CROWDSTRIKE

FALCON CLOUD WORKLOAD PROTECTION

Breach prevention for cloud workloads and containers

CLOUD WORKLOAD PROTECTION THAT TRANSFORMS THE WAY DEVOPS WORKS

The need for speed and agility in today's digital business requires changes to IT infrastructure, most notably the shift to cloud-native architectures and the adoption of DevOps. This shift has led many businesses to move to containers, microservices and Kubernetes (K8s) to improve the efficiency and scalability of development efforts and form the very foundation for their next-generation, immutable infrastructure.

Additionally, continuous integration/continuous delivery (CI/CD) introduces ongoing automation and continuous monitoring throughout the application lifecycle, from integration and testing to delivery and deployment, resulting in faster innovation. This shift toward CI/CD is not without risk as infrastructure, DevOps and security teams look for ways to ensure containers and microservices remain secure and compliant while eliminating security blind spots.

As containers introduce a new environment and a different management construct with Kubernetes, security teams are finding it difficult to keep up. The result is an increase in risk due to poor visibility; fragmented approaches to detecting and preventing threats; misconfigurations for cloud workloads, containers and serverless; and the inability to maintain compliance.

Common challenges to securing containers include:

- Lack of visibility into cloud workloads, containers and Kubernetes environments
- Ineffective vulnerability management for container images, registries, libraries and hosts
- Securing container orchestration
- Protecting cloud-native workloads and containers at runtime
- Lack of cloud security skills and a growing attack surface
- Meeting and maintaining compliance and enforcing security policies

Manual processes and traditional solutions can't match the rapid change and unique challenges organizations now face with containers. Alternatives can include complex cloud security platforms or siloed tools, which can add more vendors and increase the complexity of your organization's overall security.

KEY BENEFITS

Continuously scans and identifies vulnerabilities, threats, embedded secrets and compliance violations

Delivers unparalleled visibility with detailed cloud workload events, container events and metadata

Identifies cloud workloads running in your environment, including those running with potentially risky configurations

Provides continuous runtime protection for all cloud workloads and containers

Enables and accelerates threat hunting and investigation for any workload

Protects immediately without sacrificing performance, matching the speed of DevOps

Adapts to the dynamic scalability of cloud workloads and containers in real time

THE CROWDSTRIKE APPROACH TO SECURING CLOUD WORKLOADS AND CONTAINERS

CrowdStrike secures its cloud infrastructure by focusing on staying ahead of adversaries, relentlessly reducing its attack surface and obtaining total visibility of events taking place in the environment. Stopping breaches across cloud workloads, containers and Kubernetes environments using cloud-scale data and analytics requires a tightly integrated platform. Each function plays a crucial part in identifying vulnerabilities early, detecting threats, protecting at runtime and enforcing compliance, and they must be designed and built for speed, scale and reliability.

CrowdStrike's experience in operating one of the largest security clouds in the world provides unique insights into adversaries, enabling the delivery of purpose-built CrowdStrike® solutions that create less work for DevSecOps teams, defend against data breaches and optimize cloud deployments.

KEY CAPABILITIES

VULNERABILITY SCANNING AND MANAGEMENT

Gain complete visibility into workloads, containers and hosts — on premises and in the cloud.

- **Improve decision-making:** Gather insights and details about your cloud workloads and containers — images, registries, libraries and containers spun from those images.
- **Uncover hidden threats:** Find hidden malware, embedded secrets, configuration issues and more in your images to help reduce the attack surface.
- **Gain visibility into container environments:** Get full visibility into running containers to uncover details surrounding file access, network communications and process activity.
- **Identify vulnerabilities faster:** Save valuable time with pre-built image scanning policies enabling you to quickly catch vulnerabilities, misconfigurations and more.
- **Identify risky container configurations:** Quickly identify risky and misconfigured containers such as those with rare mount points or links that can indicate compromise.
- **Eliminate threats prior to production:** Block exploitable vulnerabilities based on indicators of attack (IOAs) before runtime, eliminating headaches for security teams.
- **Continuously monitor:** Identify new vulnerabilities at runtime, alert and take action without having to rescan images.

CLOUD WORKLOAD PROTECTION OPTIMIZED FOR DEVOPS

Provides one platform for all workloads and containers

Secures cloud workloads and containers wherever they run

Integrates directly into the CI/CD pipeline for image and registry scanning

Works on Day One: Deploys and is operational in minutes without requiring reboots, fine-tuning or complex configuration

Intelligently prioritizes incidents by severity and criticality

Streamlines the triage process and automates response

AUTOMATED CI/CD PIPELINE SECURITY

Integrate security as part of the CI/CD pipeline.

- **Accelerate delivery:** Create verified image policies to ensure that only approved images are allowed to progress through your pipeline and run in your hosts or Kubernetes clusters.
- **Identify threats earlier:** Continuously scan container images for known vulnerabilities, configuration issues, secrets/keys and OSS licensing issues.
- **Assess the vulnerability posture of your pipeline:** Uncover malware missed by static scanners before containers are deployed.
- **Improve security operations:** Streamline visibility for security operations by providing insights and context for misconfigurations and compliance violations.
- **Integrate with developer toolchains:** Seamlessly integrate with Jenkins, Bamboo, GitLab and more to remediate and respond faster within the DevOps toolsets you already use.
- **Enable DevSecOps:** Reporting and dashboards drive alignment and a shared understanding across security operations, DevOps and infrastructure teams.

RUNTIME PROTECTION

Protect cloud workloads and containers wherever they reside.

- **Secure hosts and containers:** CrowdStrike Falcon® runtime protection defends containers against active attacks.
- **Gain broad container support:** Falcon supports containers running on Linux and is deployable across Kubernetes environments such as EKS. It also supports container as a service (CaaS) such as Fargate, providing the same level of protection. Technology previews are available for AKS, GKE and Red Hat OpenShift.
- **Leverage market-leading protection technologies:** Machine learning (ML), artificial intelligence (AI), IOAs and custom hash blocking automatically defend against malware and sophisticated threats targeting containers:
  - **ML and AI:** Falcon leverages ML and AI to detect known and unknown malware within containers without requiring scanning or signatures.
  - **IOAs:** Falcon uses IOAs to identify threats based on behavior. Understanding the sequences of behavior allows Falcon to stop attacks that go beyond malware, including fileless attacks.
- **Stop malicious behavior:** Behavioral profiling enables you to block activities that violate policy with zero impact to legitimate container operation.
- **Investigate container incidents faster:** Easily investigate incidents when detections are associated with the specific container and not bundled with the host events.
- **See everything:** Capture container start, stop, image and runtime information, and all events generated inside the container even if it only runs for a few seconds.
- **Deploy seamlessly with Kubernetes:** Deploy easily at scale by including Falcon as part of a Kubernetes cluster.
- **Improve container orchestration:** Capture Kubernetes namespace, pod metadata, process, file and network events.

THREAT GRAPH BREACH PREVENTION ENGINE

Predict and prevent modern threats in real time through the industry's most comprehensive set of endpoint, cloud workload, and container telemetry; threat intelligence; and AI-powered analytics.

- **Integrated market-leading threat intelligence:** Falcon leverages enriched threat intelligence to deliver a visual representation of relationships across account roles, workloads and APIs to provide deeper context for faster, more effective response.
- **Automate threat prevention:** Deep AI and behavioral analysis identify new and unusual threats in real time and take the appropriate action, saving valuable time for security teams.
- **Accelerate response:** CrowdStrike Threat Graph® puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.
- **Reduce alert fatigue:** The targeted threat identification and management approach cuts through the noise of multi-cloud environment security alerts, reducing alert fatigue.
- **Unravel attacks and improve response:** CrowdStrike's CrowdScore™ Incident Workbench helps unravel attacks and improve response time by distilling and correlating security alerts into incidents, automatically triaging, prioritizing and highlighting those that deserve urgent attention.

SINGLE SOURCE OF TRUTH WITH POWERFUL APIs

A single data source gives security teams fast access to everything they need to respond and investigate.

- **Benefit from DevOps-ready automation:** Powerful APIs allow automation of CrowdStrike Falcon functionality, including detection, management, response and intelligence.
- **Optimize business performance:** Unlock security orchestration, automation and other advanced workflows to optimize business performance.
- **Integrate with CI/CD pipelines:** Chef, Puppet and AWS Terraform integrations support CI/CD workflows.
- **Get protection at the speed of DevOps:** Falcon protects immediately and matches the speed of DevOps, adapting to the dynamic scalability of containers in real time with CI/CD integration via API and pre-boot scripts.

MANAGED DETECTION AND RESPONSE FOR THE CLOUD

The first and only fully managed cloud workload protection solution delivers 24/7 expert security management, threat hunting, monitoring and response for cloud workloads — backed by CrowdStrike's industry-leading Breach Prevention Warranty.

- **24/7 expertise to defend the cloud:** Arms you with seasoned security professionals who have experience in cloud defense, incident handling and response, forensics, SOC analysis and IT administration. The team has a global footprint, allowing true 24/7 "follow the sun" coverage.
- **Powered by Falcon Cloud Workload Protection:** Provides comprehensive breach protection for workloads and containers, enabling you to build, run and secure applications with speed and confidence.

- **Continuous human threat hunting:** Includes 24/7 monitoring by the Falcon OverWatch™ team, CrowdStrike's human threat detection engine that hunts relentlessly to see and stop the most sophisticated hidden threats.
- **Surgical remediation:** The team remotely accesses the affected system to surgically remove persistence mechanisms, stop active processes, clear other latent artifacts and restore workloads to their pre-intrusion state without the burden and disruption of reimaging.
- **Breach prevention warranty:** CrowdStrike stands strongly behind its breach protection capabilities by providing a Breach Prevention Warranty to cover costs in the event a breach occurs within the protected environment. (Breach Prevention Warranty not available in all regions.)

SIMPLICITY AND PERFORMANCE

Use one platform for all workloads and containers — it works everywhere: private, public and hybrid cloud environments.

- **Simplifies DevSecOps adoption:** Reduce the overhead, friction and complexity associated with protecting cloud workloads, containers and serverless environments.
- **Provides a single pane of glass:** One console provides central visibility over cloud security posture, workloads and containers, regardless of their location.
- **Offers complete policy flexibility:** Apply at the individual workload, container, group or higher level, and unify policies across both on-premises and multi-cloud deployments.
- **Scales at will:** No rearchitecting or additional infrastructure is required.
- **Provides broad platform support:** The Falcon platform supports Open Container Initiative (OCI)-based containers such as Docker and Kubernetes and also self-managed 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.

ABOUT CROWDSTRIKE

CrowdStrike, 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 upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

Start Free Trial
of Next-Gen AV

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