CROWDSTRIKE | aws

# Securing cloud workloads with CrowdStrike and AWS

**Security teams face increasing challenges from lack of visibility, complex solutions and sophisticated attacks. CrowdStrike integrations with AWS solutions can help provide:**

### ENHANCED VISIBILITY

Continuous and comprehensive AWS workload monitoring, including container visibility, ensuring nothing is missed and stealthy attacks can be stopped

### BREACH PROTECTION

Protect against breaches with unparalleled coverage. Defend AWS workloads against threats from malware to the most sophisticated attacks

### REDUCED OVERHEAD

Reduces the overhead, friction and complexity associated with protecting AWS cloud workloads

### AUTOMATED SECURITY

Enable cloud security to keep up with the dynamic and flexible nature of AWS workloads

## Where CrowdStrike and AWS work together

### CrowdStrike & AWS compute services

- Containers workloads
- Amazon EC2 instances –including Graviton
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service

### CrowdStrike & AWS Cloud services integrations

- AWS Control Tower
- AWS Security Hub
- AWS System Manager
- AWS PrivateLink
- Amazon GuardDuty

### Public sector solutions

- US government compliance
- NIST framework
- Falcon on AWS GovCloud

### CrowdStrike security products

- CrowdStrike Falcon Complete – Security-as-a-Service
- Falcon Discover for Cloud
- Falcon APIs and RTR - CI/CD Integrations

**All available on AWS Marketplace, a curated digital software catalog that helps you find, test, buy, and provision software and data products**

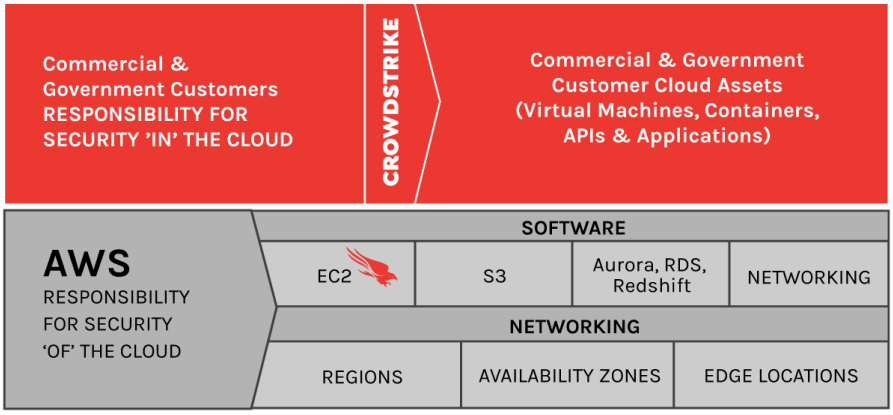
aws marketplace

# Strengthen security and compliance with CrowdStrike and AWS

## CrowdStrike and AWS help provide complete security for the cloud through a commitment to the Shared Responsibility Model

Customers have their choice of security configurations **IN** the Cloud

AWS is responsible for the security **OF** the Cloud




aws partner network
Advanced Technology Partner
Security Competency

# Public sector security support with Falcon on AWS GovCloud

## AWS GovCloud

- AWS GovCloud (US) is FedRAMP high certified
- Meets all government compliance regulations, including:
  - DOJ's Criminal Justice Information Systems (CJIS) Security Policy
  - U.S. International Traffic in Arms Regulations (ITAR)
  - Export Administration Regulations (EAR)
  - Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) for Impact Levels 2, 4 and 5
  - FIPS 140-2
  - IRS-1075

## Falcon on AWS GovCloud

- Falcon provides next-gen antivirus, endpoint detection and response (EDR), and IT hygiene
- Delivered via a single lightweight agent, from within the trusted AWS GovCloud
- Each component is tailored for securing the U.S. public sector, FedRAMP authorized and delivered from AWS GovCloud (US)
- Purchase through AWS Marketplace can help with streamlined procurement process

# Get started with CrowdStrike and AWS today

CrowdStrike in AWS Marketplace

CrowdStrike Endpoint Security for AWS

CrowdStrike Free Trial

CrowdStrike Falcon Endpoint Protection

CrowdStrike Falcon Discover

CrowdStrike Falcon Complete

Falcon for AWS

AWS Security services

CROWDSTRIKE | aws