דוח לדוגמה — כל הנתונים בדויים · כך נראה הדוח השבועי שמגיע ללקוחות ShvoIT כל יום ראשון. לסקירה חינם של החשבון שלכם: shvoit.co.il/aws-report
054-4541632

AWS Weekly Security & Cost Audit

Demo Company Ltd (sample) · account 123456789012 · 2026-11-22T08:00 UTC

Regions scanned: 4 (eu-west-1, eu-central-1, us-east-1, us-west-2)
Expected regions: eu-west-1
Previous run: 2026-11-15 08:00 UTC

2 critical and 4 high findings require action – 1 of them new since 2026-11-15 08:00 UTC.

2	4	8	6	3	2	3
CRITICAL	HIGH	MEDIUM	LOW	INFO	NEW	RESOLVED

Priority actions (Critical & High)

Severity	Area	Finding	Recommended action
CRITICAL	Network	**Security group open to internet: 3389/RDP** NEW `sg-0a1b2c3d4e5f60718:tcp:3389-3389` eu-west-1 office-legacy-sg | 0.0.0.0/0 | used by: i-0f1e2d3c4b5a69788	Restrict source to office/VPN IPs or put behind SSM/VPN.
CRITICAL	IAM	**Root account has access keys** `root` Key last used 41 days ago	Delete root access keys; use IAM roles/users instead.
HIGH	IAM	**Access key older than 365 days** `ci-deploy (AKIA…7QX2)` Created 2024-08-02, used yesterday	Rotate the key; prefer OIDC/role-based CI credentials.
HIGH	IAM	**Console user without MFA** `dev-user01` Last console login 3 days ago	Enforce MFA for all console users.
HIGH	Network	**Security group open to internet: 22/SSH** `sg-0123abcd4567ef890:tcp:22-22` eu-west-1 bastion-sg | 0.0.0.0/0 | used by: i-0aa11bb22cc33dd44	Restrict source to office/VPN IPs or use SSM Session Manager.
HIGH	S3	**Bucket allows public read** `demo-marketing-assets` eu-west-1 Bucket policy grants s3:GetObject to *	Block public access; serve via CloudFront with OAC if public content is needed.

New since last run

Severity	Area	Finding
CRITICAL	Network	**Security group open to internet: 3389/RDP** NEW `sg-0a1b2c3d4e5f60718:tcp:3389-3389` eu-west-1 office-legacy-sg | 0.0.0.0/0 | used by: i-0f1e2d3c4b5a69788
MEDIUM	S3	**Bucket without versioning** NEW `demo-backups` eu-west-1 Holds DB dumps

Resolved since last run

Severity	Area	Finding
CRITICAL	S3	**Bucket allows public write** `demo-uploads-tmp` eu-west-1 Fixed after last week's report
HIGH	IAM	**Console user without MFA** `ops-admin`
MEDIUM	Network	**Security group open to internet: 3306/MySQL** `sg-0fedcba9876543210:tcp:3306-3306` eu-west-1

Spend (last 7 days)

$1,284.37 vs $1,402.90 previous week (▼ $118.53)

Amazon EC2	$612.40
Amazon RDS	$298.15
Amazon S3	$121.88
AWS Data Transfer	$97.30
Amazon CloudFront	$64.20
Other	$90.44

By area

Area	CRITICAL	HIGH	MEDIUM	LOW	INFO	Total
Cost				6	1	**7**
IAM	1	2			1	**4**
Network	1	1				**2**
S3		1	1			**2**
Compute			2			**2**
Logging			2			**2**
RDS			2			**2**
Edge			1			**1**
DNS					1	**1**

Trend

Run	CRITICAL	HIGH	MEDIUM	LOW
2026-11-01	4	7	11	9
2026-11-08	3	6	10	8
2026-11-15	2	5	9	7
2026-11-22	2	4	8	6

All findings (23)

Severity	Area	Finding	Recommended action
CRITICAL	Network	**Security group open to internet: 3389/RDP** NEW `sg-0a1b2c3d4e5f60718:tcp:3389-3389` eu-west-1 office-legacy-sg | 0.0.0.0/0 | used by: i-0f1e2d3c4b5a69788	Restrict source to office/VPN IPs or put behind SSM/VPN.
CRITICAL	IAM	**Root account has access keys** `root` Key last used 41 days ago	Delete root access keys; use IAM roles/users instead.
HIGH	IAM	**Access key older than 365 days** `ci-deploy (AKIA…7QX2)` Created 2024-08-02, used yesterday	Rotate the key; prefer OIDC/role-based CI credentials.
HIGH	IAM	**Console user without MFA** `dev-user01` Last console login 3 days ago	Enforce MFA for all console users.
HIGH	Network	**Security group open to internet: 22/SSH** `sg-0123abcd4567ef890:tcp:22-22` eu-west-1 bastion-sg | 0.0.0.0/0 | used by: i-0aa11bb22cc33dd44	Restrict source to office/VPN IPs or use SSM Session Manager.
HIGH	S3	**Bucket allows public read** `demo-marketing-assets` eu-west-1 Bucket policy grants s3:GetObject to *	Block public access; serve via CloudFront with OAC if public content is needed.
MEDIUM	S3	**Bucket without versioning** NEW `demo-backups` eu-west-1 Holds DB dumps	Enable versioning + Object Lock for backup buckets.
MEDIUM	Compute	**Workload outside expected regions** `i-0cc55dd66ee77ff88` us-east-1 t3.medium running 63 days	Confirm the workload is intended; terminate or move to eu-west-1.
MEDIUM	Compute	**Unencrypted EBS volume** `vol-0b9c8d7e6f5a43210` eu-west-1 200 GiB gp2, attached to i-0aa11bb22cc33dd44	Enable EBS encryption by default; migrate the volume via snapshot copy.
MEDIUM	Edge	**CloudFront distribution without WAF** `E2DEMO7XAMPLE` www.demo-company.example	Attach an AWS WAF web ACL with managed rule groups.
MEDIUM	Logging	**CloudTrail not multi-region** `demo-trail` Trail logs eu-west-1 only	Convert the trail to multi-region.
MEDIUM	Logging	**GuardDuty not enabled** `eu-west-1` eu-west-1 No detector in an active region	Enable GuardDuty in all regions with workloads.
MEDIUM	RDS	**RDS instance not Multi-AZ** `demo-prod-db` eu-west-1 db.m6g.large, PostgreSQL 15	Enable Multi-AZ for production databases.
MEDIUM	RDS	**RDS automated backups retention < 7 days** `demo-prod-db` eu-west-1 Retention: 1 day	Raise backup retention to at least 7 days.
LOW	Cost	**gp2 volumes that can move to gp3** `11 volumes` eu-west-1 ~20% saving · ~$35/month	Modify volumes to gp3 (no downtime).

LOW	Cost	**Old EBS snapshots (>180 days)** `42 snapshots` eu-west-1 ~1.8 TB · ~$90/month	Apply a snapshot lifecycle policy (DLM).
LOW	Cost	**Unused Elastic IP** `eipalloc-0a9b8c7d6e5f4a3b2` eu-west-1 ~$3.60/month	Release the Elastic IP.
LOW	Cost	**Idle EC2 instance (CPU < 3% for 14 days)** `i-0bb22cc33dd44ee55` eu-west-1 m5.xlarge · ~$140/month	Stop, downsize to t3.large, or terminate.
LOW	Cost	**Unattached EBS volume** `vol-0d1e2f3a4b5c6d7e8` eu-west-1 100 GiB gp3 · ~$8/month	Snapshot if needed, then delete.
LOW	Cost	**Unattached EBS volume** `vol-0e2f3a4b5c6d7e8f9` eu-west-1 500 GiB gp2 · ~$50/month	Snapshot if needed, then delete.
INFO	Cost	**No Savings Plan coverage** `account` On-demand compute ~$1,050/month	Consider a 1-year Compute Savings Plan (~25-30% saving).
INFO	DNS	**Route 53 hosted zone without DNSSEC** `demo-company.example`	Consider enabling DNSSEC signing.
INFO	IAM	**IAM Access Analyzer not enabled** `eu-west-1` eu-west-1	Enable Access Analyzer to detect external sharing.