

Falcon Data Security for Cloud

Data security posture management (DSPM) for data in motion and at rest — find what data is sensitive, monitor risky movement in real time, and reduce exposure

Modern data security for cloud-native environments

Sensitive data no longer sits idle in cloud storage — it moves continuously across APIs, third-party applications, cloud storage, and databases. This creates new risks for organizations that rely on point-in-time scans or posture tools that only assess data at rest. Without runtime visibility, security teams are blind to active threats like unauthorized transmissions, policy violations, and misconfigurations in fast-moving cloud environments.

CrowdStrike Falcon® Data Security for Cloud unifies DSPM at rest with runtime visibility in motion, giving security teams continuous insight into where sensitive data lives and how it's accessed and transmitted across cloud infrastructure. Powered by Extended Berkeley Packet Filter (eBPF) and delivered through the lightweight CrowdStrike Falcon® sensor, it monitors data in motion across APIs, third-party applications, cloud storage, and databases without proxies, sidecars, or added infrastructure. This architecture delivers runtime context and faster detection and response within the Falcon platform.

With Falcon Data Security for Cloud, teams can identify and reduce cloud data exposure, detect threats as they happen, and accelerate investigation and response — without slowing down developers or introducing friction into cloud-native environments.

Key capabilities

Gain Full Visibility into Cloud Data Movement

- **Runtime monitoring across cloud services:** Continuously observe sensitive data in motion across APIs, third-party applications, cloud storage, and databases using eBPF-powered runtime visibility.
- **Deep telemetry and context:** Capture full details of each data flow — including source, destination, method, classification, and user identity — to uncover unauthorized transmissions and misconfigurations in real time.
- **Unified classification across domains:** Use a shared classification engine across Falcon Data Security to apply consistent labels for payment card industry (PCI) data, personally identifiable information (PII), protected health information (PHI), and intellectual property (IP).
- **eBPF-powered telemetry without overhead:** Leverage eBPF technology to observe data flows directly at the kernel level, enabling real-time, low-latency visibility without the need for proxies, sidecars, or deep instrumentation.

Key benefits

- **Full DSPM coverage (at rest and in motion):** Discover and classify sensitive data across cloud storage and databases, and monitor sensitive data flows across APIs, SaaS applications, and cloud services in real time.
- **Frictionless deployment:** No proxies, sidecars, or additional infrastructure — and delivered via the existing Falcon Linux sensor.
- **Unified classification:** Apply consistent policies across endpoint and cloud with a shared classification engine.
- **Integrated response:** Enrich detections with full context, and automate response via CrowdStrike Falcon® Fusion SOAR.
- **Scalable data discovery:** Customize lightweight scans for data at rest across cloud storage and databases.
- **Fast time-to-value:** CrowdStrike Falcon® Cloud Security for Containers customers get instant activation — no retooling required.

Realize Precision Data Security

- **AI-powered classification for unstructured cloud data:** Combine a purpose-built language model with deterministic rules to expand unstructured data classification coverage and reduce false positives while preserving explainability.
- **Out-of-the-box detections:** Detect high-risk activity rapidly, including data sent to public S3 buckets, unencrypted transfers to the internet, and sensitive data exposed via unauthenticated APIs.
- **Context-rich detections:** Enrich alerts with classification tags and full-flow metadata — enabling more precise triage, routing, and prioritization based on sensitivity and risk.
- **Streamlined investigation and response:** Trigger Falcon Fusion SOAR playbooks for immediate action, notifying owners, recommending remediation, and enabling more efficient incident response.

Accelerate Cloud Coverage and Deployment

- **Lightweight deployment model:** Deploy instantly across Kubernetes and Linux virtual machine (VM)-based workloads — including EKS, AKS, self-managed on-premises Kubernetes, and cloud VMs — using the Falcon Linux sensor, with no retooling or additional sensors required.
- **Scalable data-at-rest scanning:** Run customizable scans across cloud services like S3, RDS, Redshift, and DynamoDB to discover and classify sensitive data without slowing operations.
- **Fast time-to-value:** Activate Falcon Data Security for Cloud instantly in environments already running Falcon Cloud Security for Containers, simplifying adoption and accelerating protection.

[Schedule a demo today](#)

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/>

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

