Provided by:

AWSight

AWS Security Insights

awsight.com

Comprehensive AWS security monitoring and compliance solutions designed specifically for growing businesses. Get enterprise-grade security insights without the enterprise complexity.

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.

20	300+	80%
Critical Security Checks	AWS Security Controls	Incident Prevention

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 300 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: 2-4 hours for initial assessment
Ongoing Effort: 1-2 hours per month for maintenance
Risk Reduction: Prevents 80% of common cloud security 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. For growing companies, these seemingly small oversights can have devastating consequences:

- **Financial Impact:** Beyond the immediate costs, companies face an average of 280 days to identify and contain a breach
- **Regulatory Penalties:** GDPR fines can reach 4% of annual revenue, while HIPAA violations average $2.2 million per incident
- **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 a security incident

Why AWS Security is Different

AWS operates on a "shared responsibility model" where Amazon secures the infrastructure, but customers are responsible for securing their data and applications. This creates unique challenges:

- **Complexity:** Over 200 AWS services with thousands of configuration options
- **Default Settings:** AWS defaults prioritize ease of use over security
- **Rapid Change:** New features and services launch constantly, each with their own security considerations
- **Skill Gap:** Most IT teams lack dedicated AWS security expertise

The SMB Security Advantage

While enterprise organizations struggle with complex, expensive security solutions, small and medium businesses have a unique opportunity to implement focused, effective security measures:

- **Agility:** Faster decision-making and implementation cycles
- **Focused Scope:** Fewer systems and applications to secure
- **Cost Efficiency:** Targeted security investments with immediate ROI

- **Modern Architecture:** Ability to build security into new systems from the ground up

Beyond Compliance: Building Security Culture

This checklist isn't just about meeting regulatory requirements—it's about building a security-conscious culture that scales with your business:

- **Proactive vs. Reactive:** Prevent incidents rather than responding to them
- **Continuous Improvement:** Regular security assessments become routine business practice
- **Employee Awareness:** Team members understand their role in maintaining security
- **Customer Confidence:** Demonstrate your commitment to protecting customer data

The following 20 security checks represent the foundation of a robust AWS security posture. Each check includes specific implementation steps, business justification, and clear success criteria. By completing these items, you'll address the vast majority of security vulnerabilities that affect growing companies.

Automated Security Management with AWSight

While this checklist provides the roadmap for securing your AWS environment, manually implementing and maintaining these 20+ security controls can be time-consuming and error-prone. **AWSight** automates this entire process, continuously monitoring your AWS infrastructure against all 300+ security best practices—not just these 20 critical ones.

With AWSight, you get:

- **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 move beyond manual checklists? Visit **awsight.com** to see how automated security monitoring can protect your growing business while freeing your team to focus on innovation rather than security maintenance.

1 Root Account Security

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

- [ ] Enable MFA on root account
  Prevents unauthorized access even if password is compromised
- [ ] Create IAM users for daily operations
  Limits root account exposure and provides audit trails
- [ ] Remove access keys from root account
  Eliminates programmatic access to most powerful account
- [ ] Set up account contact information
  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+ character passwords
  Makes brute force attacks computationally infeasible
- [ ] Require uppercase, lowercase, numbers, symbols
  Increases password entropy and crack resistance
- [ ] Password expiration (90-180 days)
  Limits exposure window if passwords are compromised
- [ ] Prevent password reuse (last 12 passwords)
  Forces users to create genuinely new 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
  Adds second authentication factor beyond passwords
- [ ] Require MFA for console access
  Protects web-based AWS management interface
- [ ] Require MFA for CLI/API access to sensitive operations
  Secures programmatic access to critical functions
- [ ] Document MFA device recovery procedures
  Prevents lockout situations 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 through ACL changes
- [ ] Block public bucket policies
  Stops public access through policy modifications
- [ ] Ignore public ACLs
  Provides additional layer against public ACL settings
- [ ] Restrict public bucket policy access
  Blocks public policies from being applied

Why critical:

Public S3 buckets cause 70% of cloud data breaches

5 CloudTrail Logging

CloudTrail is enabled and properly configured

- [ ] CloudTrail enabled in all regions
  Captures all API activity across your entire AWS account
- [ ] Log file validation enabled
  Detects if logs have been tampered with or deleted
- [ ] Logs stored in secure S3 bucket
  Provides durable storage with proper access controls
- [ ] Multi-region trail configured
  Ensures global visibility regardless of region usage

Why critical:

Without CloudTrail, you're blind to security incidents

6 VPC Flow Logs

VPC Flow Logs enabled for network monitoring

- [ ] Enable VPC Flow Logs for all VPCs
  Captures network traffic metadata for analysis
- [ ] Capture accepted, rejected, and all traffic
  Provides complete visibility into network activity
- [ ] Store logs in CloudWatch or S3
  Enables analysis and long-term retention of flow data
- [ ] Set up log retention policies
  Balances storage costs with compliance requirements

Why critical:

Network visibility is essential for incident response

7 Security Groups Configuration

Security groups follow least privilege principles

- [ ] No security groups allow 0.0.0.0/0 on port 22 (SSH)
  Prevents global SSH access that attracts brute force attacks
- [ ] No security groups allow 0.0.0.0/0 on port 3389 (RDP)
  Blocks worldwide RDP access vulnerable to attacks
- [ ] Remove unused security groups
  Reduces attack surface and management complexity
- [ ] Use descriptive security group 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 instances use default security groups
  Default groups often have overly permissive settings
- [ ] All instances use IMDSv2 (Instance Metadata Service v2)
  Prevents SSRF attacks that steal instance credentials
- [ ] No instances have public IP addresses unless required
  Reduces internet exposure and attack surface
- [ ] EBS volumes are encrypted
  Protects data at rest from unauthorized access

Why critical:

EC2 instances are primary attack targets

9 RDS Database Security

RDS databases are properly secured

- [ ] RDS instances are not publicly accessible
  Keeps databases isolated from internet access
- [ ] RDS encryption at rest is enabled
  Protects stored data from physical access threats
- [ ] RDS backup retention is configured (7+ days)
  Enables recovery from corruption or ransomware
- [ ] RDS automated backups are enabled
  Ensures consistent backup creation without manual intervention

Why critical:

Database breaches have the highest financial impact

10 IAM Unused Credentials

Remove unused and dormant IAM credentials

- [ ] Identify users with no activity in 90+ days
  Finds dormant accounts that may be compromised
- [ ] Remove unused access keys
  Eliminates programmatic access that's no longer needed
- [ ] Rotate active access keys regularly
  Limits exposure window if keys are compromised
- [ ] Delete unnecessary IAM users
  Reduces overall account attack surface

Why critical:

Unused credentials are attack vectors with no monitoring

11 Encryption in Transit

Data transmission is encrypted

- [ ] HTTPS enforced for all web applications
  Prevents data interception during transmission
- [ ] ELB listeners use SSL/TLS certificates
  Encrypts traffic between users and load balancers
- [ ] CloudFront uses HTTPS redirects
  Forces secure connections for CDN content delivery
- [ ] API Gateway enforces HTTPS
  Secures API communications from client applications

Why critical:
Unencrypted data can be intercepted and stolen

12 Config Service

AWS Config tracks configuration changes

- [ ] AWS Config enabled in all regions
  Monitors configuration changes across all AWS resources
- [ ] Configuration recorder capturing all resources
  Ensures comprehensive tracking of resource changes
- [ ] Config rules for compliance monitoring
  Automatically detects non-compliant configurations
- [ ] Config data retention properly configured
  Maintains historical data for compliance and forensics

Why critical:
Configuration drift leads to security vulnerabilities

13 GuardDuty Threat Detection

GuardDuty enabled for threat detection

- [ ] GuardDuty enabled in all regions
  Provides AI-powered threat detection coverage globally
- [ ] GuardDuty findings monitored and acted upon
  Ensures threats are investigated and mitigated promptly
- [ ] Trusted IP lists configured (if applicable)
  Reduces false positives from known good sources
- [ ] Threat intelligence feeds enabled
  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

- [ ] Lambda functions don't use administrative IAM roles
  Limits blast radius if function is compromised
- [ ] Environment variables are encrypted
  Protects sensitive configuration data in functions
- [ ] Functions are deployed in VPCs when appropriate
  Provides network isolation for sensitive operations
- [ ] Dead letter queues configured for error handling
  Ensures failed executions don't cause data loss

Why critical:

Over-privileged Lambda functions escalate minor breaches

15 Network Access Control Lists (NACLs)

NACLs provide additional network security layer

- [ ] Custom NACLs implemented for sensitive subnets
  Adds subnet-level network access controls
- [ ] Default NACLs reviewed and hardened
  Ensures default settings don't allow excessive access
- [ ] Egress rules restrict unnecessary outbound traffic
  Prevents data exfiltration and lateral movement
- [ ] NACL rules documented and maintained
  Ensures rules remain effective and understood

Why critical:

Defense in depth - security groups aren't enough

16 Secrets Manager

Credentials stored securely, not in code

- [ ] Database passwords stored in Secrets Manager
  Encrypts and rotates database credentials automatically
- [ ] API keys rotated automatically
  Limits exposure window of compromised keys
- [ ] Application secrets removed from environment variables
  Prevents secrets exposure in process lists and logs
- [ ] Secrets access logged and monitored
  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

- [ ] Default EBS encryption enabled
  Automatically encrypts all new EBS volumes
- [ ] Existing unencrypted volumes identified
  Finds legacy volumes that need encryption
- [ ] EBS snapshots are encrypted
  Protects backup data from unauthorized access
- [ ] Customer-managed KMS keys used where appropriate
  Provides additional control over encryption keys

Why critical:
Unencrypted data violates most compliance frameworks

18 CloudWatch Monitoring

Security monitoring and alerting configured

- [ ] CloudWatch alarms for critical security events
  Provides real-time notification of security incidents
- [ ] Root account usage monitoring
  Detects unauthorized use of most powerful account
- [ ] Failed login attempt alerting
  Identifies potential brute force attacks early
- [ ] Unusual API call pattern detection
  Spots anomalous behavior indicating compromise

Why critical:
Late detection makes breaches exponentially more expensive

19 Access Analyzer

IAM Access Analyzer identifies overprivileged access

- [ ] IAM Access Analyzer enabled
  Continuously analyzes resource permissions for external access
- [ ] External access findings reviewed regularly
  Identifies resources accessible from outside your account
- [ ] Unused access findings remediated
  Removes permissions that are never actually used
- [ ] Access Analyzer integrated into CI/CD pipeline
  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 for all critical resources
  Ensures consistent backup creation without manual intervention
- [ ] Cross-region backup replication enabled
  Protects against regional disasters and outages
- [ ] Backup recovery procedures documented and tested
  Ensures backups actually work when needed
- [ ] Recovery time objectives (RTO) defined and validated
  Sets expectations for business continuity planning

Why critical:

Ransomware attacks target backups - test your recovery plan

Implementation Priority

Week 1 (Immediate)

Items 1-4: Root account, IAM, MFA, S3 public access

Impact: *Prevents 90% of common attack vectors*

Week 2 (High Priority)

Items 5-8: Logging, monitoring, network security

Impact: *Provides visibility and network protection*

Week 3-4 (Medium Priority)

Items 9-16: Database security, encryption, threat detection

Impact: *Protects data and enables automated threat response*

Month 2 (Long-term)

Items 17-20: Advanced security controls and business continuity

Impact: *Comprehensive security posture and resilience*

Compliance Framework Mapping

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

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

Need Help Implementing These Checks?

Manual security assessments are time-consuming and error-prone. Many growing companies find that automated Cloud Security Posture Management (CSPM) solutions provide continuous monitoring of all 300+ AWS security controls with executive dashboards and automated reporting.

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.