Researchers Need a Browser that Doesn't Expose Them

Any collection of publicly available information starts with the browser. Research teams need an on-demand, low impact and completely insulated browser for accessing the Internet without revealing their location or identity. Access to the open, deep, and dark web from one interface over normal IT infrastructure increases speed and performance while reducing IT support workload for organizations of every size.

A SECURE EFFICIENT BROWSER FOR RESEARCH

Silo Research Toolbox allows users to safely render content, store data, transform it into known-benign format, 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.

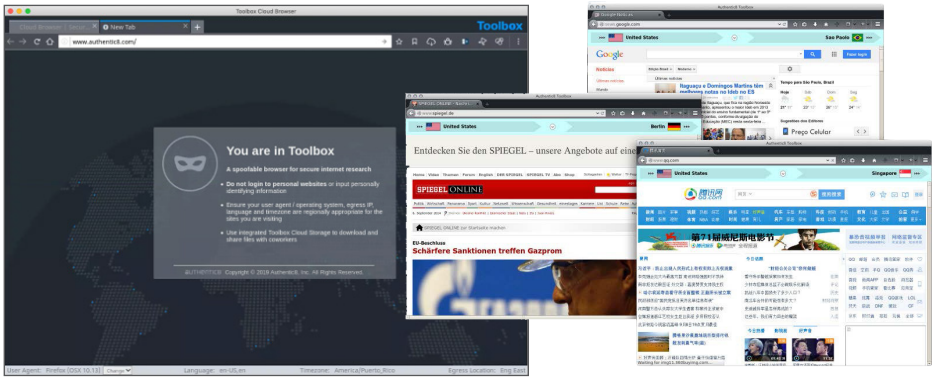
Silo Research Toolbox is a managed attribution and research suite layered over Silo. It allows users to spoof IPs to over 30 locales worldwide, manipulate their hardware & software fingerprints, and to collect, annotate, and store internet-based PAI. It includes tools for post-fetch language translation, web-code and traffic analysis, and linkage tracking.

PRIMARY BENEFITS

- Conduct secure, misattributed, and anonymous research on the open, deep and dark web
- Operational security, managed attribution, and speed for high-risk web research
- Geographically distributed data analysis and collections
- Includes all the tools necessary to review and capture open source data without revealing identity or exposing resources
- User agent and browser fingerprint spoofing
- Post-facto language translation
- No new infrastructure required

SILO RESEARCH TOOLBOX IS A VIRTUAL BROWSER IN THE CLOUD

Clicking a Toolbox app brings up an isolated container 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.

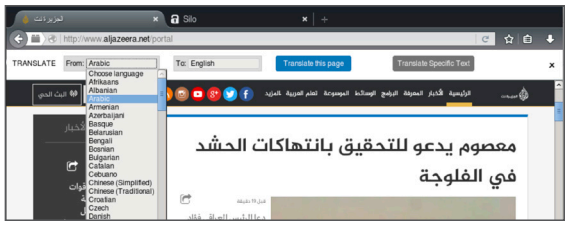


Silo running three Toolbox instances, each exiting from Authentic8 egress nodes around the world.

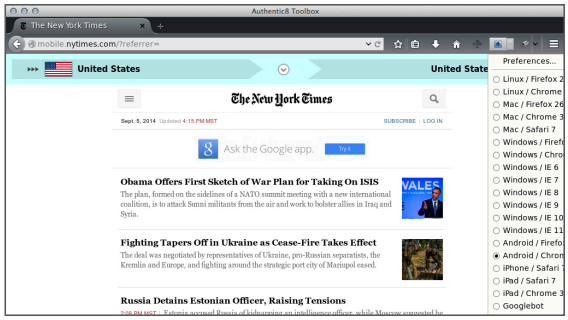
BROWSER ISOLATION AND MANAGED ATTRIBUTION BUILT FOR RESEARCH TEAMS

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.

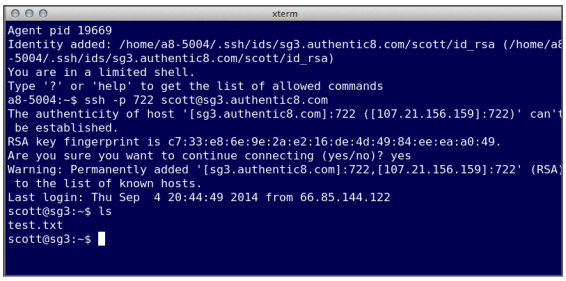


Each toolbox instance can spoof different user agent stings. When combined with a local egress node, client type and client IP are misattributed.



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
XTERM SUPPORT	Configurable with SSH Key bindings
LOGGING	Encrypted user and admin logs
LOG ACCESS	Within admin console (non-encrypted), or via API

To learn more, visit www.authentic8.com