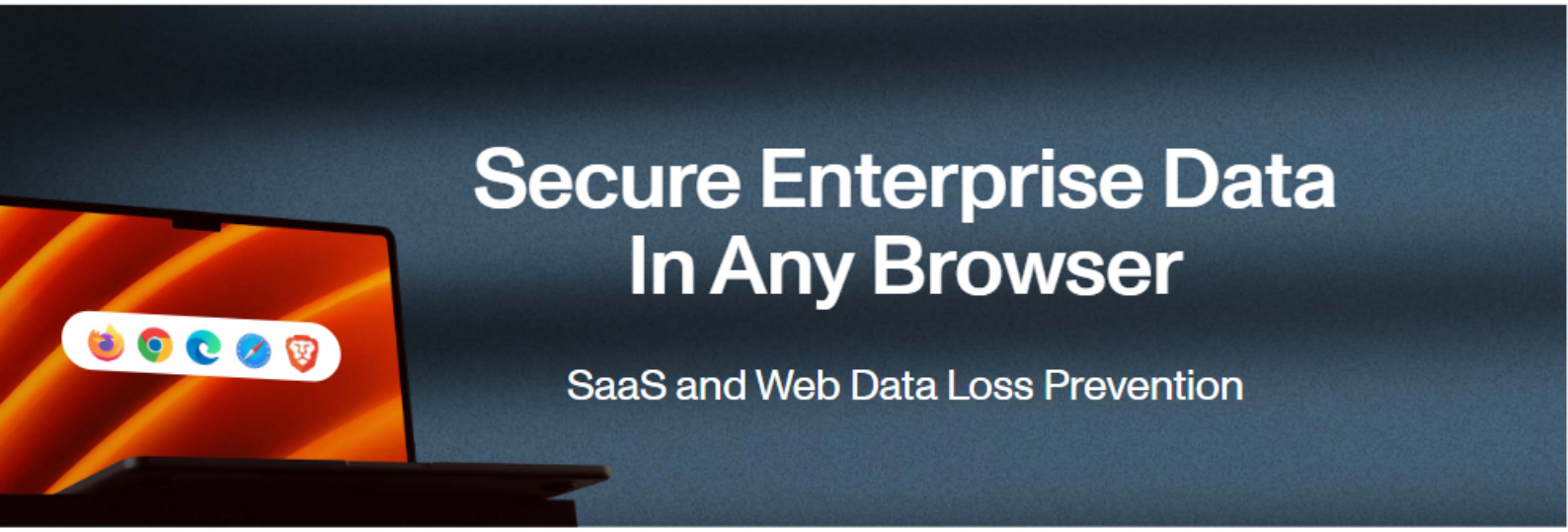
seraphic Fine-grained control and policy enforcement



Secure Enterprise Data In Any Browser

SaaS and Web Data Loss Prevention

Enterprise data is everywhere

Organizations' dependence on internal and SaaS web apps continues to increase, meaning that—not only does sensitive data exist both on- and off-premises—it is access by a single client: the browser. Moreover, types of data in these applications can range from proprietary Intellectual Property (IP) to Payment Card Information (PCI) to regulated Personally Identifiable Information (PII) or healthcare data, all of which may be accessed by a combination of regular employees on managed devices or 3rd parties and affiliates on unmanaged devices.

Users can access sensitive data from more places than ever before

Key data loss concerns

The proliferation of enterprise data and the growth of hybrid work have exacerbated the risks, including:

- **Accidental** or negligent disclosure of data
- **Intentional data theft** by employees/ 3rd parties (insider threats) or external actors
- **Unauthorized data transfer** between corporate and personal/ unsanctioned web apps and cloud storage (data "hairpinning")
- Consistent **policy enforcement** and protection of data across managed and unmanaged devices

Organizations must also be able to log the flow of data to support investigations and 3rd Party Risk Management (TPRM).

The average cost of a data breach rose to $4.45M in 2023 (up 15% over 3 years)

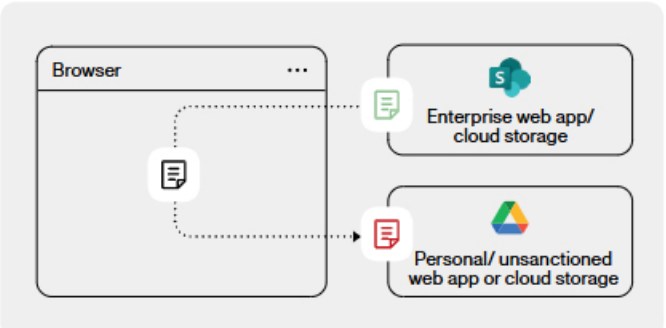
Existing solutions are insufficient

Historically, the main channels for data loss were email and copying data to removable media. Because email is centrally controlled, it is easier to address. Meanwhile, the advent of cloud storage has all but eliminated the need for removable storage.

Despite the fact that web apps and cloud storage are now significant repositories of enterprise data, many organizations rely on tools adapted from the architecture of email DLP:

- They require proxies or other in-line inspection that can negatively impact user experience
- They may require API integrations with SaaS services, which can reduce or delay protection
- They provide limited or no control of internal web apps
- They provide little or no control of user actions within the browser
- They have limited visibility into

Browsers have replaced email and removable media as the primary data loss vector



Data flowing from enterprise resources through the browser can easily be leaked to unsanctioned sites and apps.

Why Seraphic

Seraphic Security provides a comprehensive set of controls to protect enterprise data as it moves into and out of the browser with a minimal installation footprint that is easily deployed to managed or unmanaged devices.
Seraphic enables organizations to identify sensitive data by creating **Sensitive Data Profiles** using:

Predefined PII

- Personal data (e.g., addresses, date-of-birth, int'l phone numbers, Social Security numbers)
- Financial data (e.g., routing numbers, credit card numbers)
- Medical record identifiers
- Login account details (Basic Auth user/ password, access tokens) and API keys
- Source code
- Custom Regular Expressions (RegEx)

The robust scanning engine can:

- Detect and block encrypted file content
- Allow / Scan / Block password-protected compressed archives (e.g., .zip, .rar, .7z)
- Use Optical Character Recognition (OCR) to inspect non-text files for sensitive data

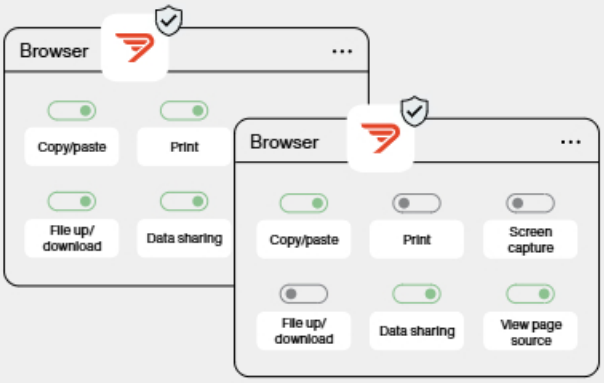
Seraphic's DLP policies enable organizations to:

- Allow/ deny user actions in the browser (copy/ paste/ print/ screen cap/ right click/ view page source)
- Restrict file upload by size and extension
- Redact / mask PII in web pages and files
- Watermark internal and SaaS web app pages
- Control data sharing between sites/ apps based on data source and destination
- Restrict logins to SaaS services using personal accounts or other corporate accounts

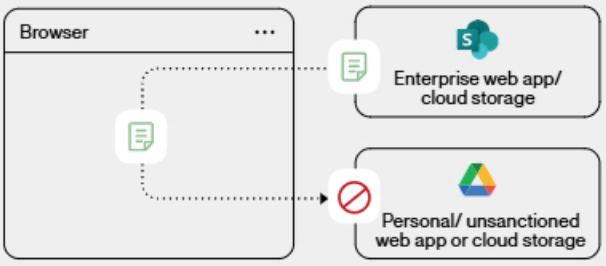
Policies can be applied i**n Passive Mode** (alert only) or **Active Mode** (block and alert) and logs can be exported to SIEMs for correlation or audit

Comparison of protection

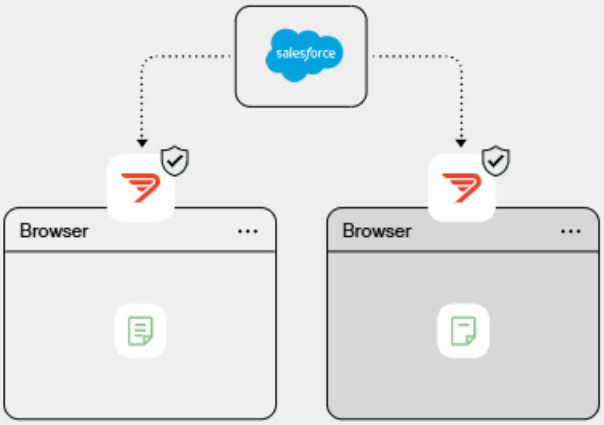
Seraphic has a flexible and granular rule framework that enables different **policies** for different **user** (employee vs. 3rd party) and **device** (corporate vs. personal) types.



Seraphic provides **controls and logging** for all user actions in the browser



Seraphic can **block data transfer** between corporate resources and unsanctioned apps or cloud storage



Seraphic can dynamically **mask sensitive data** as it is displayed in the browser