CROWDSTRIKE

CrowdStrike Products

Soultion Brief

Falcon Cloud Security:

Cloud Workload Protection

Secure hosts, virtual machines, containers and serverless deployments

Challenges

In the current digital era, organizations are rapidly migrating to the cloud, seeking the benefits of scalability, flexibility and efficiency. However, this transition introduces significant security challenges, particularly in protecting diverse and dynamic cloud workloads. Business leaders are increasingly concerned about safeguarding sensitive data against sophisticated cyber threats, ensuring compliance with evolving regulatory standards and maintaining operational resilience. For technical teams, the complexity is compounded by the need to secure a varied landscape of virtual machines, containers and serverless workloads across multi-cloud environments. They face the intricate task of detecting and mitigating threats in real time and ensuring seamless integration with existing security infrastructure.

This complex landscape highlights the urgent need for advanced cloud workload protection (CWP) capabilities — capabilities that not only addresses the multifaceted security challenges but also align with the strategic goals of scalability and agility in cloud operations.

Solution

CrowdStrike Falcon® Cloud Security provides CWP capabilities for complete visibility into workload and container events, enabling faster and more accurate detection, response, threat hunting and investigation, and ensuring nothing goes unseen or unprotected in an organization's cloud environment. It secures the entire cloud-native stack, on any cloud, across all workloads, containers and Kubernetes applications. With Falcon Cloud Security, organizations can automate security and detect and stop suspicious activity, zero-day attacks and risky behavior to stay ahead of threats and reduce the attack surface. Falcon Cloud Security supports continuous integration/continuous delivery (CI/CD) workflows, allowing you to secure workloads at the speed of DevOps without sacrificing performance.

Key benefits

- Get unified visibility and protection across the entire cloud
- Use a single solution to see and stop cloud attacks
- Shift-left and automate DevSecOps

Key capabilities

Runtime Security

- **Comprehensive visibility and protection:** Get runtime visibility and protection for Linux and Windows hosts, containers and Kubernetes, as well as serverless compute like AWS Fargate.
- **Stop cloud breaches:** Identify zero-day threats in real time through CrowdStrike Threat Graph®, the industry's most comprehensive set of endpoint and workload telemetry, threat intelligence and AI-powered analytics.
- **Accelerate response with enriched threat intelligence:** Gain visibility into relationships across account roles, workloads and APIs for deeper context, leading to faster, more effective response.
- **Agentless snapshot scanning:** When an agent can't be installed, organizations can gain full visibility into cloud workloads by detecting malware, vulnerabilities and installed applications with native agentless snapshot capabilities.
- **One-Click XDR:** Scan the cloud environment with native agentless visibility to identify unprotected workloads and automatically deploy the CrowdStrike Falcon agent for end-to-end protection. Only CrowdStrike can identify unprotected cloud workloads and automatically protect them with industry-leading extended detection and response (XDR) and endpoint detection and response (EDR) for consistent, complete breach prevention.
- **Cloud attack path visualization:** Leveraging CrowdStrike® Asset Graph™, organizations can see a unified view of the entire path an attacker can take, from host to cloud, to compromise a cloud environment. Only CrowdStrike consolidates real-time data from native agent-based and agentless capabilities to enable organizations to prioritize and reduce risks in their cloud environment.

Container Security

- **Complete visibility and protection into the container environment:** With CrowdStrike's single lightweight agent, you can secure both Kubernetes and containers running on it. Capture container start, stop, image, and runtime information, unidentified and rogue containers and all events generated inside the container, even if it only runs for a few seconds.
- **Investigate container incidents faster:** Easily investigate incidents when detections are associated with the specific container and not bundled with the host events.
- **Prevent attacks on container environments:** Uncover hidden threats in open source packages and third-party images to prevent attacks on your container-based applications. Also, protect serverless containers such as AWS Fargate.
- **Enforce container immutability (container drift):** Ensure only secure images are allowed to progress through your pipeline and run in your Kubernetes clusters or hosts.
- **Improve container orchestration:** Capture Kubernetes namespace, cluster, pod metadata, process, file and network events.
- **Prevent vulnerable deployment:** Save time with Kubernetes Admission Controller by using predefined policies to prevent vulnerable deployments.

Key features

- Protection for AWS, Google, Azure, Kubernetes and OpenShift
- **Pre-runtime:**
  - CI/CD Security (Pre-runtime)
  - Container Image Assessment
  - Image Assessment Policies
  - Infrastructure-as-Code (IaC) Security
  - Registry Integrations
- **Runtime:**
  - Container Asset Visibility
  - Next-Generation Antivirus
  - Endpoint Detection and Response
  - Indicators of Attack (IOAs)
  - Drift Prevention
  - Rogue Container Detection
  - Kubernetes Admission Controller
  - Vulnerability Management
  - One-Click Runtime Protection
  - Cloud Attack Path Visualization

CI/CD Security (Pre-runtime)

- **Ensure safe 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.
- **Align security and developers:** Streamline visibility and drive alignment through reporting and dashboards to provide shared understanding across security operations, DevOps and infrastructure teams.
- **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.
- **Benefit from the broadest industry image assessment:** Integrate with 16 code registries for more complete coverage and the ability to find vulnerabilities — no matter which registry is being used — through auto perform malware, secrets and vulnerability detections with software composition analysis (SCA).
- **Infrastructure-as-code (IaC) security:** Easily scan for vulnerabilities in container images across AWS, Azure and GCP while supporting 10+ IaC platforms to drive a more efficient application life cycle. Only CrowdStrike combines IaC with agent-based and agentless capabilities in one platform.

Vulnerability Management

- **Get visibility and risk management in a unified platform:** Gain visibility into vulnerabilities and prioritize risk around your cloud workloads, containers, images, registries and Lambda functions.
- **Identify vulnerabilities prior to production:** Improve security and save time by assessing your images prior to production through supported registries or running local image assessment.
- **Monitor continuously:** Identify new vulnerabilities at runtime, including runtime image assessment, and alert and take action without having to rescan images.

MDR for Cloud

- **24/7 expertise to defend the cloud:** Benefit from the expertise of seasoned security professionals who have experience in cloud defense, incident handling and response, forensics, SOC analysis and IT administration.
- **Continuous human threat hunting:** 24/7 monitoring is provided by the CrowdStrike Falcon® Adversary OverWatch™ team, CrowdStrike's human threat detection engine that hunts relentlessly to see and stop the most sophisticated hidden threats.
- **Surgical remediation:** The Falcon Adversary OverWatch 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 should a breach occur within the protected environment.

*Breach Prevention Warranty not available in all regions.

Industry Recognition

FROST & SULLIVAN

Learn why Frost & Sullivan ranked CrowdStrike as a leader in Cloud-Native Application Security Platform (CNAPP)

THECHANNELCO. CRN®

Learn more how CrowdStrike won the 2022 CRN Tech Innovator Award for Best Cloud Security

FORRESTER®

Forrester named CrowdStrike a Leader in The Forrester Wave™: Cloud Workload Security, Q1 2024, with the top score in the Strategy category and highest scores possible in Innovation and Vision criteria.

Get a FREE
Cloud Security Risk Review →

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 | X | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/