CROWDSTRIKE

White Paper

A Modern Approach to Confidently Stopping Data Exfiltration

CrowdStrike Falcon Data Protection stops data theft more effectively

Many organizations have quickly adapted to a cloud-first world where the data lives and moves. But when business transactions happen in the cloud, your employees can still download data from several web and software-as-a-service (SaaS) applications, use it as the business dictates, and move it to several other locations like web applications, cloud drives and USB storage devices — either in its entirety or in parts. Organizations have been using several endpoint data loss prevention (DLP) tools over the past two decades, but many have challenges in confidently identifying sensitive data movement — from the origin to the destination — without impacting the user experience and business productivity.

There are three main challenges that get in the way of implementing an effective data protection strategy. The first big challenge is having to deploy and manage too many endpoint agents. The second challenge is getting consistent and deep visibility into data flows from the source to the destination. Finally, there can be reluctance to enforce blocking controls as they may negatively impact user experience and productivity.

Moving away from content-centric DLP solutions — and at the same time aiming to reduce deployment and operational complexity and improving the user experience — will set the right foundational elements for a modern data protection strategy.

$4.45M

average total cost of a breach[1]

75%

of businesses reported that more than 40% of their data stored in the cloud is sensitive[2]

29%

of organizations struggle to manage their complex DLP environments[3]

[1] IBM, Cost of a Data Breach Report 2023

[2] Thales, 2023 Cloud Security Study

[3] CSA, Data Loss Prevention and Data Security Survey Report

How CrowdStrike Protects Your Data

CrowdStrike Falcon® Data Protection, a module in the industry-leading CrowdStrike Falcon® platform, takes a modern approach to securing your enterprise data from adversaries. Falcon Data Protection is the industry's only AI-powered solution for exceptional data protection built on a unified agent and single console. By combining content with context, Falcon Data Protection provides deep real-time visibility into what is happening with your sensitive data, including data artifacts, as they move from the source to the destination.

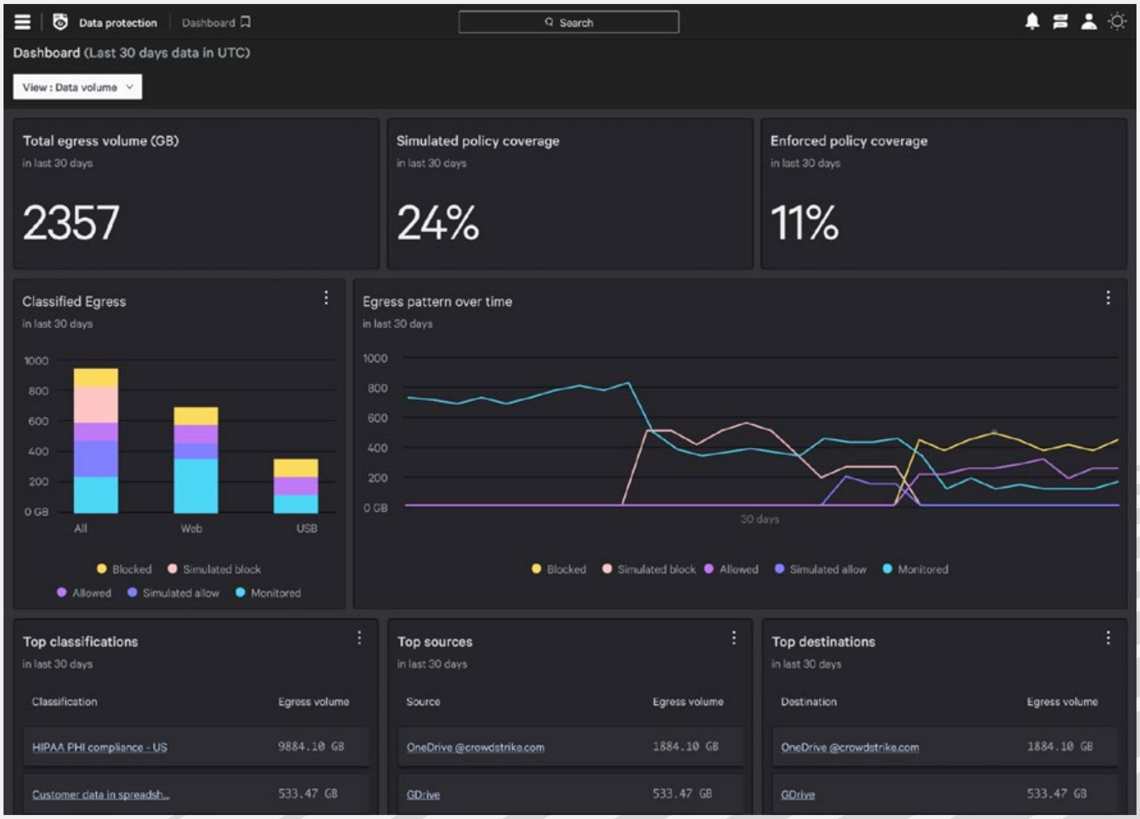
Falcon Data Protection adds the much-needed context to content, which has been missing on traditional DLP solutions, to empower enterprises to prevent data theft in today's cloud-first environments.

Falcon Data Protection enables you to:

- Reduce deployment complexity
- Get instant contextual visibility into data flows
- Classify data to get enhanced context into sensitive data movement
- Simplify rules, enforce with confidence and improve the user experience
- Simplify management with a unified console
- Get extended visibility across endpoints and identities

Falcon Data Protection Stops Unauthorized Data Exfiltration

By inspecting data as it arrives on the endpoint, Falcon Data Protection identifies not only the originating source but unique features within data, allowing it to be tracked as it moves between files. Unlike most traditional DLP solutions that are content-centric, Falcon Data Protection identifies data that is exiting (egressing) from an endpoint as sensitive based on its originating source, content, who's moving the data, and even derivatives of a sensitive file that have been copied and pasted.



Dashboard (Last 30 days data in UTC)

Total egress volume (GB)
in last 30 days
2357

Simulated policy coverage
in last 30 days
24%

Enforced policy coverage
in last 30 days
11%

Top classifications
in last 30 days

Classification	Egress volume
HIPAA PHI compliance - US	9884.10 GB
Customer data in spreadsh...	533.47 GB

Top sources
in last 30 days

Source	Egress volume
OneDrive @crowdstrike.com	1884.10 GB
GDrive	533.47 GB

Top destinations
in last 30 days

Destination	Egress volume
OneDrive @crowdstrike.com	1884.10 GB
GDrive	533.47 GB

Falcon Data Protection dashboard showing data exfiltration

Reduce deployment complexity

The foundation to any endpoint data protection strategy is getting the deployment right — without "deployment regrets." Falcon Data Protection simplifies deployment as it's built into the cloud-native CrowdStrike Falcon® platform's unified sensor. This modern approach removes the need for on-premises infrastructure, and the lightweight Falcon sensor is optimized for performance. If you already have the Falcon sensor on your endpoints, you can deploy Falcon Data Protection in minutes, not days or weeks as is often the case with traditional data protection deployments. After deployment, all you need to do is enable it for your hosts to start seeing data flows. The Falcon Data Protection dashboard gives you instant insight into data egress trends, and you can drill down to understand your data's end-to-end flows.

Get instant contextual visibility into data flows

One of the many challenges with traditional data protection solutions is the lack of context tied to content. With your employees downloading data from cloud applications and moving it to other applications on the web or in the cloud, content inspection alone doesn't provide the complete picture. Content-centric solutions result in false positives and privacy issues. For example, during a tax season, a data protection strategy based only on content inspection for social security numbers will trigger a flurry of false positives. While employees may genuinely be submitting tax documents, the use of Social Security numbers will not only trigger false positives but also create privacy issues with employees' tax documents being scrutinized.

Even before you configure and classify sensitive data, Falcon Data Protection provides all data flows as "monitored" flows — i.e., all data from origin to destination — providing you with early insights on data movement in your enterprise to help you formulate protection policies.

You can get more granular with the data flows by defining web sources like Microsoft Office 365 applications, Google Workspace and Box with account-level information to help you distinguish between managed/unmanaged applications. This gives you a clearer context to differentiate between data flowing to and from managed/unmanaged apps — like files containing personally identifiable information (PII) flowing from a managed OneDrive to a personal OneDrive — to avoid having to deal with false positives.

Classify data to get enhanced context into sensitive data flows

It's important to discover and understand the sensitive data that traverses across your organization. In addition to knowing where the data is going, you should also know what the data might contain according to sensitivity that is determined by your organization.

With custom data classification, Falcon Data Protection identifies sensitive data in motion that's trying to egress via web browsers and USB devices in real time. Classifications must be flexible in order to protect data in all states. Falcon Data Protection includes various classification attributes:

- **Content patterns:** 70+ predefined content patterns for PII, payment card industry (PCI) information, protected health information (PHI) and more, as well as support for custom regex and keywords
- **Web source:** 10,000+ popular web apps/sites available for tracking visibility, in addition to extended capabilities for account-level context for Microsoft O365 apps, Google Workspace apps, and Box, as well as support for custom web sources based on domain name or IP address
- **True file type:** Content-aware scanning that allows rules to trigger based on the actual file type, even if the file's extension is obfuscated
- **Microsoft Information Protection (MIP) labels:** Identification of files containing MIP sensitivity labels and enforcement of rules based on specific labels — this flexible approach provides visibility and protection for a wide variety of data protection use cases

Being as specific as possible when defining what "sensitive" means for your organization's data reduces the risk of data theft, avoids fatigue from numerous false positives and protects the privacy of your users.

Simplify rules, enforce with confidence and improve the user experience

Creating and enforcing effective, simple data protection rules can not only stop data theft, it can improve the overall productivity of your organization. Once you clearly define custom data classifications, Falcon Data Protection makes it very easy to define, test and enforce the rules attached to these data classifications to effectively detect and stop data egress. You can get granular visibility into sensitive data movement with precedence-based rules that allow you to either block by default — that is, lock down data but with exceptions — or allow by default with specific block rules.

For example, to have better control over PII data egress from files downloaded from Salesforce, you can define precedence-based rules to **block** all users from uploading customer data that originated from Salesforce to any location. But you can **allow** C-suite and specific users to upload it across web locations, and **allow** all users to upload data that originated in Salesforce only back to Salesforce.

Once you've defined your specific rules, you can take a measured approach to determine the potential impact of the policies using Falcon Data Protection's simulation mode. You can visualize policies via simulated data flows to help avoid end-user frustration when testing block rules, and avoid alert fatigue and false positives for your resource-constrained security team. Once you have studied and analyzed "what-if" scenarios of the policies in simulation mode, you can enforce them with confidence.

Simplify management with a unified console

A recent survey[4] by Cloud Security Alliance (CSA) showed that organizations are looking for DLP solutions that simplify management. Over a third of survey respondents prefer unified policies and single-console solutions. Also, several respondents indicated that manual version updates are a significant challenge in implementing DLP solutions.

Since Falcon Data Protection is part of the CrowdStrike platform, you don't have to juggle multiple consoles to connect the dots to stop data exfiltration. You get granular visibility on every data flow for specific sources, egress channels and destinations to get additional information on why a sensitive data/file was moved to an unmanaged cloud drive and by which user. From the unified console, you can understand all data protection events that match the PII rule that you defined with rich contextual information. For example, if a user tries to move PII data that contains U.S. Social Security numbers from Salesforce into their personal Google Drive, you will see the policy action that was enforced for this event.

Get extended visibility across endpoints and identities

Falcon Data Protection further extends your contextual visibility by leveraging other Falcon products like CrowdStrike Falcon® Insight XDR endpoint protection and CrowdStrike Falcon® Identity Protection to understand device posture and vulnerabilities, user risk score, user group, whether the user has privileged access, and more. Analysts can leverage Falcon Data Protection's telemetry to confidently investigate and establish the "why" to detect unauthorized data exfiltration and stop data theft more effectively.

[4] Cloud Security Alliance, Data Loss Prevention and Data Security Survey Report

> "I'm really impressed by the persistent source attribution that points back to the data's true source, even after changing the file name, duplicating the data and uploading it across multi-vendor cloud storage platforms."
>
> — Insider Threat Operations Lead at a Fortune 100 company

Ready to learn more?

Watch this short video to see Falcon Data Protection in action.

Experience it first-hand — request a demo.

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.