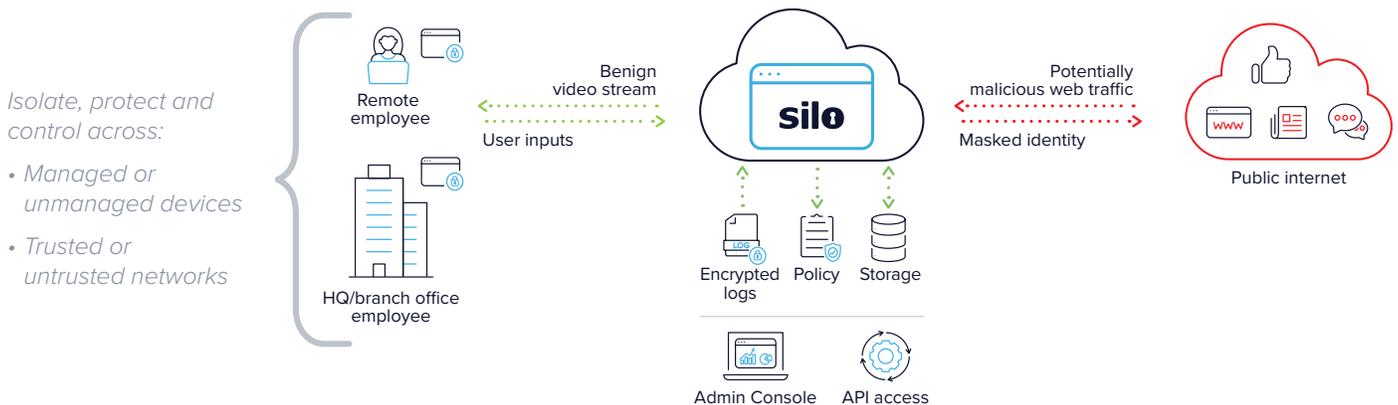# Secure web access

The web is a core component to all job functions as well as employees' personal lives while at work. But every page view and email link exposes an organization's infrastructure and critical data to threats and abuse. Despite large investments in traditional web gateways, malicious code from phishing and ransomware attacks continues to enter corporate networks and individual user actions continue to go unchecked.

The web without risk or compromise

Secure web access with Silo enables browsing and email link access through an isolated, cloud-delivered web browsing environment. It provides IT with centralized visibility and fine-tuned control of untrusted web access and users' data transfer actions. Organizations can insert "always on" or conditional protection through a purpose-built remote browser or seamlessly within user workflows.

Isolate, protect and control across:
- *Managed or unmanaged devices*
- *Trusted or untrusted networks*

Remote employee

HQ/branch office employee

Benign video stream
User inputs

silo

Encrypted logs   Policy   Storage

Admin Console   API access

Potentially malicious web traffic
Masked identity

Public internet

Use case 1

Integrate Silo with your secure web gateway, firewall or SSE solution

- Redirect specific web requests to Silo (e.g., uncategorized/untrusted site categories, all social media traffic)
- Provide policy-controlled access (e.g., enforce up/download and copy/paste)
- Launch Silo API seamlessly "in tab" within the user's native browser

Use case 2

Use Silo as a separate or replacement browsing environment

- Route all web traffic through the Silo secure enterprise browser
- Or isolate risky use (e.g., separating personal from work browsing)
- Fine-tune policy controls and establish audit oversight

Features and benefits

Silo is a cloud-delivered isolation and control environment designed to prevent browsing, email links and user actions from compromising corporate data. Securely enable access to untrusted web resources by enforcing access and data transfer policies to eliminate risk.

Full isolation from all browsing and email link threats

- Don't let any web code enter your environment — render it remotely in one-time-use, cloud-based browsing containers

- Allow access to untrusted or unknown URLs to enable user productivity without network and data risk

Fine-tuned access and data transfer policy controls

- Safeguard sensitive information against leakage and theft with rich policy control

- Manage access in real time from a centralized console that integrates with your existing IT stack

Isolation and control where, when and how you want

- Insert isolation and control of web access — from risky links only, to personal browsing, to all browsing — based on your risk posture

- Deliver isolated web access transparently to users in a familiar browsing environment by integrating with existing redirection technologies or through a purpose-built, enterprise browser

- Regain visibility into user web and data activities through detailed logging

Commercial enterprises and government agencies from around the globe trust Silo by Authentic8 with their most valuable data. Authentic8 undergoes regular third-party audits and assessments in line with its certifications:

Our certifications

 Authorized Moderate Impact Level — FedRAMP

 SOC 2 Type 2: Trust Services Criteria — AICPA SOC aicpa.org/soc4so

 PCI — Level 2 Service Provider

 HIPAA COMPLIANT

 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