CROWDSTRIKE

Blueprints for Secure AWS Workloads

Full workload and container visibility and protection from CrowdStrike Falcon Cloud Security, plus a comprehensive view of alerts through AWS Security Hub, are the sharpest tools to build secure cloud architectures

aws PARTNER

- Public Sector
- Amazon Linux Ready
- Marketplace Seller
- Security Software Competency

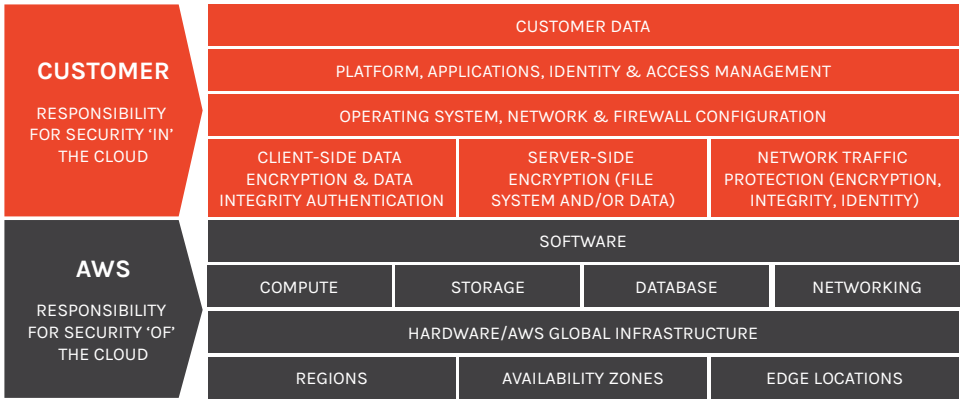
CrowdStrike eBook

Table of Contents

Outdated blueprints leave today's cloud architectures vulnerable to attacks

While cloud adoption has skyrocketed, many security postures are still stuck in the past. Extending legacy, on-premises security tools to work in the cloud has proved to be inadequate, leaving cloud architects and DevOps teams without a clear blueprint for securing applications, workloads, and infrastructure.

Establish a strong security foundation with Amazon Web Services (AWS) and CrowdStrike—a leader in cloud-delivered endpoint and workload protection. The combination of CrowdStrike Falcon and AWS Security Hub delivers centralized and automated management of threat alerts from AWS services including Amazon GuardDuty. With CrowdStrike Falcon Cloud Security, you can enhance the security of your AWS workloads and adopt the Shared Responsibility Model.



CrowdStrike Falcon Cloud Security Protects Your Workloads Running on AWS

AWS protects your cloud infrastructure

AWS Security Hub delivers a comprehensive view of security alerts and compliance

- Aggregate alert data from Falcon and native AWS services like Amazon GuardDuty
- Monitor the status of your AWS infrastructure through visual displays
- Conduct compliance checks

CrowdStrike Falcon Cloud Security protects your AWS workloads through a single lightweight agent

- Advanced cloud-native application security, including breach prevention, workload protection and cloud security posture management.
- Simplify your security stack with a single agent that has small footprint on AWS resources for better performance
- Shrink the amount of architecture necessary for full security visibility and reduce complexity to derive more value from your AWS investments

Falcon and AWS build seamless security into your workflows

CrowdStrike's integration with AWS Security Hub enables a comprehensive, real-time view of high-priority security alerts. CrowdStrike's API-first approach brings together Falcon Cloud Security and AWS Security Hub, making it easier for your entire team—including DevOps, CISO, cloud architects, and operations—to automate security tasks and improve overall protection.

SEE IT—WITH COMPLETE VISIBILITY

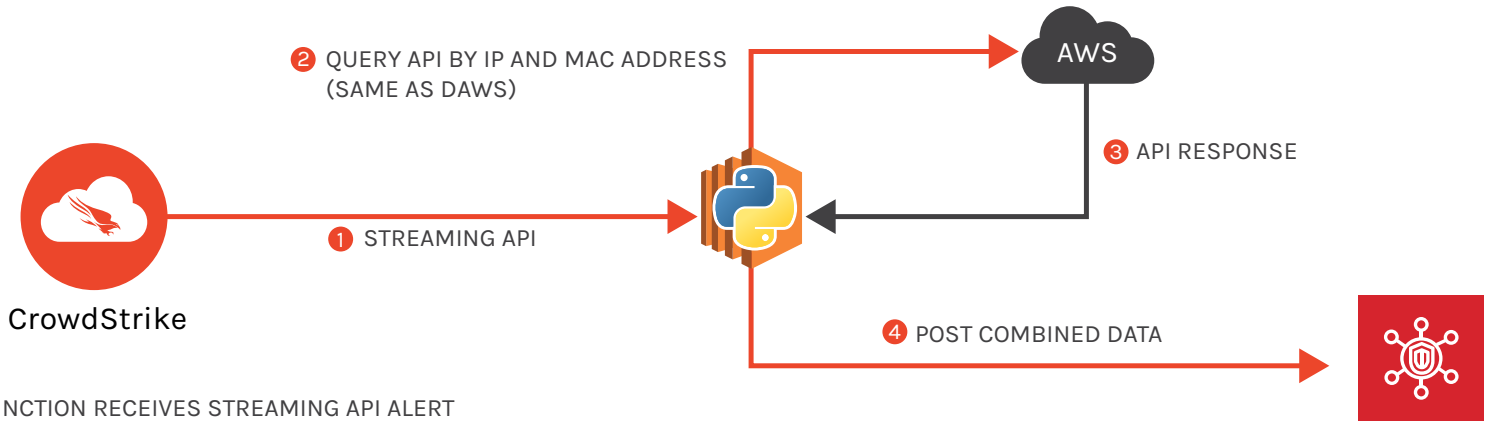
Falcon Cloud Security protects your AWS workloads across the entire threat lifecycle by combining machine learning, artificial intelligence, behavioral analytics, and proactive threat hunting in a single solution.

SECURE IT—WITH BETTER PERFORMANCE

Falcon Cloud Security works everywhere—Amazon Elastic Cloud Compute (Amazon EC2) instances, Amazon Elastic Container Service (Amazon ECS) on Amazon EC2, and Amazon Elastic Kubernetes Service (Amazon EKS) on Amazon EC2—providing endpoint and workload security even when they're offline.

DEFEND IT—WITH A SIMPLIFIED ARCHITECTURE

Falcon Cloud Security simplifies complex DevSecOps pipelines and increases operational reliability by simplifying cloud architectures. Falcon consolidates your endpoint and workload agents with an extensible platform that grows and adapts to your needs without adding complexity.



1. LAMBDA FUNCTION RECEIVES STREAMING API ALERT
2. LAMBDA FUNCTION QUERIES AWS API FOR INFORMATION
3. IF MATCHED TO AN EC2 INSTANCE DATA IS RETURNED
4. EC2 AND CROWDSTRIKE DATA IS COMBINED, FORMATTED AND SENT TO AWS SECURITY HUB

See it—with complete visibility

With alerts from Amazon GuardDuty and Falcon Cloud Security, aggregated through AWS Security Hub, your team has a single-pane-of-glass view that delivers the situational awareness necessary for strategic security and resource decisions. Automating routine security analysis speeds up your ability to find and address the most critical incidents among the noise.

Leverage Threat Graph intelligence

Discover potential threats quickly and accurately with AI-powered Threat Graph intelligence—achieving a level of protection for your AWS workloads previously not possible.

Automate security tasks

Without Threat Graph, analysts would have to manually gather endpoint and workload telemetry, add intelligence feeds, write correlation rules, and finally pivot the data to determine how security events might be related. But with Falcon Cloud Security, all the intelligence, events, and their relationships are captured in one place, enabling security administrators to automate analysis for smarter and deeper visibility when investigating potential breaches.

Integrate security into CI/CD pipelines

Falcon Cloud Security enables cloud security teams to keep up with the dynamic and flexible nature of AWS workloads. Seamless support for CI/CD deployment workflows comes through powerful APIs and streamlined integration with AWS Security Hub.

DevOps teams drive more automation

- Automate delivery of development pipelines
- Reduce the complexity of deployment and management
- Achieve security at the speed of application delivery

Security teams gain deeper insights

- Add more context to your AWS security alerts
- Understand the impact of security events
- Simplify incident response
- Identify intent based on indicators of attack
- Reduce false positives and increase security efficiencies

7+ trillion
events/week

200K
new IOCs published daily

200+
adversaries tracked

1.2+ million
malware samples processed daily

Secure it—with better performance

With CrowdStrike, you only need one sensor to protect all your endpoints and workloads—from IoT devices, to laptops, to cloud compute instances. Using AWS Security Hub as your dashboard, you can aggregate and prioritize security alerts from Falcon Cloud Security and Amazon GuardDuty to protect Amazon EC2 instances or containers running on Amazon ECS and Amazon EKS.

Keep Amazon EC2 instances secure and performant

Falcon Cloud Security uses cloud-native scaling to secure Amazon EC2 instances with minimal impact on runtime performance, and no storm scans or invasive signature updates. It provides protection against all advanced attacks that bypass traditional perimeter and signature-based approaches.

Protect containers running on Amazon ECS and Amazon EKS

Falcon Cloud Security runs on the Amazon EC2 instance node, protecting all containers running on it, including those managed by Amazon ECS and Amazon EKS. From known malware to the most sophisticated attacks, Falcon protects containers through workload monitoring and discovery, looking at parameters such as the container's unique identifier and configuration type, then funnels alerts to AWS Security Hub.

Shift container security left within CI/CD pipelines

Moving security tasks earlier in the software development lifecycle enables teams to discover flaws before they take a major toll. By adding Falcon Cloud Security to your CI/CD deployment workflows, you gain runtime security for Amazon ECS and Amazon EKS workloads, as well as visibility into containerized applications. View and mange events like risky container images through the AWS Security Hub dashboard.

1
lightweight agent

0
reboots required

DevOps teams can code more easily

- Achieve malware protection without integrating a legacy appliance
- Simplify code and scripts with a single agent that attaches seamlessly

Security teams improve understanding

- Correlate AWS alerts with Falcon Cloud Security detection for faster triage and remediation
- Provide a threat hunting platform for the operations team

Defend it—with a simplified architecture

Efficiency gains from Falcon Cloud Security and AWS Security Hub working in tandem help you speed time to detection, investigation, and remediation to stop more breaches. Integrated service for full security means a more efficient team that spends less time managing separate workstreams. Maximize the power of AWS Security Hub to aggregate events by leveraging the threat intelligence and simplified architecture of CrowdStrike.

Simplify AWS architectures

Other security vendors often require complex routing for legacy applications that must be inserted into the packet flow, and numerous workload agents to provide antivirus, EDR, and container security that are separately installed and managed. This can add complexity to your AWS environments and increase downtime. As a single agent, Falcon delivers the same level of security with less overhead.

Speed response times

Prioritized incidents within AWS Security Hub help streamline the triage process, allowing your team to address the most critical threats first.

Boost efficiency for greater cost savings

The ability to procure Falcon Cloud Security in the AWS Marketplace allows you to take advantage of integrated metering and billing, while also optimizing spend for elastic workloads.

100,000 nodes
in a day for immediate deployment

75%
more efficient

DevOps can get started faster

- Bake in security and remediation with an endpoint sensor
- Skip the installation—CrowdStrike ties in from a SaaS-based console
- Bootstrap one single security service for total protection

Cloud architects streamline designs

- Consolidate architecture for simpler builds
- Scales as cloud workloads expand — no need for additional infrastructure
- Powerful APIs enable automation of all functional areas for defense-in-depth

Operate with excellence

Cybersecurity is not simply a technology problem—protecting your AWS workloads also requires effective people and processes. Ignoring security operations can result in damage and remediation efforts that slow down DevOps and reduce up-time of your critical applications. These impacts can be prevented if the security technologies are configured properly and kept up to date, and the security alerts that precede an incident are triaged, investigated, and remediated promptly.

Many organizations struggle with this operational side of security because the skilled staff needed to execute cybersecurity 24/7/365 can be difficult and expensive to hire.

Augment your team with managed detection and response

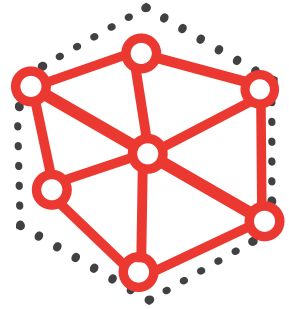
CrowdStrike Falcon Complete is a managed detection and response (MDR) service that augments the effectiveness of the Falcon platform with the efficiency of a dedicated team of security professionals. Falcon Complete delivers relentless focus on managing and monitoring your endpoint and workload security and responds to threats with speed and precision—so you don't have to.

DevOps teams experience fewer disruptions

- 24/7 monitoring with surgical remediation eliminates threats quickly without affecting the underlying workload

Security teams gain immediate expertise and effectiveness

- Security policies continuously tuned for maximum effectiveness
- Threats identified and eradicated in minutes
- Peace of mind, backed by a Breach Prevention Warranty



The 1-10-60 framework is the ideal timing we recommend companies try to meet to be faster than the adversaries:

<1 Minute
time to detect threats

<10 Minutes
time to understand threats

60 Minutes
time to eliminate threats

Get started with CrowdStrike on AWS today

For more information on CrowdStrike and AWS solutions, visit:

- CrowdStrike Falcon Cloud Security
- CrowdStrike page in the AWS Marketplace
- Gain an understanding of your security posture with a Cloud Security Risk Review