silo
BY AUTHENTIC8

DATA SHEET

Secure Browsing

In today's "perimeter-less" and web-first world, the browser is the essential application across the workforce. The modern work environment has employees executing every manner of work within the browser all day, everyday. Employees also need (or expect) to access websites on corporate devices for personal reasons, though it significantly increases an organization's attack surface and overall exposure.

Despite significant investments in traditional web security solutions, relying on standard browsers leaves administrators blind and the organization exposed as users access cloud apps or visit untrusted websites for work or personal browsing.

Eliminate your primary attack surface: the web

Secure Browsing provides IT with centralized visibility and fine-tuned control of untrusted web access and users' data transfer actions.

Secure Browsing can be used to secure employee personal web browsing from company devices within their existing browser by triggering isolation via API from your existing security stack. Or it can be provided as a distinct, zero-risk browser with a familiar user experience based on Chromium for all enterprise browsing.

Neither option requires software installation.

Option 1:
Redirect employee's personal web browsing

Securely allow access to potentially risky sites

- Integrate Silo isolation API into existing security stack
- Set policy for personal browsing websites (e.g., social media, entertainment, financial services categories) to redirect into isolation
- Set desired DLP policies for personal browsing activity (e.g., up/download, copy/paste, print)
- User's URL request is redirected into isolation within existing browser
- Data transfer actions are restricted as designed

Option 2:
Provide users with distinct, isolated browser

Fully isolate all web-based activity (i.e., app access, browsing, link opens)

- Deploy Silo as the organizations go-to browser, replacing the existing browser
- Set DLP policies for data transfer actions that can be taken in the enterprise browser
- All web activity occurs in the fully isolated, controlled browser
- Data transfer actions (e.g., up/download, copy/paste, print) are restricted as designed

Features and benefits

Secure Browsing is a cloud-based environment that eliminates your attack surface when browsing or clicking links.

Full isolation from all browsing and email link threats

- Achieve zero-risk web browsing by keeping all web code off your network — shift your browsing to one-time-use, isolated cloud browsing containers
- Allow access to untrusted or unknown URLs to enable user productivity without network and data risk

Fine-tuned access and data transfer policy

- Prevent sensitive data leak and theft using Silo's rich data transfer controls
- Manage access in real time from Silo's centralized console that integrates with your existing IT stack

Isolation and control where, when and how you want

- Isolate and control web access — including risky links, full access for personal browsing or all browsing — based on your risk posture
- Regain visibility into user web and data activities through detailed logging

silo
BY AUTHENTIC8

Silo by Authentic8 separates the things you care about like apps, data and devices from the things you can't trust like external websites, users and unmanaged devices. With a cloud-native platform, full isolation and complete policy and audit control, Silo enables full use of the web without risk of exploit, data leak or resource misuse.

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