

FALCON CLOUD WORKLOAD PROTECTION

Breach prevention for cloud workloads and containers

CLOUD WORKLOAD PROTECTION ACROSS ALL ENVIRONMENTS

CrowdStrike Falcon® Cloud Workload Protection provides comprehensive breach protection across private, public, hybrid and multi-cloud environments — all delivered via the lightweight Falcon agent and managed by the CrowdStrike® cloud-native platform. The Falcon platform allows customers to rapidly adopt and secure technology across any workload.

KEY CAPABILITIES

VISIBILITY INTO CLOUD WORKLOADS

Comprehensive visibility into cloud workload events and instance metadata enables detection, response, and proactive threat hunting and investigation, ensuring that potentially malicious activities don't go unnoticed.

- Gathers metadata at the instance level to easily identify owners of assets involved in an alert
- Groups hosts by account ID, allowing for quick and easy visualization and identification of assets per owner
- Automatically detects and intelligently prioritizes suspicious and malicious activity
- Continuously monitors events to provide visibility into workload activities, including activities running inside containers; a full set of enriched data and event details allows investigations against ephemeral and decommissioned workloads
- Delivers proactive threat hunting across all workloads and endpoints from the same console
- Detects and investigates attacks that span multiple environments and

KEY BENEFITS

Gain comprehensive workload visibility from a single console

Automatically discover cloud workload footprints

Eliminate friction with key cloud integrations

Secure workloads at the speed of DevOps without sacrificing performance

Pay for what you use with a consumption-based billing option

Seamlessly migrate from on-premises to cloud with a consistent level of visibility and protection

Enable and accelerate threat hunting and investigation in the cloud

FALCON CLOUD WORKLOAD PROTECTION

- different types of workloads, and pivots from endpoint to instances to containers
- Provides response capabilities that allow you to contain and investigate compromised workloads and take action
 - Includes CrowdScore™ Incident Workbench to unravel attacks and improve response time by distilling and correlating security alerts into incidents, automatically triaging, prioritizing and highlighting those that deserve urgent attention

MULTI-CLOUD WORKLOAD DISCOVERY

Falcon provides visibility into the scope and nature of public and hybrid cloud footprints.

- Automatically discovers existing cloud workload deployments — without installing an agent — by enumerating existing Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances, Google Cloud Platform (GCP) Compute Engine instances and Microsoft Azure virtual machines
- Provides real-time information about workloads including context-rich metadata about system size and configuration, networking, and security group information for AWS, GCP and Azure
- Identifies workloads that are not protected by the Falcon platform
- Offers insight into your cloud footprint so you can secure all workloads, uncover and mitigate risks, and reduce the attack surface

CONTAINER SECURITY

Falcon provides protection and visibility without impacting container performance.

- Secures the host and container via a single Falcon agent running on the host
- Investigates container incidents easily when detections are associated with the specific container and not bundled with the host events
- Captures container start, stop, image and runtime information, and all events generated inside the container even if it only runs for a few seconds
- Provides visibility into container footprint including on-premises and cloud deployments, and shows container usage, including trends, uptime, images used, and configuration to identify risky and misconfigured containers
- Offers a single management console for host and container security

RUNTIME PROTECTION

The Falcon platform combines the best and latest technologies to protect against active attacks and threats when workloads are the most vulnerable — at runtime.

- Delivers machine learning (ML) and artificial intelligence (AI) to detect known and unknown malware
- Includes behavior-based indicators of attack (IOAs) that detect sophisticated threats such as fileless and malware-free attacks
- Provides exploit protection
- Includes custom IOAs, whitelisting and blacklisting to tailor detection and prevention
- Offers integrated threat intelligence to block known malicious activities and deliver the complete context of an attack, including attribution
- Provides 24/7 managed threat hunting to ensure that stealthy attacks don't go undetected

MULTI-CLOUD AND BROAD OS SUPPORT

The CrowdStrike Falcon platform provides comprehensive protection coverage that can be deployed across Windows and Linux (Amazon, Red Hat, CentOS, Oracle, SUSE, Ubuntu and Debian). It is compatible with AWS, Microsoft Azure and GCP and works with any hypervisor, including vSphere and Hyper-V.

SUPPORTED CONTAINERS

Falcon supports Open Container Initiative (OCI)-compliant containers such as Docker, orchestration platforms such as self-managed Kubernetes, and hosted orchestration platforms such as GKE (Google Kubernetes Engine), EKS (Amazon Elastic Kubernetes Service), ECS (Amazon Elastic Container Service), AKS (Azure Kubernetes Service) and OpenShift



FALCON CLOUD WORKLOAD PROTECTION

API-LED CLOUD INTEGRATIONS

Falcon eliminates friction to boost cloud security efficiency.

- Powerful APIs allow automation of CrowdStrike Falcon functionality, including detection, management, response and intelligence
- Chef, Puppet and AWS Terraform integrations support continuous integration/continuous delivery (CI/CD) deployment workflows
- Google Cloud Operating System (OS) configuration management integration automates Falcon agent deployment directly from GCP, without the need for custom scripts
- AWS PrivateLink integration enables sensor-to-cloud traffic to flow via PrivateLink, reducing internet exposure and simplifying network architectures

SIMPLICITY AND PERFORMANCE

Built in the cloud for the cloud, Falcon reduces the overhead, friction and complexity associated with protecting cloud workloads.

- One platform handles all workloads and works everywhere: private, public and hybrid clouds
- One console provides central visibility over cloud workloads, regardless of their location
- Falcon offers complete policy flexibility — apply at the individual workload, group or higher level
- It scales as cloud workloads expand — no need for additional infrastructure
- It operates with only a tiny footprint on the host and has almost zero impact on runtime performance, even when analyzing, searching and investigating
- Flexible consumption-based and annual-based subscription models support agile business planning

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 3 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.

