

Falcon Data Security

Understand what data is sensitive, see how it moves in real time, and stop data theft across the environment

Sensitive data is constantly on the move

Today's data no longer lives in one place or moves through predictable paths. It is constantly created, accessed, transformed, and shared across endpoints, browsers, SaaS applications, cloud services, GenAI tools, and emerging agentic workflows. Many of today's most damaging data incidents occur when legitimate access — whether by employees, automated processes, or adversaries using valid credentials — is misused. As data flows across environments, traditional approaches to discovery and classification break down, leaving organizations unsure where it exists, what data is sensitive, and where it's moving as threats emerge.

Despite this modern reality, security teams still rely on fragmented and outdated approaches. Many organizations struggle with noise, slow deployment, point-in-time inventories, and the inability to detect and stop data theft as it moves across endpoint, SaaS, and cloud environments. When data threats span multiple areas of the environment, teams often lack the shared context needed to quickly distinguish normal activity from real risk. In this reality, it no longer matters whether risky data movement is caused by an employee mistake, an automated process, or deliberate adversary activity using valid credentials.

Modern data security requires a fundamentally different model — one that turns data movement itself into a security signal and applies discovery, classification, and cross-domain CrowdStrike Falcon® platform context to stop data threats before exposure becomes a data breach. It must assume access is already compromised and enable teams to detect and stop data theft as it happens, not simply catalog risk. Delivering on this requires a platform-first approach that secures sensitive data where it is created, accessed, and moved — including consistent classification across environments, real-time visibility into data in motion, enforcement at the point of egress, and automated investigation and response workflows to accelerate triage and remediation.

Key benefits

- **Complete coverage — at rest and in motion:** Find sensitive content where it lives, and observe risky movement across the environment in real time.
- **Low-friction deployment:** Falcon Data Security uses the same unified lightweight Falcon sensor and single Falcon console as other Falcon modules.
- **Adversary-aware prioritization:** Platform threat telemetry and context help surface real attacks, not noise.
- **Unified classifications:** Enforce consistent data labeling and handling across hybrid environments with unified classifications — closing blind spots and simplifying policy enforcement.
- **Rapid time-to-value:** Falcon Data Security offers out-of-the-box detections and instant activation for existing Falcon customers.

Modern data security to secure data wherever it lives and moves

CrowdStrike Falcon® Data Security delivers this modern approach across environments — from endpoints, browsers, SaaS, and GenAI workflows to cloud services, storage, and workloads. Informed by real-world adversary threat intelligence, CrowdStrike enables security teams to understand where data resides, determine what data is sensitive, and see how it moves in real time to stop data theft. Teams can stop risky data movement and drive automated investigation and remediation using Falcon platform workflows, transforming data security from a visibility or compliance function into a core breach-prevention control.

Key capabilities

Advanced Classification

- **Consistent classification of sensitive data:** A shared classification engine spans endpoints, SaaS, and cloud environments, avoiding conflicting classification from multiple tools.
- **Out-of-the-box classification, without manual tagging:** Prebuilt classifiers reduce reliance on manual tagging and heavy upfront setup, enabling security teams to identify sensitive data and emerging data threats faster.
- **AI-powered classification that improves accuracy at scale:** AI-powered classification (leveraging LLM-based models) identifies sensitive data more accurately than static pattern matching alone.

Real-time Defense Across Environments

- **Defense at the moment of data movement:** Sensitive data is assessed in real time across endpoints, SaaS, browser, GenAI workflows, and cloud services, enabling teams to address threats before they become a data breach.
- **Actionable data movement context:** Source, egress channel, user, and destination context are captured to show how data actually moves, giving teams the clarity needed to respond to and stop risky behavior, not just review rule violations after the fact.
- **Enforcement and remediation:** Teams can block risky data movement at endpoint egress, prevent access to sensitive data in SaaS applications, and automate cloud data risk response actions with CrowdStrike Falcon® Fusion SOAR workflows to defend data across their environment.

Runtime Visibility into Cloud Data Activity

- **Real cloud behavior visibility, not just an inventory:** Extend visibility into cloud workloads, APIs, and services to see how sensitive data is accessed and transferred, helping teams spot unexpected access patterns and potential exposure.
- **Full data-flow details for faster investigation:** Capture key details for each data flow, including source, destination, method, classification, and user identity, so teams can quickly understand what happened and who was involved.
- **Active risk tied to the right sensitive data:** Connect runtime activity back to what data is sensitive so teams can prioritize investigations and focus response on the highest-impact exposure.

Data Security with Falcon Platform Context

- **Data threats in broader security context:** Data threats are understood alongside endpoint, identity, and cloud activity, providing the user, device, and access context behind each data interaction.
- **See who, what, and how:** Each data event can be understood with the user involved, the device in use, and the cloud access behind the interaction to speed up investigation and response.
- **Unified delivery through one sensor and console:** Delivered through the unified Falcon sensor and managed from a single console, Falcon Data Security eliminates the need for a separate data security stack, additional sensors, or new workflows and makes it easier to correlate, prioritize, and act.

Data security capabilities across the Falcon platform

Depending on the environment and use case, CrowdStrike offers Falcon modules that address different aspects of data threats.

To secure sensitive data as users work across endpoints, SaaS applications, browsers, and AI tools:

- **CrowdStrike Falcon® Data Security for Endpoint:** Provides real-time discovery, classification, and defense at the point of data egress on endpoints, including visibility and enforcement across key data movement paths such as web, removable media, local applications, printers, and SaaS destinations
- **CrowdStrike Falcon® Guardian:** Helps protect sensitive data across AI interactions while providing visibility and controls to reduce data exposure as employees, applications, and AI agents use enterprise AI.
- **CrowdStrike Falcon® Data Security for SaaS:** Delivers visibility into sensitive files across Microsoft 365 and automatically applies and manages Microsoft Sensitivity Labels so teams can consistently protect data across SharePoint and OneDrive.
Note: Initial coverage is Microsoft 365.
- **CrowdStrike Falcon® Seraphic® Enterprise Browser:** Extends Falcon Data Security coverage to browser-mediated data access by providing visibility and control over how sensitive data is accessed and handled through web browsers

To secure sensitive data in cloud environments:

- **CrowdStrike Falcon® Cloud Security:** Provides discovery and visibility into sensitive data at rest across cloud services and storage environments, helping teams understand where sensitive data resides in the cloud
- **CrowdStrike Falcon® Data Security for Cloud:** Provides advanced cloud data security including AI-powered classification and runtime visibility into cloud data in motion, observing how sensitive data is accessed and moved across cloud workloads, APIs, and services using eBPF-based telemetry
Note: Falcon Cloud Security for Containers is a prerequisite.



“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 Security), it was instant. Within days, we had visibility into our data flow.”

Bill Lucas

Senior Director of Cybersecurity,
Mastronardi Produce

[Schedule a demo today](#)

Forward-Looking Statements

This data sheet may include discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.

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/>

