silo

SILO:
SOLUTION BRIEF FOR INVESTMENT MANAGEMENT FIRMS

Access to the web is a practical reality for financial firms. Business applications, research sources, and productivity tools all live in the browser. And many firms have liberal policies allowing users to access personal social media, webmail, storage solutions, and more.

Your users are online. That could be a problem.

But you're a regulated industry and you need to ensure that your users stay compliant while online. For the most part, you may be covered. You've spent time and resources deploying a variety of technology solutions to manage the parts you control. But once your users access the web with a browser, they step outside your control; you no longer have the protections and oversight that you need to stay compliant.

This has led firms to reassess their policies on employee access to web services which are perceived as "risky." The typical approach is to blacklist services like social media, webmail, and cloud storage, along with categories of websites maintained by a third-party.

But this can create user dissatisfaction and hurt productivity if restrictions hinder the ability to do genuine research. Moreover, the line between a "safe" and "risky" website is not always clear. You may be able to block facebook.com, but you won't block financialtimes.com. An errant comment on either site could spur a response from the SEC.

Silo is a browser built for this problem.

Silo shifts the browser from the endpoint to execute in the cloud, where policies are embedded directly in the browser profile, maintaining compliance regardless of device, network, or location.

Moving the browser to the cloud gives IT admins control.

Take back control while keeping users productive.

Silo lets Admins of regulated firms have their cake and eat it too: users get access to the web for work and personal use, and admins maintain complete control and oversight. Central audit, oversight and governance mean Admins are always ready to respond to SEC discovery requests.

ADMINS GET

- A secure browser delivered as a managed service

- Complete audit logs and oversight of all user behavior

- Centralized user policies for access, passwords, and data transfer

USERS GET

- A disposable browser that is secure and leaves no data residue

- Access to social media, webmail, and cloud storage without putting the firm at risk

- "Follow me" profiles with embedded permissions for a consistent, secure experience across all devices and location

Firms deploy Silo in a variety of ways.

Some firms whitelist a few critical websites and use Silo for everything else. Other firms redirect a handful of URLs to Silo for secure rendering. Silo is flexible enough to fit into your organization, regardless of how you use it.

Silo can be launched as a stand-alone browser, setting the tone for work versus personal browsing, or integrated with your IT infrastructure automatically redirecting users to the appropriate environment.

Silo can integrate with your existing infrastructure, including secure web gateways, firewalls, SIEMs, Microsoft Active Directory, SAML-based IDP providers, and more. Silo logs are encrypted with a public key you manage, protecting your activity even from Authentic8.

	TYPE URL	CLICK URL	FORWARD URL
Silo Browser	✓	✓	✓
In-browser display	✓	✓	✓

TO LEARN MORE VISIT:

www.authentic8.com