SANS CLOUD SECURITY

Secure Service Configuration in AWS, Azure, and Google Cloud

sans.org/cloud-security

Introduction

Multiple clouds require multiple solutions. In an ideal world, you could learn the core concepts of cloud computing and apply them to whatever cloud provider your organization uses. Unfortunately, we live in a world where each of the top three most popular cloud platforms, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, radically differ from one to another in both design and implementation. These differences affect how security professionals must operate in each environment.

This poster compares and contrasts the popular security services of the top 3 cloud providers. By identifying insecure defaults and little-known security features, you can ensure the security of your organization's assets across each public cloud environment.

As SANS and other members of the security community point out insecure defaults, cloud providers have slowly corrected them. Certain assessment criteria may become unnecessary with time. For the latest details, view the digital version of this poster: **sans.org/big-3-cloud-config**

While there are vast differences between the terminology and nuances of each cloud, the fundamental principles remain the same. You can apply concepts from cloud-specific benchmarks to all three providers.

The contents of this poster are based on material from SEC510: Attack-Driven Cloud Security Controls and Mitigations, as well as the Center for Internet Security Benchmarks. CSP versions used in this poster are: AWS v1.4.0, Azure v1.4.0, and GCP v1.3.0

For more information, visit **sans.org/sec510**.

For the GIAC Public Cloud Security certification, visit **giac.org/gpcs**.

Cloud Services

Network Assessment

AWS Default VPC Assessment Criteria
Benchmark 5.3 Ensure the default security group of every VPC restricts all traffic

1. Remove the default VPC from each region
2. Modify the default VPC Network ACL
   - Remove the default ingress/egress rules
3. Modify the default security group in each region
   - Remove the default ingress/egress rules
4. Create custom VPC resources per service

Azure Network Assessment Criteria
Benchmark 6: Networking Security

6.1: Ensure that RDP access is restricted from the Internet
6.2: Ensure that SSH access is restricted from the Internet
6.3: Ensure that SQL databases do not allow ingress 0.0.0.0/0 (Any IP)

GCP Network Assessment Criteria
Benchmark 3: Networking

3.1: Ensure that the default network does not exist in a project
3.6: Ensure that SSH access is restricted from the Internet
3.7: Ensure that RDP access is restricted from the Internet

Network Flow Logging

AWS Network Logging Assessment Criteria
Benchmark 3.8 Ensure that VPC Flow Logs is enabled for every subnet in a VPC network

1. Enable flow logging in every VPC
2. At a minimum, capture "Reject" packet data
3. Configure a 365-day minimum log retention period
4. Archive logs in long-term storage (e.g., S3/Glacier)

Azure Network Logging Assessment Criteria
Benchmark 6.4 Network Security Group flow logs should be enabled, and the retention period should be set to greater than or equal to 90 days

1. Enable the flow logs option in the Network Security Group
2. Create a storage account for flow log data
3. Configure a 365-day log retention period (90 minimum)

GCP Network Logging Assessment Criteria
Benchmark 3.9: Ensure that VPC Flow logs is enabled for every subnet in VPC Network

1. View the VPC service and enumerate each subnet
2. Set each subnet's flow log attribute to true
3. Be aware of the sampling rate

Private Cloud Access

Advanced Remote Access Assessment Criteria
Require multiple factors of authentication for remote administrative access

1. Block all SSH/RDP access from the public Internet
2. Enable advanced remote access cloud services
3. Securely access cloud resources through a VPN gateway or a private direct connection

Serverless Assessment

Cloud Serverless Assessment Criteria
Review functions for the following security misconfigurations:

1. Scan functions for secrets management and persistence issues
2. Authenticate requests to publicly accessible functions
3. Use unique service accounts per function
4. Regularly audit function permissions for least privilege
5. Enable function audit and network controls (if available)

Data Encryption

Data Encryption Assessment Criteria
All data should be encrypted at rest and in-transit (there are extremely few exceptions)

Azure Database Service Encryption Assessment Criteria
Benchmark 4.1.2 Ensure that "Data encryption" is set to "On" on a SQL Database

4.6 Ensure SQL server's TDE protector is encrypted with Customermanaged key
4.4.1 Ensure "Enforce SSL connection" is set to "Enabled" for Standard MySQL Database Server
4.3.1 Ensure "Enforce SSL connection" is set to "ENABLED" for PostgreSQL Database Server

AWS KMS Audit Logging with CloudTrail
Benchmark 3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs

Storage Assessment

AWS S3 Assessment Criteria
Review S3 for the following security benchmarks:

1. Configure Block Public Access at the account level
2. Configure Block Public Access at the bucket level
3. Configure Server Access Logging for audit logging
4. Configure Object-level Logging into CloudTrail
5. Configure Default Encryption at the bucket level

Azure Storage Assessment Criteria
Benchmark 3: Storage Accounts

1. Enable the secure transfer required attribute
2. Rotate storage account access keys periodically
3. Configure logging for read, write, and delete requests
4. Expire Shared Access Signatures (SAS) tokens in less than 60 minutes
5. Ensure that SAS tokens require HTTPS connections
6. Configure Blob containers access level to Private

GCP Storage Assessment Criteria
Benchmark 5: Storage

1. Ensure that cloud storage buckets are not anonymous or publicly accessible
2. Ensure there are no publicly accessible objects in storage buckets
3. Ensure that logging is enabled for cloud storage buckets

Identity and Access Management (IAM)

AWS IAM Instance Role Assessment Criteria
Benchmark 1.18 Ensure IAM instance roles are used for AWS resource access from instances

1. Note that instances without a managed profile role often contain hard-coded credentials
2. Create a least privilege IAM role with permissions scoped
3. to the virtual machine's functional requirements
4. Verify each EC2 instance has an assigned "IAM Role"
5. gateway or a private direct connection

AWS IAM Administrative Assessment Criteria
Benchmark 1.16 Ensure IAM policies that allow full ":*" administrative privileges are not attached*

1. List all IAM policies in each account
2. Get the latest version for each policy
3. Filter by policies with the Effect attribute set to Allow
4. Identify policies with the Action and Resource attributes set to a wildcard (*)

Cryptographic Key Management

Assessment Criteria
Limit and audit all cryptographic key usage

1. Prevent individuals from decrypting production data;
2. only applications should have this permission
3. Record and audit all decryption events
4. Ensure that keys are rotated on a schedule
5. No one should be able to instantly delete a cryptographic key

Instance Metadata Service (IMDS)

Cloud Resource Hijacking
MITRE ATT&CK T1496: Consuming the victim's cloud resources to solve resource-intensive problems

- Cryptocurrency mining on cloud virtual machines
- Distributed denial-of-service (DDOS) attacks
- Password cracking on GPU virtual machines

Cloud Credential Management Assessment Criteria
Configure your Instance Metadata Service (IMDS) to be as inaccessible as possible

1. Turn off IMDS if the cloud infrastructure does
2. not need to access cloud-managed resources
3. Remove access to legacy versions of the IMDS
4. Require metadata tokens for AWS
5. Turn off GCP's v0.1 and v1beta1 IMDS
6. Limit the IP hops token responses to 1 (AWS only)

SERVICE COMPARISONS

DOWNLOAD POSTER NOW

Here is a comparison of each cloud's network traffic flow logging solutions. Download the digital poster for more comparisons of services in AWS, Azure, and GCP.

	Enabled by Default	Minimum Delay	Maximum Retention Period	Command Line Support	Log Blocked Ingress Traffic
AWS	NO	1-6 MINUTES	Indefinite	YES	YES
Azure	NO	10 MINUTES	Indefinite	Using Extension	YES
GCP	NO	5 SECONDS	3650 DAYS	YES	NO

About SEC510: Cloud Security Controls and Mitigations

Today's organizations depend on complex, multicloud environments which must support hundreds of different services across multiple clouds. These services are often insecure by default. Similar services in different Cloud Service Providers (CSPs) need to be protected using very different methods. Security teams need a deep understanding of AWS, Azure, and Google Cloud services to lock them down properly. Checking off compliance requirements is not enough to protect the confidentiality, integrity, and availability of your organization's data, nor will it prevent attackers from taking your critical systems down. With the right controls, organizations can reduce their attack surface and prevent security incidents from becoming breaches. Mistakes happen. Limit the impact of the inevitable.

sans.org/cloud-security

@SANSCloudSec www.linkedin.com/showcase/sanscloudsec www.youtube.com/c/SANSCloudSecurity

Poster Authors

Brandon Evans – @brandonmaxevans

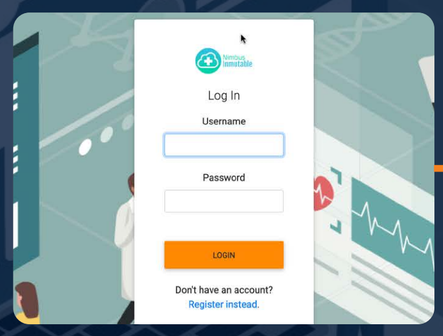
Eric Johnson – @emjohn20

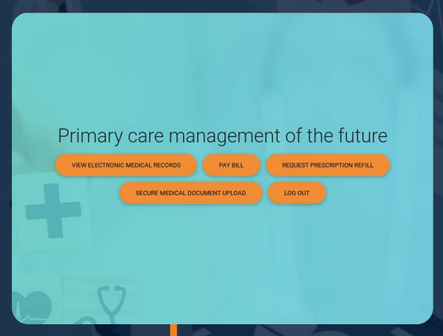
Wes Braga – @wesbragagt

CS_SEC510_v1.5_02-24

Nimbus Inmutable

SANS CLOUD SECURITY

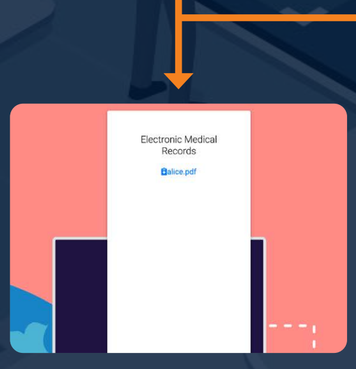


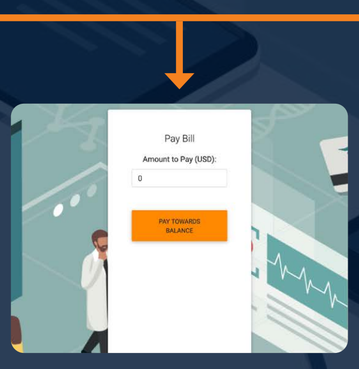


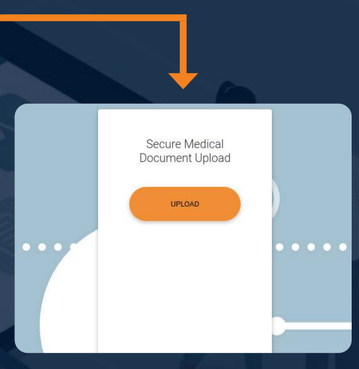
Google Cloud

aws

Nimbus Inmutable is a fictional company featured in the labs for SEC510: Attack-Driven Cloud Security Controls and Mitigations. Its corporate website runs on all three of the major clouds and leverages the cloud services available for the cloud on which it is deployed. It includes the ability to view your Electronic Medical Records, pay your bill, request prescription refills, securely upload medical documents, and more. Despite having fairly basic functionality, Nimbus uses all of the services detailed in the next slide. This illustrates how complex a modern app in the cloud can be.







Cloud Services

Compute Services

Virtual Machines

Dedicated Virtual Machines on which cloud-based applications can be run.

Containers

Logically isolated compute service running on a single cloud virtual machine.

Serverless Functions

Provide code to the cloud to be executed on a random container when an event occurs.

IAM Service

Enforce access control to other services.

Cloud Flow Logging

Provides metadata about traffic internal to the cloud's private network.

Cloud Private Networks

Allows all services and infrastructure access to be controlled at the network level.

Cloud API Logging Services

Can track all activity within a cloud account and tie it to an IAM principal.

Key Management Services

Manages cryptographic keys. Nimbus's application uses custom code to encrypt its prescription data at the record level using these keys. Additionally, AWS KMS integrates with S3, the SSM Parameter Store, the Secrets Manager, RDS, and more to encrypt the data stored in these services at rest.

Storage Accounts

Capable of storing all kinds of data. Azure Storage is used as the backend for storing logs and the data for managed databases in Azure. Nimbus stores its assets, medical records, and corporate secrets in these services. The VM proxies its asset requests, while the medical records are cached on the VM's filesystem. Intermingling data of varying sensitivity levels can be dangerous as it is error-prone.

Cloud Private Endpoint Services

Keeps traffic within the private network and allows the organization to lock down access to managed services from outside that network.

Logging Services

Used to store and view log data. Among other things, they can be used to audit flow logs and access to the cloud provider's APIs.

Secret Managers and Parameter Stores

Contain configuration and secrets used by the application. Nimbus uses these to store its database connection details and credentials, JSON Web Token (JWT) secret for user authentication, and more.

Cloud-Managed Relational Databases

Manages hosting for databases like MySQL, PostgreSQL, MSSQL, etc. Nimbus stores its user data and prescription refill requests in a cloud-managed MySQL database.

Remote Access Services

Allows authorized development and operations staff to administrate their private resources without poking holes in the cloud's firewall.

Sensitive Data Detection and Data Loss Prevention

This detects sensitive data stored in various cloud services and takes various actions to prevent data exfiltration.