Silo
By Authentic8

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 with an eye on employee satisfaction and productivity. Restrictive policies can reduce the firm's risk profile, but at a cost to the business. How to leverage the web without exposing the firm?

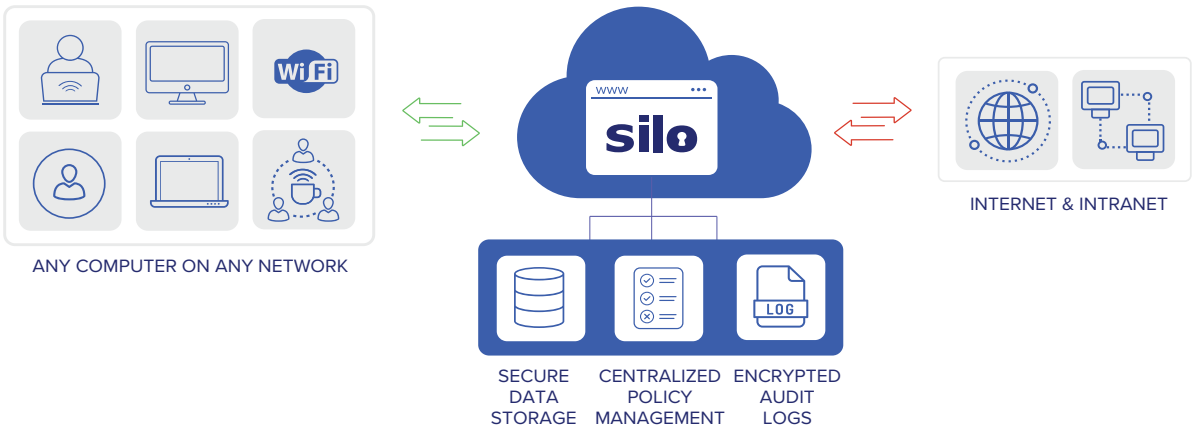
It's Time to Rethink the Browser

Instead of spending endlessly to manage around inherently insecure and unmanageable traditional browsers, innovative firms use Silo Cloud Browser to regain the security and control of their environment.

Secure Access to the Web

Silo gives employees web access without exposing the 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



Simpler, Stronger Security Architecture

Simplify your current cybersecurity stack with Silo. 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

©2019 AUTHENTIC8. ALL RIGHTS RESERVED. 2019.07.30

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 makes it easy to 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 through regional settings by group
- Support SAR requests and opt-out requirements

Control Sensitive Data & Workflows

Silo provides a secure, policy-controlled workspace for sensitive web-based workflows, 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 with 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

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.

©2019 AUTHENTIC8. ALL RIGHTS RESERVED. 2019.07.30