

How AWS can help you enhance your security posture

In accordance with the AWS Shared Responsibility Model, Amazon Web Services provides a global infrastructure built to meet requirements of the most security-sensitive organizations. You, the customer, are responsible for securing services built on top of this infrastructure. To help with this initiative, AWS services and third-party software in AWS Marketplace are available that help you strengthen your security posture in the cloud.



Meet compliance requirements



AWS supports **over 50 international** compliance standards by helping protect sensitive data and enabling data sovereignty, among other solutions.

AWS Marketplace offerings help you comply with regulatory requirements by **ensuring proper data management & enabling audit-readiness**.

Enhance event management



Amazon S3 server-side encryption (SSE) protects all log files delivered from CloudTrail to a specified Amazon S3 bucket, enabling you to get the most out of your logging and monitoring solutions.

ISV solutions available in AWS Marketplace **enable single pane of glass visibility** across your environment, enabling more effective security incident event management (SIEM).

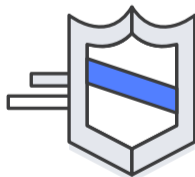
Keep your data safe



Strong safeguards **help protect customer privacy**; all data is stored in highly secure AWS data centers.

ISV AWS Marketplace offerings and AWS services provide **options for you to create & control encryption keys** to encrypt your data in motion and at rest in AWS.

Protect applications from targeted attacks



AWS global infrastructure consists of **multiple Availability Zones within Regions** designed to enable highly available and fault tolerant workloads.

Infrastructure security offerings in AWS Marketplace can help you **design for visibility and enforcement** against cyber-attacks, advanced threats & malware.



Find and deploy the solution you need in minutes



Save money with pay-as-you-go pricing



Scale globally across all AWS Regions