SOLUTION BRIEF

LEGAL


## Law firms in the Digital Age

Law firms face a delicate balance—securing their assets and complying with client audit requirements while ensuring employees stay connected and engaged so they can do their job. IT teams need to manage risk to the firm without disrupting employee satisfaction or productivity. Restrictive policies can reduce the firm's risk profile, but at a cost to the business. Firms must find a way to embrace the web without exposing the firm.

# It's time to Rethink the Browser

Instead of spending endlessly to manage around this inherently insecure and unmanageable tool, innovative firms use the Silo cloud browser to regain the security and control of their environment.


### SECURE ACCESS TO THE WEB

Silo gives employees web access without exposing your firm to surveillance or exploit. Users get a full fidelity browser for personal and work-related content, while all execution, IP attribution, and GRC occurs on a remote server.


- Access personal mail and social resources without jeopardizing firm
- Browse anonymously (no cookies, surveillance, or tracking)
- Ensure compliance with firm requirements for GRC

**ABOUT SILO** Silo, from Authentic8, is a cloud browser engineered to provide the security and control that is missing from all consumer browsers. 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 the browser, giving IT complete control over how the web is used. And with Silo available from anywhere and any device, policies follow users regardless of environment.

### PREVENT WEB DATA LOSS

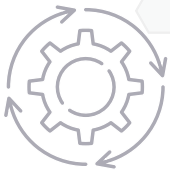
Silo lets you control the flow of firm data across web apps, including SaaS applications. Silo embeds device, access and data transfer policies in the browser, delivering web DLP controls regardless of device or network.

- Enforce policies governing up/download, copy/paste, print and more
- Restrict access to shadow IT sites
- Gain comprehensive audit logs on data transactions

### ENSURE WEB COMPLIANCE

Silo lets you comply with regional Data Privacy restrictions regarding employee use of the web. Policies can be defined at the global or group level, ensuring regional compliance. And all data is encrypted with customer-supplied keys

- Establish chain of control with centralized, encrypted audit logs
- Abide by prevailing requirements thru regional settings by group
- Support SAR requests and opt-out requirements



### CONTROL SENSITIVE DATA & WORKFLOWS

Silo provides a secure, policy-controlled work-space for sensitive web-based work-flows, enabling seamless collaboration within designated teams while preventing unauthorized access by others. It's ideal for business apps, case work, M&A projects, and more.

- Set and enforce security and data policies directly in the browser
- Centralize credential management for real-time control of Saas apps

### CONDUCT SECURE WEB RESEARCH

Silo provides teams an on-demand, low impact, and completely insulated browser for Internet research without revealing location or identity. Access websites from local IP addresses, spoof browsing platforms, and collect data while eliminating exploit risk.

- Collect, collaborate, and manage case materials in the cloud
- Prevent attribution to your employee or firm

## SIMPLER, STRONGER SECURITY ARCHITECTURE

Silo lets you simplify your current cybersecurity stack. With no exposure to the public internet, Silo reduces or eliminates reliance on endpoint, network, and gateway technologies

- Eliminate break-inspect infrastructure
- Reduce reliance on secure web gateway infrastructure
- Simplify endpoint detection solutions