







# Build Securely with AWS and CrowdStrike

Let your customers focus on their business.  
We'll handle the security.

Organizations leverage Amazon Web Services (AWS) to transform their cloud infrastructure and unlock powerful opportunities for growth, innovation, and operational excellence, while simultaneously introducing complex cybersecurity challenges. CrowdStrike helps solve these challenges by providing comprehensive protection & visibility across all AWS workloads, hosts, and containers.

Security teams face increasing challenges from lack of visibility, complex solutions and sophisticated attacks.

## CROWDSTRIKE INTEGRATES WITH AWS SOLUTIONS TO PROVIDE:

 <b>Automated security</b> Enable cloud security to keep up with the dynamic and flexible nature of AWS workloads	 <b>Reduced overhead</b> Reduces the overhead, friction and complexity associated with protecting AWS cloud workloads	 <b>Enhanced visibility</b> Continuous & comprehensive AWS workload monitoring, including container visibility, ensuring nothing is missed and stealthy attacks can be stopped	 <b>Breach protection</b> Protect against breaches with unparalleled coverage. Defend AWS workloads against threats from malware to the most sophisticated attacks
---	---	--	--



### Secure as you deploy

Instantly deploy CrowdStrike Falcon® Cloud Security across the AWS environment to ensure comprehensive protection as operations expand.



### Comprehensive AWS protection

From initial deployment to ongoing operations, safeguard AWS resources at every step—covering instances, containers, and managed services.



### See your cloud. Know your cloud.

CrowdStrike automatically discovers AWS resources as they're deployed and pinpoints misconfigurations, vulnerabilities, and elevated privileges to improve security posture.

## Core CrowdStrike security pillars

- Falcon Cloud Security
- Falcon Endpoint Protection
- CrowdStrike Services
- Falcon Identity Protection
- CrowdStrike Falcon NG SIEM



## CrowdStrike in AWS Marketplace

Available on AWS Marketplace, a curated digital software catalog that helps you find, test, buy, and provision software and data products.

### DEPLOYED ON AWS

#### Why go through AWS Marketplace?

**Cost Efficiency:** Consolidate billing into AWS and leverage committed spend (EDP/PPA discounts) to lower overall costs

**Flexibility:** Custom pricing and terms via private offers  
— 10% reduction in licensing costs\*

**Simplified Procurement:** Accelerate contract signing and procurement — 66% time savings\*

**Faster Onboarding:** Onboard vendors 75% faster\*

**Leverage Cloud Budgets:** Use AWS budget effectively with third-party software purchases

**Consolidated Billing:** Streamlined billing simplifies software management

**Compliance & Control:** Consistent way to manage software compliance and purchases

**Reliable Solutions:** Access trusted, high-quality solutions through AWS Marketplace

## What customers are saying:

*"Now with CrowdStrike, we can remediate any cloud intrusion in less than 16 minutes, which puts our minds at ease, while ensuring a great user experience for our clients."*

Kevin Tsuei,  
SVP Information Security Officer,  
Commercial Bank of California

*"CrowdStrike's CNAPP provides a deep and accurate view of the cloud threat landscape that we believe sets them apart from the competition."*

Dave Worthington,  
GM Security and Risk,  
Jemena

*"The one-click remediation testing feature stands out amongst the new CIEM capabilities for CrowdStrike [Falcon] Cloud Security."*

Frank Dickson,  
Group Vice President, Security and Trust,  
IDC

*"We wanted a force multiplier, CrowdStrike gives us the ability to be more of a cyber intelligence and cyber fraud team ... moving us from cybersecurity to overall security."*

Alex Arango,  
Deputy CISO,  
Mercury Financial

\* Source: Forrester Total Economic Impact™ study — The Partner Opportunity for AWS Marketplace ISVs

For more information visit  
[cdw.com/aws](https://cdw.com/aws)