

Sekant Security

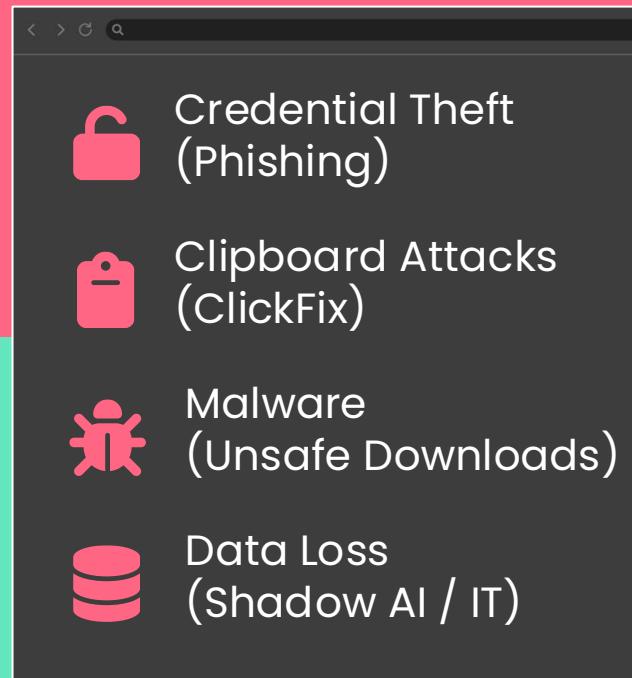
De-risk Enterprise Browsing with
Embedded Runtime Intelligence

80% of user time spent
in browsers

Browsers are where
most enterprise work
happens ... but also,
where security controls
are the weakest.

Sekant is an extension
that secures the
browser using client-
side models to detect
threats in real-time.

44% of cyber attacks
involve a browser



BENEFITS

Zero-day
detection

Real-time
response

Scalable

Complete
privacy

Foils evasion
techniques

Personalized
protection

OUTCOMES

- >85% Zero-day Phishing Detection
- 97% ClickFix Detection
- Block Unsafe Downloads
- Monitor AI prompts, data pastes & uploads



<https://sekantsecurity.com>



info@sekantsecurity.com

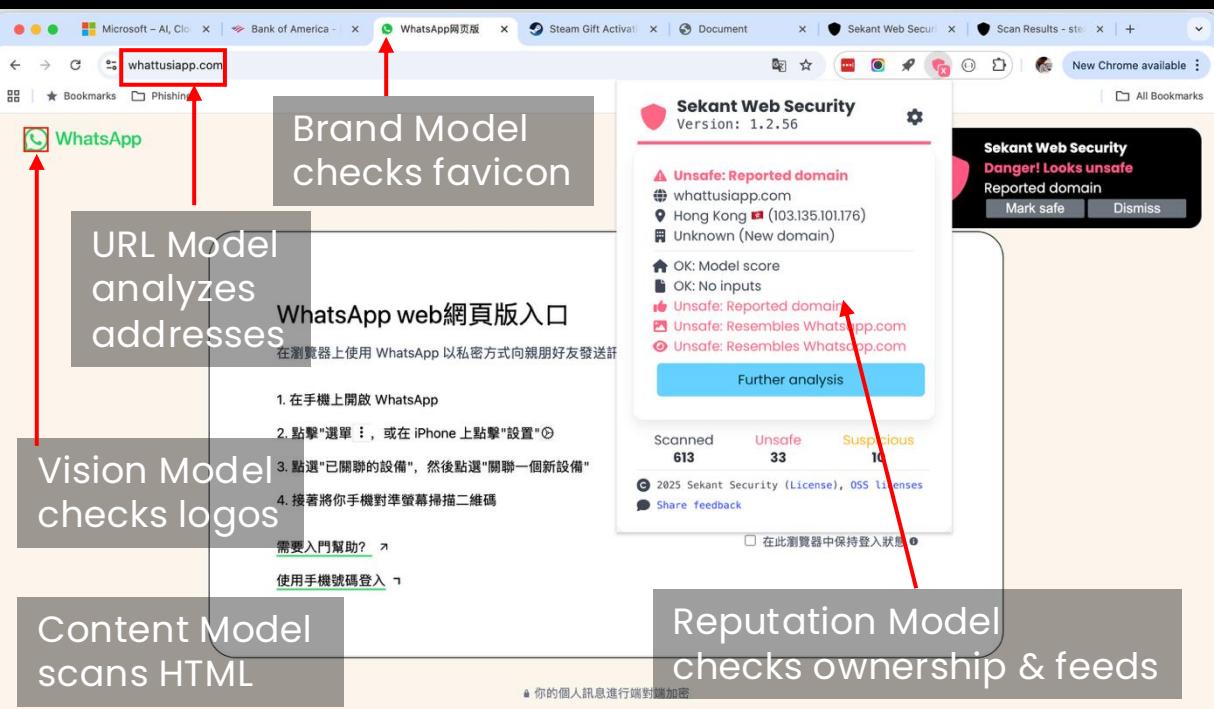


USE CASE: PHISHING PREVENTION

PROBLEM: Phishing remains the #1 entry point with 16% of data breaches attributable to it. The problem may get worse, as AI-generated phishing enables campaigns to be set up 192x faster and with 4.5x higher click-through rates.

SOLUTION: Sekant uses multiple ML & AI models to replicate analyses done by security engineers to detect zero-day phishing. All models run within the browser, so there is no server latency and complete privacy. The models self-adapt based on user browsing, to improve accuracy over time. In addition, Sekant's "Page Lock" feature can be used to block all interactions with unsafe webpages, to prevent users from accidentally entering credentials.

OUTCOME: >85% Zero-day Phishing Detection





USE CASE: CLICKFIX PREVENTION

PROBLEM: ClickFix attacks are deceptively simple: a website or document instructs the user to copy a command and paste it into PowerShell, Bash, or a terminal. What looks like a harmless "fix" expands into a malicious payload at execution time, bypassing existing defenses. This attack pattern has skyrocketed in 2025, with a 5X increase in attack volume.

SOLUTION: Sekant monitors the browser clipboard for scripts and analyzes them in real-time. It applies various de-obfuscation techniques, identifies threat patterns per MITRE ATT&CK tactics and generates a detailed verdict for malicious scripts. It can automatically clear the clipboard as well to prevent the script from being pasted.

OUTCOME: >95% ClickFix Detection Rate

drive.google.com
Verify you are human by completing the action below.

To better prove you are not a robot, please:
1. Press & hold the Windows Key + R.
2. In the verification window, press Ctrl + V.
3. Press Enter on your keyboard to finish.

Perform the steps above to finish v

Clipboard action triggers analysis and instant verdict

Script Analysis Report

Source URL: [REDACTED]
Script Type: powershell
Event Type: copy
Risk Level: MEDIUM

Summary

TOTAL TOKENS 10	THREATS DETECTED 3	URLS FOUND 2	RISK SCORE 28
--------------------	-----------------------	-----------------	------------------

Deobfuscation Analysis

Type	Count
[REDACTED]	[REDACTED]





USE CASE: SHADOW AI MONITORING

PROBLEM: Shadow AI usage has spiked by 68%, with 57% of employees now inputting sensitive corporate data into unapproved generative AI tools. Without visibility into these browser-based "copy-paste" events, enterprises face a silent, continuous leak of intellectual property and PII. Data pasted into these sites is always available to the employee, even outside enterprise network boundaries.

SOLUTION: Sekant utilizes behavior analysis to identify AI chatbot pages and monitors user prompts, data paste events and file uploads to such sites. Users are warned in real-time when they paste data or upload files, to avoid potential data loss. In addition, network requests to these sites are also logged to enable prompt extraction for forensic analysis if required.

OUTCOME: Complete visibility into Shadow AI usage

The image displays two side-by-side screenshots of a web browser window, specifically ChatGPT, illustrating Sekant's monitoring capabilities. Both screenshots show a black overlay from 'Sekant Web Security' with a yellow shield icon.

Top Screenshot: A 'Caution: Clipboard paste' message is shown. It states 'Content pasted on AI chat site' and includes 'Mark safe' and 'Dismiss' buttons.

Bottom Screenshot: A 'Caution: File uploaded' message is shown. It states 'File upload on AI chat site' and includes 'Mark safe' and 'Dismiss' buttons.

In the bottom screenshot, a file named 'basic.txt' is visible in a document preview area. The browser interface shows standard navigation buttons, a search bar with 'chatgpt.com', and a toolbar with various icons.





USE CASE: BLOCK UNSAFE DOWNLOADS

PROBLEM: With over 560,000 new malware variants detected daily, the browser is the primary conduit for "undetectable" payloads. However, "Unsafe" is more than just malware. Employees may download data or unauthorized binaries from unsanctioned sources. Admins have limited visibility or control over what is being downloaded by employees.

SOLUTION: Sekant utilizes an embedded YARA engine written in JavaScript to scan critical sections of the file in real-time—canceling unsafe downloads before they ever touch the operating system. Admins can customize the rules utilized based on company policy or threat research.

Admins can write custom rules like:

- Disallow executable downloads from new domains
- Disallow documents with macros
- Disallow files where content and extension do not match

OUTCOME: Visibility and Control over Downloads

