



Cloud Infrastructure Security Assessment

Table of Contents




- Deployment Scope
- Overview Of Your Environment
- Overview Of Issues And Top 5 Riskiest Resources
- Current State Of Compliance With Cis Controls
- Overview Of High Severity And Critical Issues By Type
- Examples Of Critical Issues Discovered

Deployment Scope

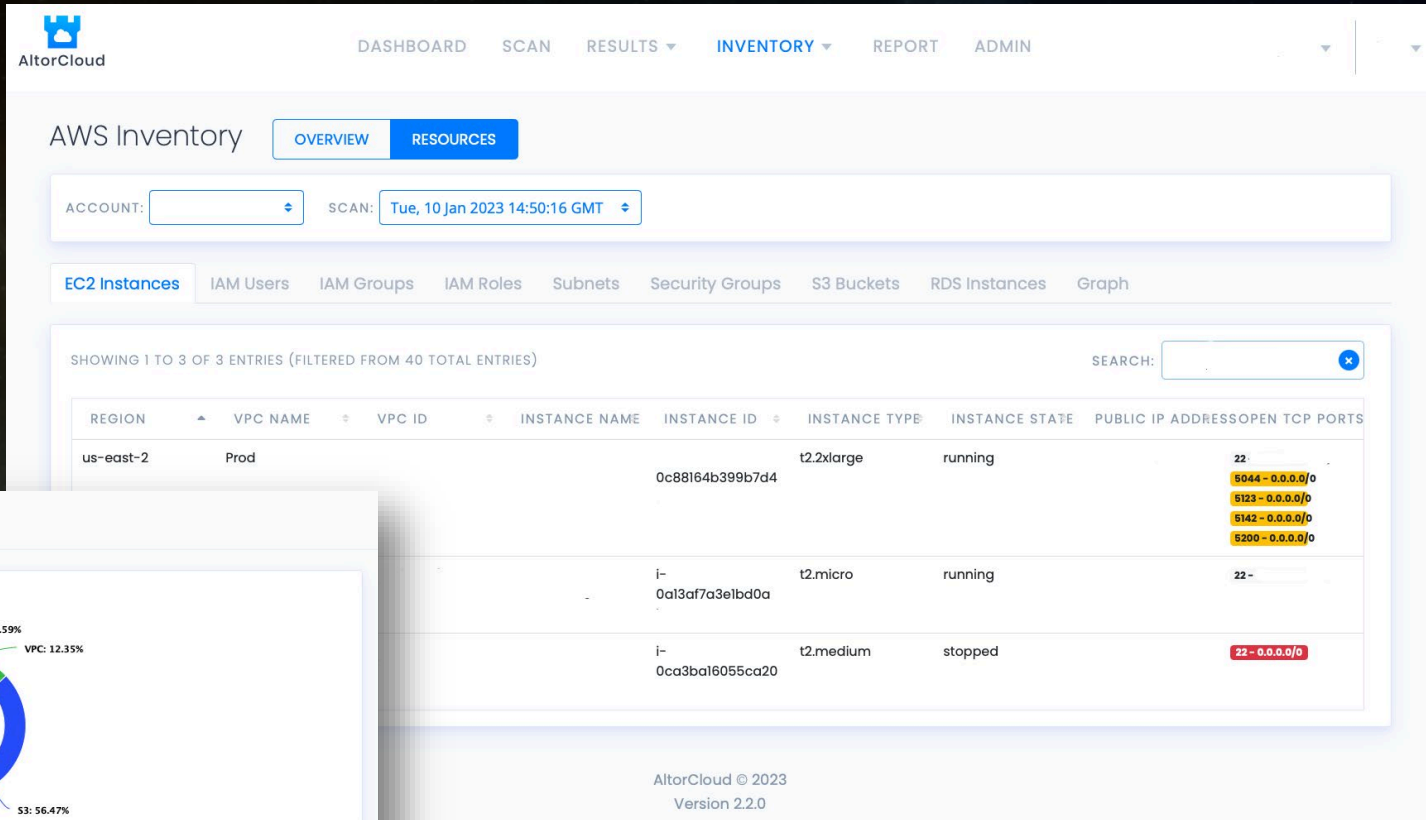
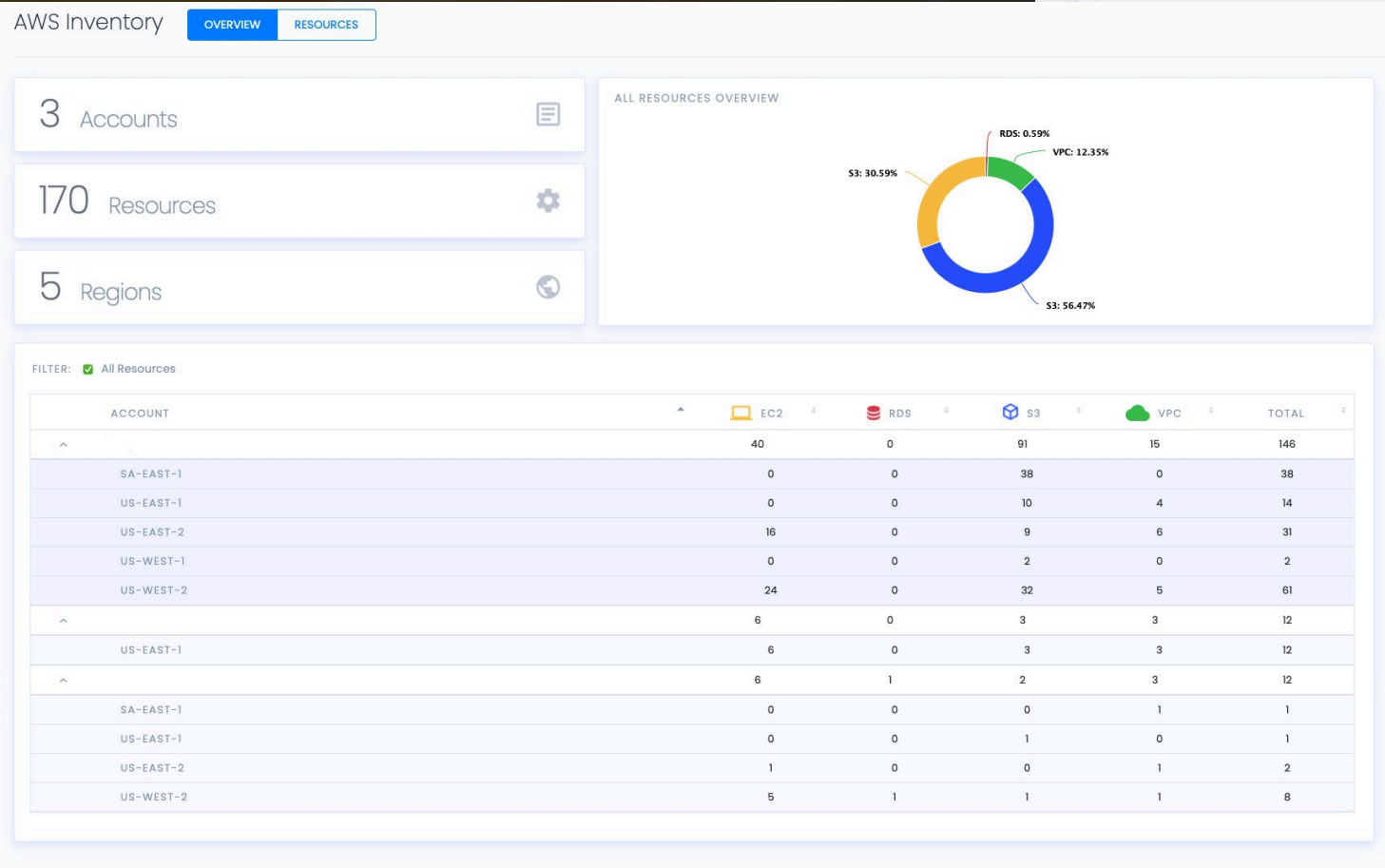
Compute Platforms Inventory

AltorCloud connects via read-only (API) scanning metadata for your three cloud provider subscriptions:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

3	AWS Accounts	
1	Azure Subscription	
1	GCP Account	

Overview Of Your Environment



Overview Of Issues And Top 5 Riskiest Resources

5

MOST AFFECTED DOMAINS

AWS

EC2

55%

65/118

IAM

44%

40/90

S3

15%

5/33

VPC

17%

3/18

CloudTrail

17%

3/18

COMPLIANCE CONTROLS PASSED BY STANDARD FOR ALL ACCOUNTS

Filter

CIS AWS

39%

59/153

CIS Azure

69%

38/55

CIS GKE

53%

9/17

CIS GCP

33%

28/84

HIPAA

29%

35/121

ISO-27001

51%

226/447

GDPR

42%

94/223

PCI-DSS

52%

101/196

AWS Security Results

AWS CHECKS:

OVERVIEW

FINDINGS

HIGH RISK

1687

Passed

54

514

Failed

53

MEDIUM RISK

491

Passed

23

851

Failed

109

LOW RISK

38

Passed

5

27

Failed

4

RISK TOTALS OVERVIEW

Failed Low Risk Checks: 0.75%


Failed Medium Risk Checks: 23.59%

Failed High Risk Checks: 14.25%

Passed Checks: 61.42%

ACCOUNT	IAM						ACCESS/NETWORK					STORAGE		LOGGING	
NAME	EC2	PASSWORD POLICY	ROOT ACCOUNT	USERS MFA	DIRECT ATTACH	ACCESS KEY ROTATION	CMK ROTATION	EXPOSED PORTS	DEFAULTS OPEN	VPC FLOW	UNUSED SGS	S3 ENCRYPT	RDS ENCRYPT	CLOUD TRAIL	OTHER
/Main	✓														
_OffSec	✓														
_Prod	✓														

VIEW MORE

 AltorCloud

Current state of Compliance with multiple Control benchmarks

COMPLIANCE CONTROLS PASSED BY STANDARD FOR ALL ACCOUNTS

CIS AWS

39%

59/153

CIS Azure

89%

38/55

CIS GKE

53%

9/17

CIS GCP

33%

28/84

HIPAA

29%

35/121

ISO-27001

51%

226/447

GDPR

42%

94/223

PCI-DSS

52%

101/196

AWS Security Results

AWS CHECKS: OVERVIEW FINDINGS

ACCOUNT:

SCAN: Tue, 10 Jan 2023 14:50:14 GMT

SHOW 10 ENTRIES

Filter (Failed - High)

SEARCH:

NAME	SERVICE	RISK	COMPLIANCE	FAILURES	ID
Check if EBS snapshots are encrypted	EC2	High	PCI v3.2.1: 3.3 GDPR...	109	7.40
Check if S3 buckets have secure transport policy	S3	High	ISO27001: A.10.1	87	7.64
Check if S3 buckets have default encryption (SSE) enabled or use a bucket policy to enforce it	S3	High	PCI v3.2.1: 3.3 PCI v3.2.1: 3.4...	67	7.34
Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to port 22	EC2	High	CIS v1.2.0: 4.1 PCI v3.2.1: 3.1...	29	4.1
Ensure the default security group of every VPC restricts all traffic	EC2	High	CIS v1.2.0: 4.3 PCI v3.2.1: 3.1...	26	4.3
Ensure there are no Security Groups without ingress filtering being used	EC2	High	ISO27001: A.13.1	20	7.4
Find VPC security groups with wide-open public IPv4 CIDR ranges (non-RFC1918)	EC2	High	GDPR ISO27001: A.13.1	17	7.78
Check if EBS Default Encryption is activated	EC2	High	GDPR ISO27001: A.10.1	15	7.61
Check if GuardDuty is enabled	GuardDuty	High	PCI v3.2.1: 3.11 ISO27001: A.12.6	14	7.13
Check if Elastic Load Balancers have SSL listeners	ELB	High	ISO27001: A.10.1	12	7.93

SHOWING 1 TO 10 OF 42 ENTRIES (FILTERED FROM 239 TOTAL ENTRIES)

1

2

3

4

5

Remediate Findings

Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to port 22

CIS v1.2.0: 4.1, PCI v3.2.1: 3.1, PCI v3.2.1: 3.2, GDPR, ISO27001: A.12.6, ISO27001: A.13.1

Risk & RemediationEvidence

Extra Info

RISK & REMEDIATION

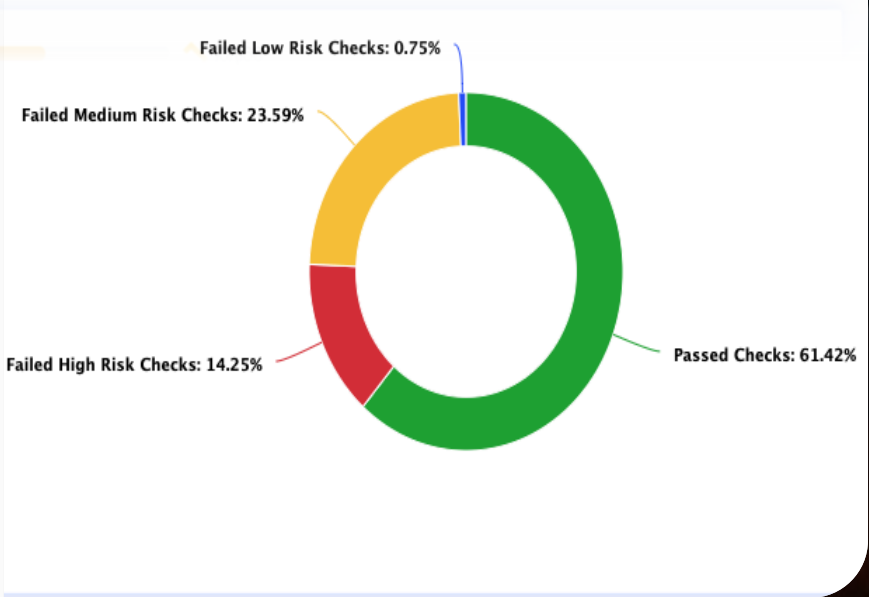
Edit

RISK DESCRIPTION

Allows access of SSH (port 22) from any computer on the Internet. The only protection against compromise is the authentication on the target EC2 instance. The organization should review and remove all security groups to prevent accidental assignment and exposure. Note that this finding will be received on publicly exposed SFTP servers, Jump Boxes and VPN endpoints. It is recommended to limit port 22 access to both types of servers to only specific sources.

REMEDIATION

Disable any inbound rules with a source of '0.0.0.0/0' for port 22 and/or all ports



Overview of High severity and critical issues by type

ACCOUNT		IAM					ACCESS/NETWORK					STORAGE		LOGGING	
NAME	EC2	PASSWORD POLICY	ROOT ACCOUNT	USERS MFA	DIRECT ATTACH	ACCESS KEY ROTATION	CMK ROTATION	EXPOSED PORTS	DEFAULTS OPEN	VPC FLOW	UNUSED SGS	S3 ENCRYPT	RDS ENCRYPT	CLOUD TRAIL	OTHER
	✓														
	✓														
	✓														
VIEW MORE															

VIEW BY RISK: ALL HIGH MEDIUM LOW

CHECKS WITH AT LEAST ONE FAILURE	
PASS RATE ⓘ	CHECK
33%	1.2 - Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
17%	1.4 - Ensure access keys are rotated every 90 days or less
67%	1.9 - Ensure IAM password policy requires minimum length of 14 or greater
67%	1.10 - Ensure IAM password policy prevents password reuse: 24 or greater
67%	1.11 - Ensure IAM password policy expires passwords within 90 days or less
36%	2.1 - Ensure CloudTrail is enabled in all regions
64%	2.3 - Ensure the S3 bucket CloudTrail logs to is not publicly accessible
3%	2.4 - Ensure CloudTrail trails are integrated with CloudWatch Logs
65%	4.1 - Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to port 22
95%	4.2 - Ensure no security groups allow ingress from 0.0.0.0/0 or ::/0 to port 3389

AltorCloud Sample report

Examples of critical issues

SHOW 10 ENTRIES Filter (Failed - High) SEARCH: iam

NAME	SERVICE	RISK	COMPLIANCE	FAILURES	ID
Ensure hardware MFA is enabled for the root account	IAM	High	CIS v1.2.0: 1.14 PCI v3.2.1: 3.8...	1	1.14
Ensure credentials unused for 90 days or greater are disabled	IAM	High	CIS v1.2.0: 1.3 PCI v3.2.1: 3.7...	3	1.3
Ensure access keys are rotated every 90 days or less	IAM	High	CIS v1.2.0: 1.4 PCI v3.2.1: 3.4...	9	1.4
Ensure users of groups with AdministratorAccess policy have MFA tokens enabled	IAM	High	GDPR ISO27001: A.9.2	2	7.1
Ensure that no custom IAM policies exist which allow permissive role assumption (e.g. sts:AssumeRole on *)	IAM	High	ISO27001: A.9.2	4	7.100

SHOWING 1 TO 5 OF 5 ENTRIES (FILTERED FROM 239 TOTAL ENTRIES) 1

Ensure hardware MFA is enabled for the root account

CIS v1.2.0: 1.14, PCI v3.2.1: 3.8, GDPR, ISO27001: A.9.2

Risk & Remediation Evidence Extra Info

RISK & REMEDIATION Edit

RISK DESCRIPTION

The root account is the most privileged user in an AWS account. MFA adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS website, they will be prompted for their user name and password as well as for an authentication code from their AWS MFA device. For Level 2, it is recommended that the root account be protected with a hardware MFA.

REMEDATION

Perform the following to establish a hardware MFA for the root account:

1. Sign in to the AWS Management Console and open the IAM console at ...

SHOW 10 ENTRIES Filter (Failed) SEARCH: secrets

NAME	SERVICE	RISK	COMPLIANCE	FAILURES	ID
Check if Secrets Manager key rotation is enabled	SecretsManager	High		1	7.163
Ensure Kubernetes Secrets are encrypted using Customer Master Keys (CMKs)	EKS	High		2	7.97
Find secrets in CloudFormation outputs	CloudFormation	High		6	7.42
Find secrets in Lambda functions variables	LAMBDA	High	ISO27001: A.14.2	4	7.59

SHOWING 1 TO 4 OF 4 ENTRIES (FILTERED FROM 239 TOTAL ENTRIES) 1

Check if Secrets Manager key rotation is enabled

Risk & Remediation Evidence Extra Info

RISK & REMEDIATION Edit

RISK DESCRIPTION

A secret can be periodically updated. You update the credentials in both the secret and the database or service when the secret is updates. Automatic rotation for your secrets can be set up in Secrets Manager. The new credentials are automatically retrieved when an application accesses the Secrets Manager.

REMEDATION

To turn on rotation (console): 1. Open the Secrets Manager console at <https://console.aws.amazon.com/secretsmanager/>. 2. On the Secrets page, choose your secret. 3. On the Secret details page, in the Rotation configuration section, choose Edit rotation. The Edit rotation configuration dialog box opens. Do the following:

Thank You

Please fill out the Contact us form for a free assessment and get a free Security eBook in the process

<https://altorcloud.com/contact/>

-  **Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software**
No Starch Press
-  **Real-World Bug Hunting**
No Starch Press
-  **Malware Data Science: Attack Detection and Attribution**
No Starch Press
-  **Practical Forensic Imaging**
No Starch Press
-  **Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation**
No Starch Press
-  **Pentesting Azure Applications: The Definitive Guide to Testing and Securing Deployments**
No Starch Press
-  **Rootkits and Bootkits**
No Starch Press
-  **Practical IoT Hacking**
No Starch Press
-  **Serious Cryptography: A Practical Introduction to Modern Encryption**
No Starch Press
-  **The Tangled Web: A Guide to Securing Modern Web Applications**
No Starch Press
-  **Black Hat Go**
No Starch Press
-  **The Ghidra Book**
No Starch Press
-  **Ethical Hacking**
No Starch Press
-  **How to Hack Like a Ghost**
No Starch Press
-  **Crypto Dictionary**
No Starch Press
-  **Black Hat Python, 2nd Edition**
No Starch Press
-  **Cyberjutsu**
No Starch Press
-  **Foundations of Information Security**
No Starch Press