silo
BY AUTHENTIC8

DATA SHEET

Silo Web Isolation Platform

Insert isolation and control where, when and how you want

In today's "perimeter-less" and web-first world, the browser has become the essential application across the workforce, even though it is also the CISO's most significant liability. Relying on standard browsers and traditional perimeter security tools leaves administrators blind. It also leaves the organization exposed as users access cloud apps or visit untrusted websites for work or personal browsing.

The Silo Web Isoation Platform is a zero-trust cloud browsing environment that shields web applications and critical data when accessed by untrusted users, devices and networks as well as offers risk-free browsing by preventing any web code from touching devices and networks.

Silo separates the things you care about from the things you cannot trust

- Isolate your apps, data and devices from malicious exploits wherever they reside
- Enforce control and oversight to prevent improper web use and avoid critical data loss
- Wire security into everyday workflows as activity shifts across devices, networks and locations

Form-factor flexibility
Transparent within existing browser OR separate distinct browser

Cloud-native delivery
Cloud-speed and scale; no client software required

Isolation integrity
Zero-exception web code isolation

Dynamic & context based
Launch explicitly, or dynamically triggered based on access or risk context

Holistic control
Follow-the-user access and data transfer policies with robust auditability

You gain speed, simplicity and cloud-native scalability with the Silo Web Isolation Platform — all without downloading software and with the ability to choose the right form factor for the job. Control unmanaged, arms-length access scenarios with the following products:

Zero-Trust Application Access: Isolated and policy-controlled access to critical applications and data

Risky Web Link Isolation: Integrate with SSE platforms to address untrusted or unknown URLs

Risky Email Link Isolation: Integrate with email gateways and cloud email security platforms to isolate email links

Secure Web Access: Air-gapped protection from browsing threats and employees' personal web use

Deployment flexibility

Silo's browsing environment runs natively from the cloud as a fully containerized architecture. Customers receive zero-exception, bi-directional web code isolation. Silo can be delivered to a user through two form factors, allowing for multiple use cases and support for diverse customer needs. Regardless of form factor, there is no software or agent that needs to be installed on the user's device.

Form factor 1: Delivering isolated, policy-enforced content

Some customers want the flexibility to weave isolated browsing into their users' current workflows based on their assessment of risk or value. By redirecting certain apps or websites into isolated tabs within the local browser, users get a seamless and transparent experience without any change in behavior.

The Silo Isolation API acts as the method by which content is redirected and policies are applied, including the ability to lock down application access through Silo and specify data transfer controls based on risk context. With this approach, it's simple to integrate context-specific isolation into web workflows and expand the value of solutions such as IdP, CASB, SSE and SWG.

API-driven and context-specific isolation is a preferred delivery method for both enterprises and OEM partners across a range of use cases.

Form factor 2: Delivering an isolated, policy-enforced browser

Some customers want to provision Silo as a distinct, isolated browser for defined use cases: either the secure workspace for business apps and the personal browser for non-business use; or the enterprise browser for all web activities. In all of these cases, the Silo browser can be configured with apps, credentials, data access and transfer policies, as well as auditing to ensure secure and compliant use —regardless of user, device or location.

Users can access the Silo cloud-based browsing environment from any local browser, creating an air gap between the web and devices and networks, eliminating an organization's primary attack surface. The Chromium-based experience is familiar to users, including maintaining browser persistence of user history, favorites and credentials.

The Silo Web Isolation Platform is built, monitored and maintained to access and safeguard the most sensitive organization data. Certifications include:

FedRAMP Authorized Moderate Impact Level

AICPA SOC SOC 2 Type 2: Trust Services Criteria

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