SILO BY AUTHENTIC8

SOLUTION BRIEF

Silo for Safe Access

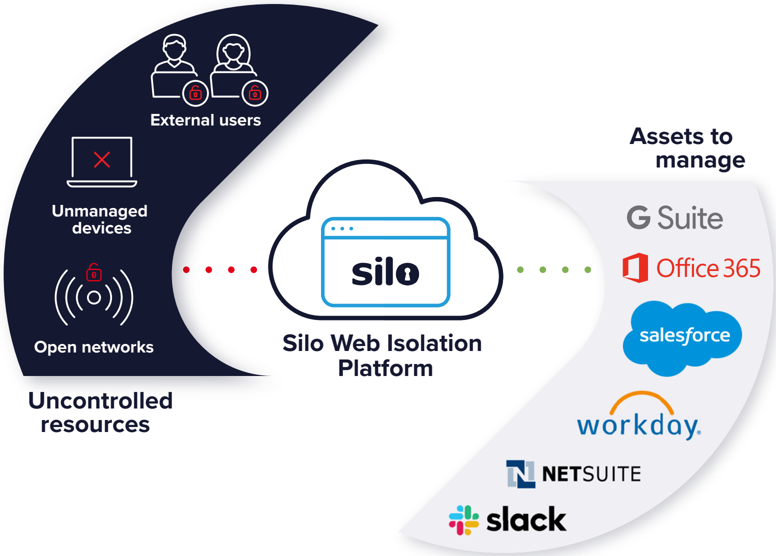
Giving law firms the web without risk

Law firms face a delicate balance: securing their assets and complying with client audit requirements while at the same time ensuring employees are connected so they can do their job. IT needs to manage risk without disrupting employee productivity. They must find a way to embrace the web without exposing the firm.

Separate the things you care about from the things you can’t trust

Silo for Safe Access is an isolated workspace that allows IT to manage use of the web regardless of the access details or the role of the user. It provides a single, secure point of leverage to control all web scenarios, regardless of computer, network or application. Silo combines access, authentication, isolation, policy and audit into a centralized browsing platform to enable Zero Trust access integrity.

Law firms are utilizing Silo for Safe Access for critical web-driven interactions such as conducting highly confidential web research and providing third parties and mobile users locked-down access to SaaS applications.



Legal research

Silo provides your legal teams with an insulated browser and cloud storage for sensitive internet research that doesn’t reveal location or identity. Your users can access websites and collect data anonymously while eliminating risk through 100-percent isolation from web-borne threats.

Partners and associates work on confidential legal matters, M&A transactions and complex litigation. The internet is a critical information resource, but using a traditional local browser leaves them open to malware exposure and even worse: being tracked and identified. Full isolation and identity obfuscation are paramount.

- Isolate users from web-borne threats and malicious files by ensuring no web data executes on their device using Silo’s remote browser
- Prevent attribution to your employee or the firm by leveraging Silo’s infrastructure where the digital fingerprint presented is not their local computer
- Collect, collaborate, manage and secure case materials in the cloud

Secure application access

The working world is more distributed than ever, encompassing partners, suppliers, contractors and remote workers. And they need access to your crown jewels — sensitive applications and data — from unmanaged and/or personal devices connected across untrusted Wi-Fi, residential broadband and third-party networks.

Silo for Safe Access lets you define specific access and user permissions, even when the devices are outside of your control. All policies are enforced in the browser, regardless of the device or the network. For example you can control the flow of firm data across web apps, including SaaS applications by embedding device, access and data transfer policies in the browser, delivering web DLP controls.

- Create secure workspaces locked down to a single app or a collection of apps that are specific to the user's role
- Completely isolate critical apps from device, browser and network vulnerabilities thanks to cloud-based rendering
- Protect sensitive data with data transfer policies (e.g., copy/paste, up/download and print restrictions)
- Encrypt connections end to end without a VPN
- Fully log user activity on any device or location, encrypted with your key

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