

Sentinel AI: Privacy is Security

How Blocking Private Data Collectors Prevents Individuals from Becoming Targets

A Privacy-First Security Solution for the Modern Internet

Executive Summary

The \$1.46 Billion Problem Everyone's Talking About—But No One Has Solved... Until Now.

Digital privacy is under siege. Cyber threats grow more sophisticated every day, and the most dangerous attacks aren't **randomly targeted**.

Each time a browser session begins, an average of **48 different companies** are silently observing. Major ad networks and analytics platforms embed fingerprinting scripts into millions of websites—often without consent. They capture search queries, shopping habits, medical concerns, and even personal anxieties.

These detailed digital profiles are then sold to anyone willing to pay—from retailers and financial institutions to cybercriminals. For internet scammers, this information becomes a **shopping list of vulnerable victims**.

- **\$1.46 billion** lost to tech support scams in 2023 alone
- **\$500–\$5,000** average loss per victim
- **\$10.3 billion** in total U.S. cybercrime losses last year

These attacks are not random. They are precision-targeted using harvested personal data. Traditional security tools such as consumer antivirus and VPNs fail to stop the root cause: **unchecked data collection**.

Sentinel AI patented technology prevents personal data from leaving the device! Thus breaking the data-collection pipeline at its source. Sentinel AI will disable data collectors' scripts and hidden surveillance tools before they can fuel the digital profiles that empower malicious advertisers and scammers.

Sentinel AI

The New Norm of Data Collection

Personal targeting is only effective when attackers can locate and profile a potential victim. Today, that task is simple, because data collection is nearly universal.

- **92% of websites** include at least one third-party tracker (*HTTP Archive*).
- The **median site loads ~27 third parties** (top 1M) and **~66 third parties** (top 1K).
- **Median of ~7 ad trackers per site** (*The Washington Post*).
- **Browser (or Device) Fingerprinting** among the Alexa top-100,000 websites, about **10%+** use canvas fingerprinting tracking. [AIMultiple](#)
- **4,000–10,000 ads per day:** a commonly cited but unverified claim (*The Ecologist*).
- **Malvertising rates:** ~0.21% of impressions involve security violations, with “dangerous or highly disruptive” attacks spiking to **1 in 9** impressions on bad days (*Confiant*).
- **Corroboration:** GeoEdge measured **1 in 75 impressions** as malvertising in Q1 2024 across the U.S. and U.K.

Everyone of these data points contributes to the creation of a digital profile—making individuals targets.

Privacy-First Security Innovative Approach

- No data collection → No valuable profiles to sell
- No profiles → No high-risk ads targeted
- No feedback loop → No Attackers cannot refine scams

Sentinel AI dismantles the surveillance economy at the source.

- **A Device System-Wide DNS (Patented) is provided which:**
 - Prevents ISP/DNS-level data collection
 - Blocks known ad-tech, broker, and telemetry domains
 - Pre-empts malicious destinations—without breaking site functionality
- **A Device System Browser Fingerprinting Shield which:**
 - Introduces controlled variability in canvas, WebGL, font, and audio signatures
 - Prevents cross-site identity stitching
 - Renders collected data less valuable to advertisers and scammers

The Privacy-First Security Approach Pays off

- Fewer high-risk ads reach the device
 - Less believable scams are displayed
 - Attackers lose the iterative feedback loop that improves their campaigns
-

Conclusion

The modern internet has become a battleground where personal data is the most valuable weapon. Every search, click, and digital interaction feeds a surveillance economy that not only drives invasive advertising but also equips cybercriminals

to launch highly effective and costly attacks. Traditional security tools focus on threats after they have already reached their target—Sentinel AI takes a different approach. By stopping data collection at its source, it eliminates the very fuel that powers malicious campaigns.

With patented DNS privacy technology and advanced fingerprinting protection, Sentinel AI ensures personal information never becomes ammunition for bad actors. In a digital world where privacy and security are inseparable, Sentinel AI delivers both—providing peace of mind and restoring control to individuals.

Sentinel AI is not just another layer of defense. It is the missing link that finally closes the data-collector-to-attack pipeline.
