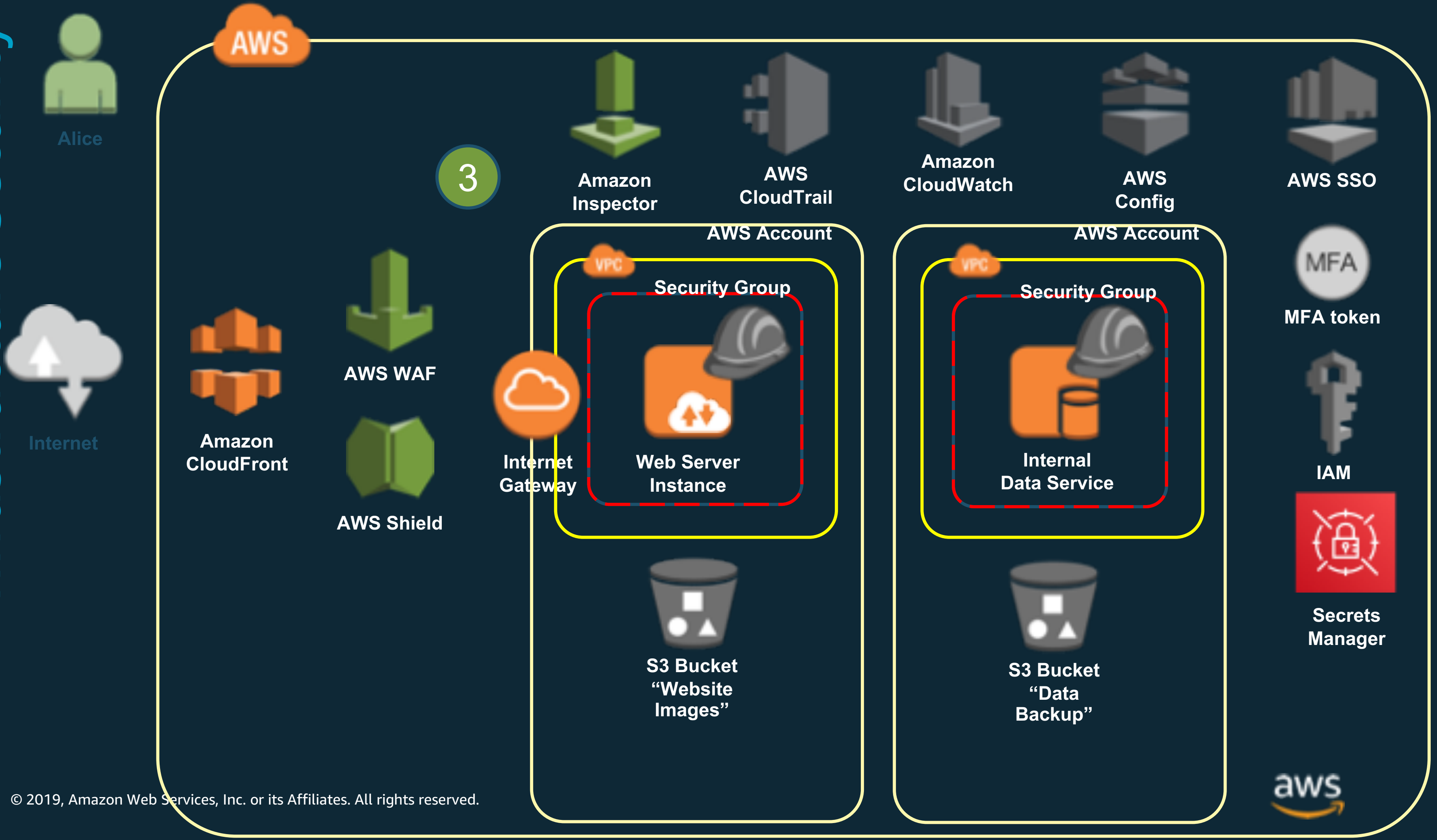
9) Manage vulnerabilities through **patching and scanning**

Amazon Inspector

Test virtual machine images and snapshots for operating system and application vulnerabilities throughout the build pipeline and into the operational environment.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	0	1

Infrastructure Security



Alice

Internet

AWS

3

Amazon Inspector

AWS CloudTrail

Amazon CloudWatch

AWS Config

AWS SSO

Amazon CloudFront

AWS WAF

AWS Shield

Internet Gateway

AWS Account

VPC

Security Group

Web Server Instance

S3 Bucket “Website Images”

AWS Account

VPC

Security Group

Internal Data Service

S3 Bucket “Data Backup”

MFA

MFA token

IAM

Secrets Manager

Best of the Best Practices: Data Protection

10) Encrypt **data at rest** (with occasional exceptions)

AWS KMS

Amazon S3

Enabling encryption at rest helps ensure the confidentiality and integrity of data. Consider encrypting everything that is not public.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	0	7

11) Use **server-side encryption** with provider managed keys

AWS KMS

Data Encryption Key

AWS Key Management Service (KMS) is seamlessly integrated with 18 other AWS services. You can use a default master key or select a custom master key, both managed by AWS.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	1	1

12) Encrypt **data in transit** (with no exceptions)

Amazon CloudFront

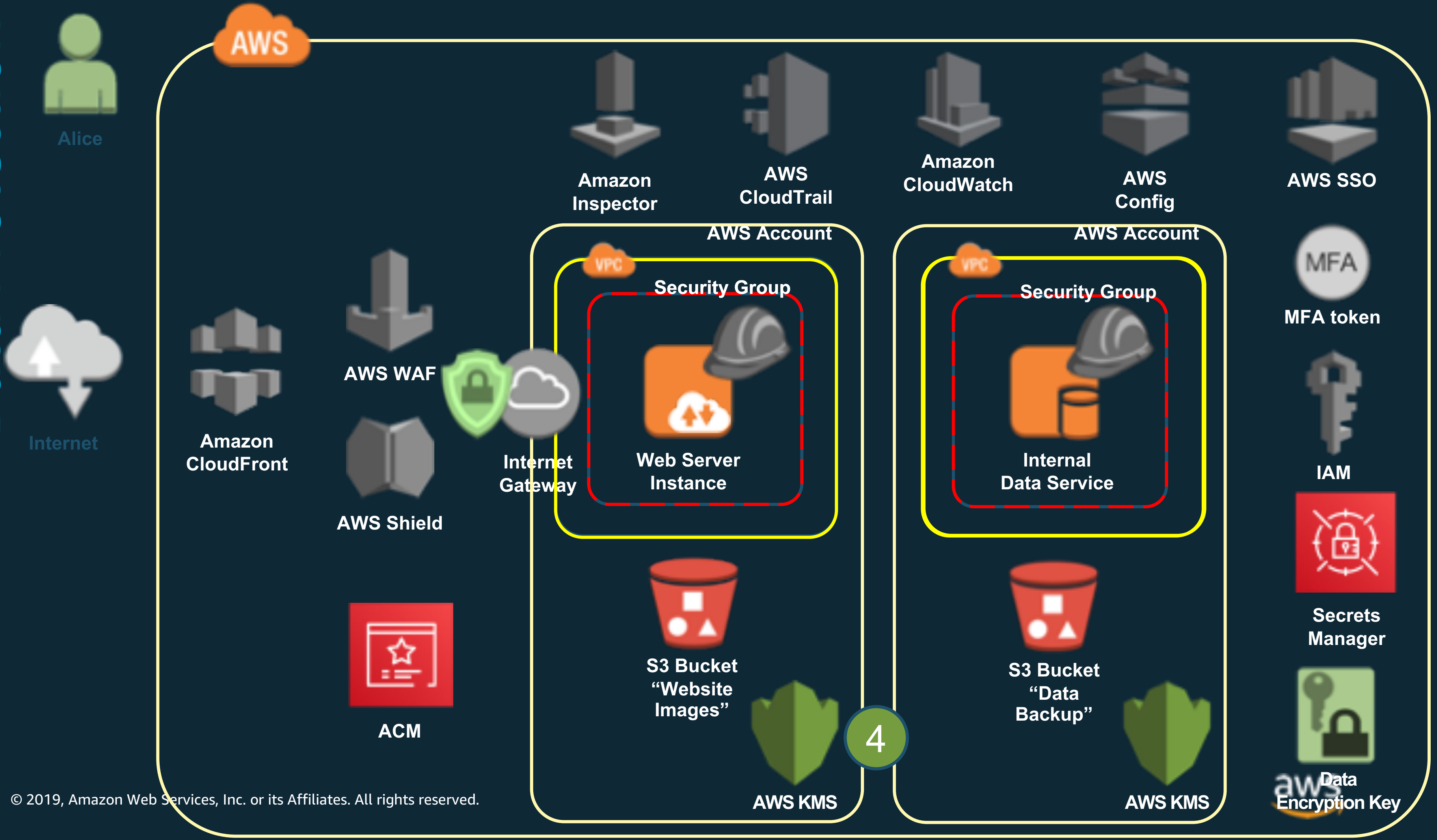
ACM

SSL / TLS / HTTPS

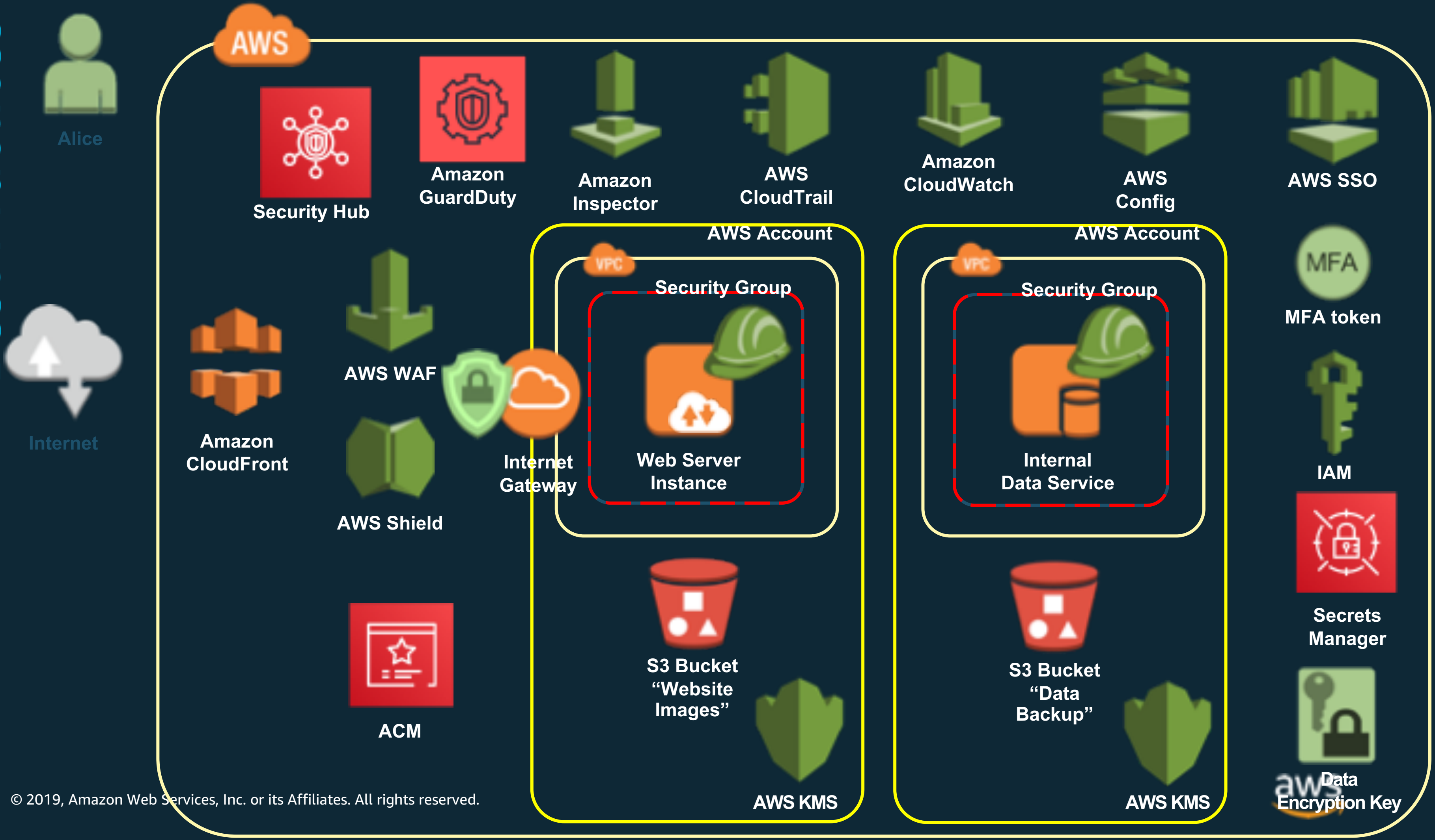
Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.

AWS Best Practices Paper	CIS Foundation Benchmark	CIS Web-Tier Benchmark
✓	0	9

Data Protection



Best Practices



Resources

AWS Security Pillar
Well Architected Framework
http://bit.ly/WellArchSec

CIS AWS Security
Foundations
Benchmark
http://bit.ly/AWSCIS

CIS AWS
Three-Tier Web
Architecture Benchmark
http://bit.ly/AWSCIS3T

https://aws.amazon.com/summits/sydney/on-demand/Tracks/secure/

Thank you!