Silo
By Authentic8

Silo™ Research Toolbox

Conduct Internet Research Securely and Anonymously

Traditional browsers and IT infrastructure lack the malware protections, secure research data management, and global anonymity framework needed for discreet threat research and online investigations. For internet research teams to work effectively, they require an on-demand, highly secure, and manageable environment to complete assignments safely — without revealing the sources or methods used during evidence collection efforts, or putting the platform at risk.

A Secure, Efficient Browser for Research

Silo Research Toolbox allows users to safely render content, store data, transform it into known-benign format, and even translate content without revealing their actions.

Silo Cloud Browser is the foundation of Toolbox; it is a one-time-use browser built on-demand in a secure cloud-based container. All web code is rendered in the cloud and converted into a high-fidelity remote display of the session, protecting endpoints from malware, ransomware, and drive-by downloads. All web activity is logged. Privileges to upload/download and to access restricted URLs are policy controlled.

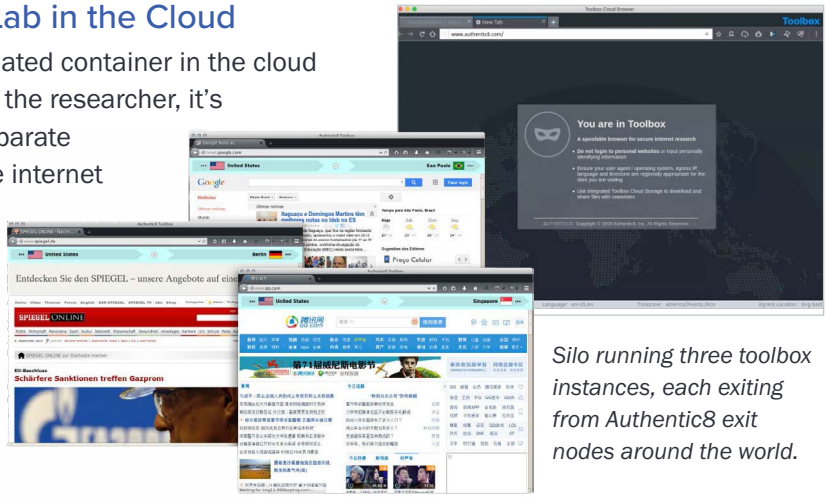
Silo Research Toolbox is a managed attribution and research suite layered over Silo. It allows researchers to spoof their true location in over 30 different countries worldwide, manipulate their hardware and software fingerprints, and to collect, annotate, and securely store internet-based Publicly Available Information (PAI). Toolbox also includes tools for post-fetch language translation, link tracking, as well as web code and traffic analysis capabilities.

Primary Benefits

- Conduct secure and anonymous research on the open, deep and dark web without complex, dedicated infrastructure
- Secure isolation, managed attribution, post-facto language translation, and auditing without the risk of identity or system compromise
- Geographically distributed data analysis and collections
- Ideal for OSINT, cyber-threat hunting, brand protection, hate speech, insider threat, geopolitical analysis, counterfeiting, intellectual property protection, etc.
- User agent and browser fingerprint spoofing
- No new infrastructure required

Your Personal Internet Research Lab in the Cloud

Launching a Toolbox session creates an isolated container in the cloud with a browser designed for researchers. To the researcher, it's just another window. But this completely separate environment can be configured to exit to the internet from one of Authentic8's global exit nodes and spoof different client environments. To the website being researched, Toolbox looks like a local device on a local network. Multiple Toolbox apps can be created and stored with various location profiles, so a single researcher can manage a variety of browser nodes.



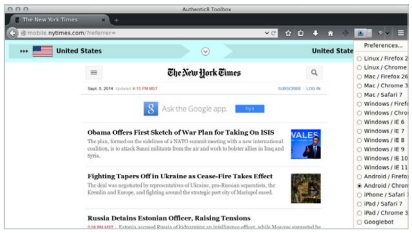
Silo running three toolbox instances, each exiting from Authentic8 exit nodes around the world.

Browser Isolation and Managed Attribution Built for Research Teams

Analysts have a single pane of glass to conduct research on the open, deep and dark web. Managers have oversight of collection, research, and investigative activity. Administrators have policy control over user privileges. Executives have the protection of non-repudiable audit logs of all online activity.

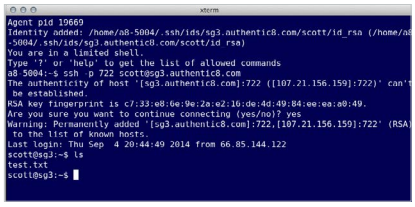
Content is fetched in its native language, but translated after the fact. Sites don't see the tell of English language requests. Regions or complete pages can be translated.

Each Toolbox instance can spoof different user agent strings. When combined with globally-deployed egress nodes, the client type and client IP can be fully obfuscated.



Researchers can use the virtual file system to download page data or binary files. Data can be stored in an integrated, secure file storage layer. Data can be uploaded to other research tools or web-based storage servers.

x-term profiles can be configured with host info and SSH keys allowing access from any device. Script-based harvesting activities can be managed securely.



Specifications

Supported platforms	Windows (XP–10), macOS, Linux, iOS
System requirements	15MB storage, ~100MB RAM
Client interfaces	SSL Port 442 Proprietary remote display
Egress node locations	World-wide from the Americas, Asia, EMEA
Java support	Java JRE v6–v8 isolated in sandbox
Analysis tools	Code analysis, TCP capture, more
Plugin support	Firefox store; any plugin not requiring restart
x-term support	Configurable with SSH key bindings
Logging	Encrypted user and admin logs
Log access	Within admin console (non-encrypted), or via API

ABOUT | Authentic8 is redefining how enterprises conduct business on the web with the Silo web isolation platform. Silo insulates and isolates all web data and code execution from user endpoints, providing powerful, proactive security while giving users full, interactive access to the web. Silo also embeds security, identity, and data policies directly into browser sessions, giving IT complete control over how the web is used. Commercial enterprises and public sector organizations use Silo solutions to provide secure web access, to control web data, apps, and workflows, and to conduct sensitive online research. Try Silo now at www.authentic8.com.