

AWSight

AWS Security Quick Start

20 Critical Checks Every Growing Company Must Fix

A comprehensive security checklist based on AWS Foundational Security Best Practices, designed specifically for small and medium businesses looking to strengthen their cloud security posture without enterprise complexity.

Table of Contents

Why This Checklist Matters	2
Security Checks 1-10: Foundation and Access Control	3
Security Checks 11-20: Encryption, Detection and Recovery	6
Implementation Priority	9
Compliance Framework Mapping	9
Next Steps	10

Why This Checklist Matters

Cloud security breaches cost SMBs an average of \$2.98 million per incident, yet most organizations focus on complex enterprise solutions when simple misconfigurations cause 80% of security incidents.

This checklist distills the most critical AWS security configurations from over 500+ available checks in the AWS Foundational Security Best Practices standard. Each item has been selected based on:

- * High Impact - Prevents the most common attack vectors
- * SMB Relevance - Practical for companies with 50-500 employees
- * Implementation Speed - Can be completed without extensive security expertise
- * Compliance Alignment - Supports PCI DSS, SOC 2, HIPAA, and GDPR requirements

Time Investment	Ongoing Effort	Risk Reduction
2-4 hours initial	1-2 hours/month	80% of incidents

The Hidden Cost of Cloud Security Gaps

Recent studies show that 95% of cloud security incidents are caused by human error and misconfigurations, not sophisticated attacks. The Verizon 2025 DBIR shows 22% of initial access comes via stolen credentials. For growing companies, these seemingly small oversights can have devastating consequences:

- * Financial Impact - Companies face an average of 280 days to identify and contain a breach
- * Regulatory Penalties - GDPR fines can reach 4% of annual revenue; HIPAA violations average \$2.2 million
- * Customer Trust - 83% of customers will stop doing business with a company after a data breach
- * Operational Disruption - Companies experience an average of 21 days of downtime following an incident

Security Checks 1-10: Foundation and Access Control

1. Root Account Security

Root account has MFA enabled and is not used for daily operations

- Enable hardware MFA on root** Use FIDO2/hardware security keys for strongest protection
- Create IAM users for daily ops** Limits root exposure and provides audit trails
- Remove root access keys** Eliminates programmatic access to most powerful account
- Set up account contacts** Enables AWS to contact you about security issues

Why critical: Root account compromise = total AWS account takeover

2. IAM Password Policy

Strong password policy is enforced organization-wide

- Minimum 14+ characters** Makes brute force attacks computationally infeasible
- Require mixed characters** Uppercase, lowercase, numbers, and symbols required
- Password expiration 90-180 days** Limits exposure window if passwords are compromised
- Prevent password reuse** Block reuse of last 12 passwords

Why critical: Weak passwords are the #1 cause of account breaches

3. MFA for All IAM Users

Multi-factor authentication required for all human users

- Enable MFA for all IAM users** Prioritize FIDO2/hardware keys for administrators
- Require MFA for console access** Protects web-based AWS management interface
- MFA for sensitive CLI/API ops** Secures programmatic access to critical functions
- Document recovery procedures** Prevents lockout when devices are lost

Why critical: MFA blocks 99.9% of automated attacks

4. S3 Bucket Public Access

No S3 buckets allow unrestricted public access

- Block public ACLs on all buckets** Prevents accidental public access via ACL changes
- Block public bucket policies** Stops public access through policy modifications
- Enable account-level block** S3 Block Public Access protects all buckets
- Enable MFA Delete on critical** Requires MFA to delete objects or change versioning

Why critical: Public S3 buckets cause 70% of cloud data breaches

5. CloudTrail Logging

CloudTrail is enabled and properly configured

- Enable in all regions** Captures all API activity across entire AWS account
- Log file validation enabled** Detects if logs have been tampered with or deleted
- Secure S3 storage** Provides durable storage with proper access controls
- CloudWatch integration** Enables real-time alerting on suspicious activity

Why critical: Without CloudTrail, you are blind to security incidents

6. VPC Flow Logs

VPC Flow Logs enabled for network monitoring

- Enable for all VPCs** Captures network traffic metadata for analysis
- Capture all traffic types** Accepted, rejected, and all traffic for visibility
- Store in CloudWatch or S3** Enables analysis and long-term retention
- Set retention policies** Balances storage costs with compliance needs

Why critical: Network visibility is essential for incident response

7. Security Groups Configuration

Security groups follow least privilege principles

- No 0.0.0.0/0 on port 22** Prevents global SSH access attracting brute force
- No 0.0.0.0/0 on port 3389** Blocks worldwide RDP access vulnerable to attacks
- Remove unused groups** Reduces attack surface and management complexity
- Use descriptive names** Improves security management and change tracking

Why critical: Open ports to the internet = easy attacker entry points

8. EC2 Instance Security

EC2 instances follow security best practices

- No default security groups** Default groups often have overly permissive settings
- Require IMDSv2 only** Prevents SSRF attacks that steal instance credentials
- No unnecessary public IPs** Reduces internet exposure and attack surface
- Encrypt all EBS volumes** Protects data at rest from unauthorized access

Why critical: EC2 instances are primary attack targets - IMDSv2 is now required

9. RDS Database Security

RDS databases are properly secured

- No public accessibility** Keeps databases isolated from internet access
- Encryption at rest enabled** Protects stored data from physical access threats
- Backup retention 7+ days** Enables recovery from corruption or ransomware
- Automated backups enabled** Ensures consistent backup creation automatically

Why critical: Database breaches have the highest financial impact

10. IAM Unused Credentials

Remove unused and dormant IAM credentials

- Find 90+ day inactive users** Identifies dormant accounts that may be compromised
- Remove unused access keys** Eliminates programmatic access no longer needed
- Rotate active keys regularly** Limits exposure window if keys are compromised
- Use IAM roles instead** IAM Access Analyzer helps identify unused permissions

Why critical: Unused credentials are attack vectors with no monitoring

Security Checks 11-20: Encryption, Detection and Recovery

11. Encryption in Transit

Data transmission is encrypted with modern protocols

- HTTPS for all web apps** Use TLS 1.3 where possible - prevents data interception
- ELB SSL/TLS certificates** Encrypts traffic between users and load balancers
- CloudFront HTTPS redirects** Forces secure connections for CDN content delivery
- API Gateway HTTPS only** Secures API communications from client applications

Why critical: Unencrypted data can be intercepted and stolen

12. AWS Config Service

AWS Config tracks configuration changes

- Enable in all regions** Monitors configuration changes across all resources
- Record all resource types** Ensures comprehensive tracking of changes
- Config rules for compliance** Automatically detects non-compliant configurations
- Proper data retention** Maintains historical data for compliance and forensics

Why critical: Configuration drift leads to security vulnerabilities

13. GuardDuty Threat Detection

GuardDuty enabled for AI-powered threat detection

- Enable in all regions** Provides AI-powered threat detection coverage globally
- Monitor and act on findings** Ensures threats are investigated and mitigated promptly
- Configure auto-remediation** Lambda functions for automated threat response
- Enable threat intel feeds** Enhances detection with latest threat indicators

Why critical: Automated threat detection catches attacks humans miss

14. Lambda Function Security

Lambda functions follow security best practices

- Least-privilege IAM roles** Limits blast radius if function is compromised
- Encrypt environment vars** Protects sensitive configuration data in functions
- Deploy in VPCs when needed** Provides network isolation for sensitive operations
- Configure dead letter queues** Ensures failed executions do not cause data loss

Why critical: Over-privileged Lambda functions escalate minor breaches

15. Network Access Control Lists

NACLs provide additional network security layer

- Custom NACLs for sensitive** Adds subnet-level network access controls
- Review default NACLs** Ensures defaults do not allow excessive access
- Restrict egress traffic** Prevents data exfiltration and lateral movement
- Document NACL rules** Ensures rules remain effective and understood

Why critical: Defense in depth - security groups alone are not enough

16. Secrets Manager

Credentials stored securely, not in code

- Store DB passwords securely** Encrypts and rotates database credentials automatically
- Auto-rotate API keys** Limits exposure window of compromised keys
- Remove secrets from env vars** Prevents exposure in process lists and logs
- Log and monitor access** Detects unauthorized access to sensitive credentials

Why critical: Hardcoded secrets in code repositories cause massive breaches

17. EBS Volume Encryption

All data at rest is encrypted

- Enable default encryption** Automatically encrypts all new EBS volumes
- Identify unencrypted volumes** Finds legacy volumes that need encryption
- Encrypt all snapshots** Protects backup data from unauthorized access
- Use customer-managed KMS** Provides additional control over encryption keys

Why critical: Unencrypted data violates most compliance frameworks

18. CloudWatch Monitoring

Security monitoring and alerting configured

- Alarms for security events** Provides real-time notification of incidents
- Root account usage alerts** Detects unauthorized use of most powerful account
- Failed login attempt alerts** Identifies potential brute force attacks early
- Unusual API call detection** Spots anomalous behavior indicating compromise

Why critical: Late detection makes breaches exponentially more expensive

19. IAM Access Analyzer

IAM Access Analyzer identifies overprivileged access

- Enable Access Analyzer** Continuously analyzes permissions for external access
- Review external access** Identifies resources accessible from outside account
- Remediate unused access** Removes permissions that are never actually used
- Integrate with CI/CD** Catches permission issues before deployment

Why critical: Excessive permissions violate least privilege principle

20. Backup and Recovery

Critical data backup and recovery procedures tested

- Automated backups configured** Ensures consistent backup creation automatically
- Cross-region replication** Protects against regional disasters and outages
- Test recovery procedures** Ensures backups actually work when needed
- Define RTO objectives** Sets expectations for business continuity planning

Why critical: Ransomware attacks target backups - test your recovery plan

Implementation Priority

Timeline	Checks	Focus Area	Impact
Week 1	1-4	Root, IAM, MFA, S3	Prevents 90% of common attacks
Week 2	5-8	Logging, Network	Visibility and network protection
Week 3-4	9-16	Data, Encryption, Detection	Data protection and automation
Month 2	17-20	Advanced Controls	Comprehensive security posture

Compliance Framework Mapping

Check Range	PCI DSS	SOC 2	HIPAA	GDPR
1-4: Identity and Access	Yes	Yes	Yes	Yes
5-8: Logging and Network	Yes	Yes	Yes	Yes
9-12: Data Protection	Yes	Yes	Yes	Yes
13-16: Threat Detection	Yes	Yes	Yes	Yes
17-20: Advanced Controls	Yes	Yes	Yes	Yes

Next Steps

1. Assessment - Use this checklist to identify security gaps in your current AWS environment
2. Prioritization - Focus on Week 1 items first for maximum impact
3. Implementation - Work through each item systematically with your team
4. Validation - Regularly audit these configurations to ensure they remain secure

Automate Your AWS Security Monitoring

Manual security assessments are time-consuming and error-prone. AWSight automates this entire process, continuously monitoring your AWS infrastructure against all 500+ security best practices - not just these 20 critical ones.

- + Daily automated assessments of your complete security posture
- + Executive dashboards that translate technical findings into business impact
- + Compliance reporting for PCI DSS, SOC 2, HIPAA, and GDPR requirements
- + Real-time alerts when security configurations drift from best practices
- + Multi-account monitoring as your business scales across AWS environments

Ready to Automate Your AWS Security?

awsight.com

Start Your Free Security Assessment Today

This checklist is based on AWS Foundational Security Best Practices and real-world security incidents affecting SMB companies. For questions about AWS security best practices or automated security monitoring solutions, visit awsight.com or contact your security team.