Layer

Browser Security Platform:

Guard your Data from Exposure in GenAI Tools

THE CHALLENGE:

Safe Use of GenAI Tools

Within the short timeframe since its release, GenAI tools have already triggered a fundamental change in the way we produce textual outputs, from executive summaries to product specs and source code. There's no doubt that we're witnessing a potential quantum leap in employee productivity, to a measure we can't yet truly evaluate.

However, we cannot ignore the whole new dimension of data exposure risk the use of GenAI tools introduces. None of the data protection tools we have in our security stacks are equipped to prevent the mass dissemination of sensitive data that results from an employee inserting it to GenAI tools.

In this eBook we provide an overview of the potential and actual risks that ungoverned use of GenAI tools entails and come to understand the limitations of existing solutions. Following, we'll introduce and explain why the emerging category of browser security platform is best equipped to balance both security and productivity requirements, enabling your employees to maximize the benefit they gain from GenAI tools, without compromising on your data protection standards.

GenAI Tools Data Exposure in Numbers

Employee usage of GenAI apps has increased

44%

over the past three months

Data pastes to GenAI apps occur around

36

times a day

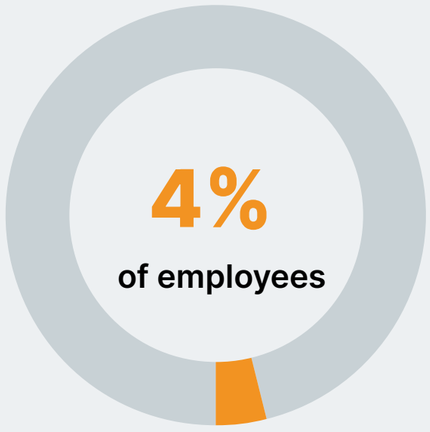
GenAI apps are visited

131

times a day

to GenAI apps included data pasting

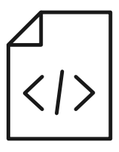
have pasted sensitive data into GenAI



paste sensitive data into GenAI on a weekly basis

Main Data Types at Risk

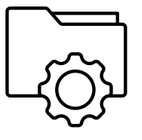
Sensitive\Internal



Source code

Client data

Regulated PII



Project planning files

What a GenAI Tools Data Exposure Scenario Looks Like

Unintentional Data Exposure

Employees paste sensitive data that gets exposed online as part of an answer to a random query. It could be a Product Manager asking for a refined PRD, an executive looking to fine tune their opening statement to the board, a developer looking to optimize her source code, and so on an so forth.

Targeted Attack

The external adversary compromises endpoints at the targeted entity and conducts GenAI tools oriented reconnaissance, gaining insights into which queries are typically associated with sensitive data. Once obtaining these insights, the adversary attempts to use them from their own browser.

The common denominator: GenAI tools enable to the exposure, and even the exfiltration, of data in a manner that's invisible to the organization's data protection radar.

Malicious Insider

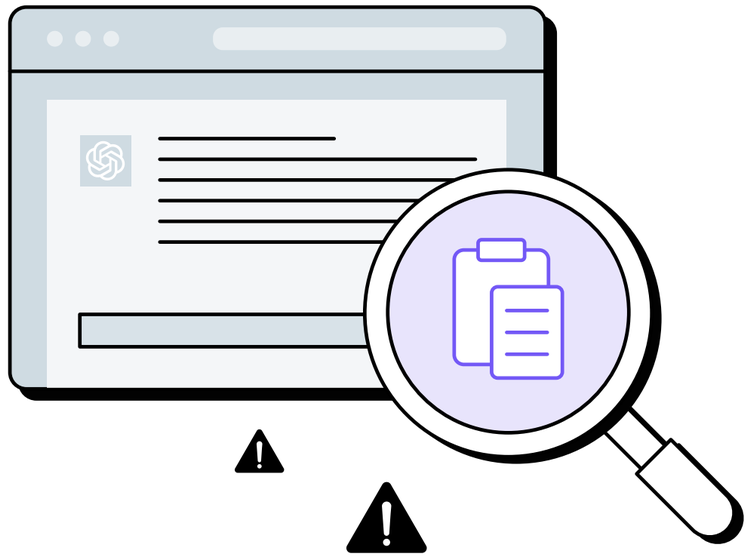
A malicious insider provides GenAI tools with an input of sensitive data, aligning it with a crafted sequence of questions. These same questions, when used by the insider from any unmanaged computer would yield this data as an output, exfiltrating it out of the organization's boundaries and control.

File-based DLP Solutions are Helpless Against Text Insertion to GenAI Tools

You may be asking yourself why you can't simply use your existing DLP solutions. After all, we rely on them to protect our data, both on-prem and in our SaaS and clous workload environments.

DLP products were built and designed to protect data that is saved and stored in **files**. So, if a file contains sensitive data, and marked by a DLP as such, there will be various restrictions in place, preventing actions such as share, download, copy, etc. However, the way users provide data to GenAI tools is rarely by uploading files. They insert text directly. Whether this insertion takes place via type, paste, or fill, it falls completely beyond the protection scope of the file-based DLP.

Let's gain insights into how organizations confront this new reality.



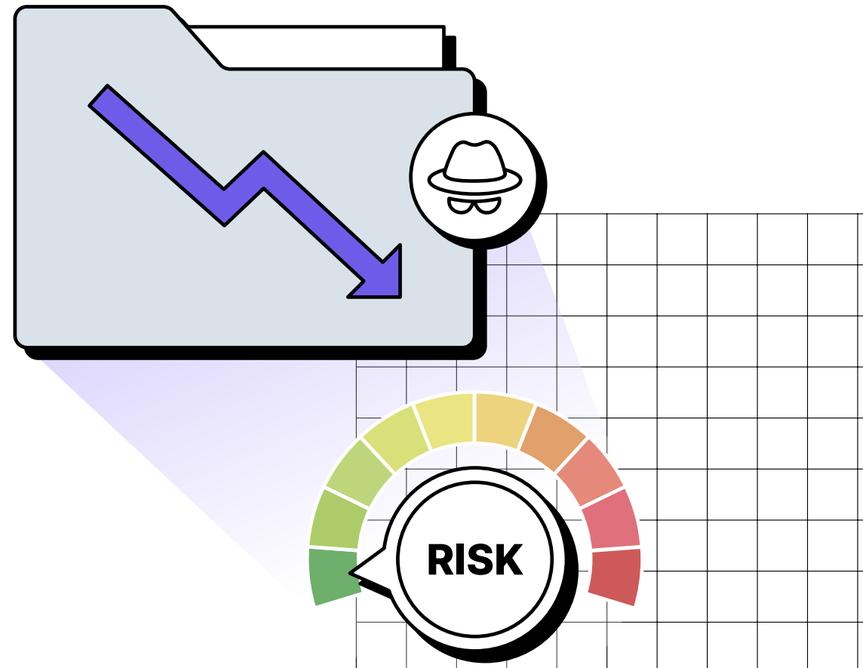
3 Common Approaches to Mitigating GenAI Tools Data Risk

Blocking Access to GenAI Tools Altogether

Blacklisting GenAI tools' URL in the organization's firewall so users cannot access it from within the internal network. This approach is practiced by several countries, as well as some big corporations including Amazon, JPMorgan Chase, and Apple.

Pros: Straightforward elimination of a significant portion of the risk.

Cons: In the long run, the productivity loss resulting from not using GenAI tools will render this approach unsustainable. Also, it doesn't address remote workers that work with unmanaged devices or connect to the Internet from external networks.



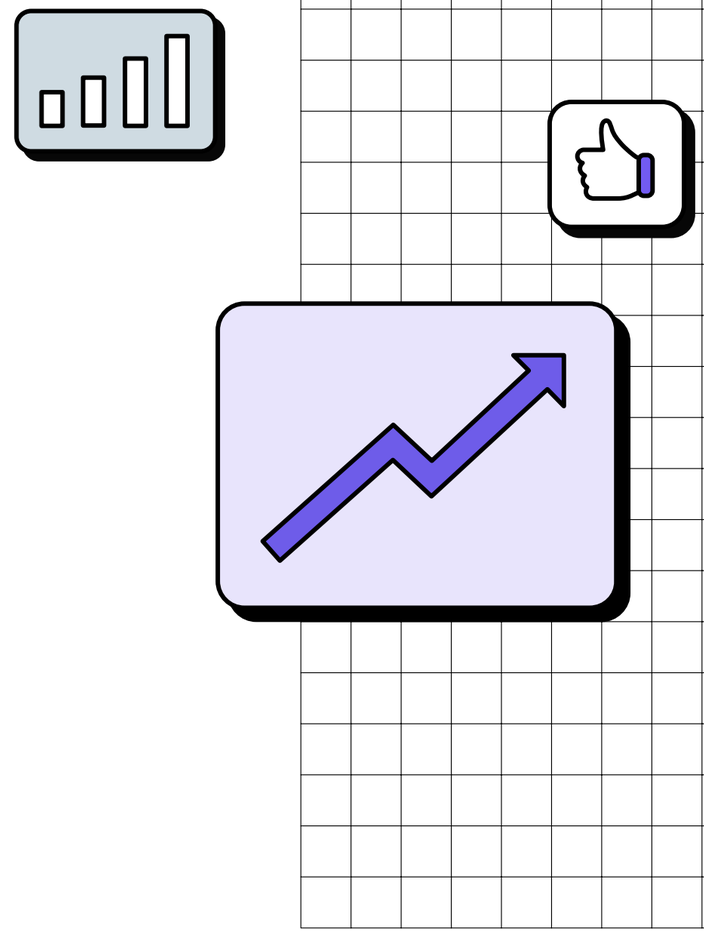
Educating Employees on Secure Use

Invest in increasing employees' awareness to GenAI tools data security issues and provide them with specific instructions as to what data they are allowed or not allowed to enter.

Pros: Employees can still use GenAI tools as productivity boosters.

Cons: At best, this approach addresses the risk of unintentional data exposure. However, while it doesn't provide any protection against malicious insiders or targeted attacks. It also lacks monitoring and enforcement tools to ensure attacks.

It also lacks monitoring and enforcement tools that the organization's data protection policies are adhered to and followed.



Controlling Users' Actions

Using a Browser Security extension to apply various monitoring and governance actions on users' activity within GenAI tools, such as blocking access, alerting, and preventing paste and fill actions, either completely or at a granular level that enforces it for sensitive data only.

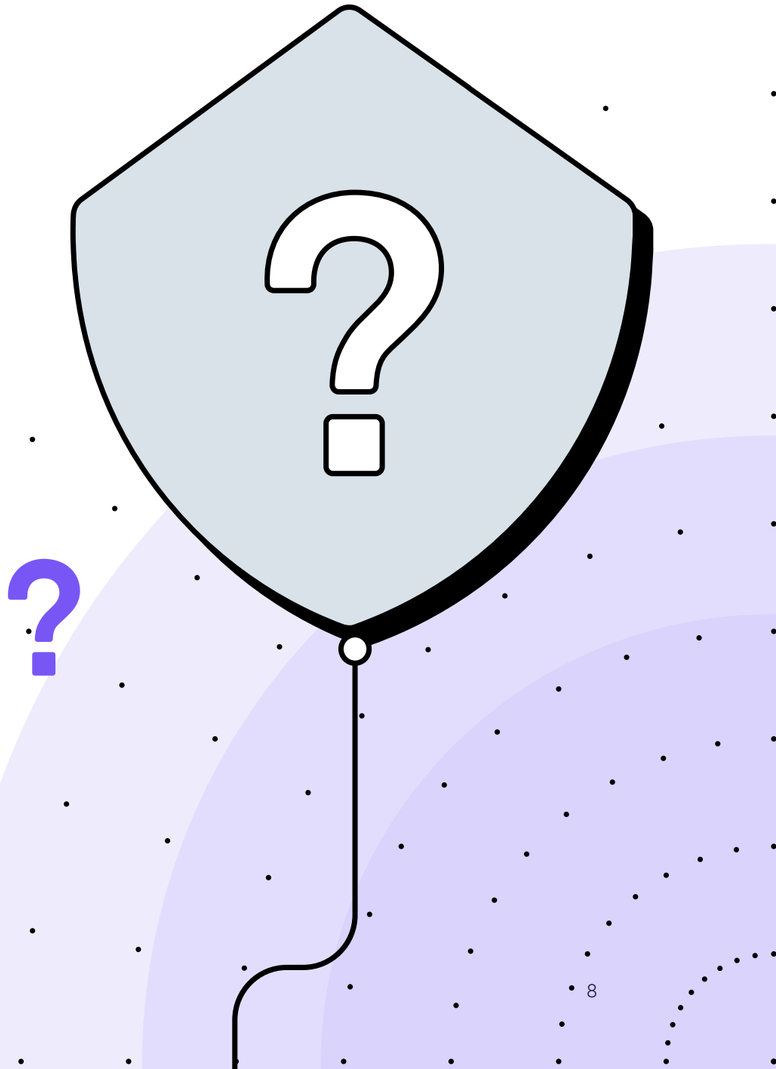
Pros: Enables employees to leverage the text generator to increase productivity, while preventing the exposure of sensitive data.

Cons: None.

What is a Browser Security Extension?

A Browser Security Extension applies continuous monitoring, risk analysis, and proactive protection on web sessions conducted from a user's browser. It's the only solution today that has real-time visibility and enforcement capabilities on the actual, live web session. The browser security extension provides insights into any browsing event: those performed by the user and those, as well as those that are initiated by the target web page. These insights enable the extension to identify events that may introduce potential risks and prevent them from taking place.

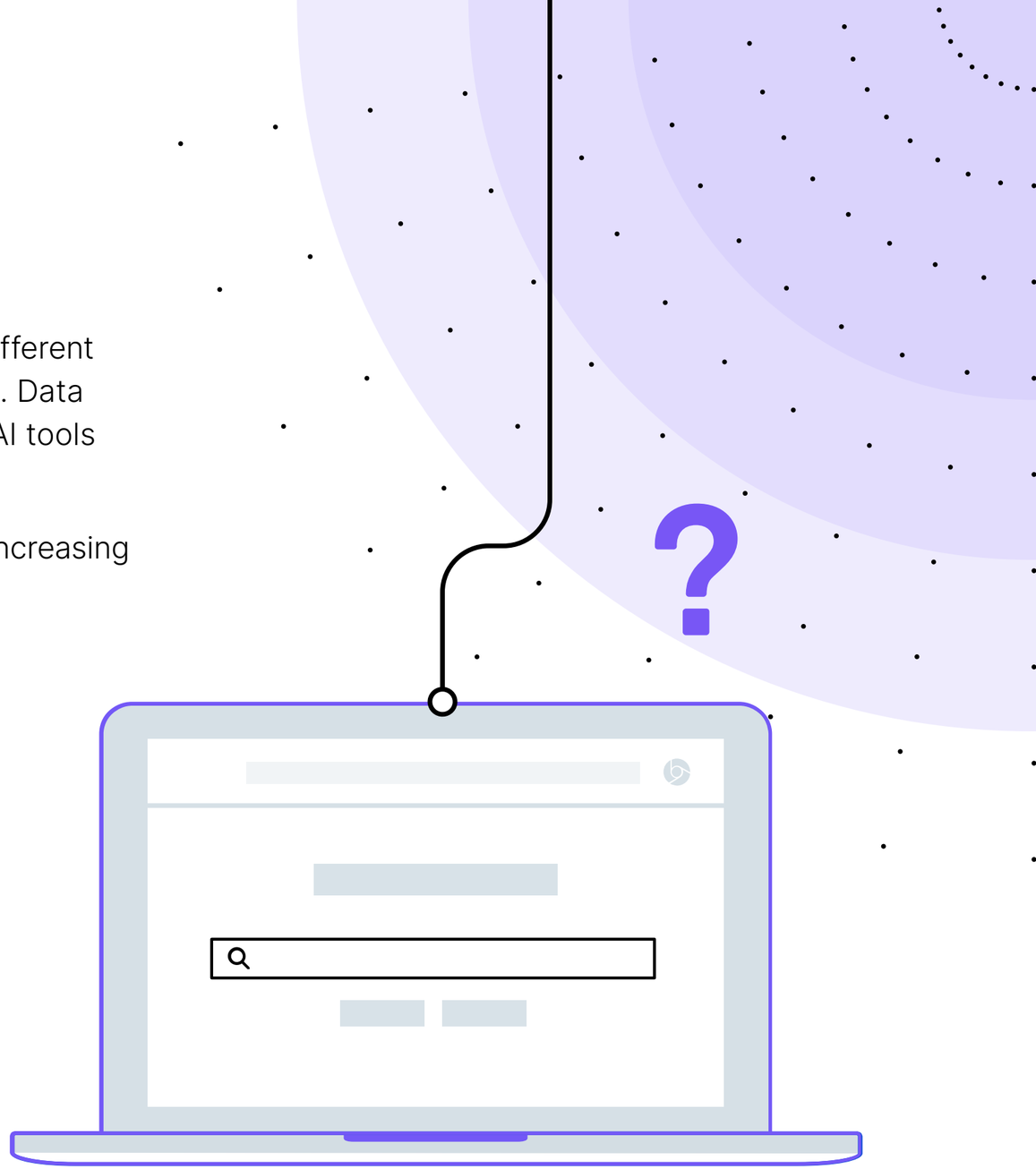
In the context of protection against data exposure on GenAI tools, a browser security extension can easily achieve what DLPs can't. Since GenAI tools are accessed via a web session, the extension can monitor and govern all the means in which users provide it with input. And since access, type, paste, and fill are events within the web session, the extension can determine for each, when it is allowed and when it is not.



GenAI Tools Protection with a Browser Security Extension

The key advantage of a Browser Security Extension is its ability to assemble different protections for various users and groups, based on their role and data access. Data protection teams can determine that while some users are blocked from GenAI tools altogether, others can access it either freely or in a controlled manner.

A browser security extension can apply three different protection levels, with increasing levels of granularity:

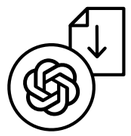


GenAI Tools Access

This protection level determines users’ ability to access the GenAI tools apps. It is a fit for users who interact with with highly confidential data on a daily basis.

Actions in GenAI tools

This level is focused on preventing data insertion actions that could put organizational data at risk, and especially ‘paste’ and ‘fill’. It enables employees to continue using GenAI tools while mitigating the risk of sensitive data being inserted.



Data Input into GenAI tools

The most granular protection level. A data protection policy is configured within the Browser Security Extension. The policy defines which data is not allowed to enter GenAI tools, through typing, pasting, or any other insertion method. Limitation could range from a broad policy of not allowing the pasting of links, to blocking specific text strings and patterns.

The Browser Security Extension Data Protection Matrix

The Browser Security Extension can either **block** or **alert** on each of the three protection levels listed above. The only thing the data protection stakeholder has to do is to determine which combination is the best fit for the different users and groups in their organization.

	GenAI Tools Access	GenAI Tools Data Insertion Actions (Type, Paste, Fill)	
		Any Input	Sensitive Data Input Only
Block	No access is allowed	Chosen action is disabled	Chosen action is disabled for sensitive data input
Warn User	Access allowed but with a data exposure warning pop up	Chosen action is allowed but with a data exposure warning pop up	Chosen action is allowed for sensitive data input but with a data exposure warning pop up
Allow	Access is allowed	Chosen action is allowed	

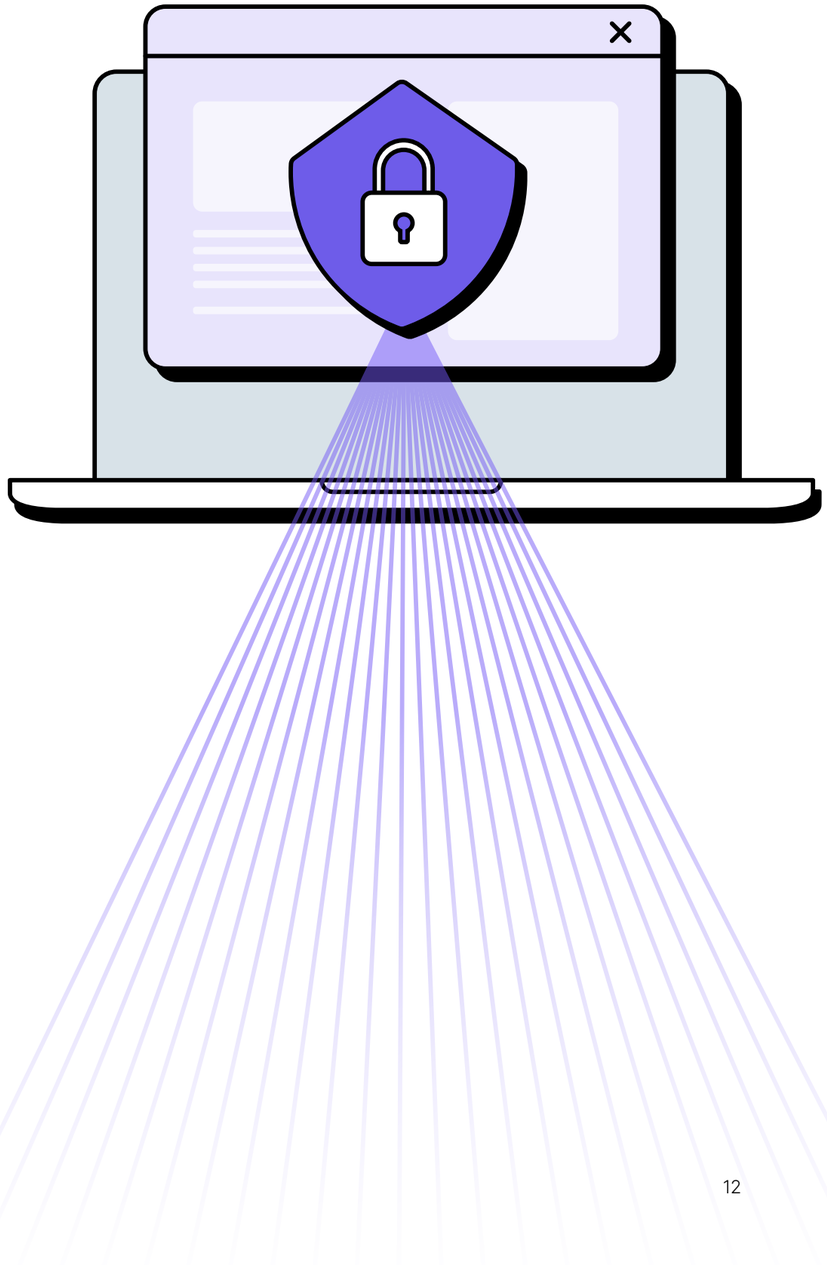
CONCLUSION:

Browser Security Extension is the Key to Secure Productivity

A Browser Security Extension is the ultimate mean to achieve a sound balance between workforce productivity and data protection. The ability to translate all existing file-based data protection policies and best practices to text-based policies that can be enforced on the actual browsing provides users consistency across their entire data interaction experience over both files and texts.

The third protection level - Data input into GenAI tools – is specifically suited to maximize the utilization of GenAI tools by the organization's users, aiming to perform minimal chirurgic protection actions only when data exposure risk arises, and nor interfering with any other GenAI tools interaction.

This type of productivity enabling security is possible only through the browser.



The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience

Integrates with All Commercial, AI and Enterprise Browsers

The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks, including:

AI Usage Security

GenAI DLP
Prevent leakage of sensitive data on AI tools

AI Access Control
Restrict user access to unsanctioned AI tools or accounts

AI Browsers Protection
Protect AI browsers against attack and exploitation

AI Misuse Prevention
Protect against prompt injection, compliance violations, and more

Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

AI Response Validation
Ensure AI response validity and data security

Enterprise Browser Security

Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

Safe Browsing
Protect all browsing activity against web exploits

Browser Extension Management
Detect and block risky browser extensions on any browser

SaaS Identity Protection
Discover and secure corporate and personal SaaS identities

Shadow SaaS & SaaS Security
Discover 'shadow' SaaS and enforce Saas security controls

AI Browsers Protection
Protect AI browsers against attack and exploitation