CrowdStrike Solutions

CROWDSTRIKE

FALCON CLOUD SECURITY: CONTAINER SECURITY

Providing DevOps-ready breach protection for containers

FULL LIFECYCLE CONTAINER PROTECTION FOR CLOUD-NATIVE APPLICATIONS

Organizations are increasingly adopting container technology such as Docker and Kubernetes to help drive efficiency and agility. Containers have changed how applications are built, tested and utilized, enabling applications to be deployed and scaled to any environment instantly. As container adoption increases, they emerge as a new attack surface that lacks visibility and exposes organizations. Blind spots lead to silent failure and ultimately breaches. Most organizations have low container visibility for the following reasons:

- Traditional security tools are not designed to provide container visibility
- Tools such as Linux logs make it difficult to uniquely identify events generated by containers vs. those generated by the host, since visibility is limited to the host
- Containers are short-lived, making data collection and incident investigation challenging because forensic evidence is lost when a container is terminated
- Decentralized container controls limit overall visibility

Once a container is launched and running, it can be compromised. Even if the image is configured properly and verified, it is susceptible to new vulnerabilities and runtime threats. The dynamic and portable nature of containers further complicates securing them. Rapid scaling means the attack surface is constantly changing, while portability across multiple environments further limits and complicates visibility.

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

KEY BENEFITS

Delivers container security without adding point products, containers and complexity

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

Delivers unparalleled visibility with detailed container events and metadata

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

Provides continuous runtime protection for containers

Offers a single management console for host and container security

Protects immediately without sacrificing performance, matching the speed of DevOps

Adapts to the dynamic scalability of containers in real time

CONTAINER SECURITY THAT IS FAST AND SCALABLE

CrowdStrike Falcon® Cloud Security automates the secure development of cloud-native applications, delivering full stack protection and compliance for containers, Kubernetes and hosts across the container lifecycle. This solution replaces outdated methods with an immutable infrastructure approach that optimizes cloud resources and ensures that applications are portable and always deployed securely. Falcon Cloud Security comes complete with vulnerability management, continuous threat detection and response, and runtime protection, combined with compliance enforcement and automated continuous integration/continuous delivery (CI/CD) pipeline security, enabling DevOps teams to stay secure while building in the cloud.

Stopping breaches in container 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. Containers are designed and built for speed, scalability and reliability.

CrowdStrike has deep experience in operating one of the largest security clouds in the world, providing unique insights into adversaries and enabling the company to deliver purpose-built solutions that defend against data breaches, create less work for security teams and optimize cloud deployments.

KEY CAPABILITIES

VULNERABILITY SCANNING AND MANAGEMENT

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

- **Improve decision making:** Gather insights and details about your container — images, registries, libraries and containers spun from the 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, and alert and take action without having to rescan images.

CONTAINER SECURITY OPTIMIZED FOR DEVOPS

Provides one platform for all workloads and containers

Secures containers wherever they run

Integrates directly into the CI/CD pipeline for container 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 tool sets you already use.
- **Enable DevSecOps:** Reporting and dashboards drive alignment and a shared understanding across security operations, DevOps and infrastructure teams.

RUNTIME PROTECTION

Protect running containers wherever they reside.

- **Secure hosts and containers:** CrowdStrike Falcon® runtime protection defends containers against active attacks.
- **Gain broad container support:** The CrowdStrike Falcon® platform 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:** The Falcon platform leverages ML and AI to detect known and unknown malware within containers without requiring scanning or signatures.
  - **IOAs:** The Falcon platform uses IOAs to identify threats based on behavior. Understanding the sequences of behavior allows the Falcon platform 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.
- **Detect rogue containers:** Maintains an up-to-date inventory as containers are deployed and decommissioned, detects and scans rogue images, and identifies and stops containers launched as privileged or writable.
- **Container drift prevention:** Enforces container immutability by detecting new binaries created and executed inside containers.
- **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 it as part of a Kubernetes cluster.
- **Improve container orchestration:** Capture Kubernetes namespace, pod metadata, process, file and network events.

INCIDENT RESPONSE AND FORENSICS FOR WORKLOADS AND CONTAINERS

Prevent silent failure by capturing container-specific events for visibility, proactive threat hunting and forensic investigation.

- **Real-time visibility:** Stream container information and activity to the Falcon platform in real time for in-depth insight, enabling security teams to uncover hidden threats, hunt and investigate.
- **Powerful search:** Easily filter events generated inside containers from the worker node, and search based on detailed container metadata such as images, mode, configuration type and more.
- **Proactive threat hunting:** Once deployed, the Falcon platform immediately begins to record container details and activity, enabling proactive threat hunting where security teams can hunt, get query results in seconds and easily pivot from one clue to the next.
- **Continuous availability:** Event details that provide forensic evidence and a full set of enriched data are continuously available, even for ephemeral containers after they have been decommissioned.
- **Ability to unravel entire attacks on one screen:** An easy-to-read process tree provides full attack details in context for faster and easier investigations.

SIMPLICITY AND PERFORMANCE

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

- **Simplify DevSecOps adoption:** Reduce the overhead, friction and complexity associated with protecting cloud workloads, containers and serverless environments.
- **Ensure stability of critical systems:** Minimize the impact to critical systems while ensuring they are always protected with a single agent that runs in user mode, and update policies to a running container no restart required.
- **Single pane of glass:** One console provides central visibility over cloud security posture, workloads and containers regardless of their location.
- **Complete policy flexibility:** Apply at individual workload, container, group or higher level, and unify policies across both on-premises and multi-cloud deployments.
- **Scales at will:** There is no rearchitecting or additional infrastructure required.
- **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.

Schedule a Demo

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

ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:
https://www.crowdstrike.com/

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**