silo BY AUTHENTIC8

DATA SHEET

Zero-Trust Application Access

Securing access to business apps against today's reality of roaming users, untrusted networks and personal devices is an IT nightmare — especially so when those users are third parties like contractors and suppliers.

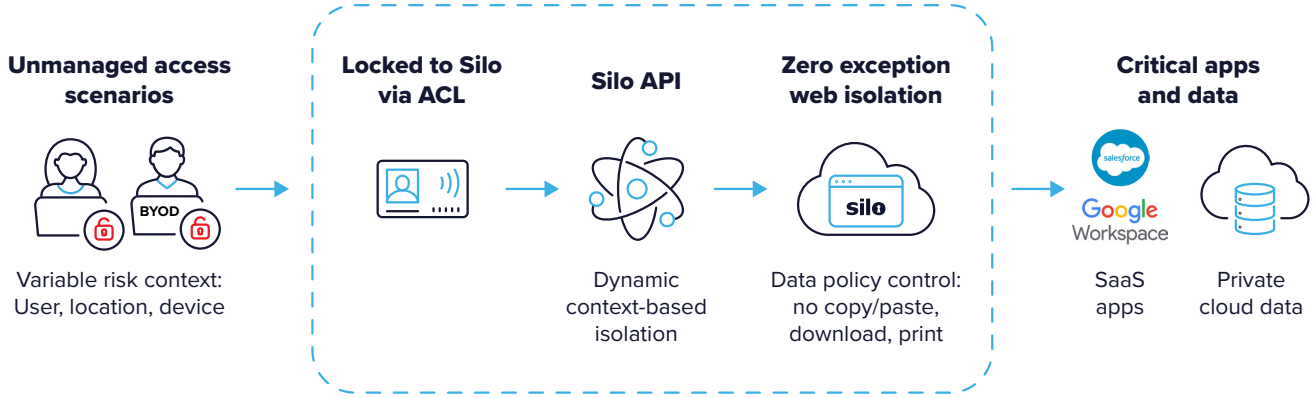
Traditional perimeter security tools, including VDI and VPNs, are blunt instruments. They lack the context-aware security, data transfer control and visibility needed for a workforce whose activity constantly shifts across devices, networks and applications.

Isolate and control access to critical applications and data

With Zero-Trust Application Access, organizations can seamlessly weave isolated content delivery into unmanaged device workflows based on an assessment of risk or value. IT can control these arms-length application access scenarios without any software installed on the user device or change in user behavior.

Zero-Trust Application Access leverages an isolation API in the Silo Web Isolation Platform. The API enables content to be redirected and policies applied, including policies to lock down application access through Silo and specify data transfer controls based on context. The isolated sessions take place transparently within a tab of the user's local browser.

Integrate context-specific isolation into web workflows and expand the value of existing solutions such as IdP, CASB, SSE and SWG.



Lock down access to your critical web applications without fear of "last-mile" vulnerablitiy

Purpose-configure to precisely control and audit how your data is used

Deliver zero-trust access with speed, simplicity (no client software) and cloud-native scalability

Features and benefits

Zero-Trust Application Access protects critical corporate data by inserting a cloud isolation and control layer between applications and users that locks down interactions based on user, device and network risk posture. By implementing conditional isolation and data protection, you eliminate risk while establishing governance.

EXAMPLE LOCATION	LOCATION TRUSTED?	DEVICE MANAGED?	DEVICE COMPLIANT?	ACCESS POLICY	DATA RIGHTS
Employee on corporate network with managed device	✓	✓	✓	Direct access	Full
Employee at home on managed device that got infected	✗	✓	✗	Isolated access	No downloads or copy/paste to and from local device
Supplier accessing supply-chain portal	✗	✗	?	Isolated access	Full
Contractor accessing SaaS applications	✗	✗	?	Isolated access	No downloads or copy/paste to local device

Airtight app isolation from compromised devices and networks

- Create an airgap between users and corporate data to lock down app access in a cloud-based browsing environment
- Eliminate risk from compromised devices and networks by ensuring they have no direct interaction with critical applications and data

Visibility and context-aware policy control extended to unmanaged devices

- Safeguard sensitive information against leakage and theft with rich policy control, including for app access and data exchange
- Enforce policy on any user across any device, network or web application, even as a user's access scenario changes

Isolation and control where, when and how you want

- Have the flexibility to insert isolation for individual apps based on access scenarios or risk context
- Deliver isolated applications to users seamlessly in a tab within their existing local browser — no software downloads required

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

PCI Level 2 Service Provider

AICPA SOC SOC 2 Type 2: Trust Services Criteria

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