SANS CLOUD SECURITY

sans.org/cloud-security

Secure Service Configuration in AWS, Azure & GCP

Based on content from

SEC510: Cloud Security Controls and Mitigations

GIAC Public Cloud Security (GPCS)

sans.org/SEC510

SANS The most trusted source for cybersecurity training, certifications, degrees, and research

Table of Contents

Introduction

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 need to be protected using very different methods across Cloud Service Providers. 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.

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.

The contents of this poster are based on material from **SEC510: Cloud Security Controls and Mitigations**, as well as the Center for Internet Security Benchmarks. CIS 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**.

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

	SSRF Protection	Token Timeout	Token Scope	Requires REST API	Prevents Extraction
AWS v1	NO	6 HOURS	NO	NO	NO
AWS v2	**YES**	6 HOURS	NO	NO	**YES**
Azure	**YES**	24 HOURS	**YES**	**YES**	NO
GCP v1	**YES**	**1 HOUR**	NO	**YES**[1]	NO

[1] GCP credentials can be used in the gcloud CLI if the attacker modifies the SQLite database it uses, but it is arguably easier to just use the API instead.

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 to the virtual machine's functional requirements
3. Verify each EC2 instance has an assigned "IAM Role" 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 (*)

	Organization Policy	Principal Policy	Resource Policy	Conditional Policy	Default SA Policy
AWS	DEFAULT FEATURE	YES	YES	YES	NO ACCESS
Azure	PREMIUM ONLY	YES	LIMITED	NO	NO ACCESS
GCP	DEFAULT FEATURE	NO	LIMITED	PARTIAL	EDITOR PERMISSIONS

Multicloud Identity Federation

	Long-Lived Credentials	Workload Identity	SAML Support	OIDC Support	AWS Sigv4	Privilege Escalation
AWS	YES	YES	YES	YES	YES	YES
Azure	YES	YES	NO	YES	NO	NO
GCP	YES	YES	YES	YES	YES	YES

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

	Connected to the Internet	Admin Ports Open	Ingress Filtering	Egress Filtering	Consistent Controls
AWS	YES	**NO**	**YES**	NO	**YES**
Azure	YES	**NO**	**YES**	NO	NO
GCP	YES	YES	**LIMITED**	**LIMITED**	**YES**

Network Flow Logging

AWS Network Logging Assessment Criteria

Benchmark 3.9 Ensure VPC flow logging is enabled in all VPCs

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 3.8 Ensure that VPC Flow Logs is Enabled for Every Subnet in a 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

	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**	3,650 DAYS	**YES**	NO[2]

[2] Firewall Rules Logging provides an alternative way to detect traffic blocked by the firewall.

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

	Internal Service Routes	Network Conditions for Service Access	Custom Service Endpoints	Endpoint Policy	Consistent Perimeter
AWS	YES	YES	YES	YES	NO
Azure	YES	YES	YES	NO	YES
GCP	YES	YES	YES	NO	YES

	Internal Shell Access	Site-to-Site VPN	Point-to-Site VPN
AWS	YES	YES	YES
Azure	YES	YES	YES
GCP	YES	YES	NO

Cryptographic Key Management

Assessment Criteria

Limit and audit all cryptographic key usage

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

	Flexible Access Policy	Audit Logging	Deletion Schedule	Automatic Key Rotation	Single-Tenant Option
AWS	**YES**	**YES**	**7-30 DAYS**	**YES**	**YES**
Azure	**YES**[3]	**YES**	**7–90 DAYS**	NO[4]	**YES**
GCP	**YES**	**YES**	**1–120 DAYS**	**YES**	NO

[3] Multiple Key Vaults are necessary to grant a principal different permissions for different keys.
[4] Both symmetric and asymmetric keys are supported by the Azure Dedicated HSM and the Azure Key Vault Managed.

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

```
1  resource "aws_s3_bucket" "cloudtrail" {
2      bucket = "cloudtrail"
3      force_destroy = true
4      policy = data.aws_iam_policy_document.cloudtrail_s3.json
5  }
6
7  resource "aws_cloudtrail" "aws_api_calls" {
8      name = "aws-api-calls"
9      s3_bucket_name = aws_s3_bucket.cloudtrail.id
10     include_global_service_events = true
11     kms_key_id = aws_kms_key.cloudtrail.arn
12 }
```

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

	Block Public Access Policy	Access Logging	Default Encryption	Data Retention
AWS	**YES**	**YES**	**YES**	**YES**
Azure	**YES**	YES	**YES**	**YES**
GCP	YES	**YES**	**YES**	**YES**

Data Exfiltration

	Disk Snapshots	Database Snapshots	Signed URLs	Misc. Resources
AWS	YES	YES	**YES**	YES
Azure	**YES** (SHORT-LIVED SAS)	**NO**	**YES**	**NO**
GCP	YES	NO	**YES**	YES

Sensitive Data Detection and Loss

	Data Sources	Custom Identifiers	Storage Config Auditing	Other DLP Capabilities
AWS	S3	**YES**	**YES**	NONE
Azure	**MANY**	**YES**	**YES**	**MANY**
GCP	**STORAGE, BIG QUERY, DATASTORE, EXTERNAL**	**YES**	NO	**DE-IDENTIFICATION, API INTEGRATION**

Serverless Assessment

Cloud Serverless Assessment Criteria

Review functions for the following security misconfigurations:

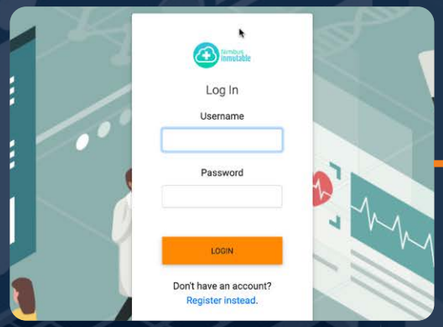
1. Scan functions for secrets management and persistence issues
2. Authenticate requests to publicly accessible functions
3. Use unique service accounts per function
4. Regularly audit function permissions for least privilege
5. Enable function audit and network controls (if available)

	Root User	Warm Environment	Credential Timeout	Read-Only File System	Default Network
AWS	**NO**	11 MINUTES	12 HOURS	**YES**[6]	YES
Azure	YES	6 MINUTES	8 HOURS	NO	YES
GCP	**NO**	**3 MINUTES**	**30 MINUTES**	NO	YES

	Default SA	Custom SA	HTTP(S) Access	VPC Integration
AWS	**LEAST PRIVILEGE**	**YES**	**OPTIONAL**	**YES**
Azure	**LEAST PRIVILEGE**	**YES**	REQUIRED	YES[7]
GCP	EXCESSIVE	**YES**	**OPTIONAL**	YES[8]

[6] AWS Lambda allows write access to the /tmp directory for temporary storage and processing.
[7] Only available with a Premium App Service plan.
[8] Only available with a GCP Organization and VPC Service Controls enabled.

Nimbus Inmutable

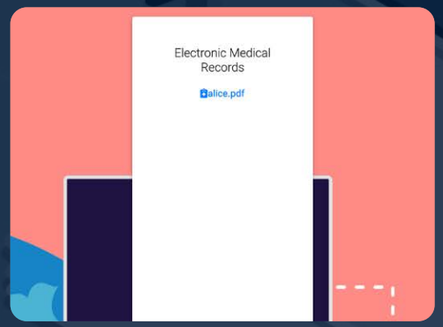


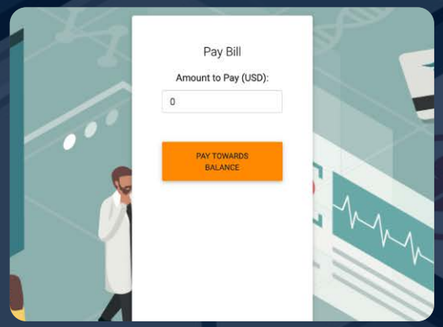
Google Cloud

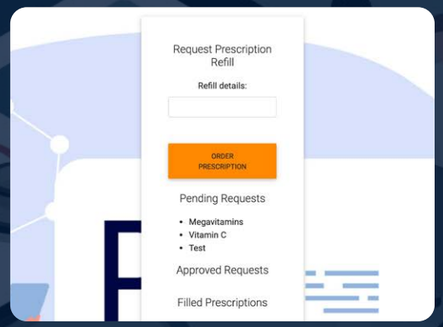
aws

Azure

Nimbus Inmutable is a fictional company featured in the labs for SEC510: 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 (EMRs), pay your bill, and request prescription refills. 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.

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. Remote Access Services: Allows authorized personnel to access SSH and other network-protected services.

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

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

IAM Service
Enforce access control to other services.

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

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.

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

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.

Sensitive Data Detection and Data Loss Prevention
This detects sensitive data stored in various cloud services and takes various actions to prevent data exfiltration.

Cloud Security Resources

SANS staff, authors, and instructors produce thousands of free content-rich resources for the information security community annually. These resources aim to provide the latest in research and technology available to help support awareness and growth across a wide range of IT and OT security considerations. This next section provides a succinct list of cloud security resources, both inside and outside of SANS, as well as direct links to a number of general SANS free resources.

Posters, Cheat Sheets, and Tools

Multicloud Command-Line Interface
sans.org/posters/multicloud-cheat-sheet

Cloud Security Free Tools
sans.org/tools/?focus-area=cloud-security

Nine Key Cloud Security Concentrations & SWAT Checklist
sans.org/posters/nine-key-cloud-security-concentrations-swat-checklist

Whitepapers, Blogs, and Webcasts

SANS Cloud Security Blog
sans.org/blog/?focus-area=cloud-security

SANS Cloud Security Webcasts
sans.org/webcasts/?focus-area=cloud-security

Multicloud Survey 2023: Navigating the Complexities of Multiple Clouds
sans.org/blog/sans-2023-multicloud-survey-navigating-the-complexities-of-multiple-clouds

Cloud Agnostic or Devout
sans.org/blog/cloud-agnostic-or-devout

Destroying Long-Lived Credentials with Workload Identity Federation
sans.org/webcasts/destroying-long-lived-cloud-credentials-workload-identity-federation

AWS Resources

Getting Started with AWS
https://aws.amazon.com/getting-started/hands-on

SANS Free Resources

SANS Free
sans.org/free

SANS Blogs
sans.org/blog

SANS Newsletters
sans.org/newsletters

SANS Reading Room
sans.org/reading-room

SANS Webcasts
sans.org/webcasts

SANS Posters
sans.org/security-resources/posters

SANS Internet Storm Center
isc.sans.edu

Microsoft Azure Resources

Azure Security Podcast (@AzureSecPod)
https://azsecuritypodcast.azurewebsites.net

SANS Cloud Security Discord
https://discord.gg/umWK85gGT2

Pen Testing Azure Applications by Matt Burrough
www.amazon.com/Pentesting-Azure-Applications-Definitive-Deployments/dp/1593278632

Google Cloud Resources

Google Cloud Security Resources
https:/cloud.google.com/security/resources

Google Cloud Security
https:/cloud.google.com/security

Cloud Security Training Environments

CloudGoat
https://github.com/rhinosecuritylabs/cloudgoat

TerraGoat
https://github.com/bridgecrewio/terragoat

ServerlessGoat
https://github.com/OWASP/Serverless-Goat

flAWS 2
http://flaws2.cloud

About SANS Cloud Security

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 Cloud Security Linkedin
https://linkedin.com/showcase/sanscloudsec

SANS Cloud Security Twitter
https://twitter.com/SANSCloudSec

SANS Cloud Security Youtube
https://sansurl.com/cloudsecyoutube

SANS Cloud Ace Podcast
www.sans.org/podcasts/cloud-ace

SANS Cloud Security Courses

SEC388: Introduction to Cloud Computing and Security
Ground school for cloud security.
www.sans.org/sec388

SEC488: Cloud Security Essentials | GCLD
License to learn cloud security.
www.sans.org/sec488

SEC510: Cloud Security Controls and Mitigations | GPCS
Multiple clouds require multiple solutions.
www.sans.org/sec510

SEC522: Application Security: Securing Web Apps, APIs, and Microservices | GWEB
Not a matter of "if" but "when." Be prepared for a web app attack. We'll teach you how.
www.sans.org/sec522

SEC540: Cloud Security and DevSecOps Automation | GCSA
The cloud moves fast. Automate to keep up.
www.sans.org/sec540

SEC541: Cloud Security Threat Detection | GCTD
Attackers can run but not hide. Our radar sees all threats.
www.sans.org/sec541

SEC549: Cloud Security Architecture
Design it right from the start.
www.sans.org/sec549

SEC588: Cloud Penetration Testing | GCPN
Aim your arrows to the sky and penetrate the cloud.
www.sans.org/sec588

FOR509: Enterprise Cloud Forensics and Incident Response | GCFR
Find the storm in the cloud.
www.sans.org/for509

LDR520: Cloud Security for Leaders
Strategically maximize your cloud investment.
www.sans.org/ldr520

SANS Cloud Security Flight Plan

		DevOps Professionals	Cloud Security Analyst	Cloud Security Engineer	Cloud Security Architect	Cloud Security Manager
BASELINE	**SEC388: Introduction to Cloud Computing and Security**		●			●
FOUNDATIONAL	**SEC488: Cloud Security Essentials** GIAC Cloud Security Essentials (GCLD)		●	●	●	●
CORE	**SEC510: Cloud Security Controls and Mitigations** GIAC Public Cloud Security (GPCS)	●	●	●	●	
	SEC540: Cloud Security and DevSecOps Automation GIAC Cloud Security Automation (GCSA)	●		●	●	
	SEC541: Cloud Security Threat Detection GIAC Cloud Threat Detection (GCTD)		●	●		
	SEC549: Cloud Security Architecture			●	●	●
SPECIALIZATION	**SEC522: Application Security: Securing Web Apps, APIs, and Microservices** GIAC Certified Web Application Defender (GWEB)	●				
	SEC588: Cloud Penetration Testing GIAC Cloud Penetration Tester (GCPN)		●	●		
	FOR509: Enterprise Cloud Forensics & Incident Response GIAC Cloud Forensics Responder (GCFR)		●			
LEADERSHIP	**LDR520: Cloud Security for Leaders**				●	●

About the Authors

Brandon Evans | bevans@sans.org | @brandonmaxevans

Brandon is the owner and an InfoSec Consultant at On-Brand Technologies LLC, a consultancy helping organizations secure their applications and other workloads in multicloud environments, specializing in AWS, Azure, and Google Cloud. Prior to starting his consultancy, Brandon led the secure development training program at Zoom Video Communications. He began his career as a Software Engineer, where he worked on both the core product of a startup, later acquired by a Fortune 500 organization, and on various products spanning a multi-billion dollar enterprise. Brandon is lead author for SEC510: Cloud Security Controls and Mitigations, a contributor to SEC540: Cloud Security and DevSecOps Automation, host of Cloud Ace podcast. Learn more about Brandon at **sans.org/profiles/brandon-evans**.

Eric Johnson | ejohnson@sans.org | @emjohn20

Eric is a Co-founder and Principal Security Engineer at Puma Security and a Senior Instructor with the SANS Institute. His experience includes cloud security assessments, cloud infrastructure automation, static source code analysis, web and mobile application penetration testing, secure development lifecycle consulting, and secure code review assessments. Eric is the lead author and an instructor for SEC540: Cloud Security and DevSecOps Automation and a co-author and instructor for both SEC549: Cloud Security Architecture and SEC510: Cloud Security Controls and Mitigations. Additionally, Eric is a SANS Security Awareness Developer Training Advisory Board Member and SANS Analyst for Application Security and DevSecOps Surveys. Learn more about Eric at **sans.org/profiles/eric-johnson**.

Wes Braga | wesbragagt@gmail.com | @wesbragagt

Wes designed Nimbus Inmutable, the website featured on this poster and used in SEC510: Cloud Security Controls and Mitigations.

SANS The most trusted source for cybersecurity training, certifications, degrees, and research