

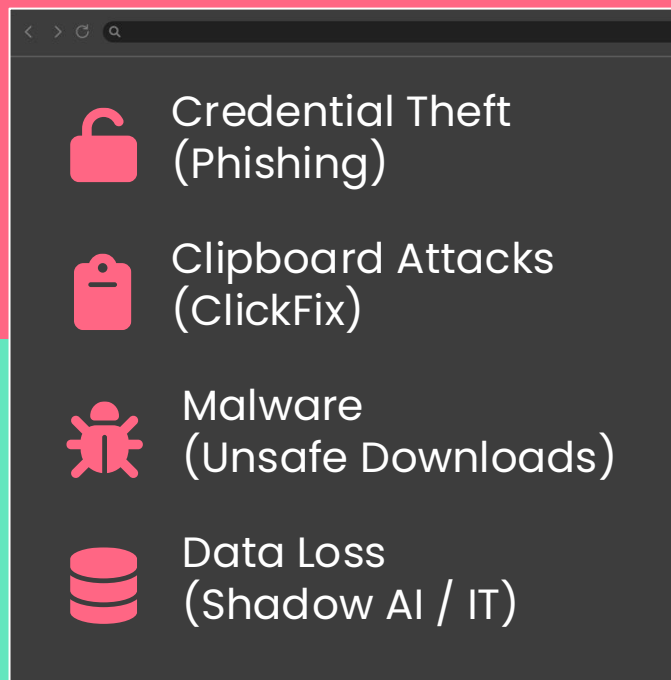
Sekant Security

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.

44% of cyber attacks
involve a browser





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

BENEFITS


 Zero-day
detection

 Scalable

 Foils evasion
techniques

 Real-time
response

 Complete
privacy

 Personalized
protection

OUTCOMES

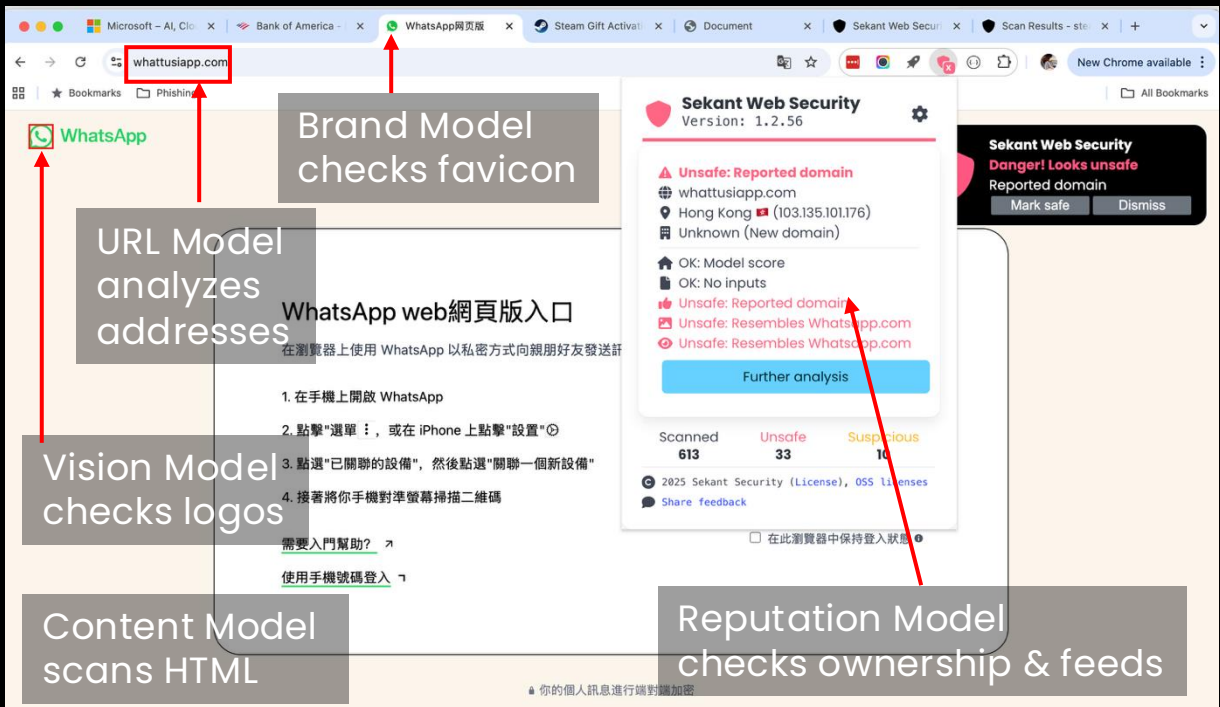
- >85% Zero-day Phishing Detection
- 97% ClickFix Detection
- Block Unsafe Downloads
- Monitor AI prompts, data pastes & uploads

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



The screenshot illustrates a browser window with multiple tabs. The active tab shows a phishing attempt on the WhatsApp website. The URL bar displays 'whattusiapp.com', which is highlighted by a red box and labeled 'URL Model analyzes addresses'. The page content includes the WhatsApp logo, which is labeled 'Vision Model checks logos', and a 'WhatsApp web網頁版入口' (WhatsApp web version entry) section. The page text is in Chinese and describes how to use WhatsApp on a web browser. A 'Brand Model checks favicon' label points to the WhatsApp logo. A 'Content Model scans HTML' label points to the page content. A 'Reputation Model checks ownership & feeds' label points to the 'Further analysis' button in the Sekant Web Security overlay. The overlay itself shows a 'Danger! Looks unsafe' warning, a 'Reported domain' of 'whattusiapp.com', and a 'Model score' of 'Unsafe: Reported domain'. It also displays a table with 'Scanned 613', 'Unsafe 33', and 'Suspicious 10'.

Microsoft - AI, Clo... x Bank of America... x WhatsApp網頁版 x Steam Gift Activ... x Document x Sekant Web Secu... x Scan Results - ste... x +

whattusiapp.com

Brand Model checks favicon

URL Model analyzes addresses

WhatsApp web網頁版入口

在瀏覽器上使用 WhatsApp 以私密方式向親朋好友發送詳

1. 在手機上開啟 WhatsApp

2. 點擊"選單"，或在 iPhone 上點擊"設置"⚙

3. 點選"已關聯的設備"，然後點選"關聯一個新設備"

4. 接著將你手機對準螢幕掃描二維碼

需要入門幫助? ➔

使用手機號碼登入 ➔

Sekant Web Security

Version: 1.2.56

⚠ Unsafe: Reported domain

whattusiapp.com

Hong Kong 🇭🇰 (103.135.101.176)

Unknown (New domain)

🏠 OK: Model score

📄 OK: No inputs

🔴 Unsafe: Reported domain

🔴 Unsafe: Resembles WhatsApp.com

🔴 Unsafe: Resembles WhatsApp.com

Further analysis

Scanned 613 Unsafe 33 Suspicious 10

© 2025 Sekant Security (License), OSS licenses

Share feedback

在此瀏覽器中保持登入狀態

Reputation Model checks ownership & feeds

Content Model scans HTML

Vision Model checks logos

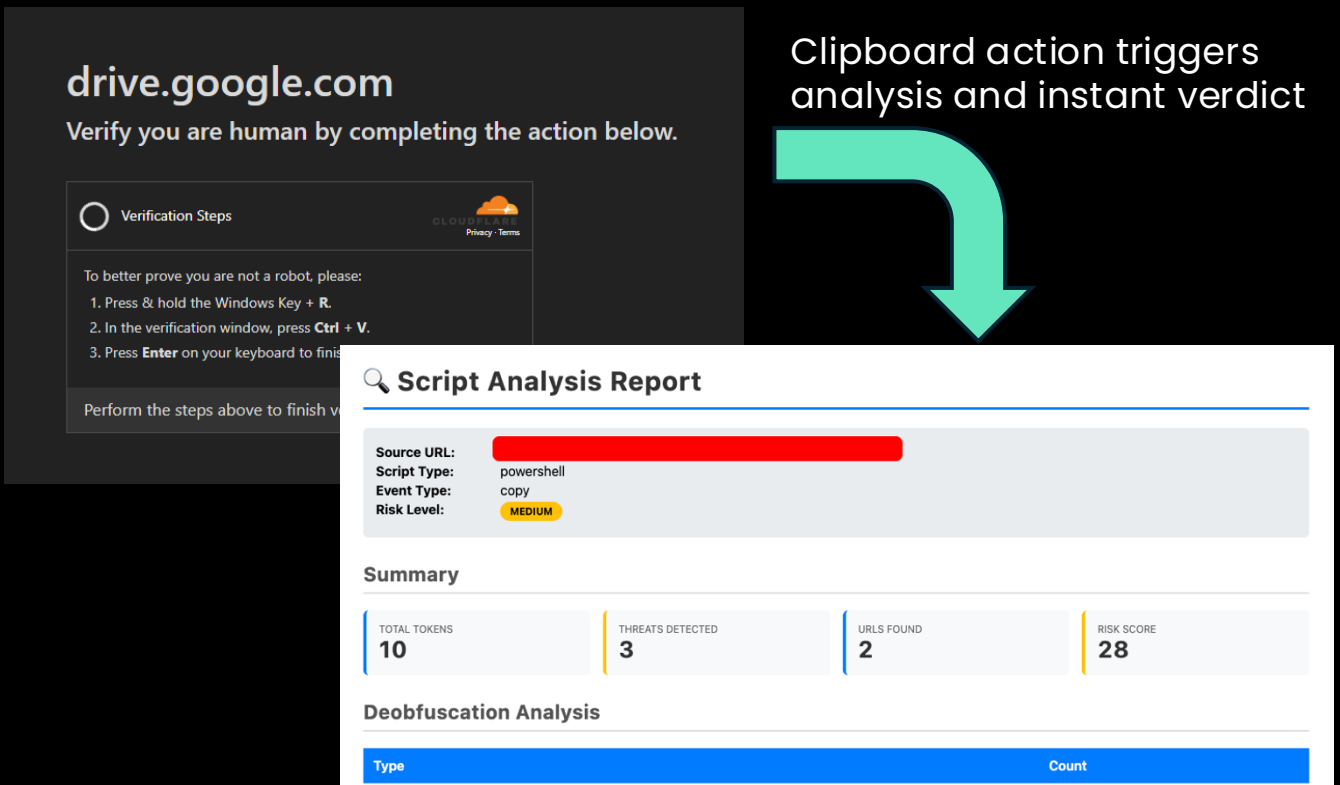


USE CASE: CLICKFIX PREVENTION

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



The image illustrates a ClickFix attack and its detection by Sekant Security. On the left, a screenshot of the **drive.google.com** verification page shows instructions for a user to copy a command. A large green arrow points from this page to the right, where a **Script Analysis Report** is displayed. The report details the analysis of a PowerShell script copied from the drive.google.com source, identifying it as a medium-risk threat.

Clipboard action triggers analysis and instant verdict

Script Analysis Report

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

Summary

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

Deobfuscation Analysis

Type	Count
[Table content continues]	

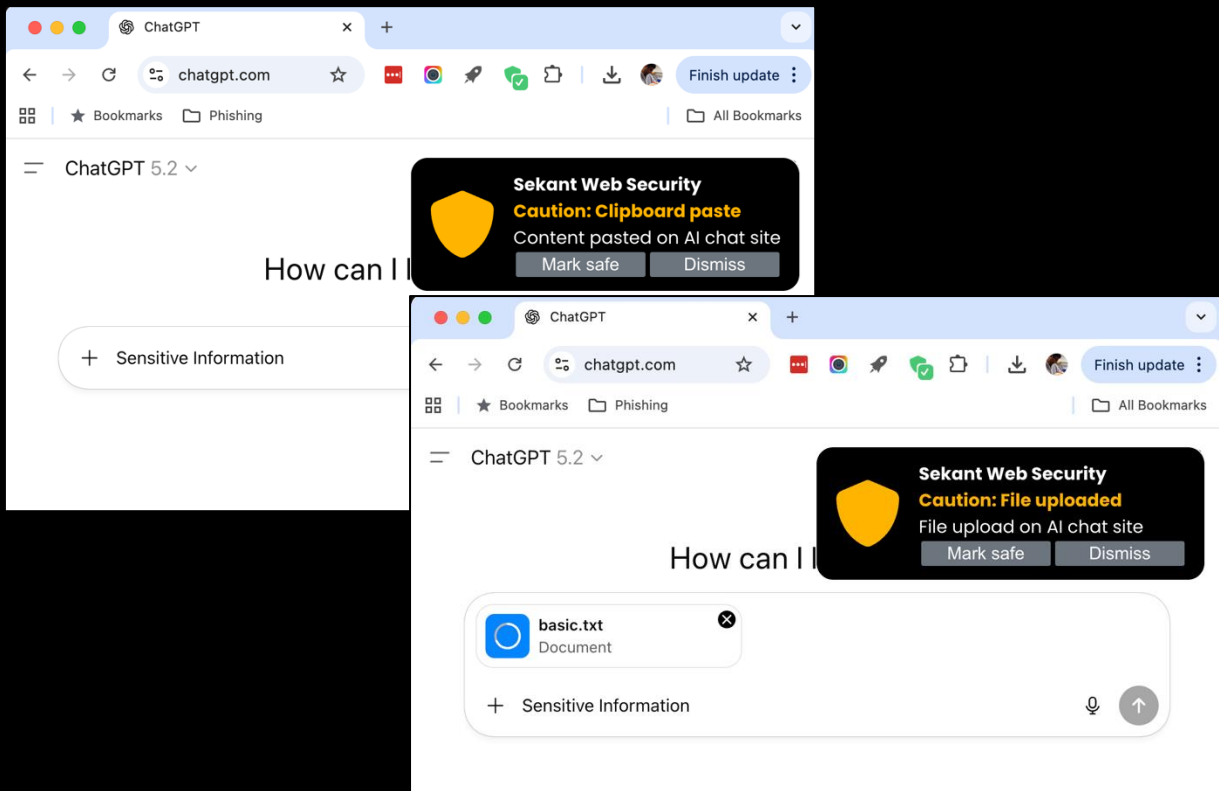


USE CASE: SHADOW AI MONITORING

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



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

