COALFIRE

Coalfire extends security of Amazon Web Services (AWS)

aws partner network

Advanced Consulting Partner

Public Sector Partner

Coalfire, a cybersecurity advisory firm, has been working with AWS and many ecosystem partners on their security and compliance validations, certifications, and authorizations for a variety of initiatives over the years. Coalfire is an advisor and/or assessor to AWS, its U.S. East/West and GovCloud environments, and ecosystem partners, delivering supporting services for Payment Card Industry Data Security Standards (PCI DSS) and 3-D Secure (3DS), HIPAA Security Rule, ISO, Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG), HITRUST, and FedRAMP®, as well as penetration testing.

Coalfire's work with AWS enables business in the cloud by demonstrating AWS' proactive approach to cloud security. Additionally, Coalfire educates the AWS ecosystem of partners, clients, and prospects on how to leverage AWS' security investment and what they each need to do. Coalfire is an Advanced Partner Network Consulting Partner with Government Competency.

AWS SECURITY POSTURE

Since 2012, Coalfire has worked with AWS to provide advisory services or assessment services to meet government or industry requirements.

- **FedRAMP:** Supported AWS' initiatives with FedRAMP in both the Agency Authority to Operate (ATO) and FedRAMP Joint Authorization Board (JAB) Provisional-ATO (P-ATO) process for GovCloud and U.S. East/West Regions. This included the formal assessment of the cloud environment and services contained within the authorization boundary to meet FedRAMP requirements. Assisted with the continuous improvement of AWS' security posture by being a trusted partner in their continuous monitoring and remediation efforts.
- **DoD SRG:** Assessed the organization for Impact Level II authorization, conducting technical testing, privacy review, and controls assessment. Completed DoD SRG Level 2 for AWS U.S. East/West and DoD SRG Levels 4 and 5 for AWS GovCloud.
- **PCI DSS:** Audited to PCI DSS, resulting in a report on compliance (ROC) for various services. This ensures the cardholder data environment (CDE) met compliance through their efforts to increase security around the CDE.
- **PCI 3DS:** Assessed the AWS infrastructure. Developed a white paper, outlining how customers can leverage AWS to support 3DS workloads.
- **HITRUST:** Completed a validated assessment of the AWS infrastructure and 122 services.
- **HIPAA advisory:** Provided HIPAA advisory support for the AWS ProServe team.
- **Penetration testing:** Identified and exploited critical vulnerabilities, and then provided remediation guidance, which demonstrated that AWS' network and information assets were protected from threats. These penetration tests were conducted as part of compliance requirements and standalone proactive testing initiatives.

LEVERAGE AWS SECURITY INVESTMENTS

Businesses looking to migrate or build new applications in the cloud can now leverage the work AWS has put into PCI DSS, HIPAA Security Rule, DoD SRG, and FedRAMP.

SECURITY BY DESIGN

The Coalfire Engineering Team can design, build, and optimize compliant and secure-by-design AWS reference architectures to the following standards:

U.S. Public Sector:
FISMA, FedRAMP, CJIS, IRS 1075, and DFARS/ NIST SP 800-171

Financial:
FFIEC, PCI DSS, SOC, and ISO 27001/2/18

Healthcare:
HIPAA, HITRUST, SOC 2 Type 1/2, and ISO 27001/2/18

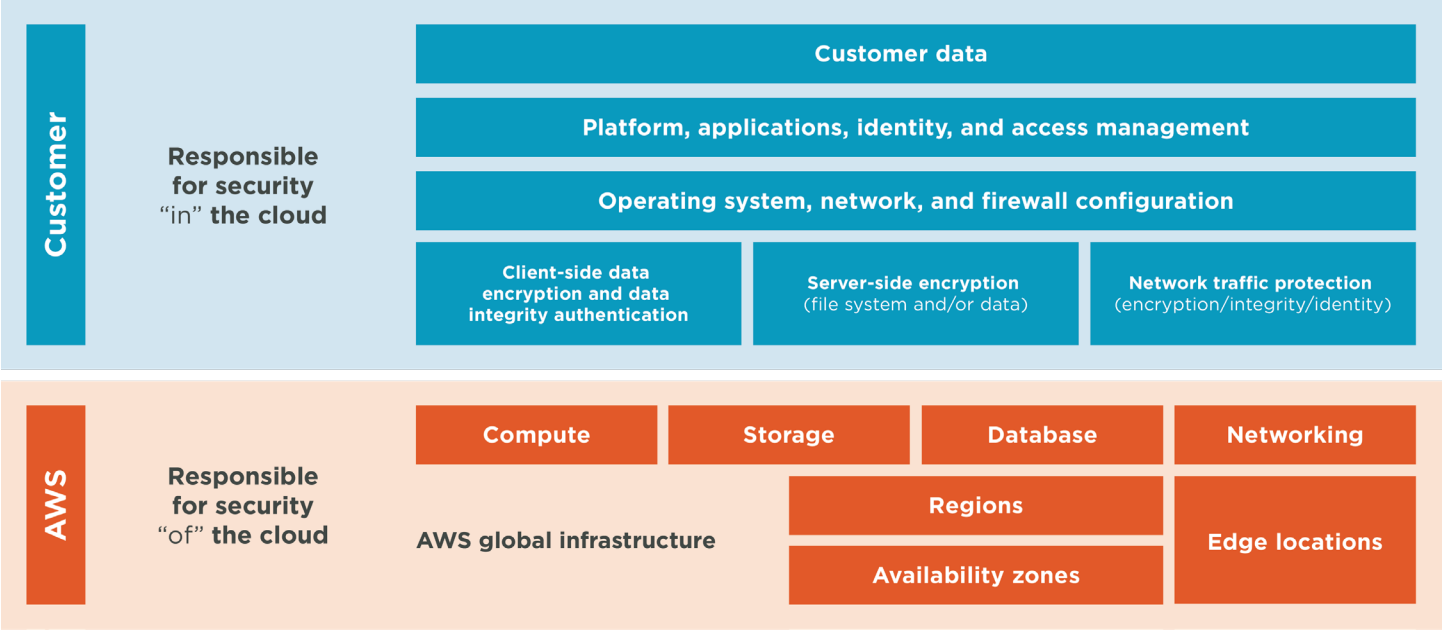
AWS' work to protect the cloud enables clients to focus on securing the data they put into the cloud for their business needs.

Using its broad security and architecture understanding of the AWS IaaS environments and regulatory compliance, Coalfire can develop and provide reference architectures for various client industries. As new client onboarding increases, a referenceable architecture set can help ensure that migration or deployment on AWS meets best practices for industry or multi-industry compliance and efficiently gets clients up and running in a secure, compliant manner on AWS.

AWS' SECURITY IN THE CLOUD

Clients should no longer question security in the cloud with AWS, as AWS has built security in as a foundational element and is developing security tools that clients can use to increase their security postures. AWS' shared responsibility means clients can only leverage AWS to a point, through control inheritance, before clients must implement or undertake their own security programs to ensure their unique businesses also meet security and compliance requirements.

AWS shared responsibility



About Amazon Web Services

Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform.

To learn more, visit **Coalfire.com/AWS**

About Coalfire

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com**

COALFIRE

For more information about Coalfire, visit **Coalfire.com**, or to speak to an expert about your organization's security needs, visit **Coalfire.com/contact**.