INSTITUTE FOR DEFENSE ANALYSES

DATAWorks 2023: Preparing for Public Sector Test and Evaluation in the Commercial Cloud

Tye W. Botting, Project Leader

Brian T. Conway
Stacey L. Allison

April 2023

Public release approved. Distribution is unlimited.

IDA Document NS D-33391

Log: H 2023-000040

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

About This Publication
This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-19-D-0001, Task BD-09-2299(94), “Cyber-Net Centr” for the Office of the Director, Operational Test and Evaluation. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments
The IDA Technical Review Committee was chaired by Dr. V. Bram Lillard and consisted of Dr. Elizabeth A. Green, Dr. Kelly M. Avery, Dr. Keyla Pagan-Rivera, and Dr. Miriam E. Armstrong from the Operational Evaluation Division.

For more information:
Dr. Tye W. Botting, Project Leader
tbotting@ida.org • (703) 845-2050

Dr. V. Bram Lillard, Director, Operational Evaluation Division
vlillard@ida.org • (703) 845-2230

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-33391

DATAWorks 2023: Preparing for Public Sector Test and Evaluation in the Commercial Cloud

Tye W. Botting, Project Leader

Brian T. Conway
Stacey L. Allison

Executive Summary

IDA presents this briefing at the Defense and Aerospace Test and Analysis Workshop (DATAWorks) to assist the government test and evaluation community in planning and conducting adequate cyber testing of government systems within commercial cloud offerings. Cyber testing of the customer-managed segments of cloud offerings follows an identical approach to traditional on-premises systems, but the details of cloud deployments may be complex and require more extensive planning and information gathering.

Over the past decade, multiple administrations have emphasized the need for government agencies, including the Department of Defense, to shift on-premises information systems to cloud offerings. By operating through commercial cloud services, the government can reduce the amount of infrastructure that they must directly manage and focus effort on delivering services. However, operating in the cloud introduces new risks. Notably, the security of government information systems is now shared between the cloud service provider (CSP) and the government customer, as illustrated to the right. Through this shared responsibility model, the government retains the responsibility to secure what they put "in the cloud" (in green) and how it interfaces with other systems and users.

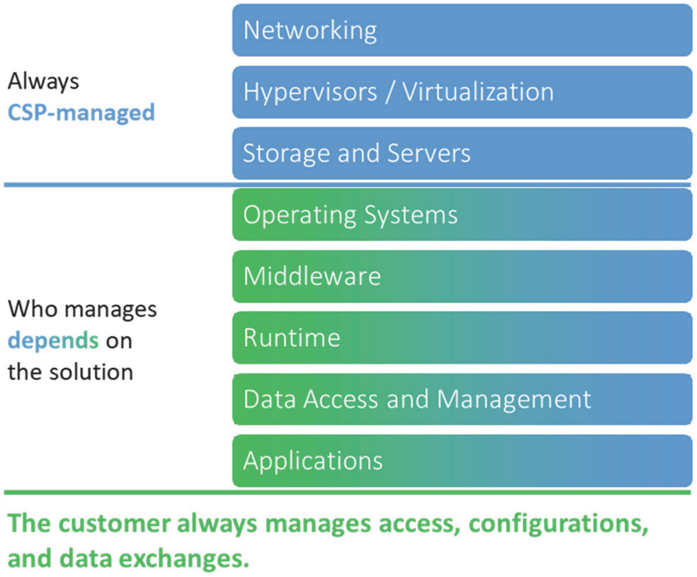

Networking
Hypervisors / Virtualization
Storage and Servers
Always
CSP-managed
Operating Systems
Middleware
Runtime
Data Access and Management
Applications
Who manages
depends on
the solution
The customer always manages access, configurations, and data exchanges.

Figure 1. Cloud shared responsibility model

CSPs provide a variety of cloud service offerings through the Federal Risk and Authorization Management Program (FedRAMP), which endorses an "authorize once, use many times" approach throughout federal agencies. Through FedRAMP, CSPs provide some assurance that their offerings are secure. Still, FedRAMP does not provide insight to the risk assumed by what the government puts “in the cloud.”

Threats have targeted both the CSP and customer-managed segments of the cloud, so the government must be cognizant of operational risk posed to both segments. Exploitations on the customer side tend to be easier to conduct, and are therefore more prevalent. At minimum, government-led cloud testing should aim to understand how threats can exploit the government-managed portion of the cloud service offering.

Each cloud service offering possesses unique deployment configurations with proprietary identity and access management controls. Furthermore, CSPs aiming to replace on-premises infrastructure offer a variety of managed services that exist within a single ecosystem. These services include databases, storage, monitoring, firewalls, artificial intelligence processing, data visualization, and many others. This briefing discusses some of the differences between traditional and cloud deployments in the context of a pair of case studies that examine how customer-managed cloud misconfigurations and weak access controls could be exploited.

To conduct effective testing, stakeholders should follow an appropriate planning approach that identifies how the system under test is deployed, how it connects to users and external systems, and necessary resources for testing. This is not all that different from other cyber testing. Access and authentication mechanisms vary between cloud service offerings and traditional on-premises infrastructure. Without test stakeholders that understand and appreciate these differences, the test may not provide useful insights on the cyber posture of the system to the operational users or acquisition executives.

This page intentionally left blank.

DATAWorks 2023: Preparing for Public Sector Test and Evaluation in the Commercial Cloud

S. Lee Allison

Brian T. Conway

April 26, 2023

Institute for Defense Analyses
730 East Glebe Road ● Alexandria, Virginia 22305

Cloud exploits can be simple to conduct, with devastating consequences

1) Hacker finds a misconfigured Jenkins server accessible on the open internet belonging to CommuteAir.

```
string sInput;
int iLength, iN;
double dblTemp;
bool again = true;

while (again) {
    iN = -1;
    again = false;
    getline(cin, sInput);
    system("cls");
    stringstream(sInput) >> dblTemp;
    iLength = sInput.length();
    if (iLength < 4) {
        again = true;
        continue;
    } else if (sInput[iLength - 3] != '.') {
        again = true;
        continue;
    } while (++iN < iLength) {
        if (isdigit(sInput[iN])) {
            continue;
        } else if (iN == (iLength - 3) ) {
            inue;
```

2) Jenkins stages, tests, and deploys code to production environments, and source code can be exfiltrated.

Some code compares CommuteAir's employee list with the TSA No Fly List.

3) Source code not only contains the TSA No Fly List, but it also contains hard-coded AWS credentials.

4) Enumerating credential access shows access to S3 buckets and database tables with employee data.

AWS S3

AWS Relational Database Service

AWS: Amazon Web Services; S3: Simple Storage Service; TSA: Transportation Security Administration

Originally reported: https://www.dailydot.com/debug/no-fly-list-us-tsa-unprotected-server-commuteair/

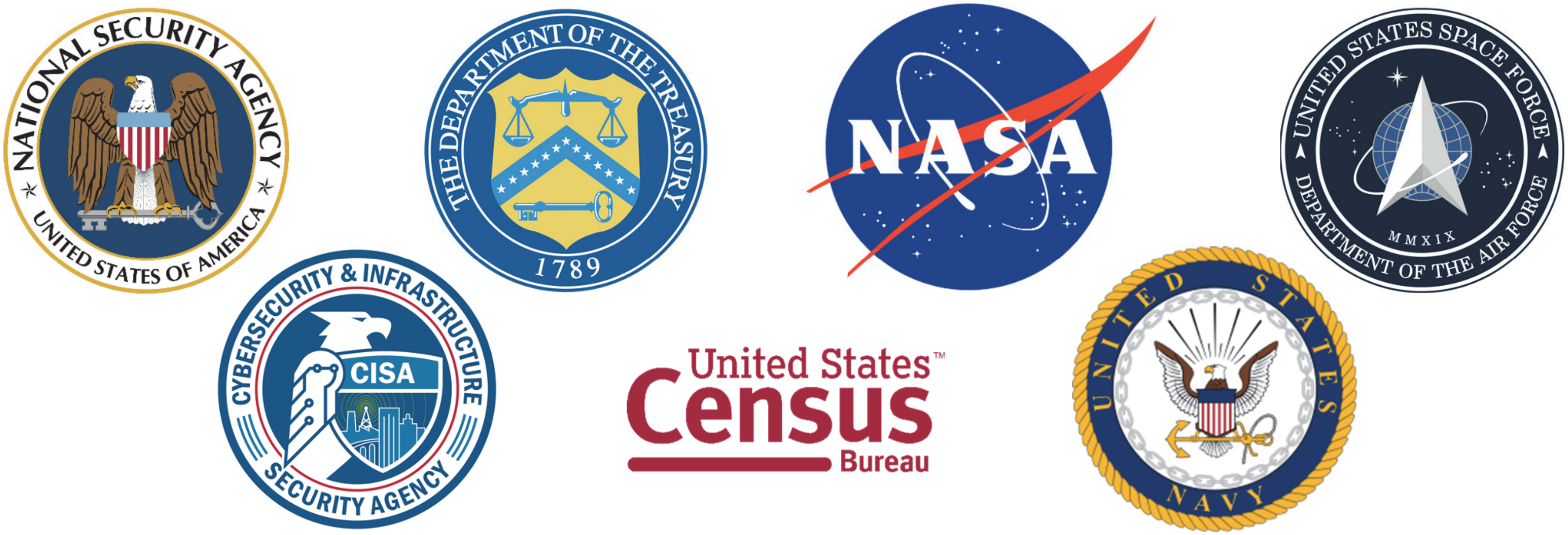
Government testing should aim to find vulnerabilities inherent to cloud deployments.

Outline

1. U.S. Government in the cloud
2. Cloud deployments
3. Cloud interfaces
4. Capital One Case Study and T&E Planning

BLUF: Cyber test and evaluation doesn't change much in commercial cloud offerings, but the details of deployments can vary quite a bit. Test stakeholders need to be cognizant of those differences during test planning.

BLUF: Bottom Line Up Front; T&E: Test and Evaluation


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
THE DEPARTMENT OF THE TREASURY
1789
NASA
UNITED STATES SPACE FORCE
MMXIX
DEPARTMENT OF THE AIR FORCE
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
United States™ Census Bureau
UNITED STATES NAVY

The public sector is rapidly shifting to utilize commercial cloud resources rather than on-premises systems

Administrations consistently release policy that drives government users to cloud solutions.

DOD Cloud Strategy of 2018: Drives implementation toward the enterprise cloud environment with an ecosystem composed of General Purpose (formerly JEDI) and Fit for Purpose clouds.

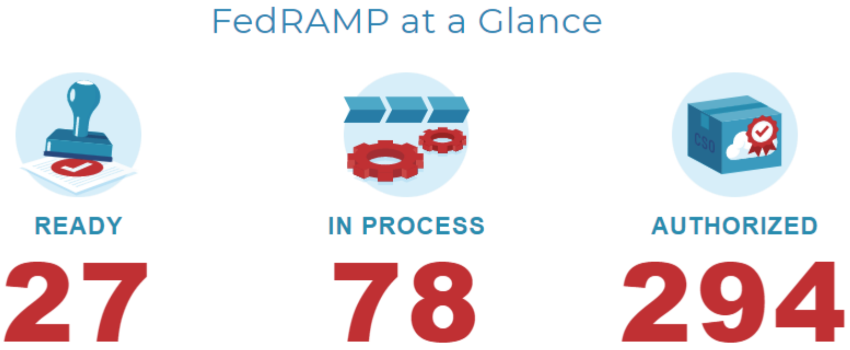
Federal Cloud Computing Strategy of 2019: A strategy to accelerate agency adoption of cloud-based solutions and take advantage of security and scalability benefits.

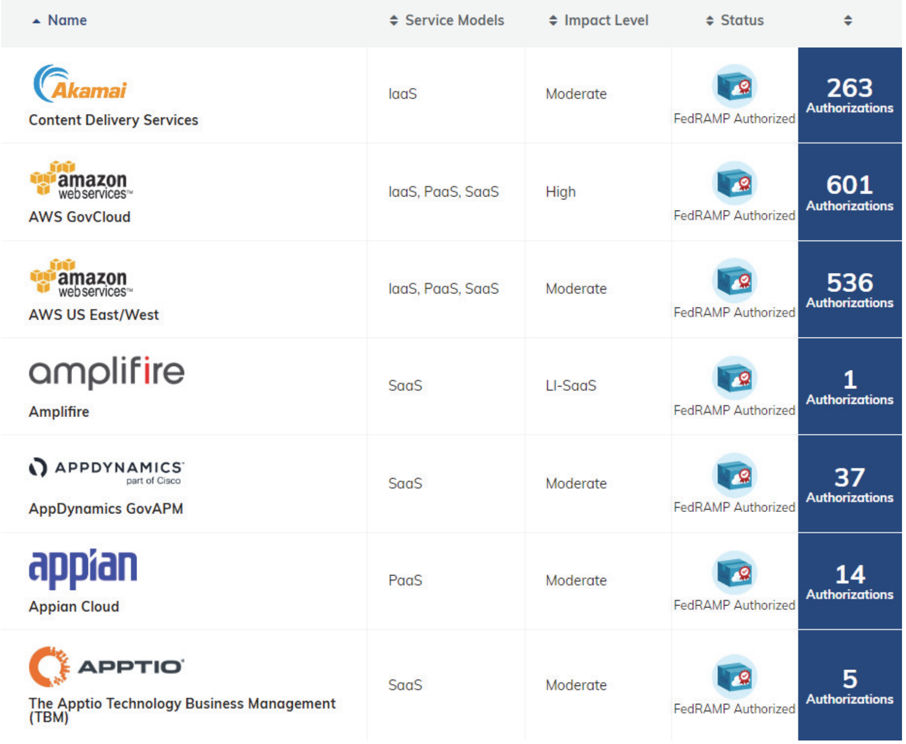
Executive Order on Improving the Nation's Cybersecurity (5/21) and National Security Memo 8 (12/21): Requires that federal agencies and DOD prioritize resources for the adoption and use of cloud technology within 60 days.

FedRAMP: Established in 2011 as a standardized process for authorizing cloud solutions. "Do once, use many times" framework to allow multiple agencies to leverage a single cloud solution.

FedRAMP: Federal Risk and Authorization Management Program; JEDI: Joint Enterprise Defense Infrastructure

FedRAMP enables the USG to authorize and reuse commercial cloud offerings



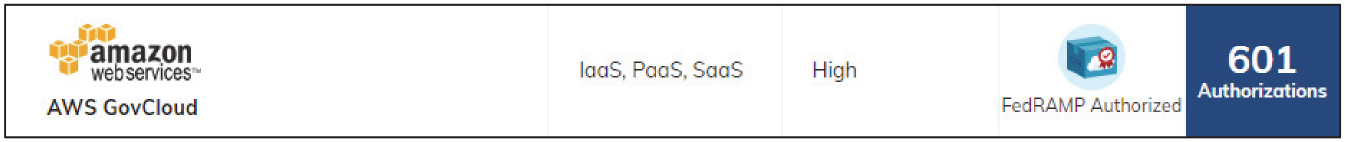


▲ Name	⬍ Service Models	⬍ Impact Level	⬍ Status	⬍
Akamai Content Delivery Services	IaaS	Moderate	FedRAMP Authorized	263 Authorizations
amazon web services AWS GovCloud	IaaS, PaaS, SaaS	High	FedRAMP Authorized	601 Authorizations
amazon web services AWS US East/West	IaaS, PaaS, SaaS	Moderate	FedRAMP Authorized	536 Authorizations
amplifire Amplifire	SaaS	LI-SaaS	FedRAMP Authorized	1 Authorizations
APPDYNAMICS part of Cisco AppDynamics GovAPM	SaaS	Moderate	FedRAMP Authorized	37 Authorizations
appian Appian Cloud	PaaS	Moderate	FedRAMP Authorized	14 Authorizations
APPTIO The Apptio Technology Business Management (TBM)	SaaS	Moderate	FedRAMP Authorized	5 Authorizations

FedRAMP

FedRAMP: Federal Risk and Authorization Management Program

Hundreds of government entities use AWS GovCloud



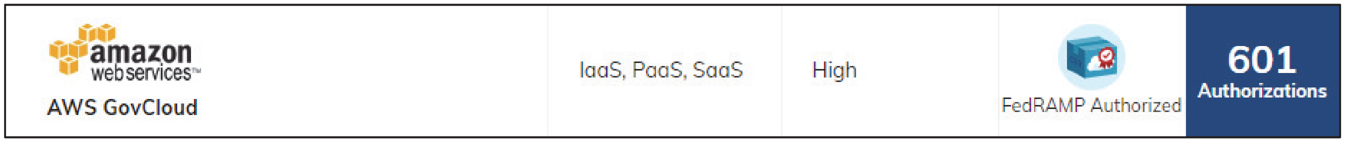
amazon web services AWS GovCloud	IaaS, PaaS, SaaS	High	FedRAMP Authorized	601 Authorizations

FedRAMP

Administration for Children & Families
Alcohol and Tobacco Tax and Trade Bureau
American Battle Monuments Commission
Bonneville Power Administration
Bureau of Alcohol, Tobacco, Firearms and Explosives
Bureau of Engraving and Printing
Bureau of Labor Statistics
Bureau of Land Management
Bureau of Safety and Environmental Enforcement
Bureau of the Fiscal Service
Centers for Disease Control and Prevention
Centers for Medicare & Medicaid Services
Commodity Futures Trading Commission
Consumer Financial Protection Bureau
Consumer Product Safety Commission
Corporation for National & Community Service (CNCS)
Council of the Inspectors General on Integrity and Efficiency
Customs and Border Protection
Cybersecurity & Infrastructure Security Agency
Defense Counterintelligence and Security Agency
Defense Health Agency
Defense Human Resource Activity
Defense Information Systems Agency
Defense Logistics Agency
Defense Nuclear Facilities Safety Board
Deparment of Homeland Security
Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of Justice
Department of Labor
Department of State
Department of the Interior
Department of the Navy
Department of the Treasury
Department of Transportation
Department of Veterans Affairs
DOI Office of the Inspector General
DOJ Office of the Inspector General
Drug Enforcement Administration
Environmental Protection Agency
Executive Office for United States Attorneys
Export-Import Bank of the United States
Farm Credit Administration
Federal Aviation Administration
Federal Bureau of Prisons
Federal Communications Commission
Federal Deposit Insurance Corporation
Federal Election Commission
Federal Emergency Management Agency
Federal Energy Regulatory Commission
Federal Housing Finance Agency
Federal Law Enforcement Training Center
Federal Law Enforcement Training Centers
Federal Reserve System
Federal Retirement Thrift Investment Board
Federal Student Aid
Federal Trade Commission
Federal Transportation Administration
FHFA Office of the Inspector General
FirstNet
Food and Drug Administration
Food and Drug Administration-Minneapolis District Office
General Services Administration
Ginnie Mae
Health Resources and Services Administration
HHS Office of the Inspector General
HUD Office of the Inspector General
Idaho Operations Office
Immigration and Customs Enforcement
Institute of Museum and Library Services
Interior Business Center
Internal Revenue Service
International Trade Administration
Justice Management Division
Los Alamos National Laboratory
Millennium Challenge Corporation
National Aeronautics and Space Administration
National Cancer Institute
National Capital Planning Commission
National Endowment for the Humanities
National Gallery of Art
National Geospatial-Intelligence Agency
National Institute of Environmental Health Sciences
National Institute of Standards and Technology
National Institutes of Health
National Labor Relations Board
National Mediation Board
National Nuclear Security Administration
National Nuclear Security Administration / Energy Efficiency and Renewable Energy
National Nuclear Security Administration / Kansas City Field Office
National Nuclear Security Administration / Lawrence Livermore National Laboratory
National Nuclear Security Administration / Nevada Field Office
National Oceanic and Atmospheric Administration
National Park Service
National Science Foundation
National Telecommunications and Information Administration
National Training Center
National Transportation Safety Board
North American Aerospace Defense Command & United States Northern Command
Nuclear Regulatory Commission
Office of Administration
Office of Justice Programs
Office of Natural Resources Revenue
Office of Personnel Management
Office of Science / Argonne Site Office
Office of the Comptroller of the Currency
Office of the Secretary of Transportation
Other Executive Branch Agency
Peace Corps
Pension Benefit Guaranty Corporation
Pretrial Services Agency
Program Support Center
Small Business Administration
Social Security Administration
State Office of the Inspector General
Strategic Petroleum Reserve
Surface Transportation Board
Tennessee Valley Authority
Transportation Security Administration
U.S. Commission for the Preservation of America's Heritage Abroad
U.S. Election Assistance Commission
U.S. International Development Finance Corporation
U.S. Office of Special Counsel
United States Agency for Global Media
United States Agency for International Development
United States Air Force
United States Army
United States Army Corps of Engineers
United States Census Bureau
United States Coast Guard
United States Commission on Civil Rights
United States Forest Service
United States Geological Survey
United States House of Representatives
United States International Trade Commission
United States Marine Corps
United States Marshals Service
United States Mint
United States Naval War College
United States Patent and Trademark Office
United States Securities and Exchange Commission
Universal Service Administrative Company
VA Office of the Inspector General
Washington Headquarters Services
Western Area Power Administration

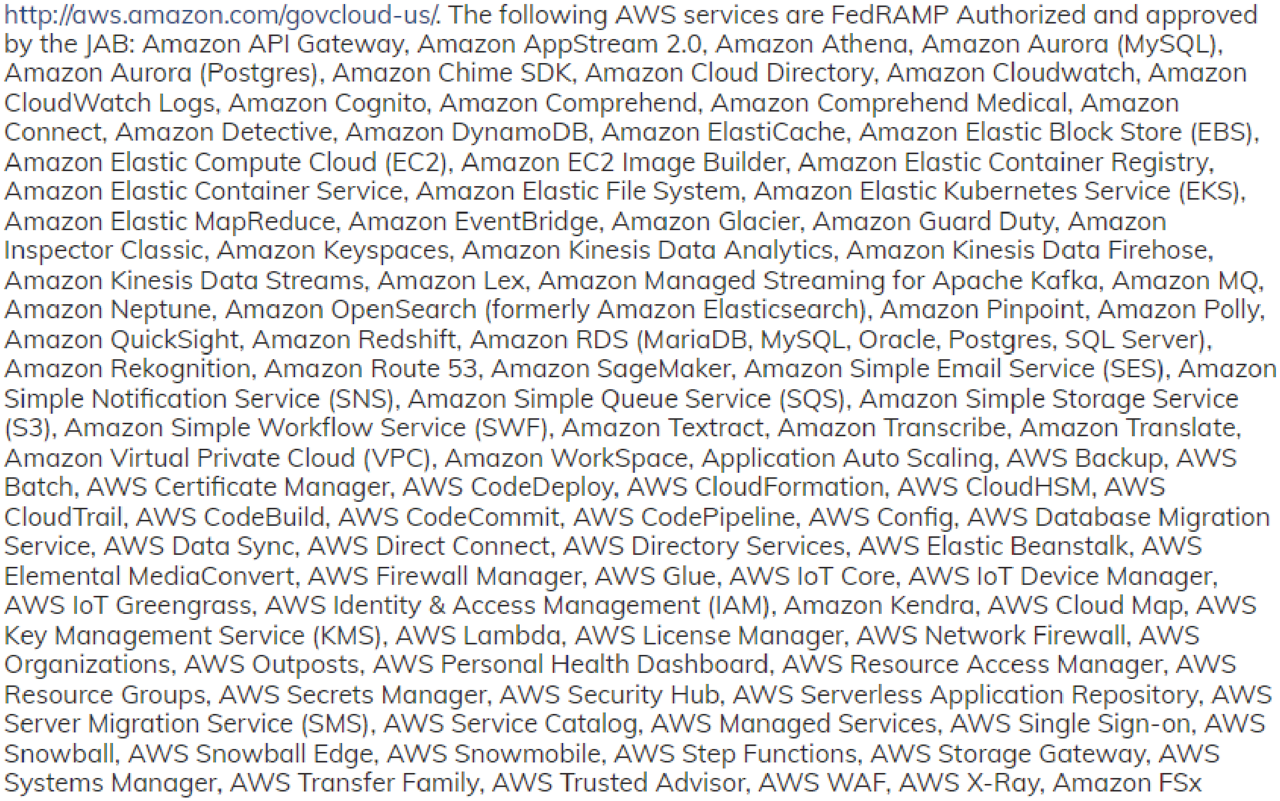
AWS: Amazon Web Services; **FedRAMP**: Federal Risk and Authorization Management Program; **IaaS:** Infrastructure as a Service;
PaaS: Platform as a Service; **SaaS:** Software as a Service

AWS GovCloud comprises numerous services that can be used by the government customer



amazon web services AWS GovCloud	IaaS, PaaS, SaaS	High	FedRAMP Authorized	601 Authorizations

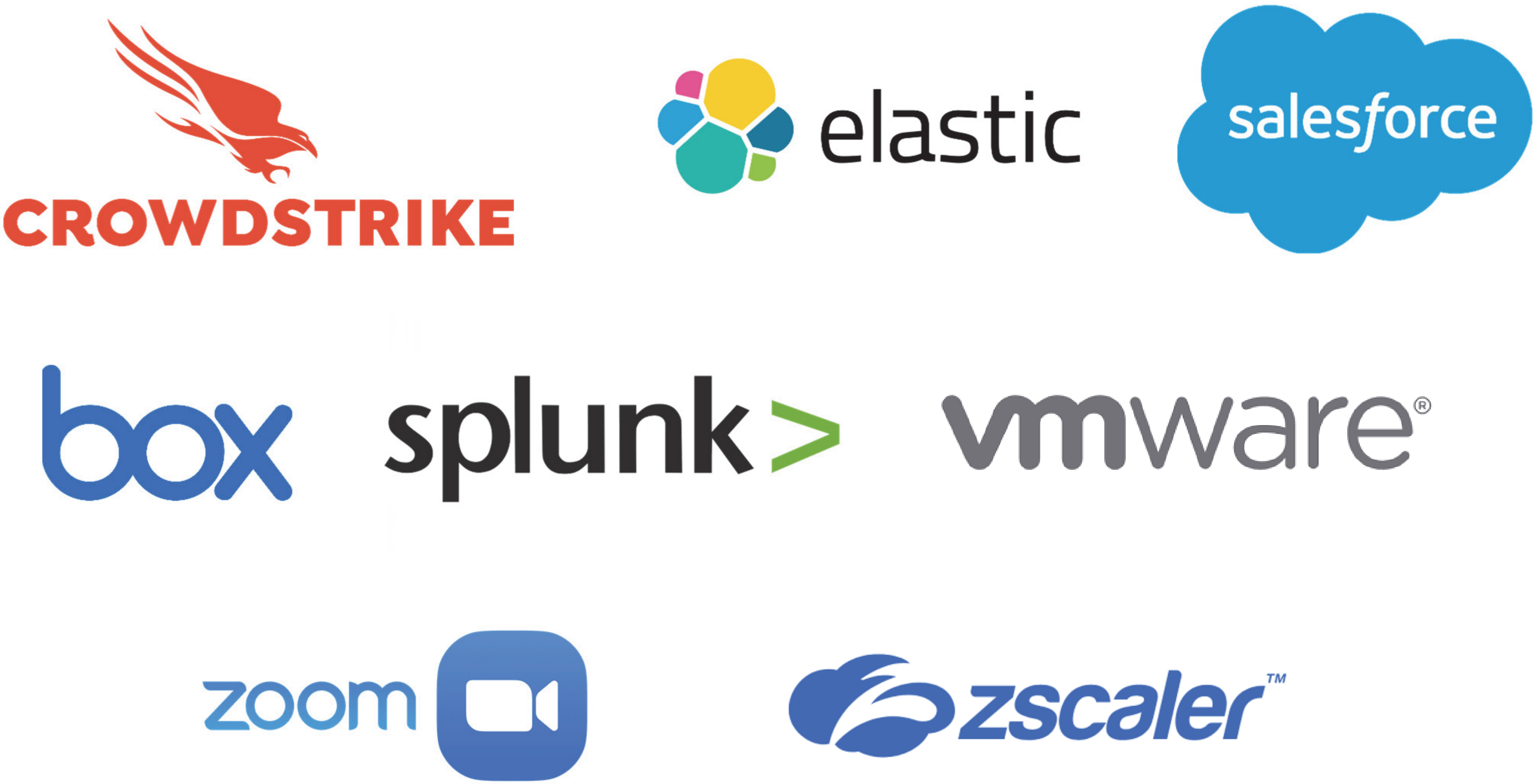
FedRAMP



http://aws.amazon.com/govcloud-us/. The following AWS services are FedRAMP Authorized and approved by the JAB: Amazon API Gateway, Amazon AppStream 2.0, Amazon Athena, Amazon Aurora (MySQL), Amazon Aurora (Postgres), Amazon Chime SDK, Amazon Cloud Directory, Amazon Cloudwatch, Amazon CloudWatch Logs, Amazon Cognito, Amazon Comprehend, Amazon Comprehend Medical, Amazon Connect, Amazon Detective, Amazon DynamoDB, Amazon ElastiCache, Amazon Elastic Block Store (EBS), Amazon Elastic Compute Cloud (EC2), Amazon EC2 Image Builder, Amazon Elastic Container Registry, Amazon Elastic Container Service, Amazon Elastic File System, Amazon Elastic Kubernetes Service (EKS), Amazon Elastic MapReduce, Amazon EventBridge, Amazon Glacier, Amazon Guard Duty, Amazon Inspector Classic, Amazon Keyspaces, Amazon Kinesis Data Analytics, Amazon Kinesis Data Firehose, Amazon Kinesis Data Streams, Amazon Lex, Amazon Managed Streaming for Apache Kafka, Amazon MQ, Amazon Neptune, Amazon OpenSearch (formerly Amazon Elasticsearch), Amazon Pinpoint, Amazon Polly, Amazon QuickSight, Amazon Redshift, Amazon RDS (MariaDB, MySQL, Oracle, Postgres, SQL Server), Amazon Rekognition, Amazon Route 53, Amazon SageMaker, Amazon Simple Email Service (SES), Amazon Simple Notification Service (SNS), Amazon Simple Queue Service (SQS), Amazon Simple Storage Service (S3), Amazon Simple Workflow Service (SWF), Amazon Textract, Amazon Transcribe, Amazon Translate, Amazon Virtual Private Cloud (VPC), Amazon WorkSpace, Application Auto Scaling, AWS Backup, AWS Batch, AWS Certificate Manager, AWS CodeDeploy, AWS CloudFormation, AWS CloudHSM, AWS CloudTrail, AWS CodeBuild, AWS CodeCommit, AWS CodePipeline, AWS Config, AWS Database Migration Service, AWS Data Sync, AWS Direct Connect, AWS Directory Services, AWS Elastic Beanstalk, AWS Elemental MediaConvert, AWS Firewall Manager, AWS Glue, AWS IoT Core, AWS IoT Device Manager, AWS IoT Greengrass, AWS Identity & Access Management (IAM), Amazon Kendra, AWS Cloud Map, AWS Key Management Service (KMS), AWS Lambda, AWS License Manager, AWS Network Firewall, AWS Organizations, AWS Outposts, AWS Personal Health Dashboard, AWS Resource Access Manager, AWS Resource Groups, AWS Secrets Manager, AWS Security Hub, AWS Serverless Application Repository, AWS Server Migration Service (SMS), AWS Service Catalog, AWS Managed Services, AWS Single Sign-on, AWS Snowball, AWS Snowball Edge, AWS Snowmobile, AWS Step Functions, AWS Storage Gateway, AWS Systems Manager, AWS Transfer Family, AWS Trusted Advisor, AWS WAF, AWS X-Ray, Amazon FSx

AWS: Amazon Web Services; **FedRAMP**: Federal Risk and Authorization Management Program; **IaaS:** Infrastructure as a Service; **PaaS:** Platform as a Service; **SaaS:** Software as a Service

AWS also forms the backbone for other FedRAMP authorized services, like…

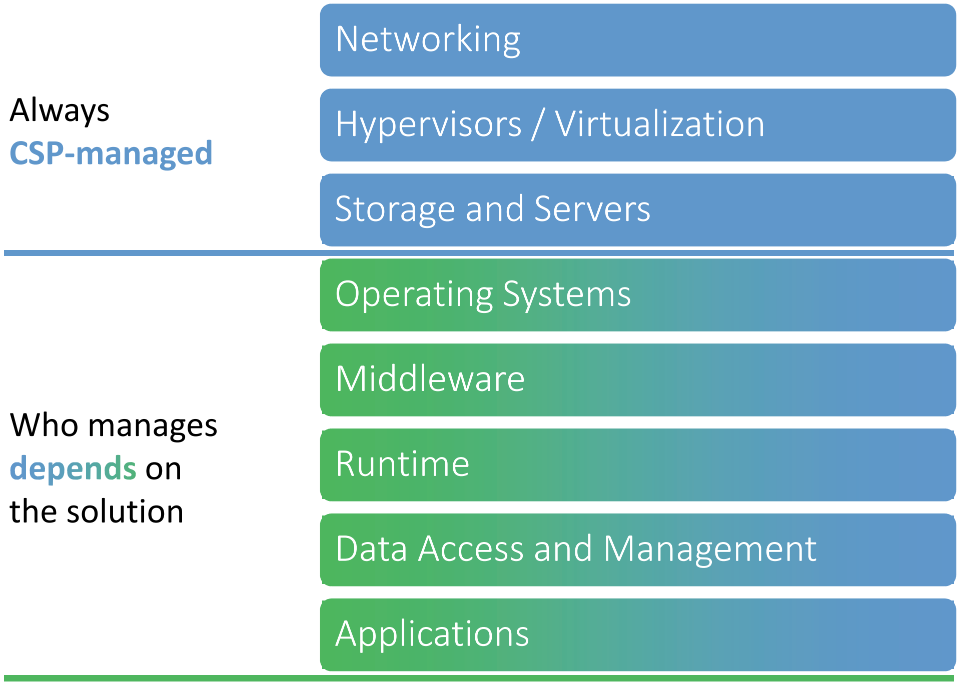


AWS: Amazon Web Services; **FedRAMP**: Federal Risk and Authorization Management Program

Customers retain responsibility for cybersecurity, even when using cloud service offerings.

Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) are the three deployment models by which DOD categorizes cloud service offerings.

Each trades off customizability for a more complete product.



Always **CSP-managed**

- Networking
- Hypervisors / Virtualization
- Storage and Servers

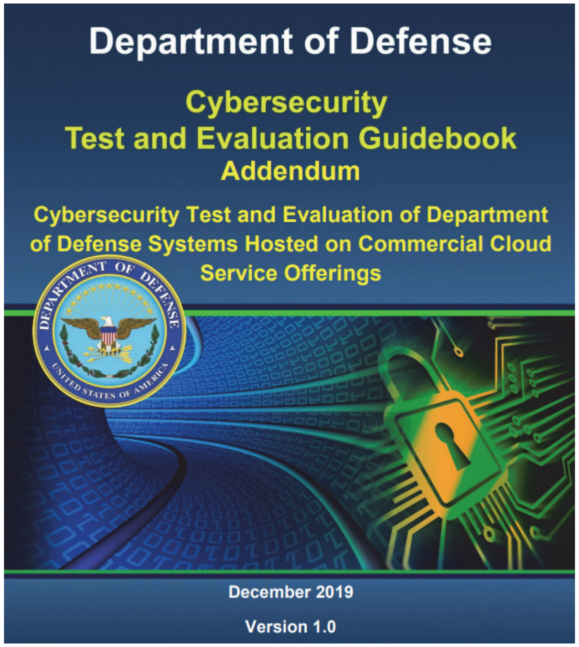
Who manages **depends** on the solution

- Operating Systems
- Middleware
- Runtime
- Data Access and Management
- Applications

The customer always manages access, configurations, and data exchanges.

CSP: Cloud Service Provider

Testers can (and should) request FedRAMP packages, which describe CSP security responsibilities



Department of Defense

Cybersecurity
Test and Evaluation Guidebook
Addendum

Cybersecurity Test and Evaluation of Department of Defense Systems Hosted on Commercial Cloud Service Offerings

December 2019

Version 1.0

> "The Chief Development Tester and OTA should understand that FedRAMP+ and provisional authorizations are considered necessary but not sufficient for evaluating the shared responsibilities of CSPs and DoD programs deploying to the commercial cloud."

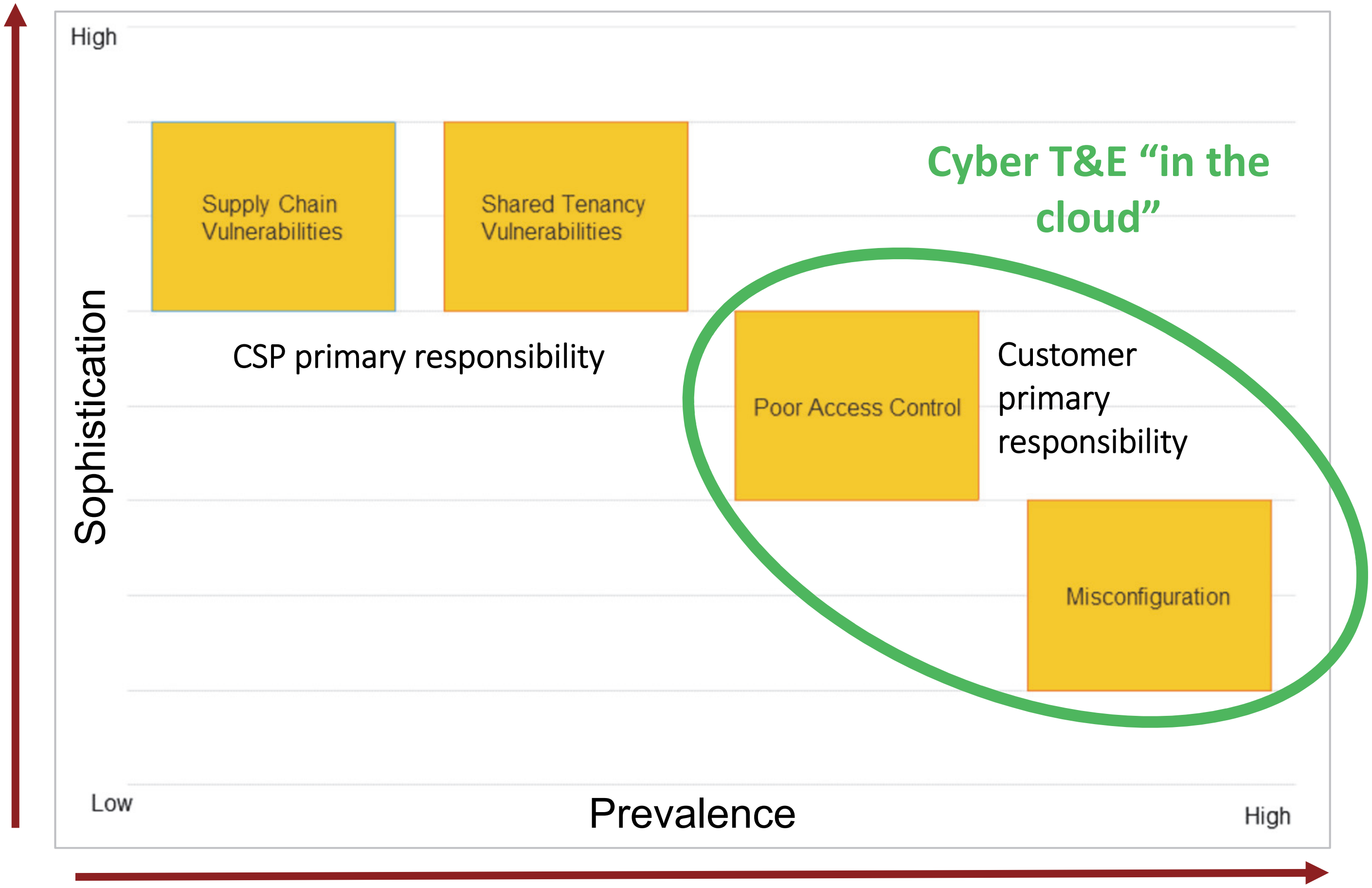
- 3rd Party (contractors) Assessment Organizations (3PAOs) conduct independent penetration tests on CSP-managed infrastructure
- CSPs provide continuous reporting on discovered vulnerabilities and plans for remediation

CSO: Cloud Service Offering; **CSP:** Cloud Service Provider; **DISA:** Defense Information Systems Agency;
FedRAMP: Federal Risk and Authorization Management Program; **NIST:** National Institute for Standards and Time

FedRAMP does NOT provide insight to how a customer secures their cloud deployments

FedRAMP: Federal Risk and Authorization Management Program

NSA analyzed threats to both customer and provider segments of cloud offerings.

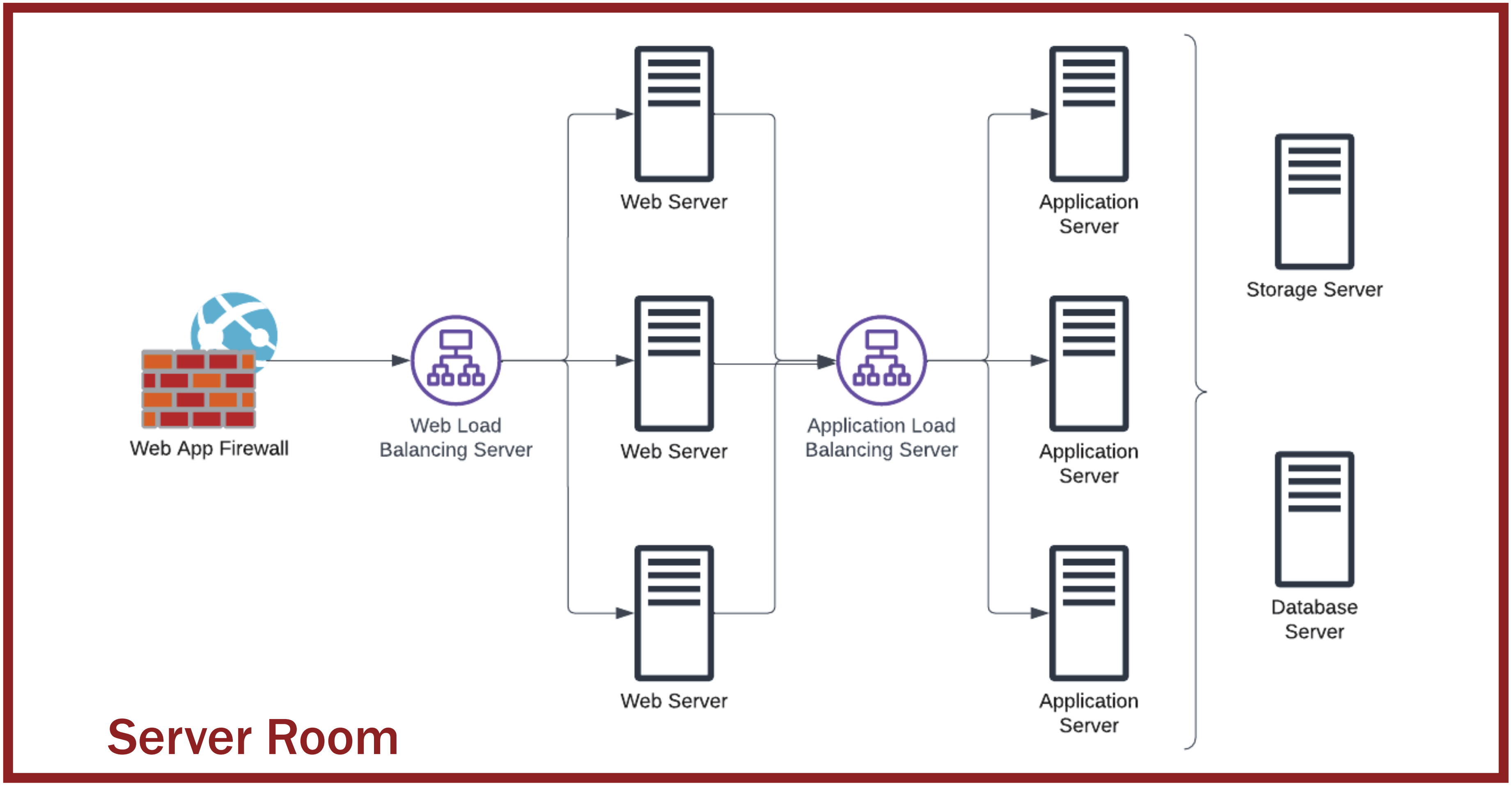


2020 NSA White Paper on Mitigating Cloud Vulnerabilities
(https://media.defense.gov/2020/Jan/22/2002237484/-1/-1/0/CSI-MITIGATING-CLOUD-VULNERABILITIES_20200121.PDF)

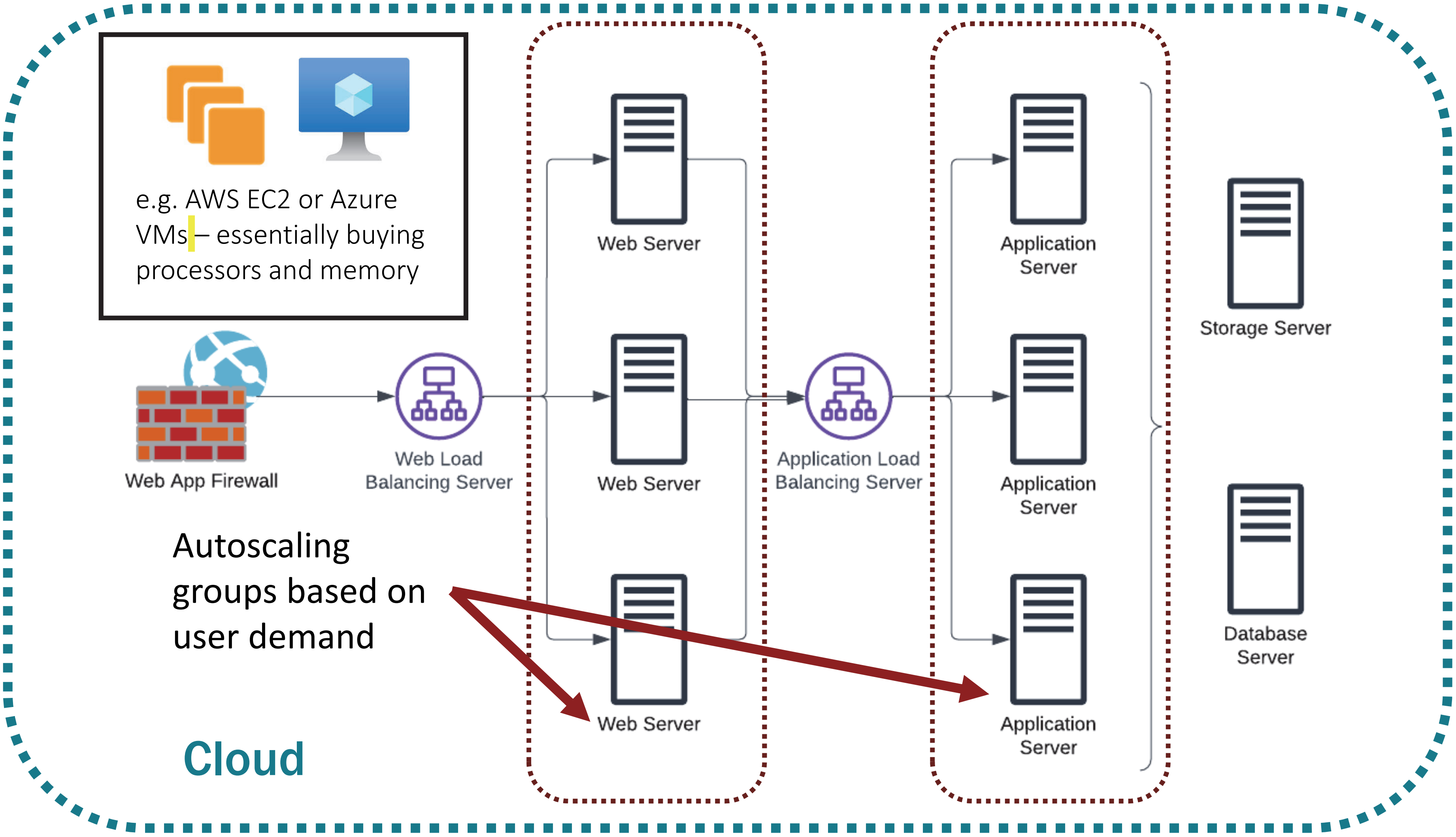
3PAO: 3rd Party Assessment Organization; **CSP:** Cloud Service Provider; **NSA:** National Security Agency; **T&E:** Test and Evaluation

Cloud service architectures and access mechanisms differ from those traditionally encountered on premises

Traditionally, organizations have built their own datacenters to host applications, like this web app



Moving to a cloud service offering allows customers to forgo networking and hardware management



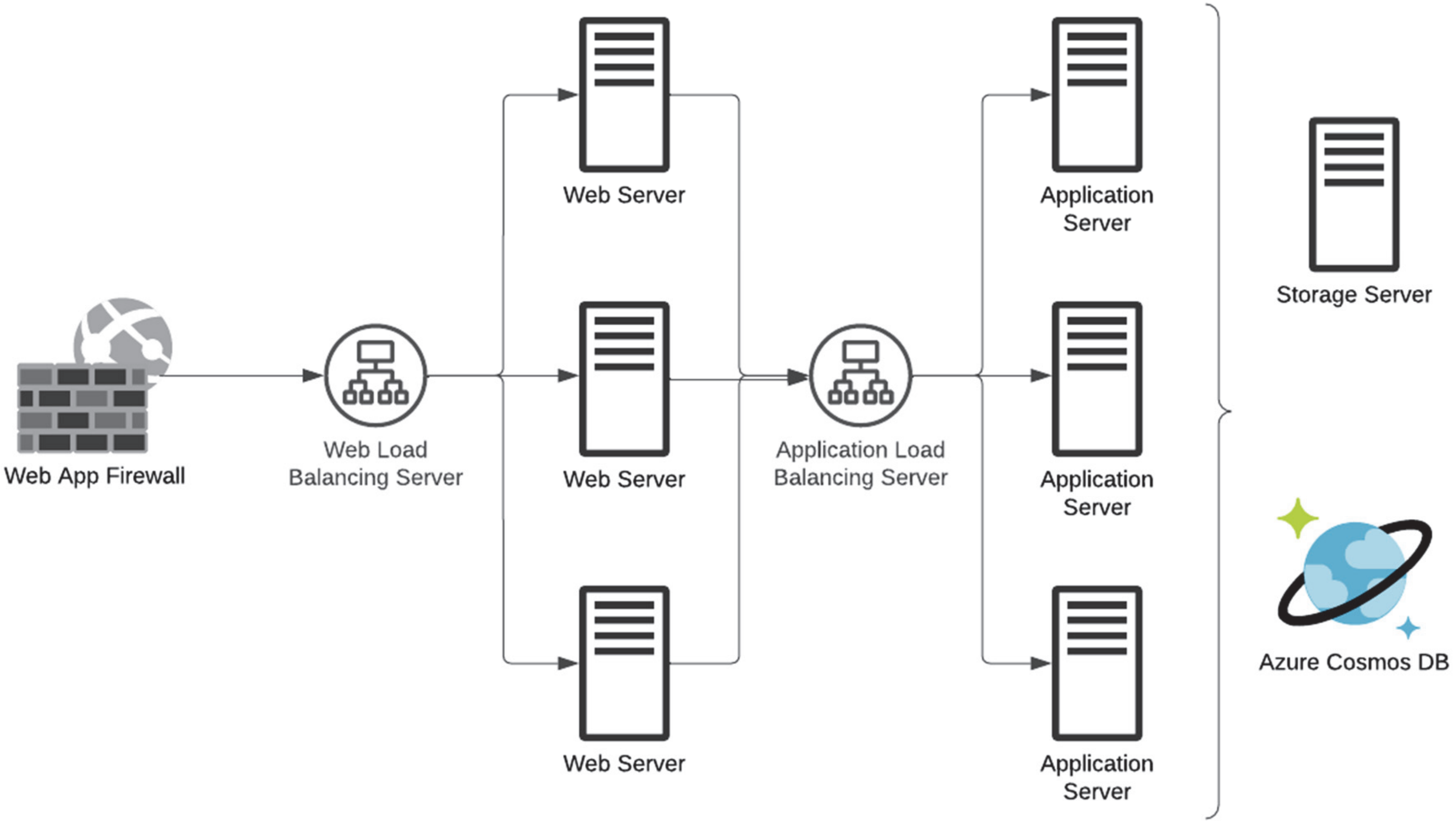
e.g. AWS EC2 or Azure VMs – essentially buying processors and memory

Autoscaling groups based on user demand

Cloud

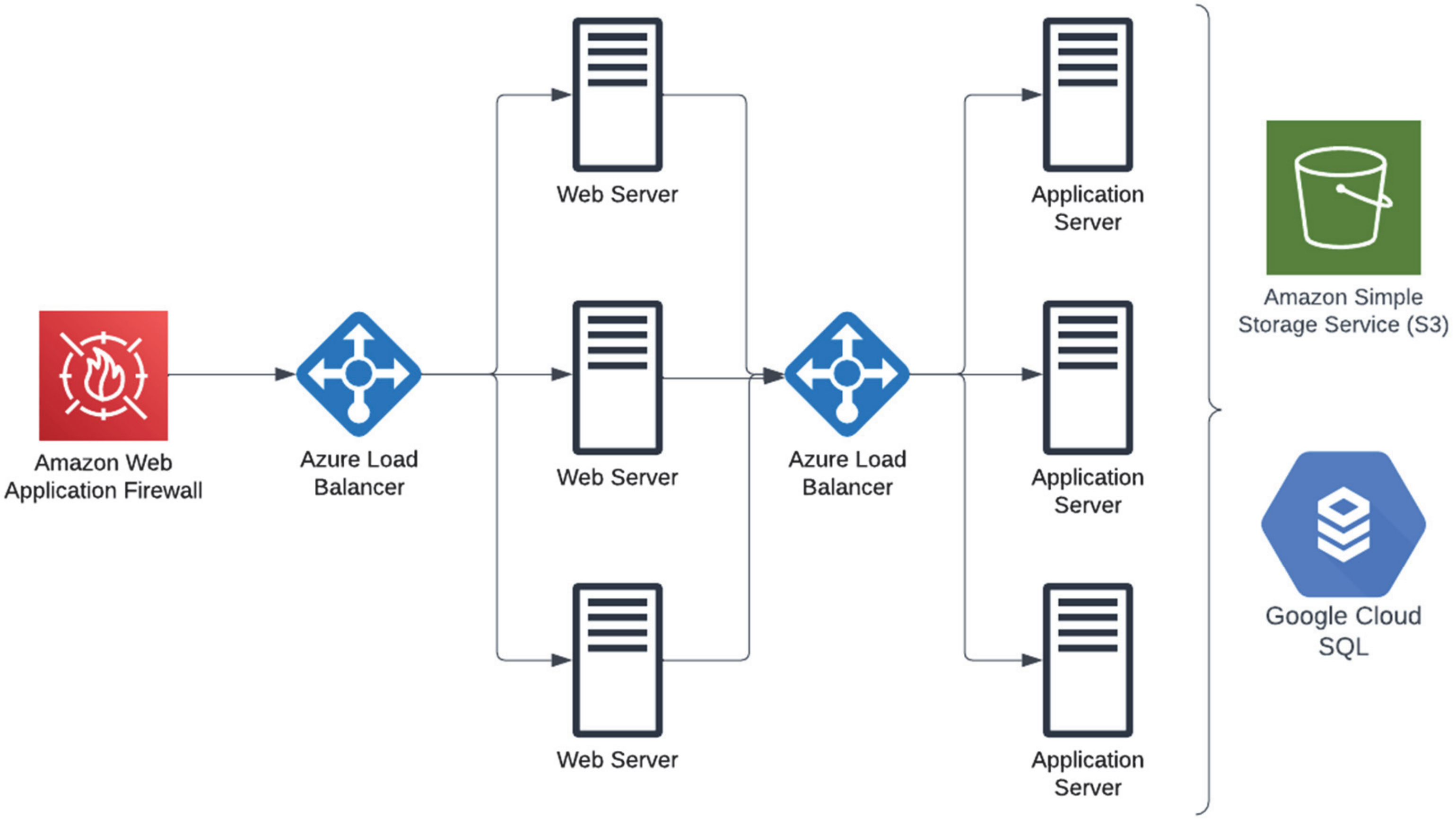
AWS: Amazon Web Services; EC2: Elastic Compute Cloud; VM: Virtual Machine

CSPs offer more services that reduce maintenance and development time and cost

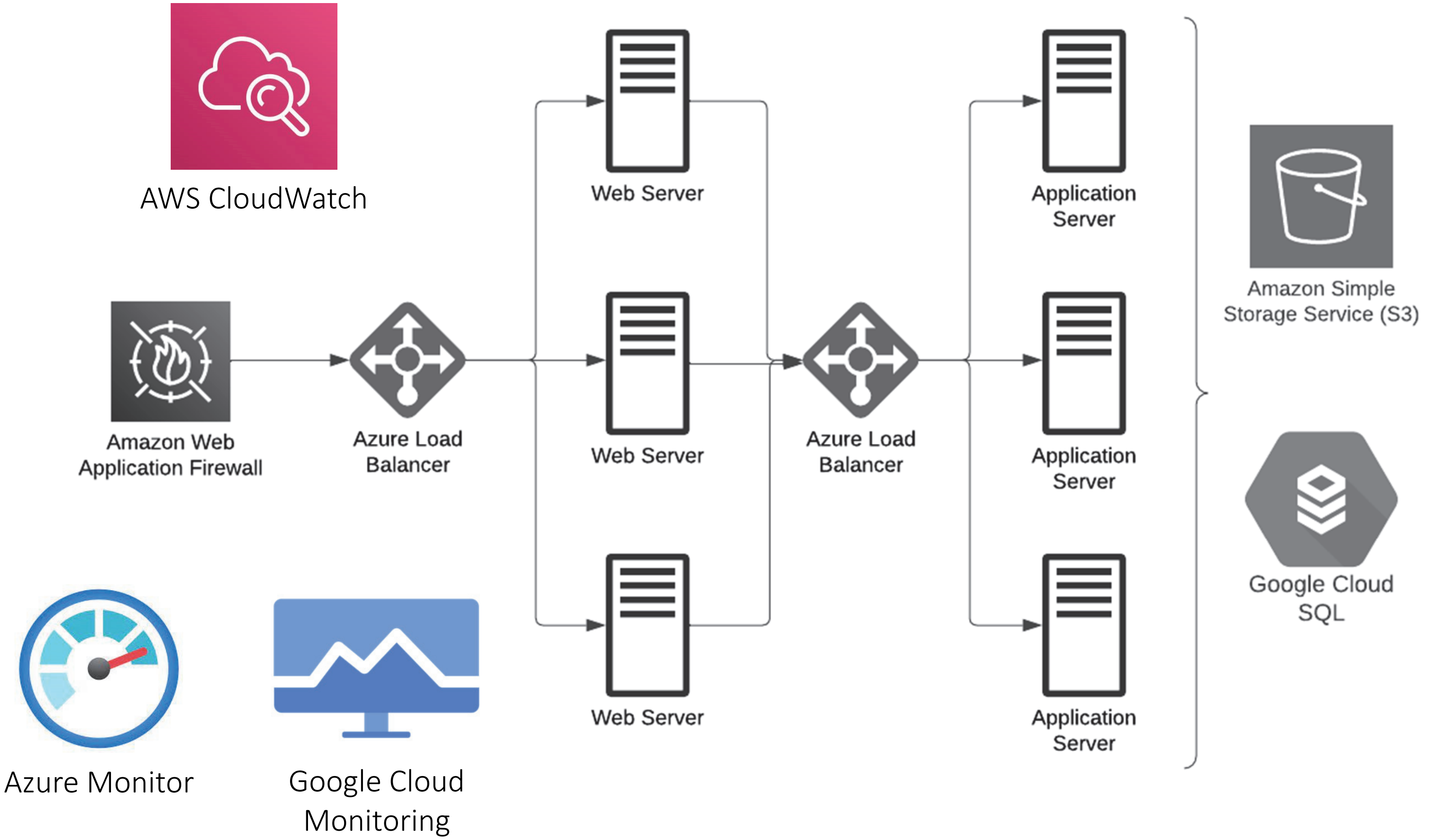


CSP: cloud service provider

… and each CSP has cloud-native services that have unique configurations and access mechanisms



… with monitoring and security alerting that is entirely customizable by the customer

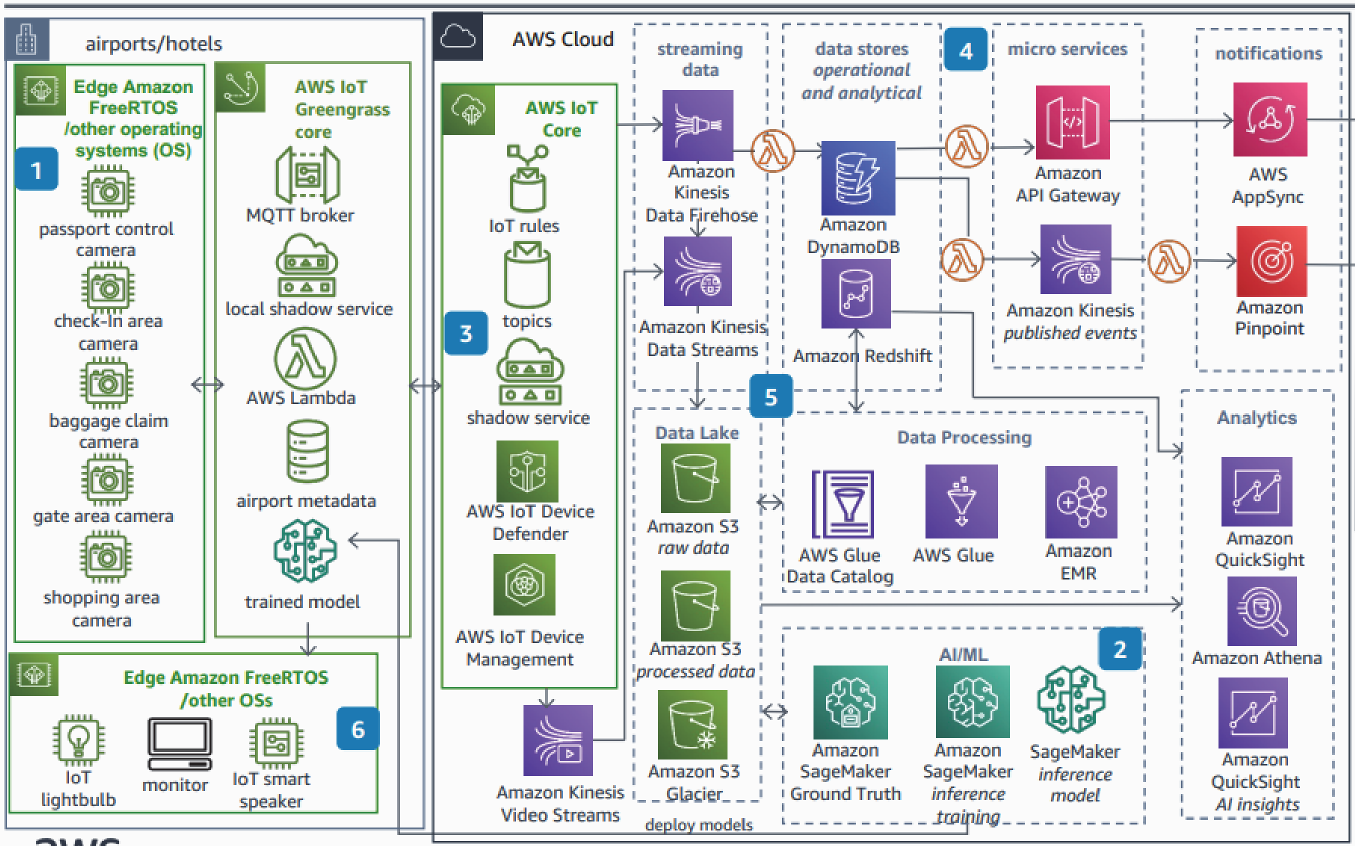


AWS: Amazon Web Services

This was a simple example, but there are much more complex use cases:

Queue Depth Management Using IoT and AI/ML

This architecture shows how you can improve customer experience using the Internet of Things (IoT) and artificial intelligence/machine learning (AI/ML) by monitoring queues using cameras, using computer vision to measure queue depth, and providing visual and audible alerts about bottlenecks and unreasonable queue depths to customer service managers.



Reviewed for technical accuracy October 12, 2022

AWS Reference Architecture

1 Place cameras in important areas to improve customer wait times.

2 **AWS IoT Greengrass, AWS IoT Core,** and **AWS IoT Device Management** manage the cameras and run inference on the edge with **AWS Lambda** and **Amazon SageMaker.**

3 To perform inference training, the cameras collect video streams for four days or more. This recording is used to tune and train **Amazon SageMaker** to generate a head detection model. **Amazon SageMaker Ground Truth** labels the heads in the training video feeds.

4 Use purpose built databases and serverless architecture to deliver microservices and alerts. **Amazon DynamoDB, Amazon Kinesis, AWS Lambda, Amazon API Gateway,** and **AWS AppSync** provide the capabilities required for the near real-time microservices, notifications, and events to build mobile apps and dashboards. The dashboard can also be used to configure queue depth, threshold alerts, and area of interest for each camera.

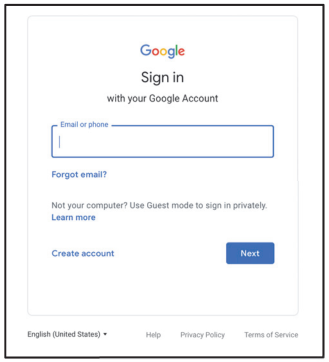
5 **Amazon Simple Storage Service** (Amazon S3), **Amazon Redshift,** and **Amazon QuickSight** provide the data lake and analytics platform for the solution. With **Amazon SageMaker,** you can build, deploy, train, and tune AI/ML models. **Amazon Athena** can be used for as-needed data analysis on the data lake.

6 Show queue depth on a monitor, notifications to a smart speaker, or update the state of an IoT lightbulb in case of a busy period such as an unexpected weather event causing flight cancellations increasing queues at check-in.

Testers must understand what is being deployed in these environments, but also how users, administrators, and other systems connect to them.

T&E stakeholders need to enumerate cloud system interfaces to enable consideration of all threat postures in test planning and conduct.

- Externally facing web applications through which users or systems can access and interact using APIs
- Direct connections through VPN, peering, or other CSP-specific connectivity
- Command line interfaces or web portals for administrative actions

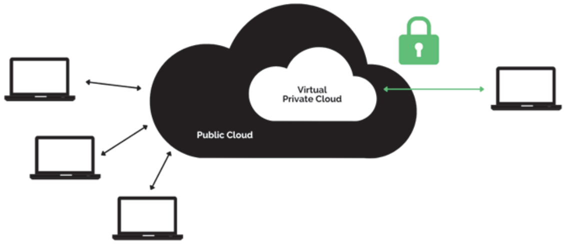


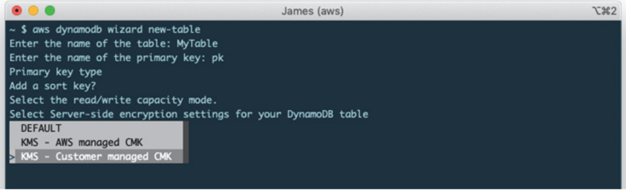
Google

Sign in

with your Google Account

Not your computer? Use Guest mode to sign in privately.



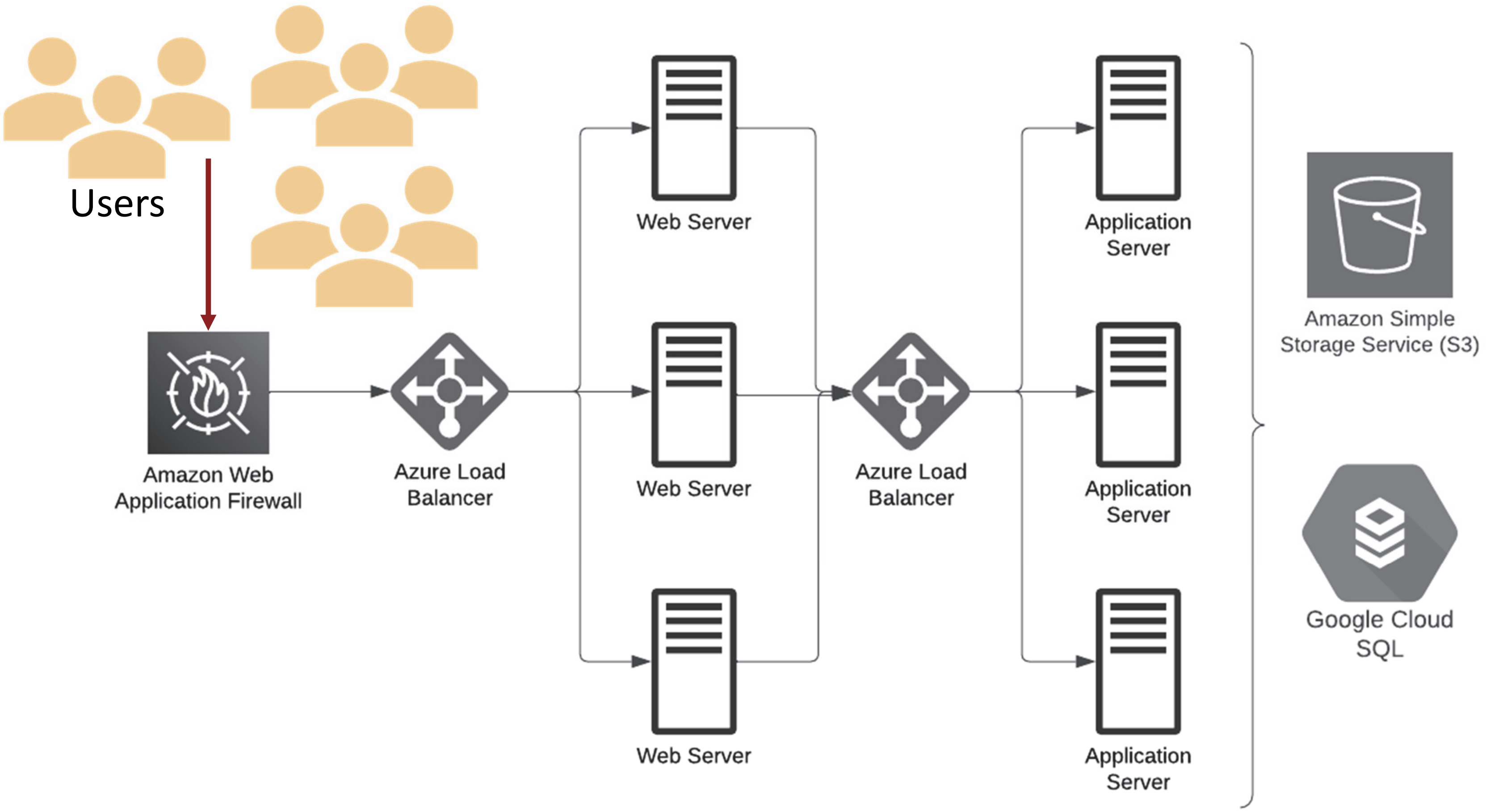


James (aws)

```
~ $ aws dynamodb wizard new-table
Enter the name of the table: MyTable
Enter the name of the primary key: pk
Primary key type
Add a sort key?
Select the read/write capacity mode.
Select Server-side encryption settings for your DynamoDB table
  DEFAULT
  KMS - AWS managed CMK
> KMS - Customer managed CMK
```

API: Application Programming Interface; **CSP:** Cloud Service Provider; **T&E:** Test and Evaluation; **VPN:** Virtual Private Network

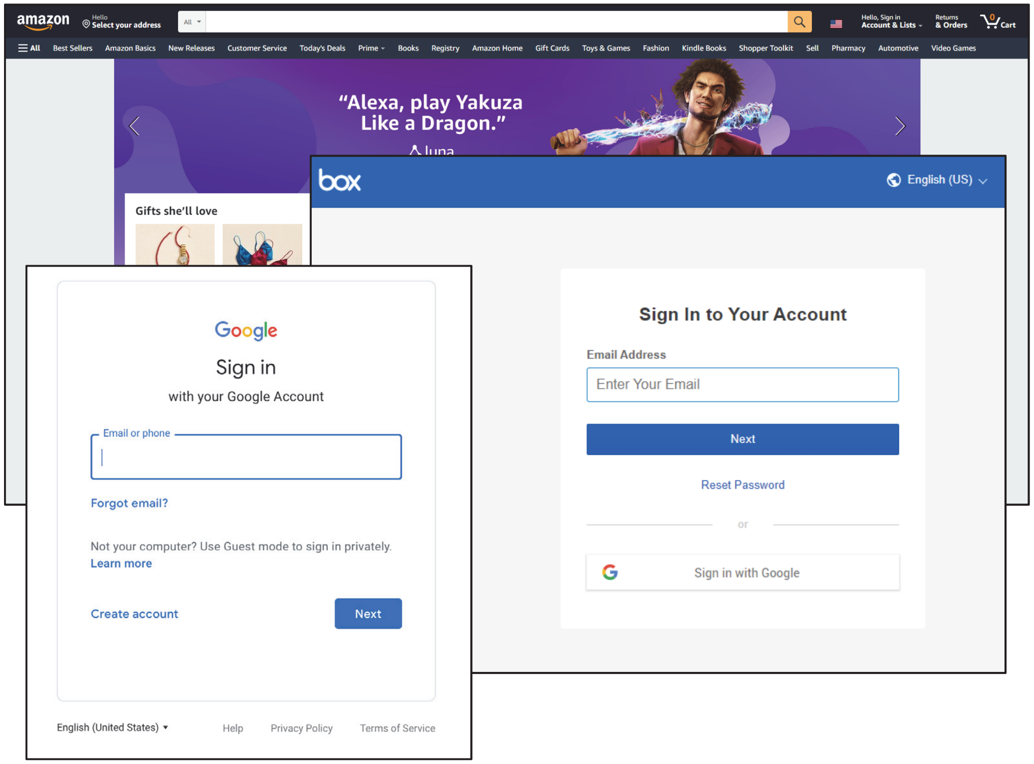
Users typically access cloud resources through an external web page



Exploitable web interfaces could result in unauthorized access to cloud resources

OWASP Top Web Application Security Risks 2021
Broken Access Control
Cryptographic failures
Injection
Insecure Design
Security Misconfiguration
Vulnerable and Outdated Components
Identification and Authentication Failures
Software and Data Integrity Failures
Security Logging and Monitoring Failures
Server Side Request Forgery

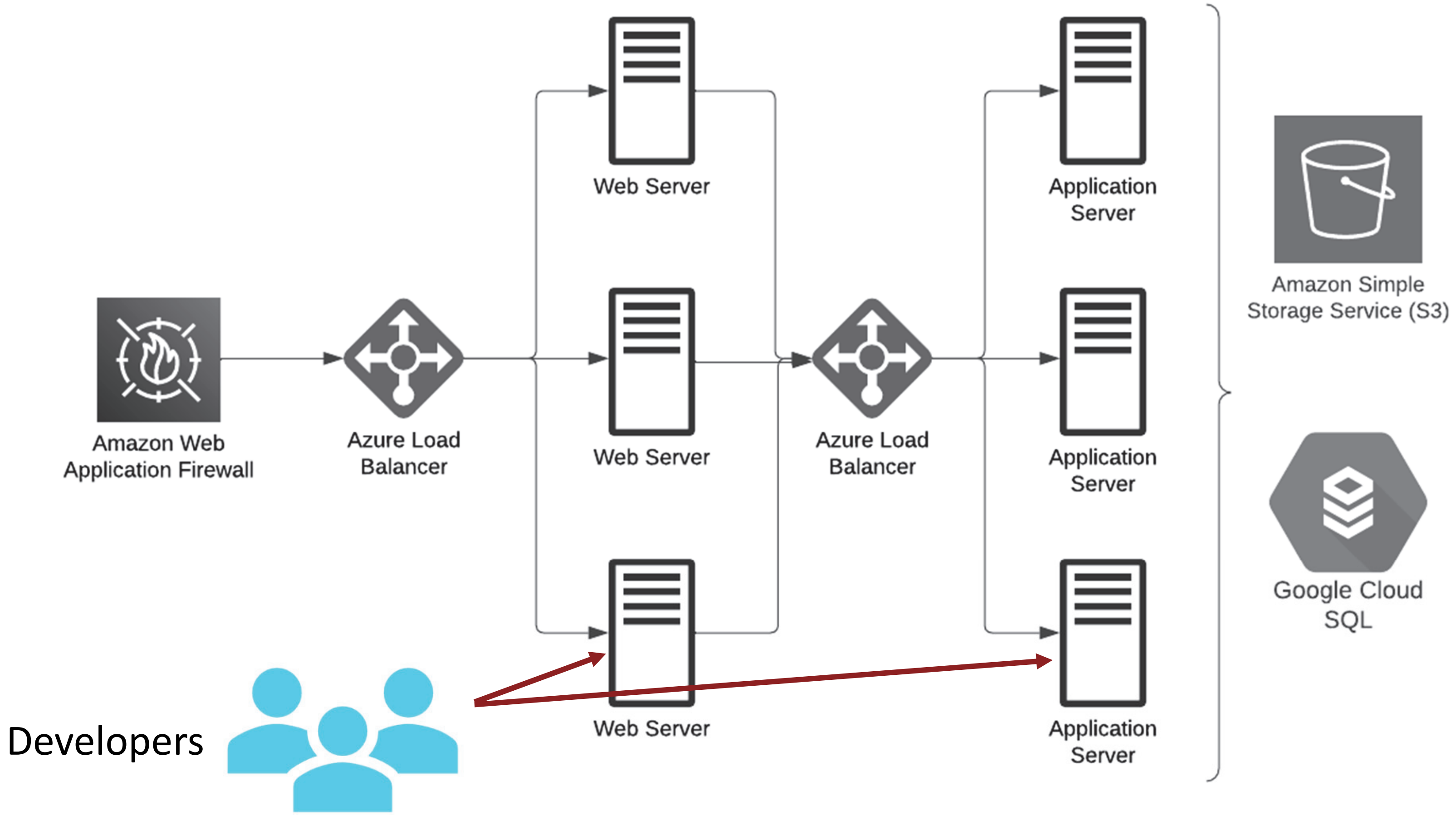
OWASP Top 10 2021 https://owasp.org/Top10/



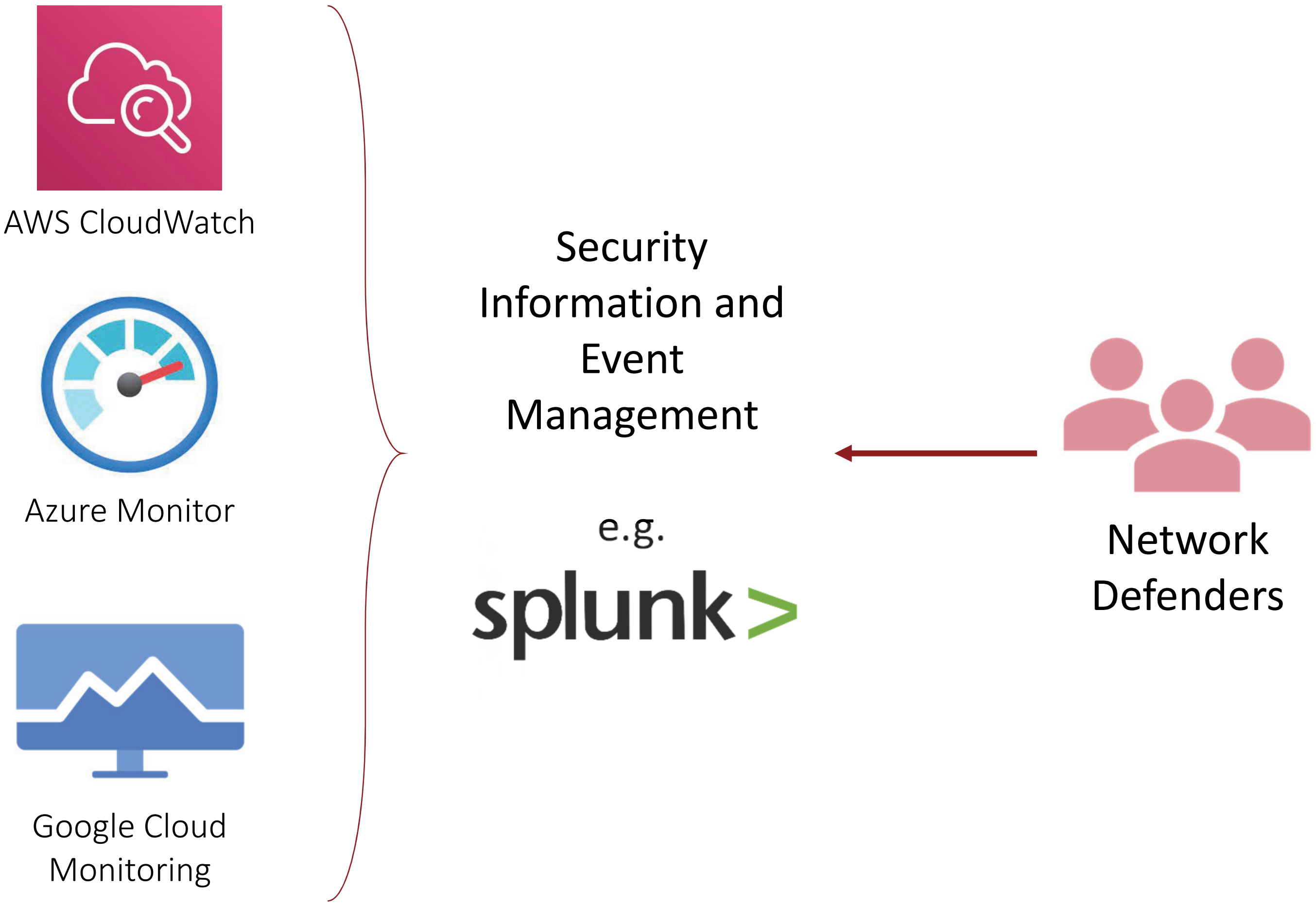
Not your computer? Use Guest mode to sign in privately.

OWASP: Open Web Application Security Project

Developers could have direct access to application servers to push updates



Defenders aggregate cloud security data, which integrate with enterprise monitoring



AWS CloudWatch

Azure Monitor

Google Cloud Monitoring

Security Information and Event Management

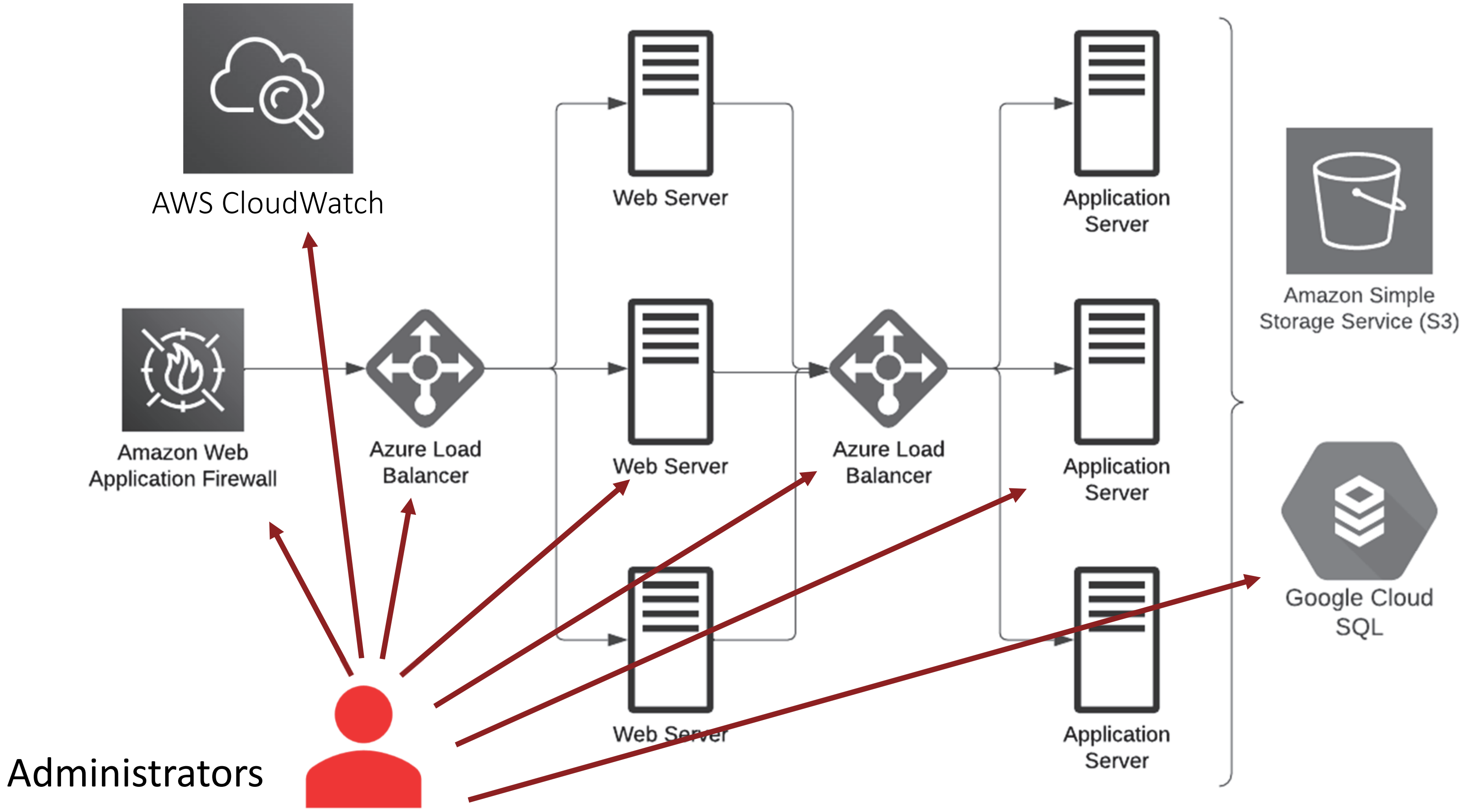
e.g.

splunk>

Network Defenders

AWS: Amazon Web Services

Administrators need to manage and configure all cloud services



Command Line Interfaces (CLIs) enable a credentialed user to manage services

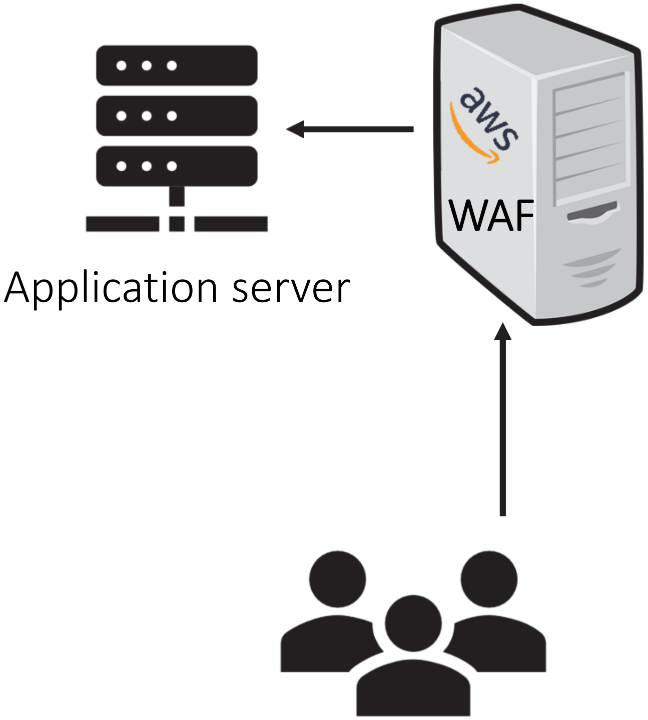
- Includes the ability to:
  - Read and write to storage and databases
  - Create new cloud assets
  - Destroy cloud assets
  - Modify security groups and access
  - Configure services
  - Perform essentially any action within a user's defined privileges
- AWS CLI, for example, requires three pieces of information:
  - AWS Access Key ID: **`AKIAIOSFODNN7EXAMPLE`**
  - AWS Secret Access Key: **`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`**
  - AWS Region: **`us-east-1`**
  - Optionally: Session token, that allows user to assume role of EC2

The CLI can be an extraordinarily convenient administrative tool – or an adversary's weapon to exploit a system

AWS: Amazon Web Services; **EC2**: Elastic Compute Cloud

The Capital One hack allowed uncredentialed outsiders to collect privileged AWS credentials

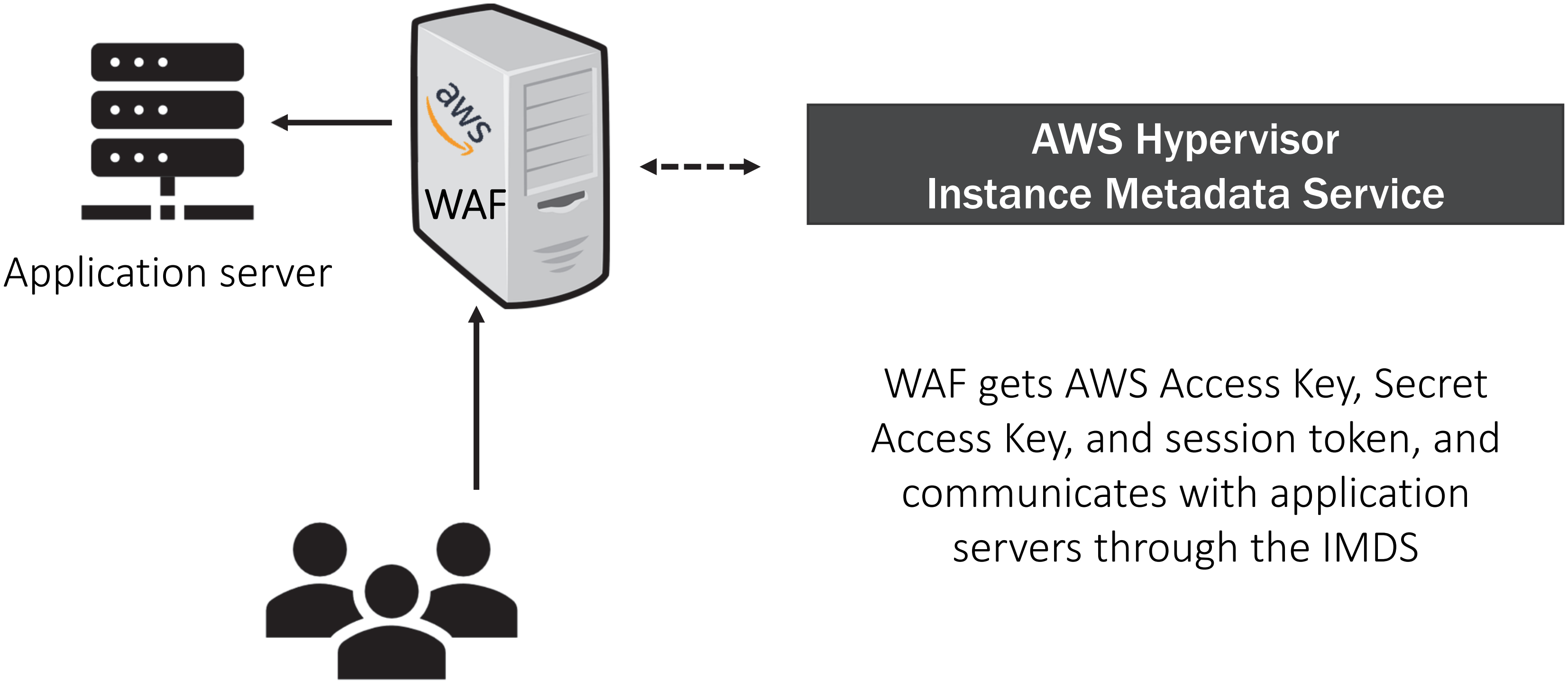
Capital One ran a web application firewall hosted in an EC2 that aimed to prevent certain attacks from hitting their applications



AWS: Amazon Web Services; EC2: Elastic Compute Cloud; HTTP: Hypertext Transfer Protocol; WAF: Web Application Firewall

The Capital One hack allowed uncredentialed outsiders to collect privileged AWS credentials

Capital One ran a web application firewall hosted in an EC2 that aimed to prevent certain attacks from hitting their applications

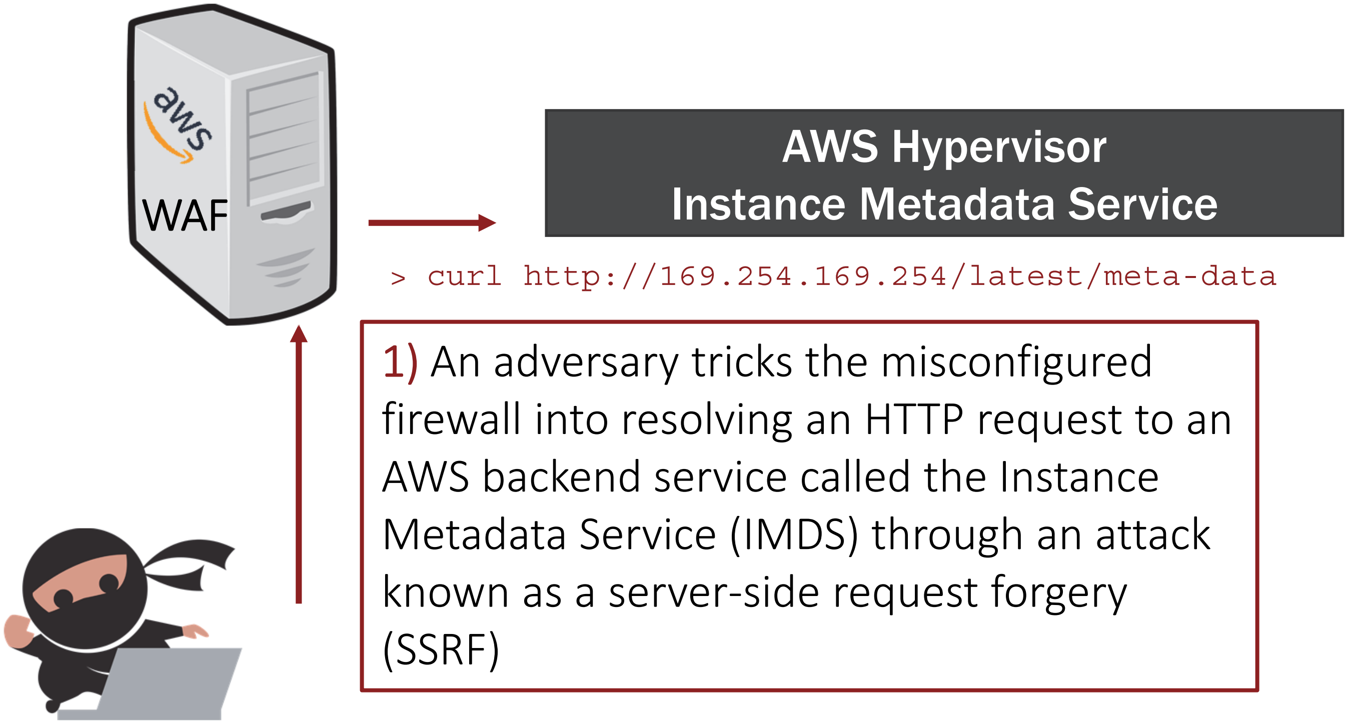


WAF gets AWS Access Key, Secret Access Key, and session token, and communicates with application servers through the IMDS

AWS: Amazon Web Services; **EC2**: Elastic Compute Cloud; **HTTP**: Hypertext Transfer Protocol; **IMDS**: Instance Metadata Service; **WAF**: Web Application Firewall

The Capital One hack allowed uncredentialed outsiders to collect privileged AWS credentials

Capital One ran a web application firewall hosted in an EC2 that aimed to prevent certain attacks from hitting their applications



AWS Hypervisor
Instance Metadata Service

```
> curl http://169.254.169.254/latest/meta-data
```

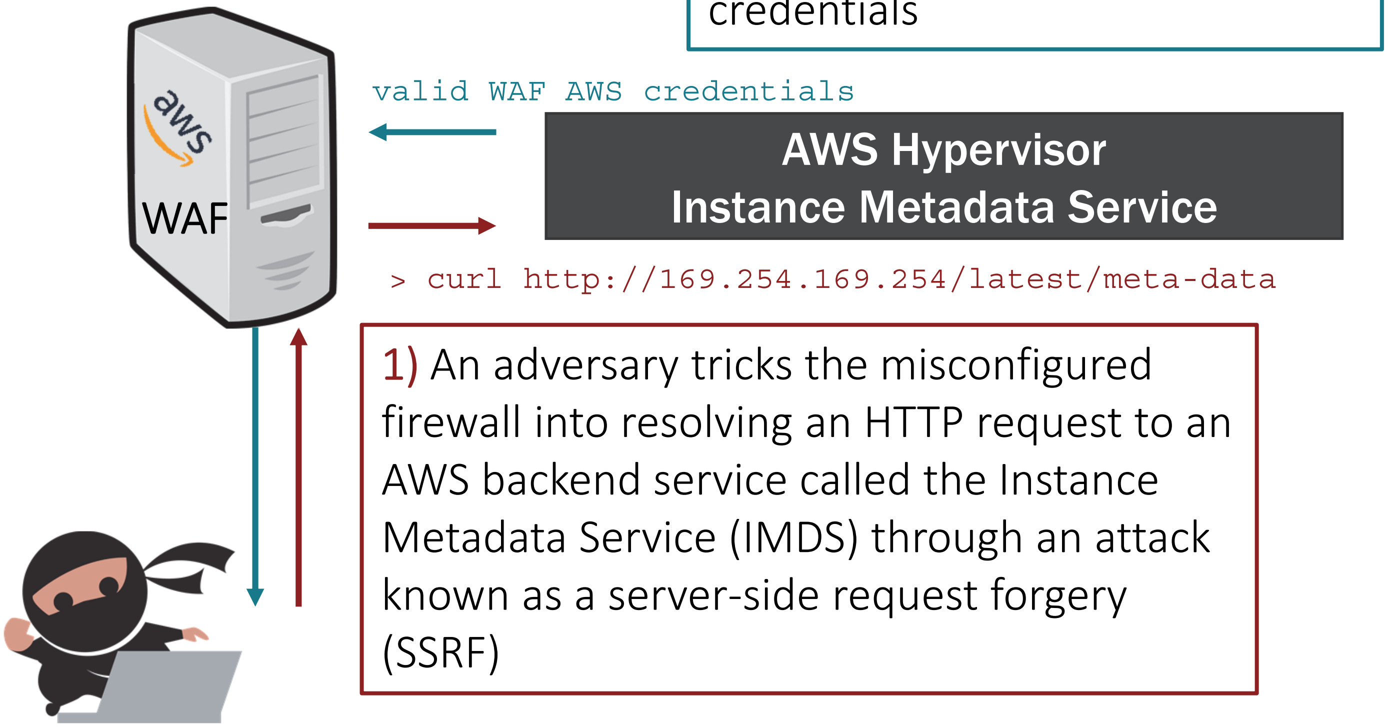
1) An adversary tricks the misconfigured firewall into resolving an HTTP request to an AWS backend service called the Instance Metadata Service (IMDS) through an attack known as a server-side request forgery (SSRF)

AWS: Amazon Web Services; **EC2**: Elastic Compute Cloud; **HTTP**: Hypertext Transfer Protocol; **WAF**: Web Application Firewall

The Capital One hack allowed uncredentialed outsiders to collect privileged AWS credentials

Capital One ran a web application firewall hosted in an EC2 that aimed to prevent certain attacks from hitting their applications

2) Instance Metadata Service provides the WAF (and adversary) with the firewall's AWS session credentials

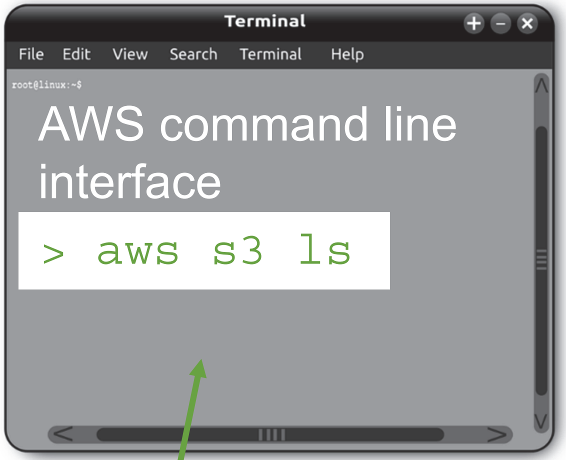


```
> curl http://169.254.169.254/latest/meta-data
```

1) An adversary tricks the misconfigured firewall into resolving an HTTP request to an AWS backend service called the Instance Metadata Service (IMDS) through an attack known as a server-side request forgery (SSRF)

AWS: Amazon Web Services; **EC2**: Elastic Compute Cloud; **HTTP**: Hypertext Transfer Protocol; **WAF**: Web Application Firewall

With valid credentials, an adversary can enumerate their access within AWS



AWS command line interface

```
> aws s3 ls
```

3) With valid WAF credentials, the adversary has its privileges, which were overloaded and could retrieve the contents of S3 buckets

The adversary exfiltrated bank account information, social security numbers, and personally identifiable information for 100 million customers.

Capital One paid an $80M fine and settled a $190M class-action lawsuit.

AWS: Amazon Web Services; **S3:** Simple Storage Service; **WAF:** Web Application Firewall

Though this is a simple vulnerability, testers need an understanding of AWS architecture to discover it

- AWS was not found responsible for this breach – Capital One failed to properly configure their web application firewall
- Still, AWS developed some improvements to the IMDS and released version 2
- However, IMDSv1 is still enabled by default for backward compatibility among customers and integrated 3rd party services

This is an example for one cloud service offering – testers need familiarity with all of those deployed as part of a system under test

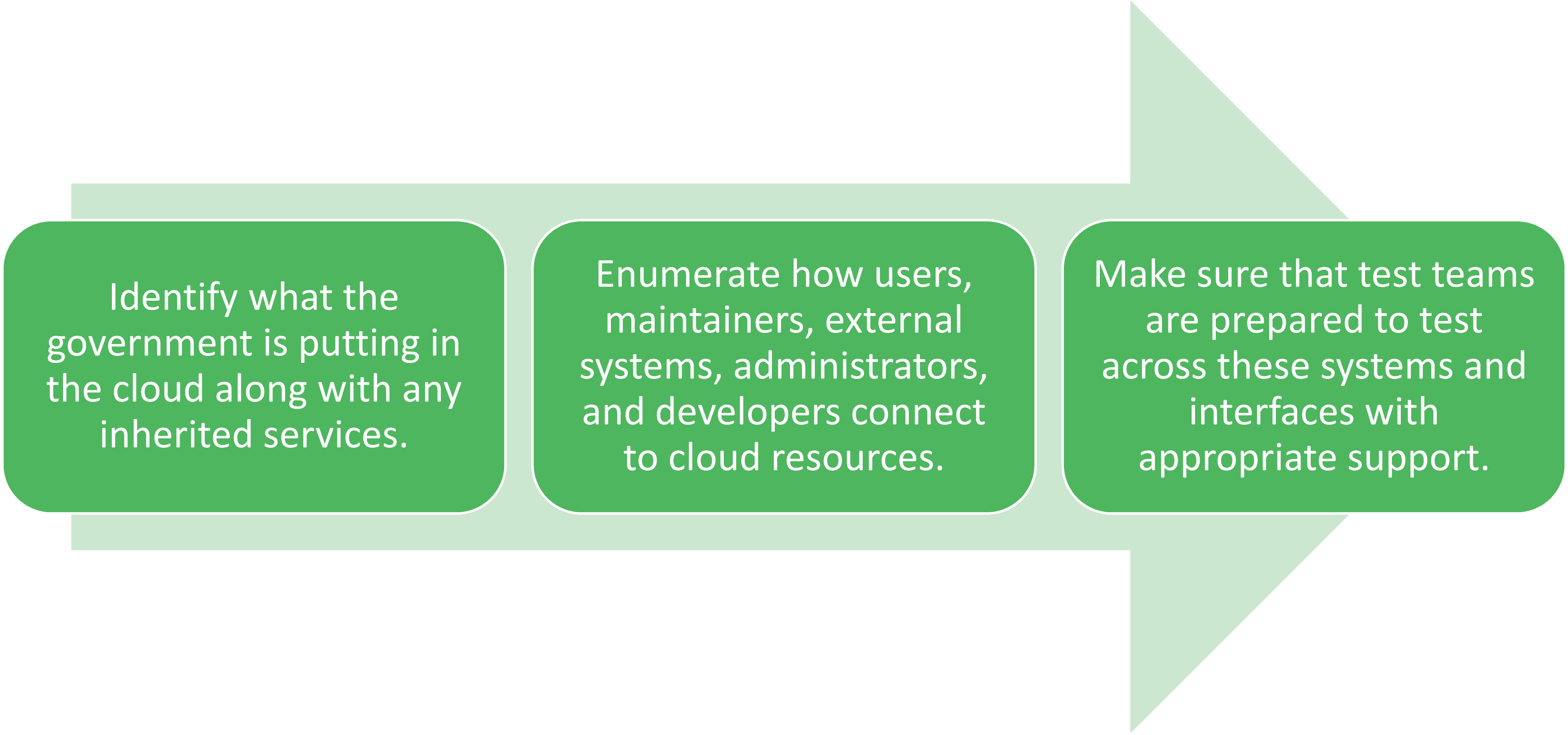
AWS: Amazon Web Services; CSO: Cloud Service Offering; IMDS: Instance Metadata Service

Test planning adjusts slightly to gather relevant information and resources

Prior to test:
List CSP services that are used within the system's environment, e.g. AWS S3, Azure SQL Database, Google Cloud Workflows
Identify any container images used to deploy applications in production so test teams may conduct scans
Enumerate interfaces to the system under test, e.g. web pages, VPN tunnels, CSP direct connections, APIs, etc.
Understand how cloud metadata and traffic is monitored, alerted, and blocked with the integration of network defenders
Ensure that the test team has sufficient familiarity with the CSP being used during test, and request augmented support otherwise
Coordinate subject matter expertise for the system under test– possibly a development contractor engineering lead

API: Application Programming Interface; **AWS:** Amazon Web Services; **CSP:** Cloud Service Provider; **S3:** Simple Storage Service; **SQL:** Structured Query Language; **VPN**: Virtual Private Network

Good testing hinges on smart and thorough planning



Identify what the government is putting in the cloud along with any inherited services.

Enumerate how users, maintainers, external systems, administrators, and developers connect to cloud resources.

Make sure that test teams are prepared to test across these systems and interfaces with appropriate support.

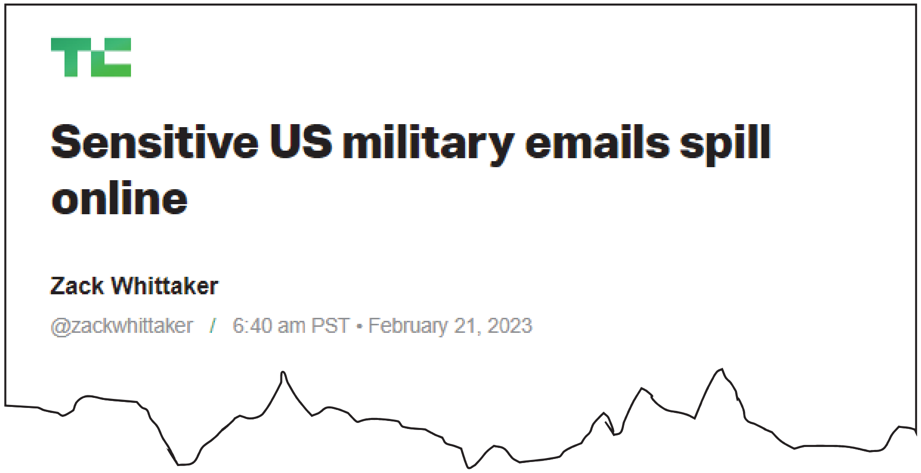
This process is no different than any other cyber test!

However, the details differ and test stakeholders need to be aware of the differences inherent to operating in the cloud.

Thanks for your attention, and happy to take any questions!

Backups

DoD unfortunately has a track record of leaving cloud resources unsecured



TC

Sensitive US military emails spill online

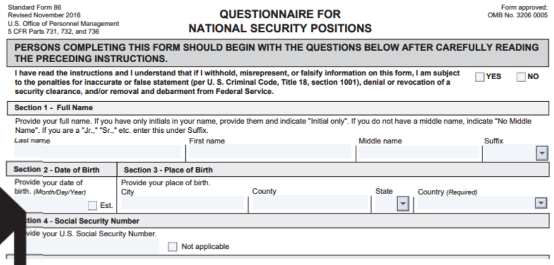
Zack Whittaker

@zackwhittaker / 6:40 am PST • February 21, 2023

https://techcrunch.com/2023/02/21/sensitive-united-states-military-emails-spill-online/

USSOCOM needed a new email server, so they bought Azure compute resources and created an email server

The customer misconfigured the server and allowed password-less logon for two weeks, and a security researcher could exfiltrate unclassified emails including one with a filled out SF-86



Standard Form 86
Revised November 2016
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR
NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U. S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service. □ YES □ NO

Section 1 - Full Name

Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix.

Last name	First name	Middle name	Suffix
			▾

Section 2 - Date of Birth

Provide your date of birth. *(Month/Day/Year)* □ Est.

Section 3 - Place of Birth

Provide your place of birth.

City	County	State	Country *(Required)*
		▾	▾

tion 4 - Social Security Number

vide your U.S. Social Security Number. □ Not applicable

USSOCOM: US Special Operations Command; **SF**: standard form

DoD unfortunately has a track record of leaving cloud resources unsecured

TC

Sensit

online

Zack Whittak

https://techcrunch

QUESTIONNAIRE FOR
NATIONAL SECURITY POSITIONS

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

“USSOCOM spokesperson Ken McGraw said in an email on Tuesday that an investigation, which began Monday, is under way. **“We can confirm at this point is no one hacked U.S. Special Operations Command’s information systems,”** said McGraw.

It’s not known if anyone other than [the security researcher] found the exposed data during the two-week window that the cloud server was accessible from the internet. **TechCrunch asked the Department of Defense if it has the technical ability, such as logs, to detect any evidence of improper access or data exfiltration from the database, but the spokesperson did not say.”**

the

owed

logon for

nd a

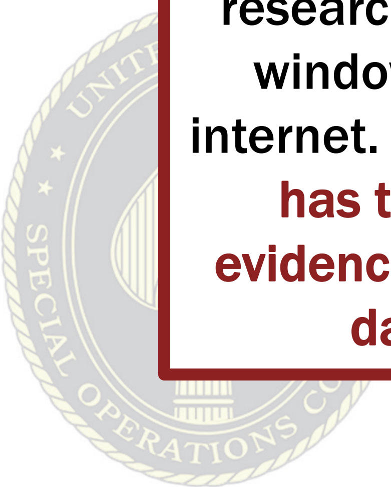
rcher

e

mails

with a

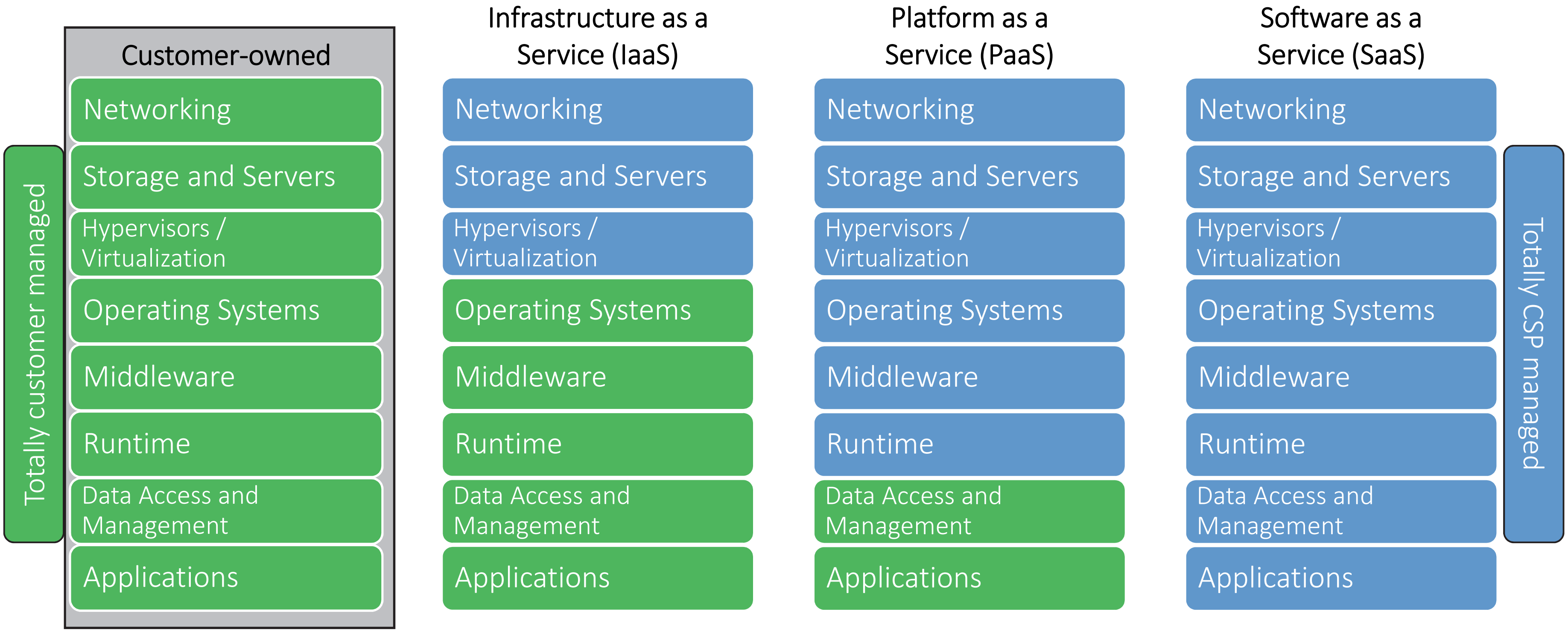
6



compute resources and created an email server

USSOCOM: US Special Operations Command; SF: standard form

Cloud solutions typically align to one of three deployment models, where each relinquishes some responsibility to the CSP



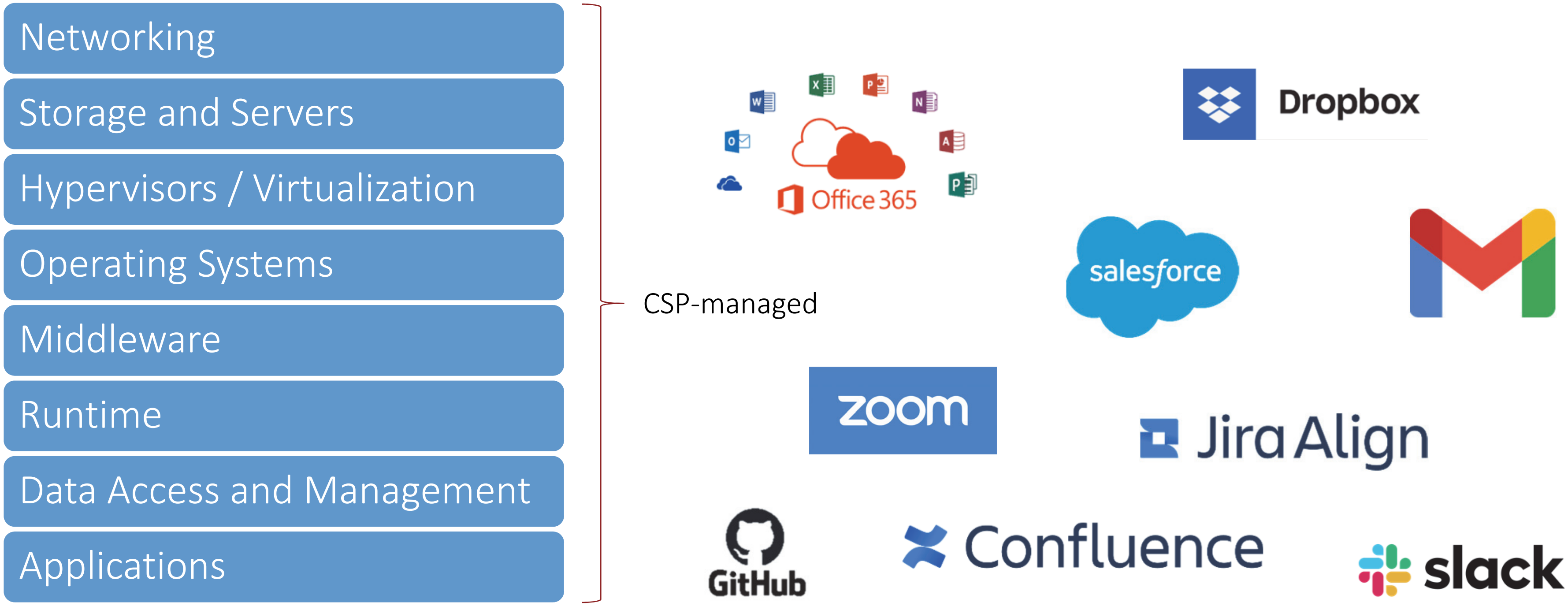
Totally customer managed

Totally CSP managed

Customer-owned	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟩 Storage and Servers	🟦 Storage and Servers	🟦 Storage and Servers	🟦 Storage and Servers
🟩 Hypervisors / Virtualization	🟦 Hypervisors / Virtualization	🟦 Hypervisors / Virtualization	🟦 Hypervisors / Virtualization
🟩 Operating Systems	🟩 Operating Systems	🟦 Operating Systems	🟦 Operating Systems
🟩 Middleware	🟩 Middleware	🟦 Middleware	🟦 Middleware
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Data Access and Management	🟩 Data Access and Management	🟩 Data Access and Management	🟦 Data Access and Management
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications

Acronyms: CSP: cloud service provider

SaaS solutions are entirely managed by the CSP, leaving the customer to manage configurations, data exchange, integration, and access control



Networking

Storage and Servers

Hypervisors / Virtualization

Operating Systems

Middleware

Runtime

Data Access and Management

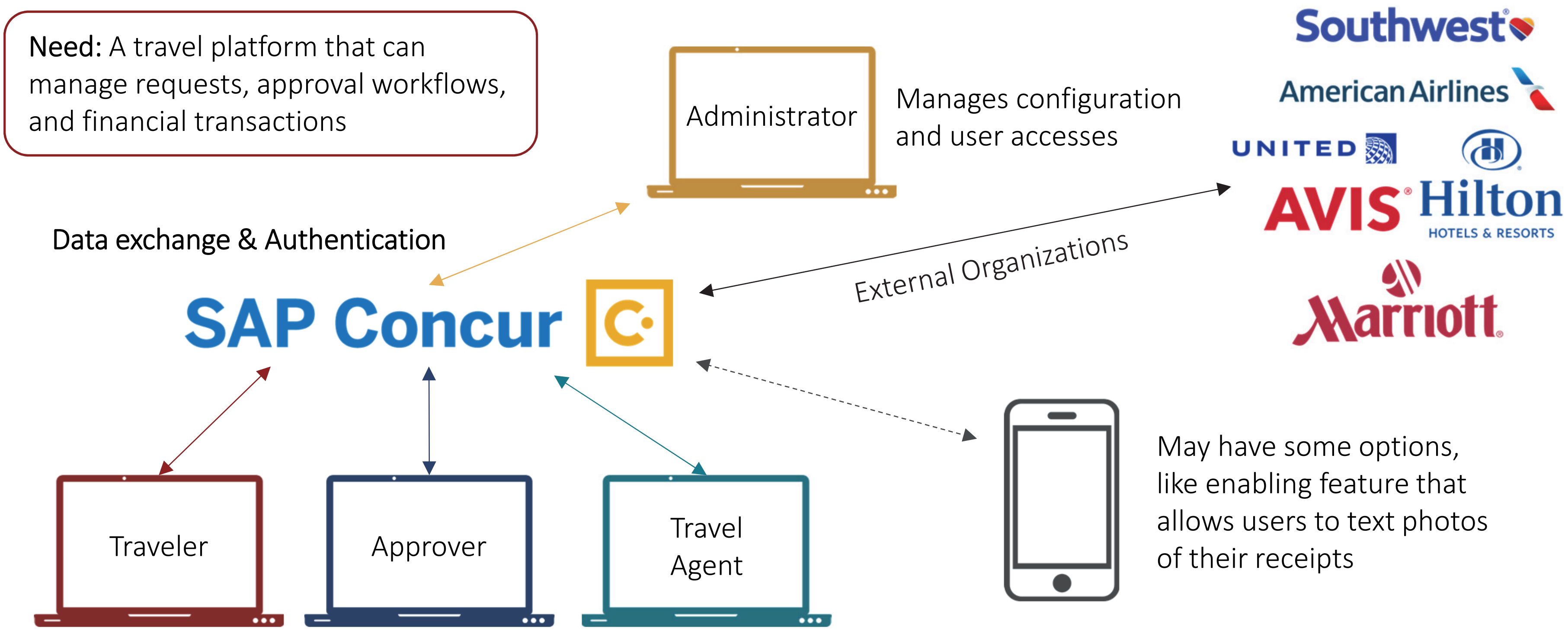
Applications

CSP-managed

Acronyms: **CSP:** Cloud Service Provider; **SaaS:** Software as a Service

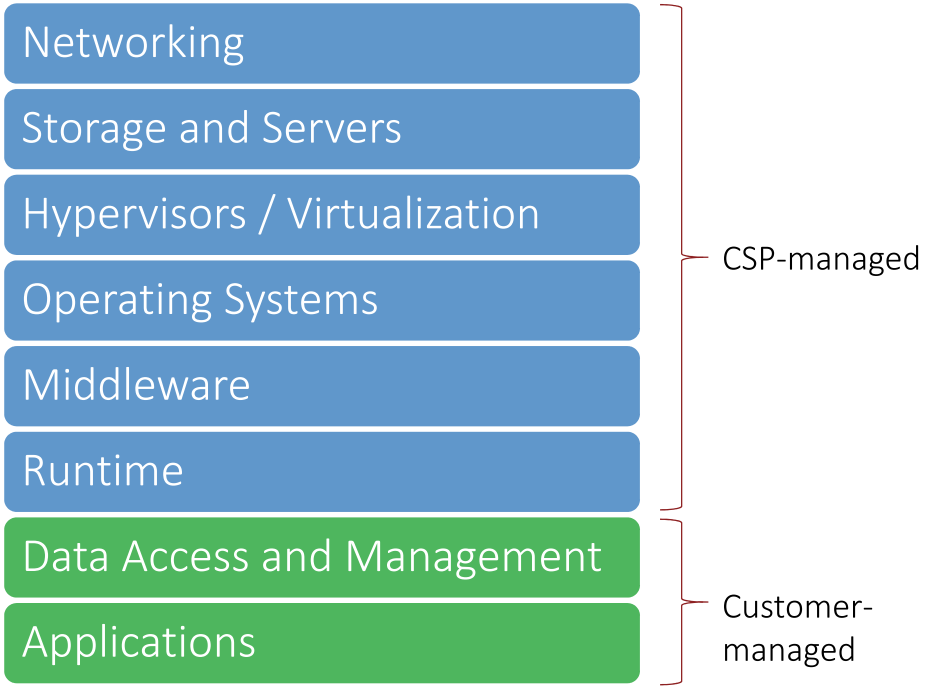
SaaS products are for specialized needs that do not require extensive customization or development – "plug and play"

Need: A travel platform that can manage requests, approval workflows, and financial transactions


Administrator
Manages configuration and user accesses
Data exchange & Authentication
SAP Concur
External Organizations
Southwest
American Airlines
UNITED
AVIS
Hilton HOTELS & RESORTS
Marriott
Traveler
Approver
Travel Agent
May have some options, like enabling feature that allows users to text photos of their receipts

Acronyms: **SaaS:** software as a service

PaaS allows a customer to focus on developing a specialized application by leveraging a service that manages infrastructure and scaling



Networking

Storage and Servers

Hypervisors / Virtualization

Operating Systems

Middleware

Runtime

Data Access and Management

Applications

CSP-managed

Customer-managed

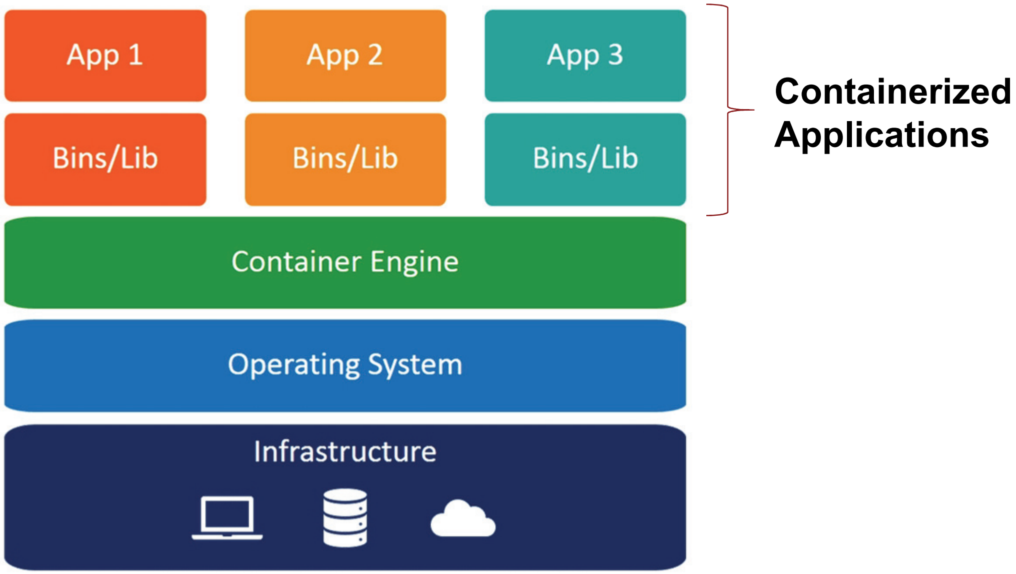
Acronyms: **CSP:** Cloud Service Provider; **PaaS:** Platform as a Service

Modern PaaS solutions use containerization, a virtualization strategy that breaks functional components of code into isolated programs

Containerized applications can be created and destroyed on a seconds to minutes timescale.

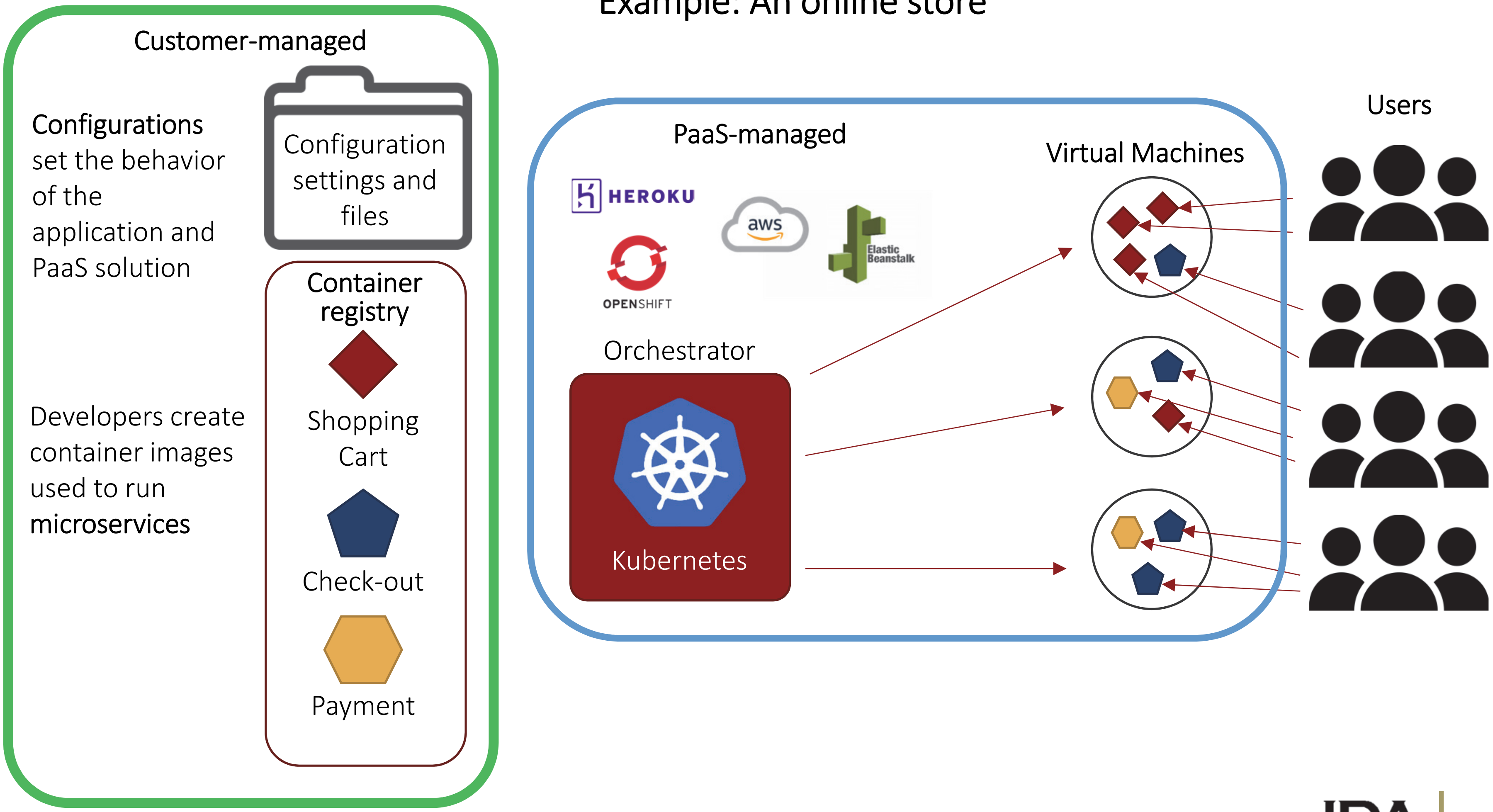
Due to the ephemeral nature of containers, deployment and management can be tricky; a PaaS solution will manage that for the developer so they can focus on the application.

Containers can also be nested inside virtual machines.



Acronyms: **PaaS:** Platform as a Service

PaaS solutions use orchestrators to balance user load and create or destroy containers based on user needs



Example: An online store

Customer-managed

Configurations set the behavior of the application and PaaS solution

Configuration settings and files

Developers create container images used to run **microservices**

Container registry

Shopping Cart

Check-out

Payment

PaaS-managed

Orchestrator

Kubernetes

Virtual Machines

Users

Acronyms: **PaaS:** Platform as a Service

CSPs now provide “serverless” functions which allow customers to create code that executes on an event-driven basis

The customer:

- Writes code and selects runtime
- Sets trigger, like inputs through APIs
- Specifies access to other systems, like databases
- Monitors code execution

```
<li><a href="index.html">Home</a></li>
<li><a href="home-events.html">Home Events</a></li>
<li><a href="multi-col-menu.html">Multiple Column Menu on Larger Viewport
<li class="has-children"> <a href="#" class="current">Header Options</a>
    <ul>
        <li><a href="tall-button-header.html">Tall Button Header</a></l
        <li><a href="image-logo.html">Image Logo</a></li>
        <li class="active"><a href="tall-logo.html">Tall Logo Image</a
    </ul>
</li>
<li class="has-children"> <a href="#">Carousels</a>
    <ul>
        <li><a href="variable-width-slider.html">Variable Image Wi
        <li><a href="testimonial-slider.html">Testimonial Slider</
        <li><a href="featured-work-slider.html">Featured Work Sli
        <li><a href="equal-column-slider.html">Equal Column Slid
        <li><a href="video-slider.html">Video Slider</a></li>
        <li><a href="mini-bootstrap-carousel.html">Mini Slider
    </ul>
</li>
```

The CSP:

- Provides customer unique execution environment
- Charges per function call and time used
- Integrates functions with CSP monitoring solutions, databases, and other services

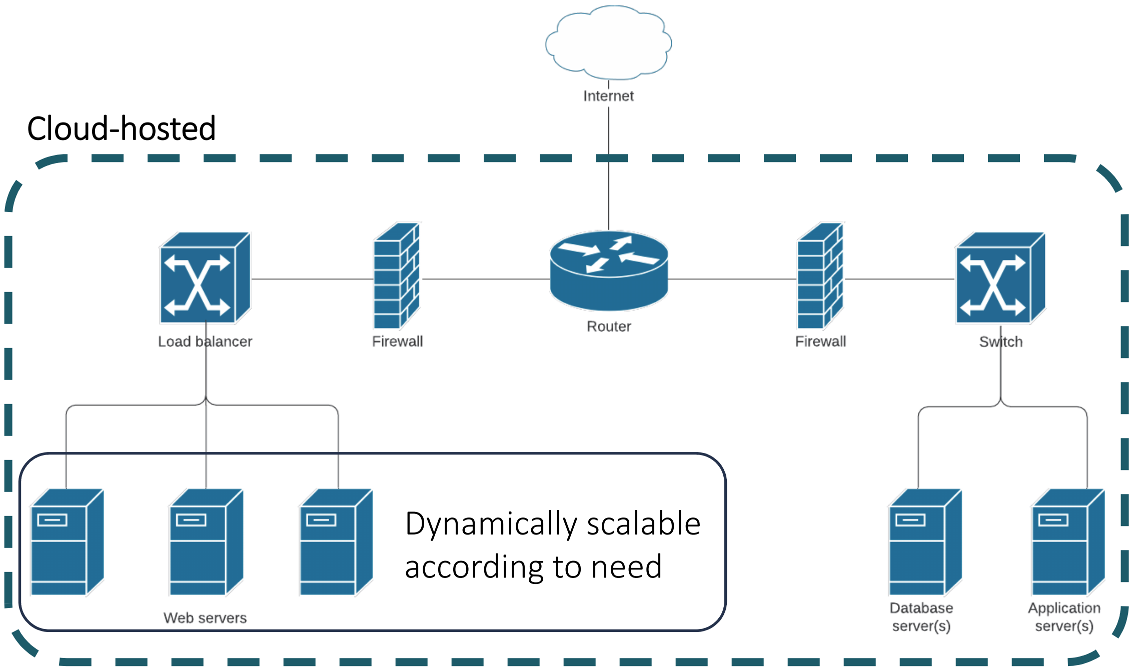
Azure Functions

AWS Lambda

GCP Cloud Functions

Acronyms: **API:** Application Programming Interface; **AWS:** Amazon Web Services; **CSP:** Cloud Service Provider; **GCP:** Google Cloud Platform

IaaS solutions still require considerable configuration and management efforts on the part of the customer



Knowing how the cloud environment is managed is critical to planning and executing an adequate cyber assessment.

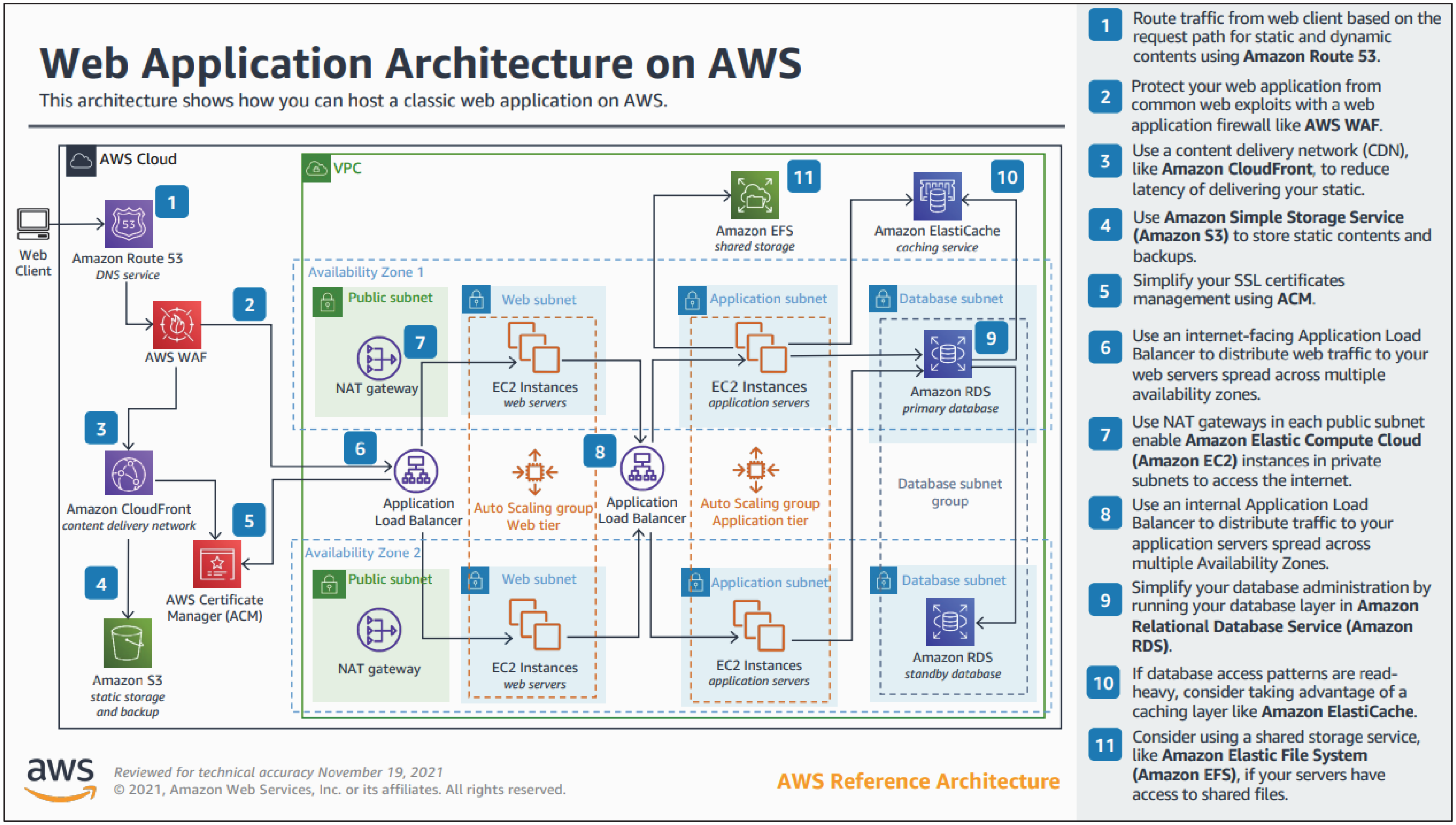
Cloud customer responsibilities:

- Purchase and maintain hardware
- Provision and configure virtual assets, including region and redundancy
- Manage cloud administrator and system privileges
- Manage network infrastructure and configure virtual network access
- Physically connect devices
- Install operating systems and manage configurations for each server
- Manage applications and files on all devices
- Manage access controls for users and administrators of servers
- Monitor and defend against malicious actors

Acronyms: **IaaS:** Infrastructure as a Service

Gray text	=	No longer a customer responsibility
Blue text	=	New customer responsibility
Black text	=	Continuing customer responsibility

CSPs provide native services to simplify the development and maintenance of a cloud solution



Web Application Architecture on AWS

This architecture shows how you can host a classic web application on AWS.

1. Route traffic from web client based on the request path for static and dynamic contents using **Amazon Route 53**.
2. Protect your web application from common web exploits with a web application firewall like **AWS WAF**.
3. Use a content delivery network (CDN), like **Amazon CloudFront**, to reduce latency of delivering your static.
4. Use **Amazon Simple Storage Service (Amazon S3)** to store static contents and backups.
5. Simplify your SSL certificates management using **ACM**.
6. Use an internet-facing Application Load Balancer to distribute web traffic to your web servers spread across multiple availability zones.
7. Use NAT gateways in each public subnet enable **Amazon Elastic Compute Cloud (Amazon EC2)** instances in private subnets to access the internet.
8. Use an internal Application Load Balancer to distribute traffic to your application servers spread across multiple Availability Zones.
9. Simplify your database administration by running your database layer in **Amazon Relational Database Service (Amazon RDS)**.
10. If database access patterns are read-heavy, consider taking advantage of a caching layer like **Amazon ElastiCache**.
11. Consider using a shared storage service, like **Amazon Elastic File System (Amazon EFS)**, if your servers have access to shared files.

aws

Reviewed for technical accuracy November 19, 2021

AWS Reference Architecture

Reference architecture pulled from https://aws.amazon.com/architecture/ on February 17, 2023

Acronyms: **AWS:** Amazon Web Services; **CSP:** Cloud Service Provider

All CSPs provide a variety of services that require different levels of management from the CSP

On-premises	Amazon Web Services	Microsoft Azure	Google Cloud
Compute server	Elastic Compute Cloud (EC2)	Azure Virtual Machines	Compute Engine
Hardware Firewall	AWS Network Firewall	Azure Firewall	Cloud Firewall
Storage server	Simple Storage Service (S3), Elastic File System, Elastic Block Store	Azure Blob, Azure Files, Azure Disks	Cloud Storage, Filestore, Persistent Disk
Database server	Relational Database Service, Amazon DynamoDB, Elasticache	Azure SQL Database, Azure Cosmos DB, Azure Cache	Cloud SQL, Datastore, Memorystore
Application server	AWS Lambda	Azure Functions	Cloud Functions
Kubernetes servers	Elastic Kubernetes Service	Azure Kubernetes Service	Google Kubernetes Engine
Domain controller	Identity and Access Management	Azure Active Directory	Cloud Identity

Acronyms: **AWS:** Amazon Web Services; **CSP:** Cloud Service Provider; **DB**: database; **IaaS:** infrastructure as a service; **PaaS:** platform as a service; **SaaS:** software as a service; **SQL:** Structured Query Language

Security and performance-monitoring services are provided by CSPs, but need to be integrated by DOD

Monitoring Activity	Amazon Web Services	Microsoft Azure	Google Cloud
Logging at the platform level (e.g., administrative actions)	CloudTrail	Activity log	Cloud Audit Logs
Comprehensive solution for collecting, analyzing, and acting on telemetry, including logs, events, and metrics	CloudWatch	Monitor	Cloud Monitoring and Cloud Logging
Detect and investigate advanced attacks on-premises and in the cloud	GuardDuty	Defender	Security Command Center

- The above table is only a subset of monitoring tools and security solutions offered by AWS, Azure, and Google Cloud.
- These systems can be used on their own or integrated with other monitoring suites as network defenders choose.

T&E stakeholders must understand how defenders integrate these monitoring services to prevent and mitigate adversaries from exploiting networks.

Acronyms: **AWS:** Amazon Web Services; **CSP:** Cloud Service Provider; **T&E:** Test and Evaluation

CSPs use instance metadata services to locally provide credentials to virtual machines

- Rather than hard code credentials into each EC2 instance, AWS provides an instance metadata service that allows the virtual hosts to request credentials from the AWS hypervisor before interacting with other AWS services, like S3 or databases
- IMDSv1 functions through a simple HTTP `GET` request
  - i.e. `curl http://169.254.169.254/latest/meta-data`
- This simplifies scaling and reduces the infrastructure needed to manage identity and access
- However, it introduces a potential attack vector via server-side request forgery, where an adversary can manipulate a web-facing EC2 to return requests to the IMDS and recover valid credentials
- The implementations vary among CSPs, but all of them leverage some sort of instance metadata service

Acronyms: AWS: Amazon Web Services; CSP: Cloud Service Provider; EC2: Elastic Compute Cloud; IMDS: Instance Metadata Service; S3: Simple Storage Service

In response to the Capital One breach, AWS tightened security in IMDS version 2

- GuardDuty alerts when EC2 instances make CLI calls from external IPs
- IMDSv2 is now a two-step process: 1) `PUT` request to obtain a token from the IMDS; 2) `GET` request with token in header to retrieve metadata
  - Many web application firewalls do not allow `PUT` requests, so server-side request forgeries that do include those can be filtered
- By default, IMDSv2 limits time to live for token responses to one server hop, so the token should not be recoverable through server-side request forgery – the IP packet is dropped after the hop from IMDSv2 to the EC2 and cannot escape AWS
- Some reverse proxy servers use an `x-Forwarded-For` header that passes the IP of the client. IMDSv2 rejects any token requests with this header
- However, IMDSv1 is still enabled by default, as legacy 3rd party services or code may not be updated to use the new schema

Acronyms: AWS: Amazon Web Services; CLI: Command Line Interface; EC2: Elastic Compute Cloud; IMDS: Instance Metadata Service; IP: Internet Protocol

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* XX-04-2023	**2. REPORT TYPE** Final	**3. DATES COVERED** *(From - To)* Apr 2023

4. TITLE AND SUBTITLE DATAWorks 2023: Preparing for Public Sector Test and Evaluation in the Commercial Cloud	**5a. CONTRACT NUMBER** HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Dr. Brian T. Conway Dr. Stacey L. Allison	**5d. PROJECT NUMBER** BD-09-2299(94)
	5e. TASK NUMBER 229994
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Institute for Defense Analyses 730 East Glebe Road Alexandria, Virginia 22305	**8. PERFORMING ORGANIZATION REPORT NUMBER** NS D-33391 H 2023-000040
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Tye Botting

14. ABSTRACT

As the public sector shifts IT infrastructure toward commercial cloud solutions, the government test community needs to adjust its test and evaluation (T&E) methods to provide useful insights into a cloud-hosted system's cyber posture. Government entities must protect what they develop in the cloud by enforcing strict access controls and deploying securely configured virtual assets. However, publicly available research shows that doing so effectively is difficult, with accidental misconfigurations leading to the most commonly observed exploitations of cloud-hosted systems. Unique deployment configurations and identity and access management across different cloud service providers increases the burden of knowledge on testers. More care must be taken during the T&E planning process to ensure that test teams are poised to succeed in understanding the cyber posture of cloud-hosted systems and finding any vulnerabilities present in those systems. The T&E community must adapt to this new paradigm of cloud-hosted systems to ensure that vulnerabilities are discovered and mitigated before an adversary has the opportunity to use those vulnerabilities against the system.

15. SUBJECT TERMS

cloud; Cybersecurity Operational Tests; Director, Operational Test and Evaluation

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Tye W. Botting
Unclassified	Unclassified	Unclassified	SAR	61	**19b. TELEPHONE NUMBER** *(Include area code)* (703) 845-2050