Silo
By Authentic8

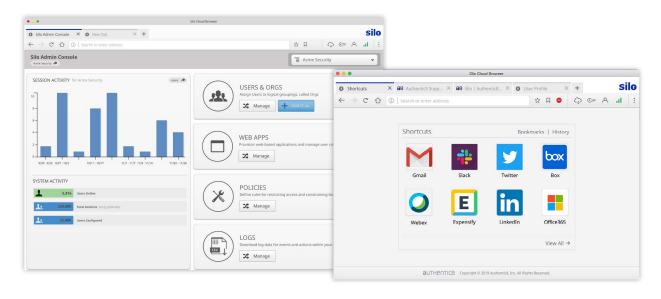## Remote Workers: Security and Control in a Zero Trust World

The digital work environment has never been more dynamic. Users access corporate resources from remote locations, often on personal devices and untrusted networks, and they access cloud applications that are outside of corporate IT policy. From on-site consultants and traveling executives to field sales representatives and work-from-home employees, IT needs to assert positive control over their compute environment. Current solutions are ad hoc, partially effective, and often circumvented by users.

The Silo Cloud Browser provides 100% isolation from web code while enforcing IT policies regardless of computer or location.

ANY COMPUTER ON ANY NETWORK

SECURE DATA STORAGE   CENTRALIZED POLICY MANAGEMENT   ENCRYPTED AUDIT LOGS

INTERNET & INTRANET

Silo for Remote Workers

Rather than struggling with a cocktail of network, device, and application controls, the Silo Cloud Browser becomes the primary application for secure remote access. It integrates VPN, IDP and SSO, CASB and DLP policies, and break-inspect infrastructure all into a single, intuitive browser.

silo
By Authentic8

Enforce IT Control, Compliance, and Security

- Centralized policy definitions
- Managed and secure, anytime, anywhere access for users
- All user data actions logged and encrypted
- Policy engine aids compliance with PCI, HIPAA, and GDPR/CA data laws

Prevent Web-borne Malware and Cyber Attacks

- 100% isolation from web code
- No risk from unmanaged devices
- All web-native content converted into benign display content — even when rendering documents

Prevent Malicious or Accidental Data Loss

- Copy/paste, up/download, print controls
- User entitlements vary based on device trustworthiness
- Eliminate the hardware and human cost of implementing break-inspect policies

Enable Seamless and Secure Access to Web Applications and Workspace

- Single pane of glass to grant or revoke access to web apps and cloud data
- Integrated credential management by user or group
- Centralized policy enforcement regardless of user environment

Maintain Anonymity and Confidentiality on the Web

- All IP and platform fingerprint data resolves to Authentic8 cloud infrastructure
- Cookies, trackers, web beacons, analytics tools, and other web surveillance techniques are neutralized
- Authorized IT maintains oversight of user activity, including TLS sites

Deploy a Simpler, Stronger, and Less Expensive Security Architecture

- No separate VPN infrastructure and no split tunneling required
- No zero-day web exposure means simpler A-V covers the endpoint
- Integrated break-inspect and logging of user actions reduces network and human burden

silo
By Authentic8

Critical Capabilities

	VPN	VDI	CASB	SWG	Silo for Remote Access
Forced encryption for all network connections	●	◔	○	○	●
100% isolation of all web code in the cloud	○	○	○	○	●
100% isolation of unmanaged devices	○	○	○	○	●
IT definition of access, security, web DLP policies in a single application	○	◐	◐	◐	●
IT policies remain intact regardless of user device or network	○	●	○	◐	●
Global, group, or user-level policy definitions	○	◐	○	◐	●
Centralized device access controls, including 2FA	○	◐	○	○	●
Centralized web DLP policies governing copy/paste, upload/download	○	◐	◐	○	●
Centralized URL category policies	○	○	◐	●	●
Centralized provisioning/revocation of SaaS applications and credentials	○	○	○	◐	●
Integrated break-inspect of TLS content	○	○	●	●	●
Encrypted log data with customer-managed keys	○	○	◐	◐	●
100% cloud-based SaaS deployment	○	◐	○	●	●
Consolidates multiple IT solutions into a single application	○	○	○	◐	●
Relative cost	$	$$$	$$	$$	$

Customer Scenarios

Silo is in use across public and private, regulated and non-regulated organizations worldwide. Silo's patented configuration capability ensures the browser meets the specific needs of the user or workflow.

Financial Services

Financial firms use Silo to comply with internal and regulatory policies without impacting employee productivity, whether they are conducting fraud research, collaborating on a deal, or accessing a personal site.

- Inherit firm's compliance policies regardless of device or network used when accessing deal rooms and sources.
- Maintain oversight of user actions in customer-encrypted logs for compliance reviews and post-issue remediation.
- Protect identity, location, and intent during M&A projects and market research.

Sales Organizations

Road warriors use Silo to securely juggle work for multiple clients and prospects as they try to stay current on internal business tasks.

- Protect client data and sensitive information even on compromised devices or networks.
- Collaborate with internal and customer teams using the latest corporate resources while maximizing oversight and compliance.
- Enable secure access to personal applications while maintaining security and control over corporate apps and data.

Consulting Firms

Consulting professionals use Silo to access employer and client resources while maintaining data segregation, internal and client policies regardless of location.

- Provision and deprovision projects and users quickly using central policies to manage access to client and employer resources.
- Protect client data and sensitive information even on compromised devices or networks.
- Collaborate with internal and client teams while maximizing oversight and compliance.

Law Firms

Law firms use Silo to improve workforce productivity, organizational performance, and client satisfaction while addressing clients' data security requirements.

- Protect client information and firm reputation with secure access and centrally managed policies.
- Increase attorney productivity with access to apps and sensitive data regardless of where, when, and how people want to work.
- Enable secure access to personal applications while maintaining security and control over corporate apps and data.

4