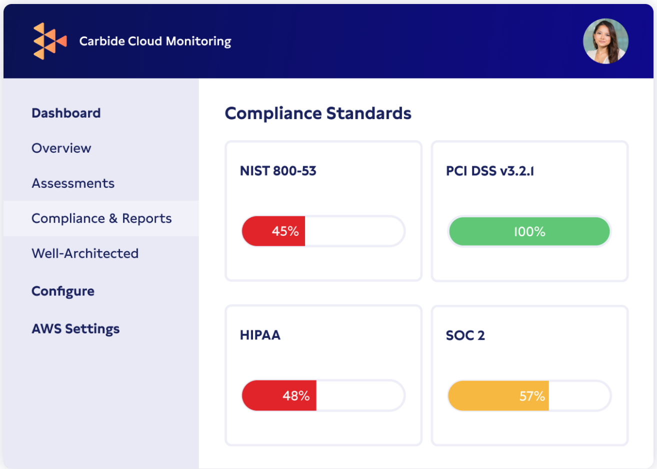
Carbide

Continuous Cloud Monitoring

There's nothing more foundational than your application and the cloud environment(s) it sits in. That's why Carbide does more than just check your security controls—we also give you the guidance and tools you need to design, operate, and optimize a secure cloud environment.



Compliance Standards

NIST 800-53 45%

PCI DSS v3.2.I 100%

HIPAA 48%

SOC 2 57%

Architecting a secure cloud environment you can trust

These days, spinning up a cloud environment is as simple as clicking a button. But making sure that environment is secure, compliant, and well architected? That takes a lot more.

Carbide Cloud Monitoring aligns with our DRIVE (Design, Review, Implement, Validate, and Evolve) methodology to support you throughout your security journey: flagging gaps, collecting evidence, and continuously monitoring your environment.

Here's just some of what you'll be able to do:

Collect evidence you need from both AWS and Azure to meet compliance requirements

Access remediation templates and scripts that make it easy to address gaps and implement best practice recommendations

Monitor your compliance status across all your AWS and Azure environments against more than a dozen frameworks/regulations

Automate AWS Well-Architected reviews for your environment and identify ways to improve performance or reduce costs

Track progress over time against more than 400 security best practices, including a robust threat management dashboard

Design & Review

In the Design & Review stage, Carbide Cloud Monitoring provides tools to design and optimize your cloud environment, including architectural recommendations for Amazon Web Services (AWS) and security recommendations for both AWS & Microsoft Azure.

AWS WELL-ARCHITECTED REVIEWS

Quickly generate an assessment of your environment against the pillars of the AWS Well-Architected Framework.

With 90% coverage for the Security Pillar (and partial coverage for other pillars), Carbide Cloud Monitoring offers security recommendations and highlights opportunities to improve performance or reduce costs through more efficient architecture.

CLOUD SECURITY GAP ANALYSIS

Using both automated and on-demand assessments, you can quickly assess your cloud security posture, even across multiple cloud environments and gain an understanding of your security maturity level across six critical areas:

- Logging & Monitoring
- Identity & Access Management
- Infrastructure Security
- Data Protection & Encryption
- Backup & Resiliency
- Cost and Usage

This analysis takes into account more than 400 security checks and best practices with details into each error, and remediation recommendations for AWS environments.

Strengthen your cloud security with Carbide Cloud Monitoring

Implementation

In the Implementation stage, Carbide Cloud Monitoring helps AWS customers build a more secure environment.

PRE-BUILT CONFIGURATION PACKAGES & GUIDED WALKTHROUGHS

Save hours with pre-built configuration packages and guided walkthroughs of common deployments of AWS settings and services such as enabling security and logging services, backups & disaster recovery, networking services, compliance monitoring, and more.

Notable packages include:

- Deploy common Service Control Policies (SCPs) to protect security and logging services
- Deploy an Amazon Virtual Private Cloud
- Set up scheduled EC2 Instance patching
- Monitoring PCI DSS compliance
- Set up Identity and Access Management events and compliance rules
- …and many more!

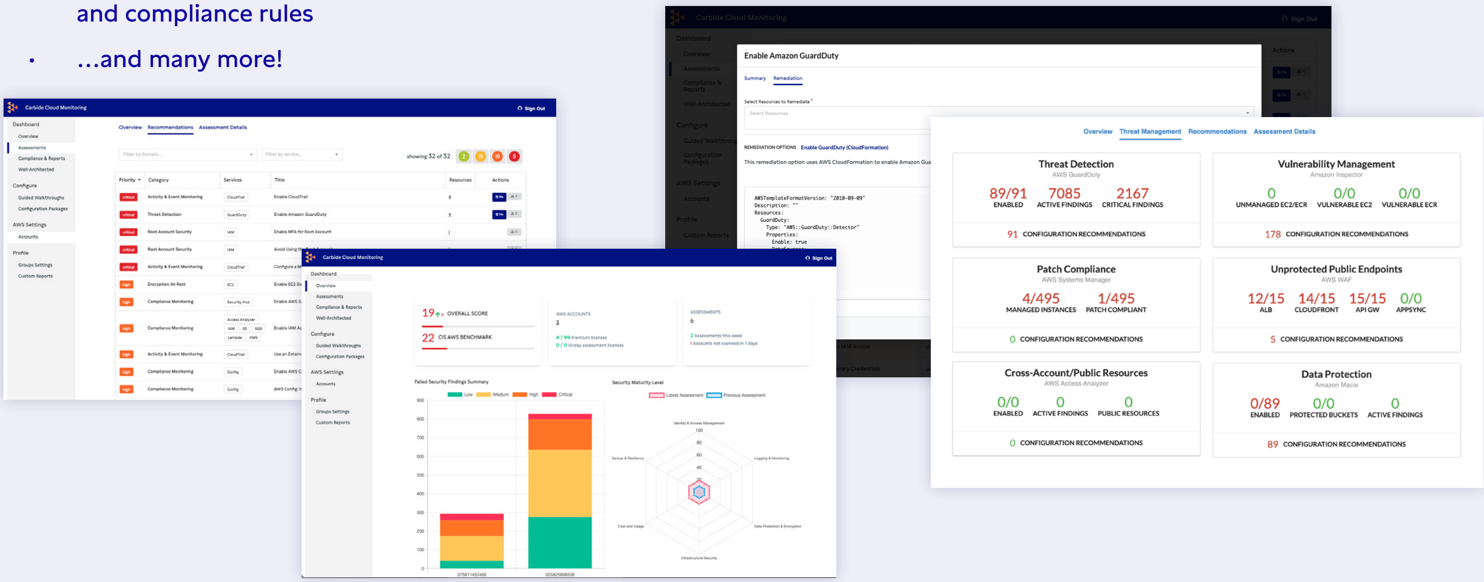
REMEDIATION TEMPLATES & RECOMMENDATIONS

Through your Well-Architecture Review and Automated Assessments, you'll get clear, actionable guidance on how to address gaps, including CLI and/or CloudFormation templates that are generated specifically for your environment.

THREAT MANAGEMENT DASHBOARD

Keep on top of emerging threats, newly identified vulnerabilities, patch management, endpoint and data protection, and access configurations, even as your environment changes over time.

Carbide Cloud Monitoring's threat management dashboard ensures you sustain your security posture by making it simple to maintain vigilance over your cloud environments.



Carbide Cloud Monitoring

Sign Out

Dashboard: Overview, Assessments, Compliance & Reports, Well-Architected

Configure: Guided Walkthroughs, Configuration Packages

AWS Settings: Accounts

Profile: Groups Settings, Custom Reports

Overview | Recommendations | Assessment Details

Filter by Domain... | Filter by service...

showing 32 of 32 — 2 | 15 | 10 | 5

Priority	Category	Services	Title	Resources	Actions
critical	Activity & Event Monitoring	CloudTrail	Enable CloudTrail	4	Fix ⚠ 0
critical	Threat Detection	GuardDuty	Enable Amazon GuardDuty	4	Fix ⚠ 0
critical	Root Account Security	IAM	Enable MFA for Root Account	1	⚠ 0
critical	Root Account Security	IAM	Avoid Using th		
critical	Activity & Event Monitoring	CloudTrail	Configure a M		
high	Encryption At-Rest	EC2	Enable EC2 De		
high	Compliance Monitoring	Security Hub	Enable AWS S		
high	Compliance Monitoring	Access Analyzer IAM S3 SQS Lambda KMS	Enable IAM Ac		
high	Activity & Event Monitoring	CloudTrail	Use an Extern		
high	Compliance Monitoring	Config	Enable AWS C		
high	Compliance Monitoring	Config	AWS Config: I		

19 ↑9 OVERALL SCORE

22 CIS AWS BENCHMARK

AWS ACCOUNTS 3

4 / 99 Premium licenses

0 / 0 10-day assessment licenses

ASSESSMENTS 6

2 Assessments this week

1 Accounts not scanned in 7 days

Enable Amazon GuardDuty

Summary | Remediation

Select Resources to Remediate *

Select Resources

REMEDIATION OPTIONS Enable GuardDuty (CloudFormation)

This remediation option uses AWS CloudFormation to enable Amazon Gua

```
AWSTemplateFormatVersion: "2010-09-09"
Description: ""
Resources:
  GuardDuty:
    Type: "AWS::GuardDuty::Detector"
    Properties:
      Enable: true
```

Overview | Threat Management | Recommendations | Assessment Details

Threat Detection — AWS GuardDuty: 89/91 ENABLED; 7085 ACTIVE FINDINGS; 2167 CRITICAL FINDINGS; 91 CONFIGURATION RECOMMENDATIONS

Vulnerability Management — Amazon Inspector: 0 UNMANAGED EC2/ECR; 0/0 VULNERABLE EC2; 0/0 VULNERABLE ECR; 178 CONFIGURATION RECOMMENDATIONS

Patch Compliance — AWS Systems Manager: 4/495 MANAGED INSTANCES; 1/495 PATCH COMPLIANT; 0 CONFIGURATION RECOMMENDATIONS

Unprotected Public Endpoints — AWS WAF: 12/15 ALB; 14/15 CLOUDFRONT; 15/15 API GW; 0/0 APPSYNC; 5 CONFIGURATION RECOMMENDATIONS

Cross-Account/Public Resources — AWS Access Analyzer: 0/0 ENABLED; 0 ACTIVE FINDINGS; 0 PUBLIC RESOURCES; 0 CONFIGURATION RECOMMENDATIONS

Data Protection — Amazon Macie: 0/89 ENABLED; 0/0 PROTECTED BUCKETS; 0 ACTIVE FINDINGS; 89 CONFIGURATION RECOMMENDATIONS

Validation

Once you've acted on the recommendations identified on your dashboard and in your reports, it's time to prove that posture to an auditor or assessor.

COMPLIANCE REPORTS

Capture your security posture across all your AWS and Azure cloud environments (e.g. development, testing, production) with both templated and customized reports.

You'll understand your posture against controls such as PCI DSS, SOC 2, NIST 800-171, HIPAA, GDPR, and more (with even more being added to the tool all the time), with enough detail to satisfy any auditor.

Evolution

Security and privacy require constant vigilance to sustain as your environment changes based on your business demands. Here's how Carbide Cloud Monitoring can help keep you on top of your security game.

CONTINUOUS DASHBOARD & AUTOMATED ASSESSMENTS

Keep security front and center with a clear dashboard across all your AWS and Azure environments, as well as automated, weekly assessments delivered directly into your inbox. You'll be able to quickly review the latest at-risk resources so you can take action quickly.