Silo BY AUTHENTIC8

SOLUTION BRIEF

Hidden costs of DIY research networks

The economics behind Silo for Research

Investigators, researchers and analysts require unique web access and tools to safely search the web. Some organizations erect homegrown “dirty” research networks that include on-premise “cold” computers running virtual machines (VMs) and a segregated internet connection. Or they subscribe to a cloud desktop-as-a-service offering and augment it with a number of VPN connections, dedicated storage and other solutions. In either scenario, organizations are finding that the DIY approach comes with a hefty price tag, entails complicated and costly management, and doesn’t fully address the needs of users or IT.

Soft costs can be expensive

Building, maintaining and managing a DIY dirty network for sensitive research costs not only IT or security tools team, but also the analysts that use it on a daily basis.

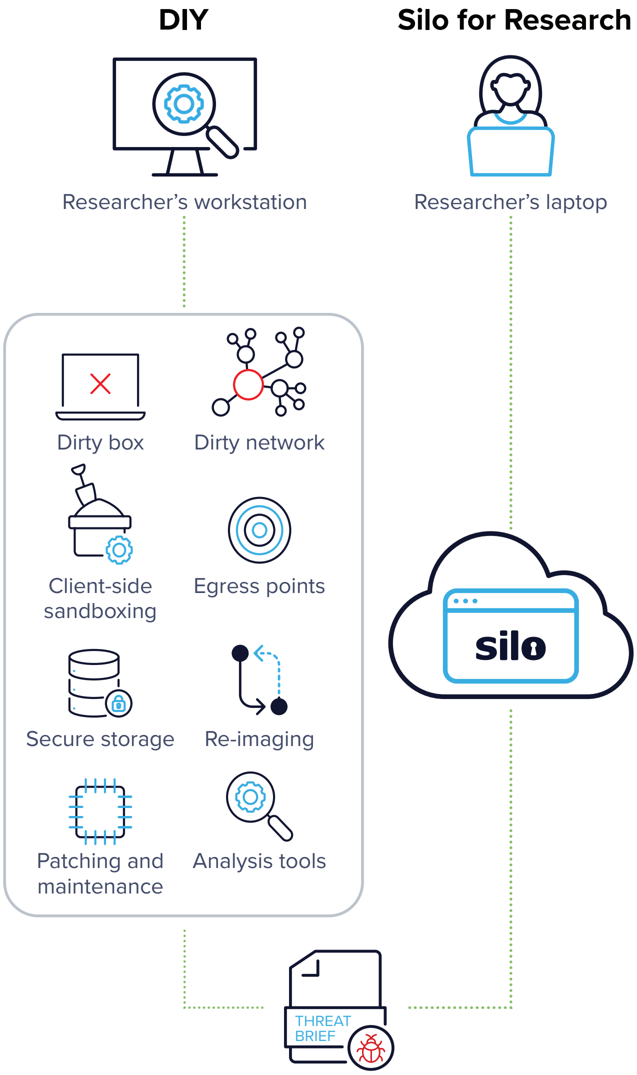
Organization’s highlight the following soft cost challenges:

Workflow inefficiencies

Disrupting the analysts’ standard workflow to log into an isolated environment or to physically relocate to use dedicated cold machines costs time. Efficiency is also lost in the time it takes to safely transfer any data, files or assets collected back to the analysts’ core work environment.

Productivity loss

Analysts conducting sensitive research often come across sites, forums and marketplaces rightfully blocked by IT. There is productivity loss for IT and the analyst through the process to request, review and enable exceptions to unblock these critical areas of the web. If requests are rejected, the only option may be for the analyst to access the cold computer/ DIY network, contributing to workflow inefficiencies as mentioned above. If no such solution exists, the analyst is at a dead end.



Disjointed tooling

Analysts require collection and analysis tools. Deploying a multi-vendor stack requires IT integration and analyst training for each tool. Browser extensions are another method of tooling, but require time to review to ensure they are secure to use and appropriate from a tradecraft perspective.

Risk

DIY dirty networks by definition are segregated environments. Visibility into analyst activity through detailed logging and the ability to enforce enterprise policy are typically non-existent. This is a risky proposition in terms of compliance and audit needs because of the types of research performed — on the surface, deep and potentially dark web.

Further, dirty networks depend on VPNs. VPN connections are notoriously unstable and do not prevent malware from reaching a machine. Sensitive business data stored on the local network can become exposed when the VPN connection drops unbeknownst to the analyst in the course of their research.

All together, these hidden soft costs of time and labor can have a major impact on the bottom line when multiplied across a team of analysts. See the chart on page X where we tally up the numbers for a DIY research network scenario on a per license basis.

WHAT'S TYPICALLY NOT ADDRESSED IN A DIY APPROACH?

- Manipulation of the analyst's digital fingerprint appearance
- In-region internet access to blend in with crowd and view sites, forums and marketplaces that may be blocked in certain regions or otherwise altered to certain visitors
- Common, integrated suite of collection and analysis tools, including automated functions
- Integrated access to the dark web
- Policy enforcement at the user-group level (e.g., dark web access, copy/paste, download/upload)
- Detailed user and admin logging for compliance and audit purposes

Hard costs of a DIY alternative to Silo for Research

Silo for Research provides full protection through:

- 100-percent cloud browser isolation
- Complete anonymity globally and the ability to manipulate an analyst's digital fingerprint
- Integrated suite of collection and analysis tools
- Centralized management with policy control and auditability

While building a robust platform such as described above internally is generally not feasible for individual organizations, let's examine the per user annual costs of an off-premise solution. The chart below assumes the deployment and management of an off-premise browser with a minimal ability to control analysts' identity and attribution.

DIY hard costs

FUNCTIONALITY	CLOSEST ALTERNATIVE TO SILO FOR RESEARCH	ANNUALIZED (PER LICENSE)
Off-premise browser for non-attribution and malware isolation in a sandbox environment	Desktop-as-a-service (DaaS)	$576
Dedicated storage that persists through sandbox rebuilds	Cloud storage (10GB)	$120
Bandwidth costs from parallel infrastructure to internet	Outbound traffic on platform-as-a-service (PaaS) (100GB/mo)	$108
Ability to access the internet in-region from 20+ user-selectable locations	20 VPN connections	$1,440
One additional concurrent session for analyst to multi-task	Additional DaaS	$576
24x7 support	15% on infrastructure	$423
	Total annual hard cost (per license)	**$3,243**

DIY soft costs

FUNCTIONALITY	CLOSEST ALTERNATIVE TO SILO FOR RESEARCH	ANNUALIZED (PER LICENSE)
IT maintenance to rebuild environments monthly to wipe malicious code	2 hrs/mo per 5 systems (IT labor @ $150k/year)	$360
Workflow inefficiencies: Analyst workflow disruption and inefficiency accessing the web through a segregated environment and transferring information	1 hr/mo per analyst (labor @ $150k/year)	$900
Productivity loss: Analyst and IT productivity lost to blocked site exception requests	1 hr/mo (30 mins each) (labor @ $150k/year)	$900
Disjointed tooling: Analyst and IT reviewing, deploying, integrating, training related to collection and analysis tooling	1 hr/mo (30 mins each) (labor @ $150k/year)	$900
	Total annual soft cost (per license)	**$3,060**

TOTAL ANNUAL HARD/SOFT COST OF DIY PROGRAM (PER LICENSE) $6,303

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity.

+1 877-659-6535
www.authentic8.com