CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Data Protection

Secure sensitive data with unified discovery, classification, and defense across endpoint, cloud, SaaS, and GenAI

One platform. Unified data protection.

Sensitive data no longer lives in one place. It moves continuously across endpoints, cloud workloads, SaaS applications, and GenAI tools. This constant movement increases exposure to insider threats and adversarial activity. Every interaction represents potential risk, whether an employee pastes confidential information into an AI tool, a cloud service transmits sensitive records, or an insider moves files to personal storage.

Legacy data loss prevention (DLP) and traditional data security posture management (DSPM) tools were not built for the dynamic nature of how data moves today. Legacy DLP relies on static policies, siloed agents, and delayed visibility that cannot keep pace with real-time data movement. Traditional DSPM solutions provide valuable discovery of data at rest but stop short of runtime visibility, leaving blind spots when sensitive data moves.

CrowdStrike Falcon® Data Protection redefines modern data security with unified, real-time protection across endpoint, cloud, SaaS, and GenAI. Built on the AI-native CrowdStrike Falcon® platform and delivered through the same lightweight unified sensor, Falcon Data Protection continuously discovers, classifies, and defends sensitive data in motion and at rest.

By consolidating endpoint and cloud data security into a single platform, Falcon Data Protection reduces security gaps, simplifies operations, and accelerates time-to-value without the complexity or lag of legacy tools.

Key benefits

- **Unified protection for modern data:** Get real-time visibility and protection across endpoint, cloud, SaaS, and GenAI from a single platform that eliminates silos and security gaps.
- **Real-time intelligence and control:** Detect and stop unauthorized data movement before it happens with AI-powered context that combines identity, device, and data telemetry.
- **Unified classifications:** Enforce consistent data labeling and handling across hybrid environments with unified classifications for endpoint and cloud— reducing blind spots and simplifying policy enforcement.

Key capabilities

See Everything in Motion

- **Gain full visibility into data movement:** Monitor sensitive data in motion and at rest across endpoints, cloud, SaaS, and GenAI from a single platform. Reduce blind spots created by siloed tools and disconnected agents.
- **See how data moves across environments:** Visualize how sensitive data travels between endpoints, SaaS applications, and cloud services. Identify patterns of data movement that reveal risky flows, unauthorized sharing, or potential insider activity.
- **Classify data consistently:** Apply consistent classifications for financial data, personally identifiable information (PII), protected health information (PHI), intellectual property (IP), and other sensitive content across endpoint and cloud using the shared Falcon Data Protection classification engine.

Stop Threats in Real Time

- **Detect and stop unauthorized activity:** Enforce policies that block sensitive data movement based on content, context, and behavior. Identify and prevent insider activity, GenAI misuse, and data exfiltration attempts before they escalate.
- **Protect against GenAI and insider risk:** Prevent sensitive data leaks to personal or corporate GenAI tools, shadow AI services, and unsanctioned destinations. Detect risky user behavior with machine learning-driven analytics.
- **Eliminate visibility gaps in encryption:** Stop egress with encrypted archives and identify sensitive content before it leaves the environment, helping security teams expose insider threats and accelerate investigations.
- **Trace data to its source:** Detect and correlate sensitive data even when renamed, reformatted, or partially modified using advanced similarity detection. Maintain visibility across browsers, removable media, and cloud services.

Respond and Evolve Faster

- **Automate investigation and response:** Trigger CrowdStrike Falcon® Fusion SOAR playbooks to enrich detections, notify owners, and execute remediation automatically. Streamline investigations with cross-domain context from endpoint, cloud, and identity telemetry.
- **Accelerate forensics and insight:** Provide investigators with content and context around events — including user, destination, and data classification details — for faster, evidence-backed response.

Falcon Data Protection across endpoint and cloud

As organizations operate across hybrid and cloud-native environments, Falcon Data Protection provides consistent, real-time protection for sensitive data in motion and at rest.

Falcon Data Protection for Endpoint

CrowdStrike Falcon® Data Protection for Endpoint provides real-time visibility and enforcement to prevent unauthorized data movement on devices. Built on the same lightweight Falcon sensor, it combines classification, behavior analytics, and policy controls to detect and stop data exfiltration before it happens.

- **Instant activation:** Enables protection immediately with no new sensors, reboots, or complex configurations
- **Encryption detection:** Reduces encrypted archive blind spots and streamlines investigations by providing a reliable, holistic view into encrypted archives' contents, identifying all sensitive data within encrypted archives proactively before it has a chance to leave the environment
- **GenAI data leak prevention:** Detects and blocks insider-driven data leaks to personal and corporate GenAI tools in real time, enforcing policies based on content type, source origin, and file type to stop unauthorized data sharing — keeping corporate data secure

- **Behavior-based detection:** Analyzes user behavior patterns using machine learning (ML) models to surface suspicious deviations across individuals, peer groups, and the organization
- **Automated policy enforcement:** Stops sensitive data theft in real time, covering both managed and unmanaged SaaS applications (e.g., Microsoft OneDrive, Google, Drive, Box)
- **Similarity detection:** Identifies and traces sensitive data back to its source — even if modified — enabling enforcement across web browsers, USBs, and other egress channels
- **Data discovery at rest:** Scans local file systems to identify and classify sensitive data such as PII, PHI, and payment card industry (PCI) information, and discovers where critical information resides before it moves to reduce exposure and meet compliance requirements
- **Cross-platform protection:** Provides real-time protection and visibility across both Windows and macOS devices, supporting diverse endpoint environments

Falcon Data Protection for Cloud

CrowdStrike Falcon® Data Protection for Cloud extends DSPM into runtime, delivering real-time visibility and protection for sensitive data in motion and at rest. It continuously monitors how data moves across APIs, third-party applications, cloud storage, and databases to detect unauthorized transfers, policy violations, and exposure risks. At the same time, it discovers and classifies sensitive data at rest across storage and databases, providing a complete picture of data activity and risk. Built on the unified Falcon platform, it activates instantly for customers with Falcon Cloud Security: Cloud Runtime Protection with Containers or Falcon Cloud Security: CNAPP with Containers, with no proxies, sidecars, or additional infrastructure.

- **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.
- **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.
- **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.
- **Lightweight deployment model:** Get protection delivered through the Falcon Linux sensor for rapid rollout in Amazon EKS and Azure AKS environments — no retooling or added sensors required.
- **Scalable data-at-rest scanning:** Run customizable scans across cloud services like Amazon S3, Amazon Relational Database Service (RDS), Amazon Redshift, Amazon DynamoDB, and Azure Blob Storage to discover and classify sensitive data without slowing operations.
- **Data-at-rest scanning:** Run customizable scanning of data at rest across cloud environments, allowing your organization to define scan cadences and scopes.

Schedule a demo today

"When you think about traditional data protection tools, deployment can take months and often requires adding new agents that slow down endpoints … with Falcon Data Protection, it was instant. Within days, we had visibility into our data flow."

Bill Lucas

Senior Director of Cybersecurity, Mastronardi Produce

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/