CrowdStrike Products

CROWDSTRIKE

aws partner network

Advanced
Technology
Partner

Security Competency

FALCON FOR AWS

Breach protection for AWS workloads

ENHANCE PROTECTION OF AND VISIBILITY INTO AWS WORKLOADS TO DEFEND AGAINST BREACHES

- **PROTECTION:** Protect against breaches with unparalleled coverage — defend against AWS threats from malware to the most sophisticated attacks
- **VISIBILITY:** Continuous and comprehensive workload monitoring, including container visibility to ensure nothing is missed and stealthy attacks can be stopped
- **SIMPLICITY:** Built in the cloud for the cloud — reduces the overhead, friction and complexity associated with protecting AWS workloads
- **AUTOMATION:** Enable cloud security to keep up with the dynamic and flexible nature of AWS workloads

CROWDSTRIKE FALCON PLATFORM — BUILT IN THE CLOUD TO PROTECT THE CLOUD

The CrowdStrike Falcon Platform offers unique breach prevention capabilities to help organizations enhance the security of AWS workloads without compromising performance.

ENHANCE PROTECTION OF AWS WORKLOADS WITH CROWDSTRIKE

- Supports Amazon Elastic Compute Cloud (Amazon EC2) instances, Amazon Elastic Container Service (Amazon ECS) & Amazon Elastic Kubernetes Service (Amazon EKS) containers, Windows and Linux, including Amazon Linux
- Integrates with AWS Security Hub for centralized and automated management of threat alerts from AWS services
- AWS Registered Security Competency
- Amazon GuardDuty threat intelligence partner
- Pay-as-you-go option

KEY SOLUTION CAPABILITIES

EC2 AND CONTAINERS PROTECTION

Falcon for AWS combines the best and latest technologies to protect cloud workloads against data breaches, malware and sophisticated attacks.

- Machine Learning and AI protect against known and zero-day malware
- Protection against prevalent cloud workload threats such as web shells, SQL shells and credential theft
- Behavior-based indicators of attack (IOAs) detect sophisticated attacks such as fileless and malware-free
- Exploit protection and blocking
- Managed threat hunting 24/7 ensures stealthy attacks don't go undetected

VISIBILITY

Falcon for AWS offers full endpoint detection and response (EDR) for cloud workloads and provides continuous and comprehensive workload visibility across your AWS environment.

- Full EDR prevents silent failure by capturing raw events for complete visibility
- Visibility into incidents involving containers with process trees showing container IDs
- Kernel level visibility provides detailed and deep insight into key workload events
- Full attack visibility provides details, context and history for every alert
- Event details and full set of enriched data is continuously available, even for ephemeral and decommissioned workloads
- Rogue instances detection help identify unprotected instances
- User account monitoring provides regular and privileged accounts identification and monitoring and historical view of user logon activities
- Application usage monitoring uncovers what is being run on your instances
- Extensive AWS visibility provides information about AWS environment, accounts and instances, such as Falcon coverage, number of AWS accounts, EC2 instances, virtual private clouds (VPCs), EBS storage — this includes security groups (IDs and names) and associated ingress and egress ACLs

SIMPLICITY

Protect cloud workloads without added complexity and overhead.

- Works everywhere and covers Windows, Linux, including Amazon Linux and containers
- Automatically kept up to date with SaaS delivery
- One console provides central visibility over cloud workloads regardless of their location
- Protection policies — complete flexibility as to how policies are applied at an individual server, group or data center level

AUTOMATION

Eliminate manual processes in key and cumbersome areas to boost cloud security efficiency.

- Automatic detection of attacker behavior, with prioritized alerts and severity weight, eliminating the need for time-consuming manual searches and assessments
- Integration with CI/CD deployment workflows

CONTAINER SECURITY

- Delivers container security through a single agent running on the node that protects the instance itself as well as all containers running on it
- Detects malicious activity involving containers
- Provides visibility into incidents involving containers with process trees showing container IDs

KEY BENEFITS

- Protect your AWS workloads against data breaches, malware and sophisticated attacks
- Gain visibility across your AWS environment via one console without sacrificing system performance
- Reduce security complexity with one platform built in the cloud to protect the cloud

- Powerful APIs that enable automation of all functional areas including detection, management, response and intelligence
- Automatically applies protection to virtual workloads as they spin up
- Automatically scales, as cloud workloads expand, with no need for additional infrastructure
- Automatically kept up to date with native cloud architecture
- Automates investigations and threat analysis to accelerate incident response

PERFORMANCE

Falcon for AWS provides the ultimate breach protection without compromising cloud performance.

- No reboots, so no inconvenience from workload downtime
- Lightweight — operates with only a tiny footprint on the endpoint
- No invasive updates — new functionality is added in the cloud without having to take resources from or disrupt cloud workloads
- No signatures — no disruption or performance impact from having to deploy signatures updates on a daily/hourly basis
- No scan storms — machine learning and pre-execution prevention in Falcon completely eliminates the need for AV scans and the performance degradation they cause on virtual systems
- Zero impact on runtime performance — even when analyzing, searching and investigating

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over two trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**

FALCON FOR AWS PROVIDES

- Instance details for your ops team, particularly those who don't have direct access to your EC2 instances
- Visibility and additional context into your AWS instances — Falcon for AWS identifies and catalogs metadata on all your EC2 instances across all regions, including instances without the Falcon sensor installed, for the AWS accounts you provide
- Extends protection to containers running on protected hosts
- Instant view of Falcon agent coverage in the AWS environment
- Total number of AWS accounts and of EC2 instances — also EC2 instances that have access to the internet and total EBS storage
- Lists all security groups (IDs and names) and associated ingress and egress ACLs
- List of virtual private clouds (VPCs)

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**