aws

CROWDSTRIKE

Data Sheet

FALCON CLOUD WORKLOAD PROTECTION FOR AWS

Breach protection for cloud workloads and containers

WORKLOAD PROTECTION ACROSS ALL ENVIRONMENTS

CrowdStrike Falcon® Cloud Workload Protection provides comprehensive breach protection across private, public, hybrid and multi-cloud environments — all delivered via the lightweight Falcon agent and managed by the CrowdStrike® cloud-native platform. The Falcon platform allows customers to rapidly adopt and secure technology across any workload in public, private and hybrid environments.

KEY CAPABILITIES

VISIBILITY INTO CLOUD WORKLOADS

Comprehensive visibility into cloud workload events and instance metadata enables detection, response, and proactive threat hunting and investigation, ensuring that potentially malicious activities don't go unnoticed.

MULTI-CLOUD WORKLOAD DISCOVERY

Falcon automatically discovers existing cloud workload deployments — without installing an additional agent — by enumerating existing Amazon Web Services (AWS) Elastic Compute Cloud (EC2) instances and Amazon Workspaces, and provides real-time information about workloads including context-rich metadata about system size and configuration, networking, and security group information across AWS deployments.

API-LED CLOUD INTEGRATIONS

Falcon eliminates friction to boost cloud security efficiency. Powerful APIs allow automation of CrowdStrike Falcon functionality, including detection, management, response and intelligence. Chef, Puppet and AWS Terraform integrations support continuous integration/continuous delivery (CI/CD) deployment workflows.

RUNTIME PROTECTION

The Falcon platform combines the best and latest technologies to protect against active attacks and threats when workloads are the most vulnerable — at runtime. This includes behavior-based indicators of attack (IOAs) that detect sophisticated threats such as fileless and malware-free attacks attacks across Windows, Linux (Amazon, RedHat, CentOS, Oracle, SUSE, Ubuntu and Debian) and Amazon Workspaces.

CONTAINER SECURITY

Falcon provides protection and visibility without impacting container performance. Falcon secures Open Container Initiative (OCI)-compliant containers such as Docker, orchestration platforms such as self-managed Kubernetes, and hosted orchestration platforms such as EKS (Amazon Elastic Kubernetes Service) and ECS (Amazon Elastic Container Service).

SIMPLICITY AND PERFORMANCE

Built in the cloud for the cloud, Falcon reduces the overhead, friction and complexity associated with protecting cloud workloads. It operates with only a tiny footprint on the host and has almost zero impact on runtime performance, even when analyzing, searching and investigating.

KEY BENEFITS

- Gain comprehensive workload visibility from a single console
- Automatically discover cloud workload footprints
- Eliminate friction with key cloud integrations including AWS PrivateLink, AWS Control Tower, AWS Security Hub and AWS GuardDuty
- Secure workloads at the speed of DevOps without sacrificing performance
- Pay for what you use with a consumption-based billing option
- Seamlessly migrate from on premises to cloud with a consistent level of visibility and protection
- Enable and accelerate threat hunting and investigation in the cloud

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.

Start Free Trial
of Next-Gen AV

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