CROWDSTRIKE
Investor Relations

CrowdStrike Delivers Advanced Threat Protection for Cloud and Container Workloads to Provide Greater Control and Visibility from Build to Runtime

February 24, 2021

New capabilities bring increased protection for cloud applications, reducing the attack surface and identifying vulnerabilities before deployment

SUNNYVALE, Calif.--(BUSINESS WIRE)--Feb. 24, 2021-- CrowdStrike, a leader in cloud-delivered endpoint and workload protection, today announced expanded Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) capabilities for the CrowdStrike Falcon® platform to deliver greater control, visibility and security for cloud workloads and cloud-native applications from build to runtime.

The expanded CSPM and CWP capabilities for the CrowdStrike Falcon platform identify and remediate vulnerabilities from development to production for a wide variety of cloud environments, including containers. Gartner has predicted that, “Growing adoption of cloud-native applications and infrastructure will increase use of container management to over 75% of large enterprises in mature economies by 2024 (up from less than 35% in 2020).”

With the incorporation of frictionless security and automated protection early in the continuous integration/continuous delivery (CI/CD) pipeline, DevSecOps teams are empowered to deliver production-ready applications with minimal impact to build cycles. Additionally, the new features will help organizations prevent compliance violations with intelligent monitoring that detects misconfigurations, vulnerabilities and threats, and delivers guided remediation that equips developers with guardrails to avoid costly mistakes.

“We continue to deliver the broadest range of cloud security capabilities in a single cloud-native platform for on-prem, private, public, hybrid and multi-cloud environments that scales,” said Amol Kulkarni, chief product officer for CrowdStrike. “CrowdStrike’s Security Cloud is one of the largest deployments in the world, providing us a unique vantage point in supporting organizations’ shift to cloud-native architectures and their adoption of development and IT operations (DevOps). The capabilities we are announcing today secure development and deployment of applications in the cloud with greater speed, efficiency and confidence.”

New Falcon Horizon CSPM Capabilities:

- **Provide cloud-native security posture management for multi-cloud environments:** Prevents, protects and remediates security risks in AWS and Azure resources. Expands assessment coverage for server, Kubernetes and serverless services to detect Indicators of Misconfiguration (IOM) in the public cloud control plane.
- **Monitor cloud identities for least privileges:** Provides end-to-end visibility to Azure Active Directory (AD) to quickly identify privileged permissions and abnormal service-to-service integration settings. Detects misconfigurations linked to prevalent tactics, techniques and procedures (TTPs) with Azure AD deployments.
- **Ensure continuous compliance:** Provides in-depth assessment against the Center for Internet Security (CIS) benchmarks with prebuilt dashboards, easy to navigate drill-down by account, region, cloud service and severity.

New Falcon Cloud Workload Protection Capabilities

- **Delivers broad support for container runtime security:** Secures applications with the new Falcon Container sensor that is uniquely designed to run as an unprivileged container in a pod. Supports Kubernetes environments, such as Amazon Elastic Kubernetes Service (EKS), and offers container-as-a-service support, including Amazon Web Services (AWS) Fargate. Technology previews available for Azure Kubernetes Service (AKS), Google Kubernetes Engine (GKE), Rancher and IBM Red Hat OpenShift.
- **Identify security threats prior to running containers in production:** Using Container Image Assessment, uncovers hidden malware, vulnerabilities, embedded secrets and configuration issues in your images at build time to reduce the runtime attack surface.
- **Stop threats when containers are most vulnerable, during runtime:** Detects malicious runtime behavior and blocks activities that violate policy with zero impact to container workloads through behavioral detection, cloud machine learning and Indicators of Attack (IoAs).
- **Uncover hidden threats:** Correlates events from containers with host and cloud data, such as Falcon Horizon, for more effective hunting and remediation.

To learn more about CrowdStrike container security, visit this landing page.

To read more about this announcement, visit the blog here.

Other related blogs are:

- Container Security with CrowdStrike

- How Identity Analyzer Improves Cloud Security

A video on the enhanced cloud protection capabilities for Falcon can be found here.

[1] "Forecast Analysis: Container Management (Software and Services), Worldwide," Gartner, May [CM1] 2020

About CrowdStrike

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload 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 and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates 5 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.

Qualifying organizations can gain full access to Falcon Prevent™ by starting a free trial.

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

Follow us: Blog | Twitter

View source version on businesswire.com: https://www.businesswire.com/news/home/20210224005329/en/

CrowdStrike
Ilina Cashiola, 202-340-0517
Ilina.cashiola@crowdstrike.com

Source: CrowdStrike