CROWDSTRIKE

Solution Brief

CROWDSTRIKE CLOUD SECURITY

Think It ... Build It ... Secure It

As a cybersecurity company that has built one of the biggest cloud architectures in the world, CrowdStrike has gained an exceptional vantage point and garnered unique experience on what it takes to secure cloud workloads and application lifecycles.

Various security challenges come with the cloud. For example, the cloud is vulnerable to human errors and more prone to shadow IT than on-premises environments. And like any other compute environment, it is exposed to runtime threats. In addition, the teams that are implementing cloud workloads might not have the security knowledge necessary to adequately protect them.

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 using cloud-scale data and analytics requires a tightly integrated platform, where each function plays a crucial part in detecting modern threats and is designed and built for speed, scale and reliability.

MODERN CLOUD INFRASTRUCTURE REQUIRES MODERN CLOUD SECURITY

The adoption of the cloud has fundamentally changed the game when it comes to how businesses go to market and develop modern applications. Today's application lifecycle places a premium on speed, requiring cloud teams to build cloud-native applications supported by a programmable infrastructure that enables businesses to change and reconfigure the cloud infrastructure on the fly. Additionally, continuous integration/continuous deployment (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 comes at a cost, as infrastructure, DevOps and security teams look for ways to ensure cloud resources remain secure and meet compliance.

As businesses continue to adopt more cloud-native toolsets, security teams are finding it difficult to keep up. The result is poor visibility and control of cloud resources, fragmented approaches to detecting and preventing misconfigurations, ineffective protection for cloud workloads and containers, and the inability to maintain compliance — ultimately leading to increased risk to the business.

KEY BENEFITS

- Provides multi-cloud visibility and a single source of truth for cloud resources
- Reduces costs and complexity with a single unified platform for on-premises, private, public, hybrid and multi-cloud environments
- Accelerates safe cloud migration and adoption
- Predicts and prevents modern threats in real time through the industry's most comprehensive set of endpoint and cloud workload telemetry, threat intelligence and AI-powered analytics
- Meets and maintains compliance
- Scales at will — no rearchitecting or additional infrastructure required
- Closes the skills gap for hard-to-find cloud security skills and improves operational efficiencies

Common cloud security challenges include:

- Lack of visibility due to cloud sprawl
- Human error resulting in an increasing number of cloud security incidents due to misconfiguration
- The need to detect, prevent and respond to threats to workloads and containers running in public, private and hybrid environments
- Meeting and maintaining compliance and enforcing security policies across multi-cloud environments
- Workloads left exposed and vulnerable due to an expanding attack surface and lack of cloud security skills

Manual processes and traditional solutions can't match the rapid change and unique challenges organizations now face. 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. Security teams must keep pace with the speed of agile software development, and they need the ability to continuously manage cloud risk. To be effective, they need to proactively assess and monitor cloud resource configuration and security policy and compliance enforcement, while delivering comprehensive breach protection for workloads and containers for any cloud — all without impacting business performance.

CROWDSTRIKE FALCON: A CLOUD-NATIVE PLATFORM DESIGNED TO PROTECT ANY CLOUD

The CrowdStrike Falcon® platform has been designed to support workloads regardless of their location. With the Falcon platform, organizations can secure instances running in all types of public clouds including Amazon Web Services (AWS), Google Cloud Platform (GCP) and Microsoft Azure. Falcon protects physical servers and virtual machines in your private data center and instances in the public cloud.

The platform is built on two common components: a single lightweight agent and a distributed cloud. The single-agent architecture supports all types of workloads but is tuned to collect data specific to the cloud infrastructure and the workload it is running on. For example, Falcon for AWS is designed to collect additional metadata from AWS. This has allowed CrowdStrike to provide its customers with multiple applications without requiring multiple agents, multiple consoles or any additional management components. The unique cloud-native architecture allows protection to be deployed seamlessly, regardless of the number of virtual private clouds (VPCs) in use.

Whether an organization is using 10 or 100 VPCs, CrowdStrike's experience in operating one of the largest cloud implementations in the world provides unique insights into adversaries and enables delivery of purpose-built solutions that reduce work for security teams, defend against data breaches and optimize cloud deployments.

DEVSECOPS-READY CLOUD SECURITY

CrowdStrike® cloud security goes beyond ad hoc approaches by unifying cloud security posture management (CSPM) with breach protection for cloud workloads and containers in a single

platform for any cloud. This cloud-native solution provides end-to-end protection from the host to the cloud and everywhere in between.

- Falcon Horizon™ CSPM provides visibility into your entire cloud infrastructure, intelligent monitoring for misconfigurations, continuous control plane threat detection, guided remediation, and security policy and compliance enforcement. With Falcon Horizon, DevSecOps teams can securely develop and deploy applications in the cloud with greater speed, efficiency and confidence.
- Falcon Cloud Workload Protection provides automated discovery into all workloads and containers, continuous cloud runtime protection, image scanning, comprehensive Kubernetes protection and managed cloud threat hunting — all on a single-lightweight agent. In addition, the solution is available in the industry's only fully managed detection and response (MDR) service for cloud workloads and containers — enabling DevOps teams to "shift left" and build securely in the cloud by fixing issues before they reach production.

CROWDSTRIKE CLOUD SECURITY CAPABILITIES

CLOUD DISCOVERY AND VISIBILITY

- **Single source of truth:** Gain comprehensive visibility of cloud assets, security configurations, workloads and containers across multi-cloud environments so you can mitigate risks and reduce the attack surface.
- **Discovery of cloud resources:** Get details automatically on deployment, including misconfigurations, metadata, networking, security and change activity.
- **Deep insights:** Visibility into workload events and instance metadata enables detection, response, proactive threat hunting and investigation, ensuring that nothing goes unseen in your cloud environments.
- **See more, know more, do more:** Detect and investigate attacks that span multiple environments and different types of workloads, pivoting from endpoint to instances to containers.
- **Eliminate security blind spots:** Quickly identify cloud resources not protected by the Falcon platform.

MISCONFIGURATION MANAGEMENT AND GUIDED REMEDIATION

- **Assess and validate:** Compare the most common to the most complex cloud application configurations to industry and organizational benchmarks, allowing you to identify violations and remediate in real time.
- **Fix issues that leave cloud resources exposed:** Identify and remediate risks such as misconfigurations, open IP ports and unauthorized modifications with guided remediation and guardrails that enable developers to avoid critical mistakes.
- **Real-time monitoring and guided remediation:** Get step-by-step remediation rules, enabling you to act quickly and eliminate issues.
- **Monitor storage:** Ensure permissions are secure and not publicly accessible.
- **Monitor database instances:** Verify that high availability, backups and encryption are enabled, as well as security groups to limit exposure.

BUILT IN THE CLOUD FOR THE CLOUD

Provides end-to-end cloud-native security

Enables discovery, visibility and compliance for any cloud

Protects workloads, hosts and containers

Reduces alert fatigue and enables faster remediation

Works on Day One — deploys and is operational in minutes, with no reboots, fine-tuning or complex configuration required

CONTINUOUS THREAT DETECTION AND RESPONSE

- **Cloud runtime protection:** Secure the host and container via a single Falcon agent running on the host with runtime protection that defends containers against active attacks.
- **Rapid investigation:** Investigate container incidents easily when detections are associated with the specific container and not bundled with the host events.
- **Monitor and capture everything:** Capture container start, stop, image and runtime information, as well as all events generated inside the container, even if it only runs for a few seconds.
- **Proactive cloud threat hunting:** Gain information on container details and activity immediately on Falcon deployment, showing security teams where they can hunt, providing query results in seconds and allowing teams to pivot easily from one clue to the next.
- **Prevent identity-based threats:** Reduce the number of tools required from three to one, and prevent users from putting your organization at risk by automating the detection and remediation of identity-based risks in Microsoft Azure, AWS and GCP.
- **Integrate cloud indicators of attack (IOAs) with threat intelligence:** Gain access to real-time alerting and reporting on more than 150 cloud adversaries based on CrowdStrike's market- leading threat intelligence and research for more effective response.
- **Benefit from continuous control plane threat detection:** Improve investigation speed by up to 88%[1] with machine learning and behavior-based TTP/IOA detections and guided remediation for all cloud accounts, services and users across the cloud estate.
- **Continuous availability:** Get event details, including forensic evidence and a full set of enriched data that are continuously available, even for ephemeral containers after they have been decommissioned.
- **Uncover hidden threats:** Receive full attack details in context from an easy-to-read process tree, enabling you to conduct faster and easier investigations.

THREAT GRAPH BREACH PREVENTION ENGINE

- **Predict and prevent modern threats:** Gain real-time protection via CrowdStrike Threat Graph®, the industry's most comprehensive sets of endpoint and workload telemetry, threat intelligence and AI-powered analytics.
- **Access enriched threat intelligence:** Receive a visual representation of relationships across account roles, workloads and APIs for a deeper context resulting in a faster, more effective response.
- **Deep AI and behavioral analysis:** Identify new and unusual threats in real time and take the appropriate action, conserving valuable security team resources.
- **Accelerate response:** Arm responders in real time, as Threat Graph empowers them to understand threats immediately and act decisively.
- **Targeted threat identification and management:** Cut through the noise of multi-cloud environment security alerts with targeted threat ID that reduces alert fatigue.

1 "The Total Economic Impact™ Of CrowdStrike Falcon®: Cost Savings And Business Benefits": A Forrester Total Economic Impact™ Study Commissioned By CrowdStrike, October 2019

SINGLE SOURCE OF TRUTH WITH POWERFUL APIS

- **Automate:** Use powerful APIs to automate CrowdStrike Falcon functionality, including detection, management, response and intelligence.
- **Enable SOAR:** Unlock security orchestration, automation and response (SOAR) and other advanced workflows to optimize business performance.
- **Support CI/CD pipelines:** Easily integrate Chef, Puppet and AWS Terraform to support CI/CD workflows.
- **Single data source:** Enable your security teams with a single source for fast access to everything they need to respond and investigate.

SIMPLICITY AND PERFORMANCE

- **Completely cloud native:** Built in the cloud for the cloud, the Falcon platform reduces the overhead, friction and complexity associated with protecting cloud workloads and meeting compliance.
- **One platform for all workloads:** Falcon protects everywhere — across private, public and hybrid cloud environments.
- **Single-pane-of-glass visibility and control:** One console provides central visibility over cloud security posture and workloads regardless of their location.
- **Complete policy flexibility:** Policies can be applied at the individual workload, group or higher level, and you can unify policies across both on-premises and multi-cloud deployments.
- **Scales at will:** The Falcon platform scales seamlessly and doesn't require any rearchitecting or additional infrastructure.
- **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.

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from 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**

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

Start Free Trial
of Next-Gen AV

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