

# Lightning in the Skies

## Cloud Security Breaches and How to Mitigate Them



**Neil Daswani, PhD**

Co-Director, Stanford Advanced Security Program

# MONGO DB RANSOMWARE ATTACKS

December 2016 / January 2017:

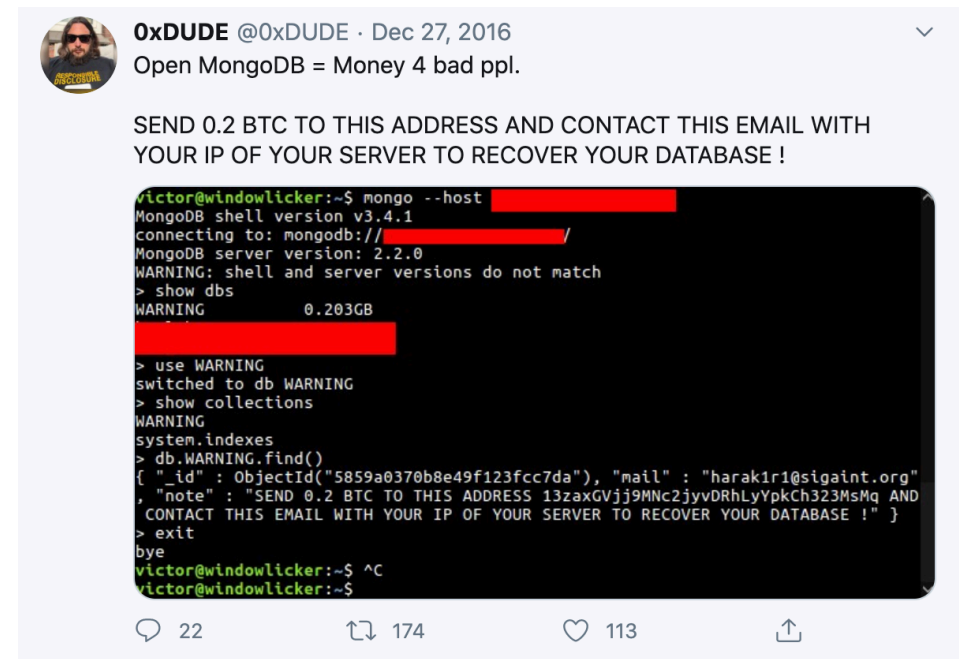
- 46,000 MongoDB databases vulnerable on AWS (based on Shodan scans)
- Over 10,000 attacks recorded
- $\geq 17$  ransoms paid

Problem: Unauthenticated connections via port 27017 could access databases with full admin rights.

Root Cause: Customers configured MongoDB installations with the default settings on AWS.

Mitigation:

- Use secure defaults. (Do not allow unauthenticated connections.)
- Limit privileges. (Don't allow full admin rights.)
- Backup. MongoDB Cloud and Ops Managers allow for continuous backup.



# SELECTED AMAZON S3 BUCKET BREACHES (2017)

Entity Breached	Data Exposed
Booz Allen Hamilton	Battlefield imagery and administrator credentials to sensitive systems
U.S. Voter Records	Personal data about 198 million American voters
Dow Jones & Co	Personally identifiable information for 2.2 million people
Verizon Wireless	Personally identifiable information for 6 million people and sensitive corporate information about IT systems, including login credentials.
Time Warner Cable	Personally identifiable information about 4 million customers, proprietary code, and administrator credentials
Pentagon	Terabytes of information from spying archive, resume for intelligence positions--including security clearance and operations history, credentials and metadata from an intra-agency intelligence sharing platform
Accenture	Master access keys for Accenture's account with AWS Key Management system, plaintext customer password databases, and proprietary API data.

# CAPITAL ONE CLOUD SECURITY BREACH (2019)

<b>What got stolen?</b>	100M US SSNs, 1M Canadian SINs
<b>What was the impact?</b>	<ul style="list-style-type: none"><li>• \$250K fine, 5 yrs. in jail for hacker</li><li>• Estimated breach costs of over \$300M</li></ul>
<b>How did it happen? Root cause?</b>	<ul style="list-style-type: none"><li>• Cap One Firewall Misconfiguration provided access to their AWS buckets. Server-Side Request Forgery (SSRF).</li></ul>
<b>How could it have been prevented?</b>	<ul style="list-style-type: none"><li>• Firewall Review</li><li>• Automated hybrid cloud security scanning.</li></ul>



# CAPITAL ONE BREACH

Attacker  
Machine



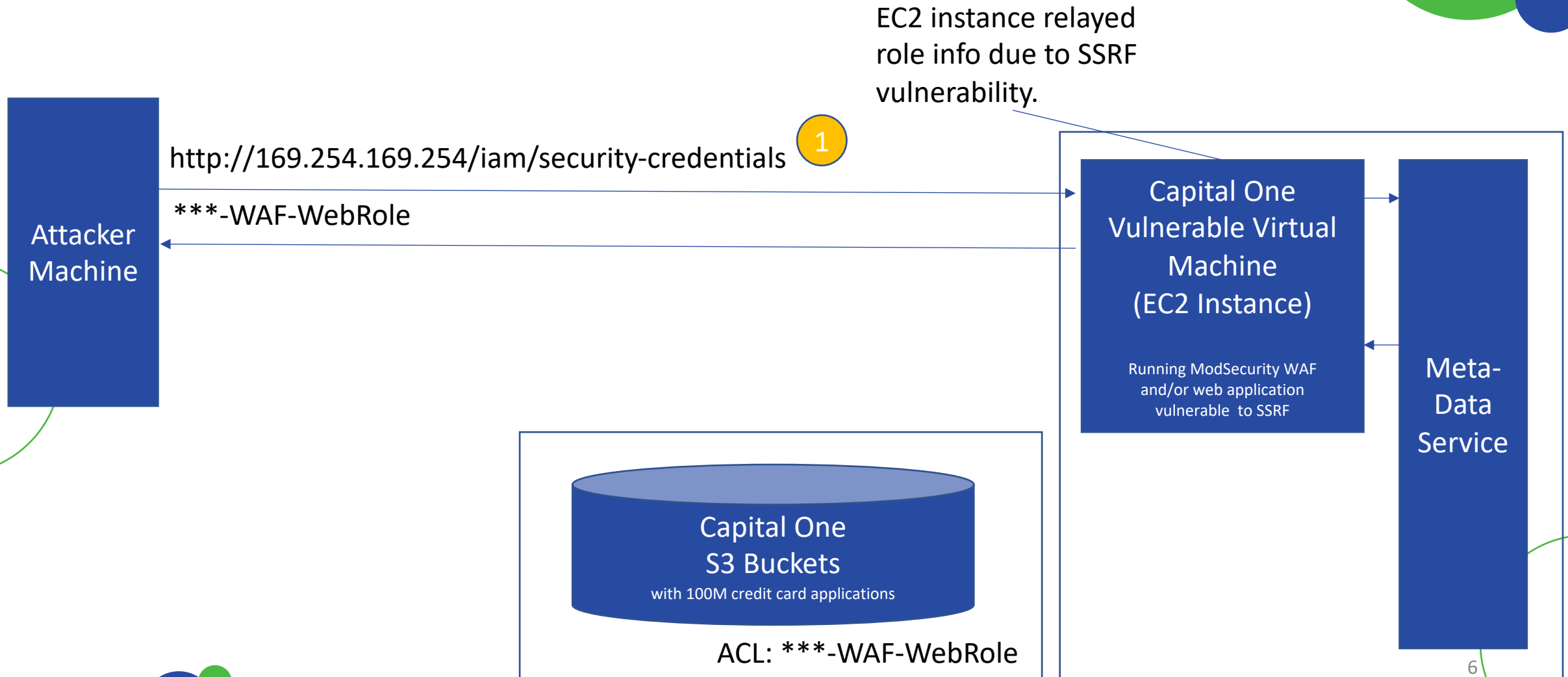
ACL: \*\*\*-WAF-WebRole

Capital One  
Vulnerable Virtual  
Machine  
(EC2 Instance)

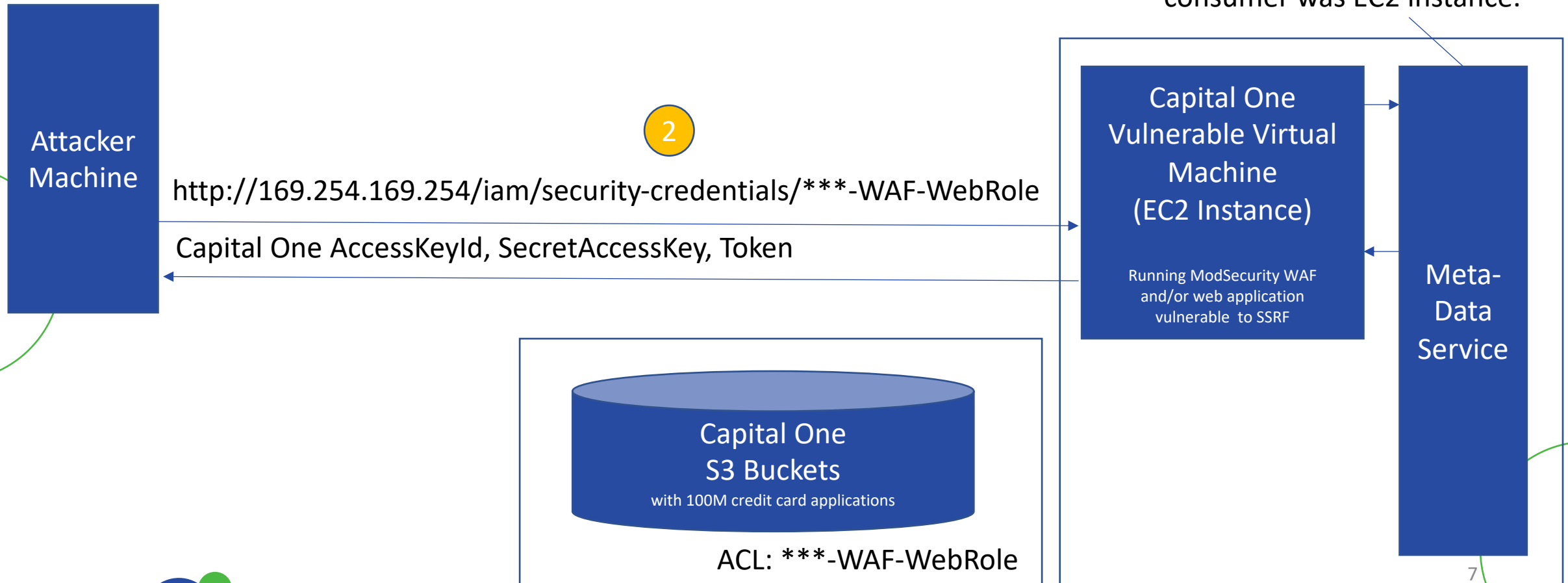
Running ModSecurity WAF  
and/or web application  
vulnerable to SSRF

Meta-  
Data  
Service

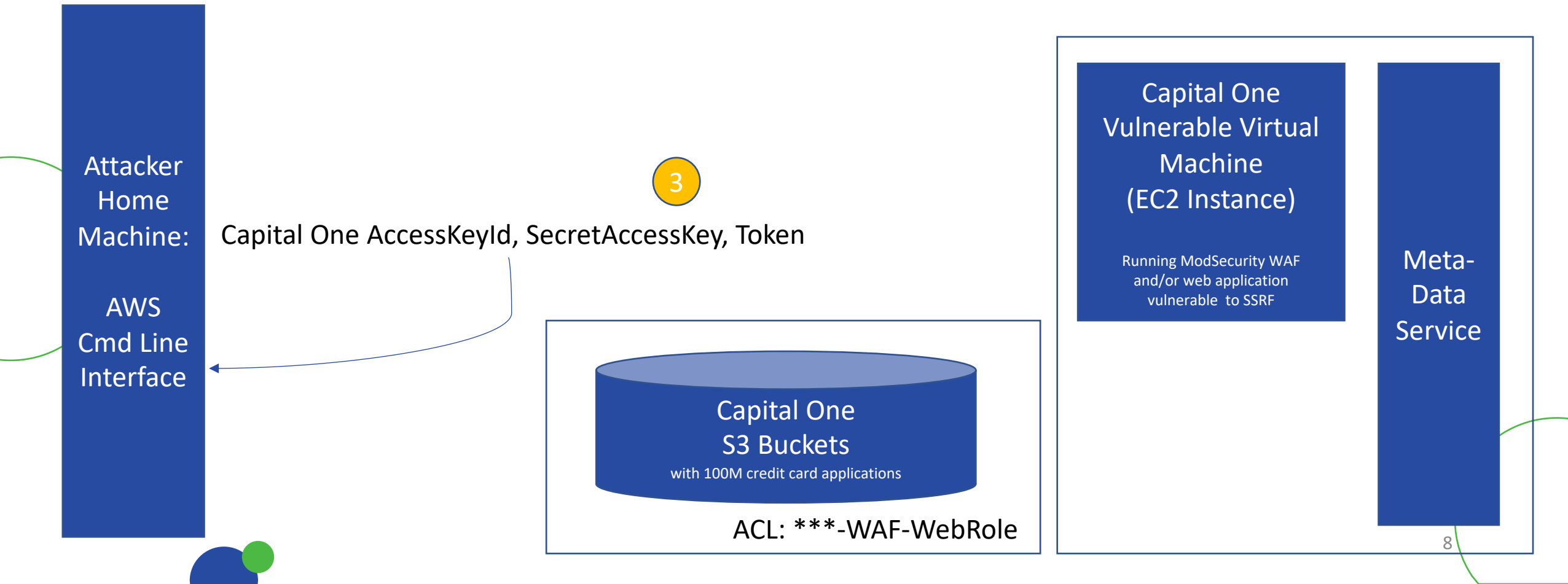
# CAPITAL ONE BREACH



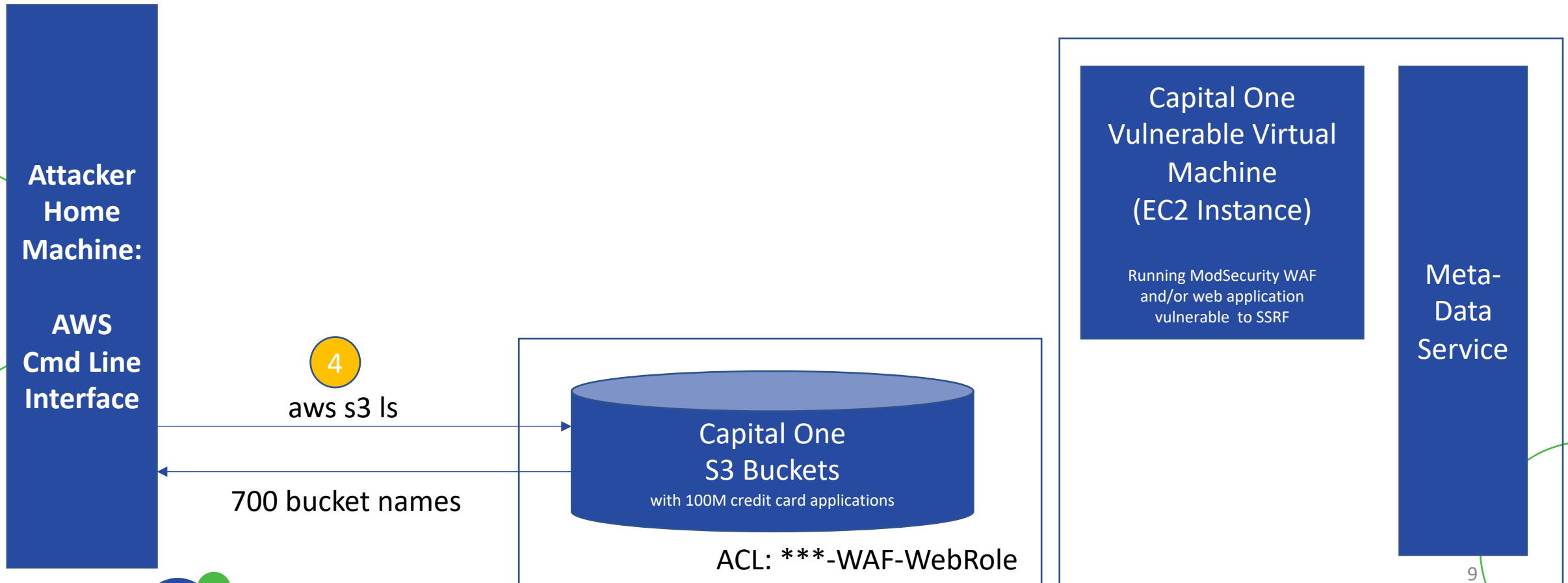
# CAPITAL ONE BREACH



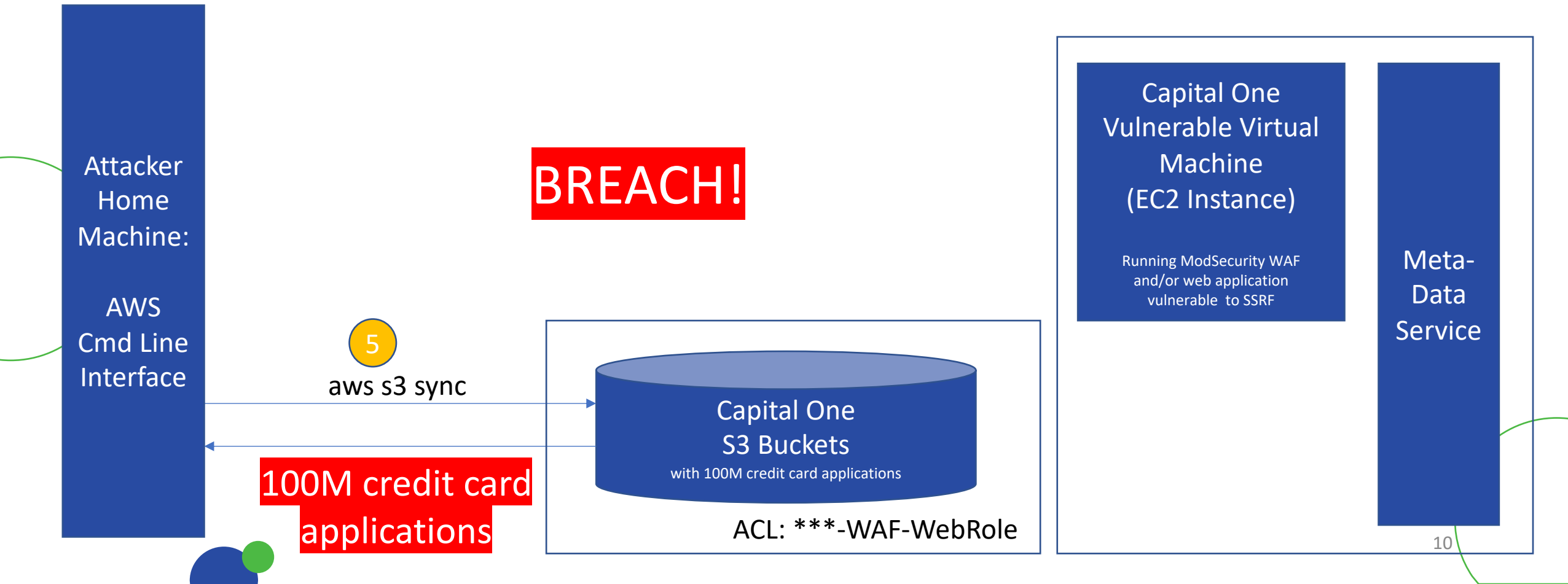
# CAPITAL ONE BREACH



# CAPITAL ONE BREACH



# CAPITAL ONE BREACH







# AMAZON S3 BUCKETS



Services ▾

Resource Groups ▾



neildaswanicsstanford ▾

Global ▾

Support ▾

Amazon S3

Buckets

Batch operations

Access analyzer for S3

Block public access (account settings)

Feature spotlight 2

Amazon S3's newest storage class S3 Intelligent-Tiering auto-tiers your data to deliver cost savings. [Learn more »](#)  
[Documentation](#)

We've temporarily re-enabled the previous version of the S3 console while we continue to improve the new S3 console experience. [Switch to the new console.](#)

## S3 buckets

[Discover the console](#)

Search for buckets

All access types ▾

[+ Create bucket](#)

[Edit public access settings](#)

[Empty](#)

[Delete](#)

1 Buckets

1 Regions



Bucket name ▾

Access ▾

Region ▾

Date created ▾



crazytestbucket

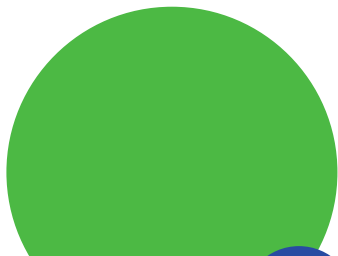
Objects can be public

US West (N. California)

Jun 24, 2020  
12:19:34 PM GMT-0700



# AMAZON S3 BUCKETS



Amazon S3 > crazytestbucket

crazytestbucket

- Overview
- Properties
- Permissions
- Management
- Access points

Type a prefix and press Enter to search. Press ESC to clear.

Upload

Create folder

Download

Actions ▾

Versions

Hide

Show

US West (N. California)

< Viewing 1 to 1 >

<input type="checkbox"/> Name ▾	Last modified ▾	Size ▾	Storage class ▾
<input type="checkbox"/> Neil-Daswani-headshot.jpg	Jun 24, 2020 12:20:41 PM GMT-0700	24.1 KB	Standard

< Viewing 1 to 1 >

Overview

Properties

Permissions

Select from

Open

Download

Download as

Make public

Copy path

**Owner**

daswani

**Last modified**

Jun 24, 2020 12:20:41 PM GMT-0700

**Etag**

98d59308e2e9e6281904b5dd5c39e747

**Storage class**

Standard

**Server-side encryption**

AES-256

**Size**


24.1 KB

**Key**

Neil-Daswani-headshot.jpg

**Object URL**

<https://crazytestbucket.s3-us-west-1.amazonaws.com/Neil-Daswani-headshot.jpg>

 crazytestbucket.s3-us-west-1.amazonaws.com/Neil-Daswani-headshot.jpg





# crazytestbucket

- Overview
- Properties
- Permissions
- Management
- Access points

- Block public access
- Access Control List
- Bucket Policy
- CORS configuration

## Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

### Block *all* public access

Off

Edit

Block public access to buckets and objects granted through *new* access control lists (ACLs)

Off

Block public access to buckets and objects granted through *any* access control lists (ACLs)

Off

Block public access to buckets and objects granted through *new* public bucket or access point policies

Off

Block public and cross-account access to buckets and objects through *any* public bucket or access point policies

Off

## crazytestbucket

Overview

Properties

Permissions

Management

Access points


Block public access

Access Control List

Bucket Policy

CORS configuration

## Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 

☒ **Block *all* public access**

Cancel

Save

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**  
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**  
S3 will ignore all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**  
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**  
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.



## crazytestbucket

Overview

Properties

Permissions

Management

Access points

Block public access

Access Control List

Bucket Policy

CORS configuration

## Block public access (bucket settings)

Public access is granted to buckets and objects by default. If you want to block all public access, turn on Block all public access. Before applying any of these settings, ensure that your application can still access the objects within, you can customize the individual settings below to suit your specific storage needs.

☒ **Block all public access**

Turning this setting on is the same as turning on Block public access to buckets and objects granted through all public access.

☐ **Block public access to buckets and objects granted through all public access**

S3 will block public access permissions that allow public access to buckets and objects granted through all public access.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through new public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

## Edit block public access (bucket settings) ✕

This will result in public access being blocked for this bucket and all objects in the bucket.

To confirm the settings, type *confirm* in the field.

Cancel

Confirm

Cancel

Save

## crazytestbucket

Overview

Properties

Permissions

Management

Access points


Block public access

Access Control List

Bucket Policy

CORS configuration

## Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 



Public access settings updated successfully

Block *all* public access

On

Edit

Block public access to buckets and objects granted through *new* access control lists (ACLs)

On

Block public access to buckets and objects granted through *any* access control lists (ACLs)

On

Block public access to buckets and objects granted through *new* public bucket or access point policies

On

# SECURING AMAZON S3 BUCKETS



crazytestbucket.s3-us-west-1.amazonaws.com/Neil-Daswani-headshot.jpg

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>008C78E161262FD8</RequestId>
  <HostId>mgVEu5TVmQaXu5/UIxptZyEofIHCNTSOaVSdHyMg2cpFJYS9hu2x94qFvyWtKAv9aCOpV2IWRck=</HostId>
</Error>
```



# Cloud Compliance – GDPR/CCPA

Maintaining Privacy Standards in the Cloud:

- GDPR is the General Data Protection Regulation indented to ensure privacy and confidentiality of information on EU citizens
- CCPA is a California State privacy law protecting the handling of citizen data
- Both standards require businesses to:
  - Track and maintain locality of personal information
  - Produce a report on demand of all personal information that is held
  - Honor right-to-be-forgotten for all personally identifiable information

# Cloud Compliance – GDPR/CCPA

Most GDPR/CCPA requirements can only be addressed at the application layer. However data localization is an IaaS consideration and arguably the most important compliance component.

Standard Requirements	IaaS Design and Operation Implications
<b>GDPR</b> <ul style="list-style-type: none"><li>• Annual data protection impact assessments</li><li>• Secure data processing and transfers</li><li>• Automated decision-making restrictions</li><li>• Limitation on select data processing activities</li></ul>	<ul style="list-style-type: none"><li>• Maintain data locality for the country of origin<ul style="list-style-type: none"><li>• Impacts global load balancing and data storage redundancy implications</li></ul></li><li>• Ensure that privileged access is based on need-to-know and that access is logged</li></ul>
<b>CCPA</b> <ul style="list-style-type: none"><li>• Restricted sale of personal information</li></ul>	
<b>GDPR and CCPA</b> <ul style="list-style-type: none"><li>• Breach notification to public</li><li>• Privacy by design at the application layer</li><li>• Privacy risk management based on architecture</li><li>• Consumer rights for data access, portability, erasure</li><li>• Right to object and rectify data errors</li></ul>	

# Data Localization – Google Cloud Platform

## Key Terms

- Region: A geographic region where resources can be hosted
- Zones: Datacenter locations within a Region

## Approach:

- When GCP resources are created, a zone is specified. This includes virtual machines, persistent disks and static IP addresses

## Data Localization in Practice using the GCP CLI

Show default Region and Zone for your tenant. If <code>google-compute-default-region</code> and <code>default-zone</code> are missing, then no default is set	<pre>gcloud compute project-info describe --project [PROJECT_ID]</pre>
Set the default Region and Zone	<pre>gcloud compute project-info add-metadata --metadata google-compute-default-region=&lt;region&gt;,google-compute-default-zone=&lt;zone&gt;</pre>
Set the default Region and Zone using the local gcloud client	<pre>gcloud config configurations activate CONFIGURATION_NAME gcloud config set compute/zone ZONE gcloud config set compute/region REGION</pre>







## Cloud Security Standards Landscape

Three representative cloud security standards:

- NIST Cloud Computer Security Reference Architecture SP 500-299
- Cloud Security Alliance – Cloud Controls Matrix
- Amazon Well Architected Framework





Note these are distinct from more general compliance standards such as: SOC II, ISO 2700x, NIST 800-53 (which can be implemented on cloud systems)



# SUMMARY



- There have been very significant cloud security breaches over the past few years. Many of them are due to inadvertent data exposure as a result of misconfigured permissions.
  - Important to: 1) leverage private by default bucket settings for new S3 buckets, and 2) lockdown legacy buckets and make any prior public buckets private as necessary.
  - There are many other aspects to cloud security besides storage permissions: configuration scanning, IAM / cloud firewalls, container security, DDoS protection, key management, SIEM monitoring, etc.
  - Cloud configurations can be leveraged to achieve compliance (GDPR, PCI, SOX, etc). There are also cloud-specific compliance frameworks and guidelines (NIST SP 500-299, CSA, AWS Well-Architected).
- 
- 

# FOR MORE INFO

Contact me at:

[daswani@cs.stanford.edu](mailto:daswani@cs.stanford.edu)  
Twitter: [@neildaswani](https://twitter.com/neildaswani)



# INTERESTED IN LEARNING MORE?

## computersecurity.stanford.edu

**Stanford Advanced Computer Security**  
Professional Certificate and Courses

**Vint Cerf, "Father of the Internet," Discusses Internet Security**



# INTERESTED IN LEARNING MORE?

## [computersecurity.stanford.edu](https://computersecurity.stanford.edu)



### Foundations of Information Security

**Professional Online Course: Open Enrollment**  
**Instructor: Neil Daswani and Dan Boneh**

Learn the foundational skills needed to build a successful cyber security career. You'll hear from experts like Dan Boneh and Neil Daswani, as well as from, Vint Cerf, co-creator of the internet, and industry security leaders from Google, LinkedIn, and LifeLock.



### CyberSecurity & Executive Strategy

**Professional Online Course: Open Enrollment**  
**Instructor: Neil Daswani, Dan Boneh and John Mitchell**

This course will help cybersecurity professionals explain and convince the importance of cybersecurity to all levels of management and executive leadership. The course provides guidance on how to quantitatively and qualitatively measure information security outcomes as well as assess risk.





# ACKNOWLEDGEMENTS

- Dan Boneh
- Andrew Ton

