CrowdStrike Solutions

CROWDSTRIKE

CONTAINER SECURITY WITH THE FALCON PLATFORM

Breach protection for containers

ENDPOINT DETECTION AND RESPONSE (EDR), RUNTIME PROTECTION AND DISCOVERY FOR CONTAINERS

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 deployed, 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 since 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.

THE CROWDSTRIKE APPROACH TO SECURING CONTAINERS

CrowdStrike offers one platform for all workloads. The CrowdStrike Falcon® platform protects workloads across all environments, including workloads and containers running in the cloud and in private, public and hybrid data centers or on-premises. The Falcon platform and intelligent, lightweight Falcon agent offer unparalleled protection and real-time visibility. Specifically tailored for containers, Falcon provides detailed insight into both the host and container-specific data and events. The Falcon platform enables and accelerates critical detection, investigation and threat hunting tasks performed on containers — even on ephemeral containers after they have been decommissioned. Security teams can secure containers at the speed of DevOps without adding friction.

KEY BENEFITS

Delivers container security without adding point products, containers and complexity

Provides runtime protection for containers

Delivers unparalleled visibility with detailed container events and metadata

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

Enables and accelerates threat hunting and investigation within containers

Protects immediately without sacrificing performance, matching the speed of DevOps

Adapts to the dynamic scalability of containers in real time

CONTAINER SECURITY WITH THE FALCON PLATFORM

EDR FOR CONTAINERS

- The CrowdStrike® Falcon platform prevents 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 quickly identify 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, Falcon 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.

RUNTIME PROTECTION

- Falcon continuously protects containers when running and also monitors events and analyzes the data in real time to automatically identify threat activity, enabling the detection and prevention of threats as they happen.
- CrowdStrike Falcon combines the best protection technologies including machine learning (ML), artificial intelligence (AI), indicators of attack (IOAs) and custom hash blocking to 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.

CONTAINER DISCOVERY

- The Falcon platform provides immediate visibility into container use in your environment — dashboards provide at-a-glance views with drill-down capability to quickly pivot to detailed displays and search:

BUILT IN THE CLOUD FOR THE CLOUD

Provides one platform for all workloads

Secures containers wherever they run

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

CROWDSCORE WORKBENCH

Combines related alerts and indicators into incidents

Streamlines the triage process

Intelligently prioritizes incidents by severity and criticality

- **Container usage:** Get visibility across all containers used in your environment, including how many, the number of hosts running containers, the number of registries, the types of containers and the engine version. Trend graphs help quickly identify anomalies such as spikes in the number of running containers and container uptime.
- **Container by host:** Search host properties to see all of the containers running on that host.
- **Container images:** View images used and easily search for vulnerable images.
- **Container configurations:** Quickly identify risky and misconfigured containers such as those with rare mount points or links that can indicate compromise. Easily monitor privileged containers and those that are running in interactive mode, can't be killed or are running with root access.

SPEED AND SIMPLICITY

- **Reduced cost and complexity:** Falcon operates with a single agent and management console, and delivers container security through a single agent running on the worker node that protects the node itself as well as all containers running on it. Host and container security is managed through the same console, no matter where containers reside.
- **Fast:** Falcon protects immediately and matches the speed of DevOps, adapting to the dynamic scalability of containers in real time with continuous integration/continuous delivery (CI/CD) via API and pre-boot scripts.
- **Lightweight:** Operating with only a tiny footprint on the host, Falcon has zero impact on container runtime performance when analyzing, searching and investigating.
- **Scales as container instances start, stop and terminate:** Host-based security automatically protects containers as they spin up, with no need for additional infrastructure, agents or dedicated security containers.
- **Provides comprehensive 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.

Start Free Trial
of Next-Gen AV

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

© 2020 CrowdStrike, Inc. All rights reserved.

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.