

Falcon Data Security for Endpoint

Understand what data is sensitive, see how it moves, and stop theft across web, GenAI tools, removable media, printers, and local applications

Modern data security to stop data loss at the endpoint

Sensitive data is constantly being created, accessed, and shared on endpoints through browser uploads, SaaS sharing, local applications, removable media, and printing. Legacy approaches create operational friction — complex deployments, ongoing policy maintenance, and false positives without enough context — leaving teams slow to respond in the moments they can't afford delays.

CrowdStrike Falcon® Data Security for Endpoint delivers real-time visibility and policy enforcement to prevent sensitive data loss across key endpoint egress channels, including web, GenAI tools, removable media, printers, and local applications. Built on the CrowdStrike Falcon® platform and delivered through the same sensor as other Falcon modules, it's easy to deploy and operationalize without disrupting end-user productivity. Fully integrated with the Falcon platform, it enables consistent classification, behavioral detection, and streamlined response workflows so teams can reduce exposure and stop data theft fast.

Key benefits

- **Understand which data is sensitive:** Discover and classify sensitive data on endpoints to inform policy and enforcement, with consistent labeling that scales across users and devices.
- **See how data moves across key channels:** Gain real-time visibility into sensitive data movement across web, local applications, GenAI tools, removable media, and printers to reduce blind spots.
- **Stop theft with precision controls:** Prevent unauthorized exfiltration using policy-based enforcement grounded in data sensitivity, user context, and behavior.
- **Fast time-to-value:** CrowdStrike customers get instant activation — no additional sensor required.
- **Unified classification:** Apply consistent policies across endpoint and cloud with a shared classification engine.
- **Multiple operating system coverage and enforcement:** Protect sensitive data on Windows and macOS endpoints.

Key capabilities

Understand Which Data Is Sensitive

- **Endpoint discovery and classification:** Identify and classify sensitive data on endpoints to power policy decisions and enforcement across channels.
- **Unified classification across domains:** Use a shared classification engine across Falcon Data Security to align policies and data labeling for financial data, personally identifiable information (PII), protected health information (PHI), and intellectual property (IP).
- **Encryption detection for investigative visibility:** Inspect encrypted archive contents in real time and see what's being packaged before it leaves the environment. Capture full context and content of attempted encrypted exfiltration for faster, evidence-backed investigations.

See How Data Moves

- **Web and application visibility:** Monitor sensitive data movement across browsers and local applications to understand who is accessing and transmitting sensitive content.
- **Removable media and print coverage:** Detect and control sensitive data written to removable media and printed to reduce common leakage paths.
- **Behavioral anomaly detection:** Surface suspicious behavior patterns across individuals, peer groups, and the organization to identify risky or unusual activity.
- **Similarity detection beyond exact match:** Detect sensitive data even when altered or partially modified, reducing evasion techniques that bypass traditional controls.
- **Falcon platform context:** Correlate data activity with endpoint telemetry, user identity, and threat intelligence across the Falcon platform to prioritize real risk and accelerate investigation.

Stop Data Theft

- **Policy-based enforcement across channels:** Block, allow, or notify actions based on sensitivity and policy across web, GenAI tools, removable media, printers, and local applications.
- **End-user justification:** Prompt users for a business justification on risky actions to reduce accidental leakage and create an audit trail aligned to policy.
- **GenAI data leak prevention:** Detect and block sensitive data shared with GenAI tools in real time across browsers and native apps.

[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/>

