UnifiedArc

CLOUD SECURITY & COMPLIANCE PLATFORM

Compliance Audit Report

Sample Organization · AWS · 2026-06-20

EXECUTIVE SNAPSHOT

SECURITY SCORE	COMPLIANCE READINESS	HIGH-RISK FINDINGS
100/100	100%	0
Grade A		

ASSESSMENT COVERAGE	OPEN FINDINGS	SECURITY MATURITY
0%	0	Optimized

ENVIRONMENT SUMMARY

INVENTORY DISCOVERED	ELIGIBLE RESOURCES	FULLY ASSESSED RESOURCES	SERVICES ASSESSED	FRAMEWORKS EVALUATED
0	0	0	0	4

Assessment Coverage Note: 0 resources were discovered across the environment. 0 are currently eligible for active security assessment and 0 were fully evaluated. Remaining resources continue to be inventoried and visible through inventory and inventory coverage while active assessment coverage expands.

TOP RISKS

No open risks - all controls passed.

FRAMEWORK SNAPSHOT

No frameworks mapped.

EXECUTIVE SUMMARY

All evaluated controls passed. The environment meets the assessed compliance requirements; maintain the configuration and re-assess regularly.

Current Risk Level:	**Low**	**Most Impacted Area:**	**None**
Most Impacted Framework:	**CIS AWS Foundations (2 gaps)**	**Estimated Remediation Timeline:**	**On track**

REPORT DETAILS

Report ID	UA-C975447289	**Generated By**	UnifiedArc Security Advisor
Tenant Ref	8151325dcdba	**Region Scope**	us-east-1 / all regions
Report Version	2.0	**Assessment Version**	Security Advisor 1.0
Control Library	2026.06 (101 AWS controls)	**Framework Scope**	CIS AWS Foundations, ISO 27001, PCI DSS, SOC 2

Read-only security posture assessment based on live cloud configuration and UnifiedArc control evaluations. No agents installed; no changes made to the environment.

REPORT PURPOSE

This report provides a read-only assessment of cloud security posture, compliance readiness, assessment coverage, and prioritized remediation actions based on live AWS configuration.

KEY TAKEAWAY

The environment meets the evaluated controls. Maintain the current configuration and re-assess regularly.

Executive Assessment

UnifiedArc evaluated 0 cloud assets across 0 AWS services, 0 region(s), and 4 compliance framework(s).

Key Observations

- Security maturity is currently classified as Optimized.
- ISO 27001 is closest to compliance readiness (77%).
- CIS AWS Foundations currently contains the highest compliance gap count (12).

Priority Actions

No priority actions - all evaluated controls passed.

The environment meets the evaluated controls. Maintain the current configuration and re-assess regularly to keep this posture verified.

Assessment Methodology

- v Read-only AWS access
- v No agents installed
- v No changes made to your resources
- v Based on live cloud configuration
- v Evidence collected directly fr[illegible]

Table of Contents

Executive Decision Summary

A 60-second view for executive decision-making - the security and compliance bottom line.

OVERALL SECURITY STATUS

Low Risk - Security Score 100/100 - Compliance Readiness 69%

Are we secure?

Low Risk - all 1 evaluated controls passed on a 100/100 security score.

Are we compliant?

69% compliance readiness; the environment meets the evaluated requirements across 4 frameworks.

What are our biggest risks?

No open findings were identified in this assessment.

What should we fix first?

Maintain the current configuration and re-assess on a regular cadence.

How long will it take?

No remediation required at this time.

What outcome should we expect?

Continued strong posture; periodic re-assessment sustains readiness.

Executive Overview

A board-level snapshot of security posture, compliance readiness, and the fastest ways to improve.

SECURITY MATURITY: OPTIMIZED

Foundational	Developing	Operational	Managed	Optimized

Benchmark Snapshot

Security Score 100 (Typical SMB 55-65 · Strong program 75+ · Highly mature 85+). Compliance Readiness 69% (Typical SMB 40-60%).

Indicative ranges for orientation only - not derived from customer data and not a ranking.

Executive Risk Statement

All 1 evaluated controls passed. The environment demonstrates optimized operational maturity and meets the evaluated compliance requirements; maintain the current configuration and re-assess regularly.

Executive Risk Summary

Current Risk Level: LOW

Credential Compromise Risk — Low
Identity and MFA controls are passing.

Audit Readiness Risk — Low
All evaluated controls passed.

Logging Visibility Risk — Low
Logging and monitoring controls are passing.

Data Protection Risk — Low
Encryption and public-access controls are passing.

CISO Recommendation
Maintain the current control configuration and re-assess on a regular cadence. Continue evidence collection and ownership discipline to sustain audit readiness and security maturity.

Assessment Confidence — Assessment Coverage: BUILDING
Reason: 0% of eligible resources are actively assessed by available security controls.

Assessment Integrity

RESOURCES DISCOVERED	RESOURCES EVALUATED	FRAMEWORKS EVALUATED	ASSESSMENT COVERAGE
0	0	4	0%
EVIDENCE SOURCE	**ACCESS TYPE**	**AGENTS INSTALLED**	**MANUAL OVERRIDES**
Live AWS API	Read-Only	None	0

Risk Exposure

0 High - 0 Medium - 0 Low Affected Resources: 0 Framework Controls Impacted: 0
Account-wide findings: 0 Findings affecting specific resources: 0

Most Critical Finding: None - all evaluated controls passed

Framework Readiness: Most ready ISO 27001 (77%) · least ready CIS AWS Foundations (60%)

Control Effectiveness Summary

Controls operating effectively 1 · Controls requiring remediation 0 · High 0 · Medium 0 · Low 0 · Assessment Coverage 0%

Top Risks

No open risks - all evaluated controls passed.

Key Business Risks

No material business risks identified from the open findings.

Recommended Next Actions

No actions needed - all evaluated controls passed.

Expected Security Improvement

All evaluated controls passed - no remediation actions required.

Baseline assessment completed. Security score, compliance readiness, and finding trends will appear after the next scheduled assessment.

Highest Risk Findings

The open findings below carry the greatest business risk. Addressing the highest-severity items first delivers the largest reduction in security and compliance risk.

All evaluated controls passed.

Top Security Strengths

Controls already passing in your environment, verified against live configuration - not assumptions.

v Root account MFA enabled - passing

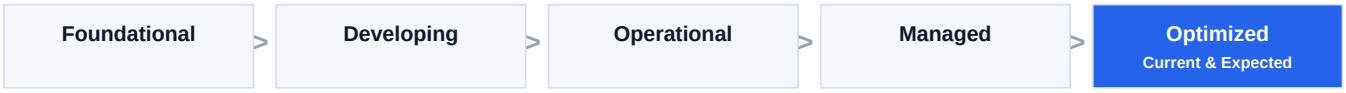
Business value: Strengthens security posture and audit readiness.

Evidence: Live configuration · Verified 2026-06-20

Frameworks: -

1 control(s) passed and reflect real, verified configuration.

Security Maturity Roadmap



Optimized (Current) Continuous improvement with strong automation.

Fastest Security Wins

Open findings prioritized based on business impact, compliance impact, and remediation effort.

No open findings - no remediation needed.

Executive Risk Matrix

Open findings mapped by likelihood and business impact; detail by impact follows below.

	LOW IMPACT	MEDIUM IMPACT	HIGH IMPACT
HIGH LIKE.	0	0	0
MEDIUM LIKE.	0	0	0
LOW LIKE.	0	0	0

Rows = likelihood of exploitation, columns = business impact; each cell counts open findings.

No open risks - all evaluated controls passed.

30-Day Remediation Roadmap

No open findings - no remediation roadmap required.

Security Trend

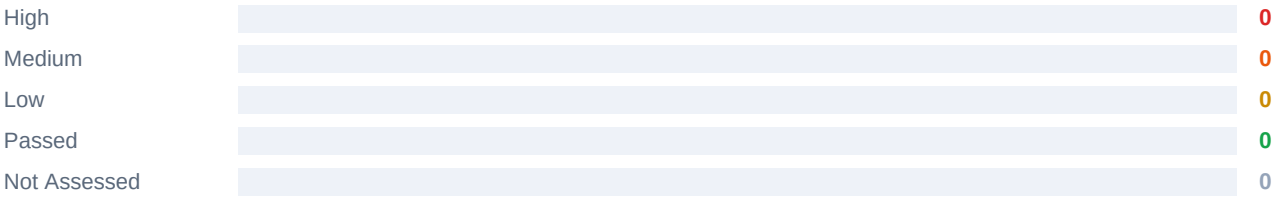
Current Security Posture: Optimized

Trend history is being collected
UnifiedArc records daily Security Advisor snapshots. Security score, compliance readiness, and open finding trends will appear after multiple completed assessment cycles.

1. Executive Summary

PASS RATE	PASSED	FAILED	RESOLVED	ACCEPTED RISK	NOT APPLICABLE
100%	1	0	0	0	0

Risk Distribution



Top 5 Risks

No failing controls.

Recently Resolved Findings

None yet.

Business Impact

No open findings. The evaluated controls passed; maintain the current configuration and re-scan regularly to keep the posture verified.

2. Audit Coverage Summary

Metric	Count
Cloud Assets Discovered	0
Accounts Assessed	0
Regions Assessed	0
AWS Services Assessed	0
Security Controls Assessed	101
Findings Generated	0

This section describes the scope of the cloud environment discovered and evaluated by UnifiedArc.

Environment Inventory Summary

No resource inventory on record yet - run a Topology/discovery scan to populate the environment inventory. (Identity/IAM controls are still evaluated directly via the APIs.)

3. Framework Coverage

Readiness = mapped controls met / mapped controls evaluated per framework. Indicative orientation, not a certified audit.

Not in current compliance profile: SOC 2, CIS, ISO 27001, HIPAA, GDPR, PCI-DSS, NIST.

Audited AWS Services

No resource inventory on record yet - run a Topology/discovery scan to populate the services list.

4. Environment Inspection Coverage

No resource inventory on record yet - run a Topology/discovery scan to measure inspection coverage.

5. Assessment Coverage by Service

Coverage Highlights
UnifiedArc discovered 0 resources, identified 0 eligible for assessment, and actively assessed 0. Additional inventoried services are continuously added to the UnifiedArc assessment library through ongoing control expansion - every discovered resource stays in cloud visibility and topology.

Per-service assessment coverage will populate once a Topology/discovery scan has inventoried this account's resources.

Top Impacted Services

No failing findings - no impacted services.

6. Controls by Category

Identity & Access (1)

Root account MFA enabled PASS

Severity: Low Frameworks: Account-level control Verified: Verified from live config

7. Accepted Risks & Exceptions

No accepted-risk exceptions were recorded for this assessment.

Evidence uploads, justifications, accepted-risk approvals, and reviewer decisions will appear here when recorded in UnifiedArc.

8. Evidence History

No evidence submissions were recorded for this assessment.

Evidence uploads, justifications, accepted-risk approvals, and reviewer decisions will appear here when recorded in UnifiedArc.

9. Remediation Summary

No open findings - nothing to remediate.

UnifiedArc Assessment Highlights

- v 1 security controls executed
- v Resource-level evidence collection
- v Read-only assessment model
- v No agents required

Why These Findings Can Be Trusted

- v Read-only access - UnifiedArc never modifies your environment
- v No agents required - nothing installed in your account
- v Live cloud configuration - findings reflect real, current state
- v Resource-level evidence - every finding ties to specific assets
- v Framework mapping - controls mapped to SOC 2, CIS, ISO 27001 and more
- v Coverage transparency - we report exactly what was and was not assessed
- v No mocked findings - results come only from evaluated controls

Auditor Notes

Scope Statement

This report is a point-in-time, read-only assessment of discovered AWS resources and evaluated UnifiedArc controls. Findings are based on live cloud configuration returned by AWS APIs. Resources that are inventoried but not actively assessed are clearly labeled as Inventory Coverage and are excluded from compliance readiness calculations.

Assessment Scope

Read-only evaluation of AWS resources discovered via cloud APIs across 0 region(s) and 0 account(s). 1 security controls assessed across 0 mapped framework(s).

Assessment Method

UnifiedArc Security Advisor reads live cloud configuration through scoped, read-only API calls. No agents are installed and no resources are modified.

Evidence Collection

Each finding is evaluated against the actual resource configuration returned by the cloud provider; affected resources are recorded per finding (see Appendix A).

Assessment Coverage

0% of eligible resources were fully assessed. Coverage is measured against eligible resources, not total discovered inventory. Resources without an applicable control are reported as Inventory Coverage (discovered and categorized but not currently covered by active assessment controls) and are never counted as failures.

Limitations

This is a point-in-time assessment of discovered resources and evaluated controls. It is an orientation tool and does not constitute a certified audit or a guarantee of compliance.

Appendix A - Affected Resources

No findings affecting specific resources were recorded for this assessment.

Appendix B - Service Coverage

Purpose: Cloud asset discovery and assessment coverage by service. Why it exists: it shows what was discovered versus actively assessed. How to use: auditors confirm assessment scope and identify inventory-only services.

Per-service coverage will populate after a discovery scan.

Appendix C - Framework Mapping

Purpose: Compliance alignment by framework. Why it exists: it maps controls met, missing, and not-yet-assessed per framework. How to use: auditors evidence framework alignment and locate the gaps to close.

No frameworks are currently mapped.

Appendix D - Control Library

Purpose: Full library of evaluated controls. Why it exists: it documents every control behind each finding and pass (101 controls). How to use: auditors reference the complete evaluated control set and its framework mapping.

Control	Category	Severity	Frameworks
EC2 IMDSv2 enforced	Compute & Containers	High	CIS, SOC2
Lambda public access	Compute & Containers	High	SOC2
EKS API endpoint not internet-open	Compute & Containers	High	CIS, SOC2
ECR scan-on-push enabled	Compute & Containers	Medium	ISO27001, SOC2
EKS control-plane logging	Compute & Containers	Medium	SOC2
EKS secrets envelope encryption	Compute & Containers	Medium	ISO27001, SOC2
Lambda env-var encryption (CMK)	Compute & Containers	Low	ISO27001, SOC2
ECR image tag immutability	Compute & Containers	Low	ISO27001, SOC2
S3 Block Public Access	Data Protection	High	CIS, GDPR, ISO27001, PCI, SOC2
Unencrypted databases	Data Protection	High	CIS, GDPR, HIPAA, ISO27001, PC
RDS snapshots not public	Data Protection	High	CIS, GDPR, SOC2
EBS snapshots not public	Data Protection	High	GDPR, SOC2
Redshift clusters encrypted	Data Protection	High	ISO27001, PCI, SOC2
Unencrypted EBS volumes	Data Protection	Medium	CIS, GDPR, HIPAA, ISO27001, PC
EBS encryption-by-default	Data Protection	Medium	CIS, ISO27001, SOC2
RDS automated backups enabled	Data Protection	Medium	SOC2
KMS key rotation enabled	Data Protection	Medium	CIS, PCI, SOC2
S3 bucket default encryption enabled	Data Protection	Medium	CIS, ISO27001, SOC2
RDS Multi-AZ enabled	Data Protection	Medium	SOC2
RDS deletion protection enabled	Data Protection	Medium	SOC2
Secrets Manager rotation enabled	Data Protection	Medium	ISO27001, PCI, SOC2
EFS file systems encrypted	Data Protection	Medium	HIPAA, ISO27001, SOC2
ElastiCache at-rest encryption	Data Protection	Medium	ISO27001, SOC2
ElastiCache in-transit encryption	Data Protection	Medium	PCI, SOC2
S3 bucket versioning enabled	Data Protection	Low	CIS, ISO27001, SOC2
S3 server access logging enabled	Data Protection	Low	CIS, SOC2
DynamoDB encryption with KMS CMK	Data Protection	Low	ISO27001, SOC2
SNS topics encrypted at rest	Data Protection	Low	ISO27001, SOC2
SQS queues encrypted at rest	Data Protection	Low	ISO27001, SOC2

RDS auto minor version upgrade	Data Protection	Low	ISO27001, SOC2
DynamoDB point-in-time recovery	Data Protection	Low	ISO27001, SOC2
AWS Config rules active	Governance	Medium	CIS, SOC2
AWS Backup plans configured	Governance	Medium	ISO27001, SOC2
Service control policies in use	Governance	Medium	CIS, SOC2
AWS Budget alerts configured	Governance	Low	SOC2
AWS Organizations in use	Governance	Low	CIS, SOC2
Required resource tags present	Governance	Low	SOC2
CloudFormation drift detection	Governance	Low	SOC2
Security alternate contact configured	Governance	Low	SOC2
Root account MFA	Identity & Access	High	CIS, HIPAA, ISO270[illegible], SOC2
Root account access keys	Identity & Access	High	CIS, HIPAA, ISO[illegible]7001, SOC2
IAM users with AdministratorAccess	Identity & Access	High	CIS, ISO[illegible] SOC2
IAM policies with wildcard admin	Identity & Access	High	CIS, ISO270[illegible]1, PCI, SOC2
IAM roles trusting external accounts	Identity & Access	High	[illegible]ISO27001, SOC2
Root user activity detected	Identity & Access	High	CIS, PCI, SOC2
IAM Access Analyzer findings present	Identity & Access	High	CIS, SOC2
IAM users without MFA	Identity & Access	Medium	CIS, GDPR, HIPAA, ISO27001, SO
Access keys older than 90 days	Identity & Access	Medium	CIS, ISO27001, SOC2
IAM password policy	Identity & Access	Medium	CIS, ISO27001, SOC2
IAM users unused for 90+ days	Identity & Access	Medium	CIS, ISO27001, SOC2
IAM access keys unused for 90+ days	Identity & Access	Medium	CIS, SOC2
IAM access keys older than 180 days	Identity & Access	Medium	CIS, PCI, SOC2
IAM Access Analyzer enabled	Identity & Access	Medium	CIS, SOC2
IAM roles unused for 90+ days	Identity & Access	Low	CIS, SOC2
Support role for incident handling	Identity & Access	Low	CIS, SOC2
RDS IAM database authentication	Identity & Access	Low	SOC2
CloudTrail (multi-region)	Logging & Monitoring	High	CIS, HIPAA, ISO27001, PCI, SOC
CloudTrail management events enabled	Logging & Monitoring	High	CIS, PCI, SOC2
No active high-severity GuardDuty findings	Logging & Monitoring	High	SOC2
GuardDuty threat detection	Logging & Monitoring	Medium	ISO27001, SOC2
CloudTrail log-file validation	Logging & Monitoring	Medium	CIS, SOC2
CloudTrail KMS encryption enabled	Logging & Monitoring	Medium	CIS, SOC2
VPC Flow Logs enabled	Logging & Monitoring	Medium	CIS, SOC2
AWS Config enabled	Logging & Monitoring	Medium	CIS, SOC2
AWS Security Hub enabled	Logging & Monitoring	Medium	SOC2
Amazon Inspector enabled	Logging & Monitoring	Medium	SOC2
CloudTrail organization trail enabled	Logging & Monitoring	Medium	CIS, SOC2
Metric filter for root account usage	Logging & Monitoring	Medium	CIS, SOC2
CloudWatch log retention configured	Logging & Monitoring	Low	SOC2
CloudTrail S3 data events enabled	Logging & Monitoring	Low	CIS, SOC2
CloudTrail Lambda data events enabled	Logging & Monitoring	Low	CIS, SOC2
Metric filter for console sign-in failures	Logging & Monitoring	Low	CIS, SOC2
Metric filter for IAM policy changes	Logging & Monitoring	Low	CIS, SOC2

Metric filter for security group changes	Logging & Monitoring	Low	CIS, SOC2
ALB access logging enabled	Logging & Monitoring	Low	PCI, SOC2
Amazon Macie enabled	Logging & Monitoring	Low	GDPR, SOC2
Amazon Detective enabled	Logging & Monitoring	Low	SOC2
Metric filter for unauthorized API calls	Logging & Monitoring	Low	CIS, SOC2
Metric filter for console sign-in without MFA	Logging & Monitoring	Low	CIS, SOC2
Metric filter for KMS CMK changes	Logging & Monitoring	Low	CIS, SOC2
Route 53 public-zone query logging	Logging & Monitoring	Low	SOC2
Redshift audit logging enabled	Logging & Monitoring	Low	PCI, SOC2
Security groups open to the internet	Network Security	High	CIS, GDPR, ISO27001, PCI, SOC2
Publicly accessible databases	Network Security	High	GDPR, ISO27001, PCI, SOC2
Load balancer listeners use TLS	Network Security	High	ISO27001, PCI, SOC2
Security groups exposing SSH (22)	Network Security	High	CIS, PCI, SOC2
Security groups exposing RDP (3389)	Network Security	High	CIS, PCI, SOC2
Redshift clusters not public	Network Security	High	PCI, SOC2
Default security group restricted	Network Security	Medium	CIS, SOC2
EC2 instances with public IP	Network Security	Medium	SOC2
Internet-facing Application Load Balancers	Network Security	Medium	CIS, SOC2
Internet-facing Network Load Balancers	Network Security	Medium	CIS, SOC2
Network ACLs allow unrestricted inbound	Network Security	Medium	CIS, SOC2
CloudFront enforces HTTPS	Network Security	Medium	PCI, SOC2
CloudFront protected by WAF	Network Security	Medium	PCI, SOC2
ACM certificates not expiring soon	Network Security	Medium	PCI, SOC2
Unattached Elastic IPs	Network Security	Low	SOC2
No unused security groups	Network Security	Low	CIS, SOC2
Default VPC present	Network Security	Low	CIS, SOC2
Load balancer deletion protection	Network Security	Low	SOC2
S3 gateway VPC endpoint present	Network Security	Low	SOC2

Evidence History: per-submission evidence, attestations and reviewer decisions are recorded in Section 8 and in the Compliance Resolution Audit Report.

Appendix E - Full Cloud Inventory Summary

Purpose: Discovered cloud inventory. Why it exists: it accounts for every discovered service and its assessment state. How to use: auditors reconcile total discovered inventory against assessed coverage.

Full cloud inventory will populate after a discovery scan.

Assessment Coverage Transparency

UnifiedArc clearly distinguishes:

- Resources actively assessed by security controls
- Resources visible through inventory coverage
- Resources visible through topology mapping

This transparency helps organizations understand exactly what was evaluated and what remains under visibility-only coverage.

This report reflects verified AWS configuration data collected through read-only access. No agents were installed and no changes were made to the environment.

Disclaimer & Methodology

This report reflects UnifiedArc Security Advisor evaluations at the time of generation. Evidence files, customer attestations, accepted-risk exceptions, and resolution records may be maintained separately within UnifiedArc. This is a read-only assessment of discovered resources and evaluated controls and does not constitute a guarantee of compliance.

UnifiedArc - unifiedarc.com · Evaluated controls and discovered resources only. For the evidence + justification trail of resolved findings, see the Compliance Resolution Audit Report.