AWS Security & Cost Audit

Executive report · 15 April 2026 · Prepared by ScionTech

SECURITY RISK SCORE

76/100 **HIGH RISK**

Lower is better. Scored on the published rubric — see methodology.

Complete account compromise possible in minutes. Databases, SSH and Redis are all reachable from the public internet.

AUDIT SCOPE

2,304	checks executed
553	failures identified
418	resources audited
4	AWS regions covered

MAPPED TO · SOC 2 · ISO 27001 · GDPR · CIS · NIST

34	152	224	2,304
CRITICAL FINDINGS	HIGH FINDINGS	MEDIUM FINDINGS	CHECKS RUN

IMMEDIATE THREAT

Security group trader-sg (sg-0a1b2c3d4e5f60718, me-central-1) exposes all 65,535 ports to 0.0.0.0/0. Instance i-0f1e2d3c4b5a69788 at 203.0.113.47 is directly internet-reachable.

COMPLIANCE EXPOSURE

Current posture breaches controls across SOC 2, ISO 27001 and GDPR. Every finding below is mapped to the specific control it fails.

READ-ONLY ASSESSMENT

Every finding was confirmed from read-only credentials. Your environment was never modified.

Quick wins — actionable this week, zero disruption

1

Security group exposes all 65,535 ports to the internet

Issue: Security group trader-sg (sg-0a1b2c3d4e5f60718, me-central-1) exposes all 65,535 ports to 0.0.0.0/0. Instance i-0f1e2d3c4b5a69788 at 203.0.113.47 is directly internet-reachable.

Action: EC2 → Security Groups → sg-0a1b2c3d4e5f60718 → delete the inbound rule 0–65535 from 0.0.0.0/0. Then move the instance to a private subnet with NAT egress only.

```
aws ec2 revoke-security-group-ingress --group-id sg-0a1b2c3d4e5f60718 --protocol -1 --port 0-65535 --cidr 0.0.0.0/0
```

IMPACT
Removes critical finding

TIME
2 min

2

Dormant admin user with an 819-day unrotated key

Issue: User 'legacy-admin' holds AdministratorAccess with an 819-day unrotated access key that has been unused for 731 days. Role admin_role_saml also holds full AdministratorAccess.

IMPACT
Removes critical finding

Action: IAM → Users → legacy-admin → Permissions → detach AdministratorAccess. Delete the access key immediately, then apply a least-privilege policy.

TIME
2 min

3

Idle NAT Gateway carrying no traffic

Issue: nat-0be31633ccf076b2d is provisioned but carries no active traffic. It is billed at $32.85/month for a gateway serving zero purpose.

Action: VPC console → NAT Gateways → select nat-0be31633ccf076b2d → Actions → Delete.

MONTHLY SAVING
$32.85

TIME
1 min

4

EBS default encryption off; unencrypted volume and snapshot

Issue: EBS encryption is disabled by default in ap-south-1. Volume vol-0aa11bb22cc33dd44 and snapshot snap-0ee55ff66aa77bb88 are unencrypted. S3 Block Public Access is not set account-wide.

Action: EC2 → Data protection and privacy → enable "Always encrypt new EBS volumes" in every region. Then enable S3 Block Public Access at the account level.

```
aws ec2 enable-ebs-encryption-by-default --region ap-south-1
```

IMPACT
Removes high finding

TIME
3 min

5

GuardDuty and Security Hub disabled in all regions

Issue: GuardDuty and Security Hub are disabled across all 4 regions. The account has zero automated threat detection capability.

Action: GuardDuty console → Enable → repeat for all 4 regions. Connect to Security Hub and activate the CIS AWS Foundations Benchmark.

```
aws guardduty create-detector --enable
```

IMPACT
Removes high finding

TIME
5 min

6

CloudTrail disabled across all regions

Issue: CloudTrail is disabled across all 4 regions. Zero API activity is being logged anywhere in the account.

Action: CloudTrail console → Create trail → enable for all regions → S3 bucket destination with MFA delete and 1-year retention.

```
aws cloudtrail create-trail --name org-trail --s3-bucket-name <bucket> --is-multi-region-trail
```

IMPACT
Removes critical finding

TIME
10 min

All 6 quick wins take **23 minutes** of engineering effort in total. Every one removes an idle resource or enables a passive control — no code changes, no downtime, no rollback plan required.

Security findings — confirmed, with business impact

	SEVERITY	DOMAIN	CONFIRMED FINDING	BUSINESS RISK	REQUIRED ACTION
1	CRITICAL	Network me-central-1	Security group trader-sg (sg-0a1b2c3d4e5f60718, me-central-1) exposes all 65,535 ports to 0.0.0.0/0. Instance i-0f1e2d3c4b5a69788 at 203.0.113.47 is directly internet-reachable.	Complete account compromise possible in minutes. Databases, SSH and Redis are all reachable from the public internet.	EC2 → Security Groups → sg-0a1b2c3d4e5f60718 → delete the inbound rule 0–65535 from 0.0.0.0/0. Then move the instance to a private subnet with NAT egress only.
2	CRITICAL	IAM global	User 'legacy-admin' holds AdministratorAccess with an 819-day unrotated access key that has been unused for 731 days. Role admin_role_saml also holds full AdministratorAccess.	One leaked key means total account takeover. An attacker can delete all data, create backdoor users and hold the account permanently.	IAM → Users → legacy-admin → Permissions → detach AdministratorAccess. Delete the access key immediately, then apply a least-privilege policy.
3	CRITICAL	Monitoring global	CloudTrail is disabled across all 4 regions. Zero API activity is being logged anywhere in the account.	No forensic trail exists if breached. Fails SOC 2 CC7.2, ISO 27001 A.12 and GDPR Article 30 audit requirements.	CloudTrail console → Create trail → enable for all regions → S3 bucket destination with MFA delete and 1-year retention.
4	CRITICAL	IAM global	Root account accessed today with only virtual MFA configured. Root should never be used for routine operations.	Compromised root credentials mean permanent account ownership. Virtual MFA offers weaker protection than a hardware token.	Investigate the root usage in CloudTrail, enable hardware MFA, and adopt AWS Organizations centralised root management.
5	HIGH	Monitoring global	GuardDuty and Security Hub are disabled across all 4 regions. The account has zero automated threat detection capability.	Active cryptomining, credential theft or data exfiltration happening right now would go completely unnoticed.	GuardDuty console → Enable → repeat for all 4 regions. Connect to Security Hub and activate the CIS AWS Foundations Benchmark.
6	HIGH	Data ap-south-1	EBS encryption is disabled by default in ap-south-1. Volume vol-0aa11bb22cc33dd44 and snapshot snap-0ee55ff66aa77bb88 are unencrypted. S3 Block Public Access is not set account-wide.	Unencrypted data at rest. Decommissioned storage media or a shared snapshot is readable without credentials.	EC2 → Data protection and privacy → enable "Always encrypt new EBS volumes" in every region. Then enable S3 Block Public Access at the account level.
7	HIGH	Workload ca-central-1	IMDSv2 is not enforced on instance i-01a2b3c4d5e6f7089. RDS instance 'app-db' (ca-central-1) has no SSL enforcement and uses the default master username.	SSRF vulnerabilities can silently retrieve IAM credentials via the metadata service. RDS traffic is unencrypted in transit.	Enforce IMDSv2 account-wide via an EC2 launch template, and enforce SSL on the RDS parameter group for app-db.

Compliance framework impact

SOC 2
Breached: CC6.1, CC6.6, CC6.7, CC7.1, CC7.2

ISO 27001
Breached: A.10.1, A.12.4, A.13.1, A.13.2, A.9.2

CIS
Breached: 1.16, 1.6, 5.2

GDPR
Breached: Art. 30, Art. 32

90-day remediation roadmap

Week 1

- → Security group exposes all 65,535 ports to the internet
- → Dormant admin user with an 819-day unrotated key
- → Idle NAT Gateway carrying no traffic
- → EBS default encryption off; unencrypted volume and snapshot
- → GuardDuty and Security Hub disabled in all regions
- → CloudTrail disabled across all regions

Weeks 2–4

- → Enable Security Hub in all regions
- → Enforce IMDSv2 on all EC2 instances
- → Enable MFA on all console IAM users
- → Isolate internet-facing instances to private subnets
- → Delete unused IAM roles and security groups

Month 2

- → Enable EBS KMS encryption in all regions
- → Enforce SSL on RDS parameter groups
- → Enable VPC Flow Logs
- → Enrol all EC2 in SSM Session Manager
- → Add VPC endpoints for S3 and DynamoDB

Month 3

- → KMS CMK auto-rotation
- → AWS Config continuous enforcement
- → Quarterly IAM access review process
- → Cost anomaly detection and budget alerts
- → Document incident response playbook

Success metrics

KPI	CURRENT STATE	90-DAY TARGET
CloudTrail coverage	0/4 regions	Multi-region, all events logged
Threat detection	Disabled everywhere	GuardDuty + Security Hub, all regions
Network exposure	Admin port open to 0.0.0.0/0	Zero public internal services
MFA coverage	30% of console users	100% users; hardware MFA for admins
Max access key age	1414 days	All keys rotated under 90 days
Security risk score	76/100 HIGH	< 40/100 MODERATE within 90 days

Assessment

> This environment carries significant operational and compliance risk today. The combination of 34 critical findings — including security group exposes all 65,535 ports to the internet — represents a threat profile that enterprise insurers and compliance auditors would flag as requiring immediate remediation. **The critical findings can be resolved in under four hours of engineering effort.**

How the score was calculated

The score runs 0–100 where **lower is better**. It combines a saturating weighted-failure density (normalised by resource count, so a large estate is not penalised for size) with posture gates for step-function risks that counting alone under-weights. Full rubric and constants are published.

Security — 76/100		
Weighted failure density	**+34.2**	weighted failures 1207 ÷ 418 resources = density 2.89
CloudTrail coverage gap	**+12.0**	0/4 regions logging
GuardDuty coverage gap	**+8.0**	0/4 regions with threat detection
Admin port open to internet	**+10.0**	security group exposes all-ports or an admin port to 0.0.0.0/0
Console MFA gap	**+4.2**	30% of console users have MFA
Root without hardware MFA	**+3.0**	root protected by virtual MFA or none
Root credentials recently used	**+2.0**	root last used 0 day(s) ago
S3 account public access block off	**+3.0**	any misconfigured bucket can be exposed publicly
EBS default encryption off	**+2.0**	new volumes created unencrypted
Stale IAM access key	**+2.0**	oldest active key is 1414 days old
Security Hub disabled	**+2.0**	no aggregated findings or CIS benchmark scoring
Posture gate cap applied	**-6.2**	raw gate total 48.2 capped at 42