silo
BY AUTHENTIC8

DATA SHEET

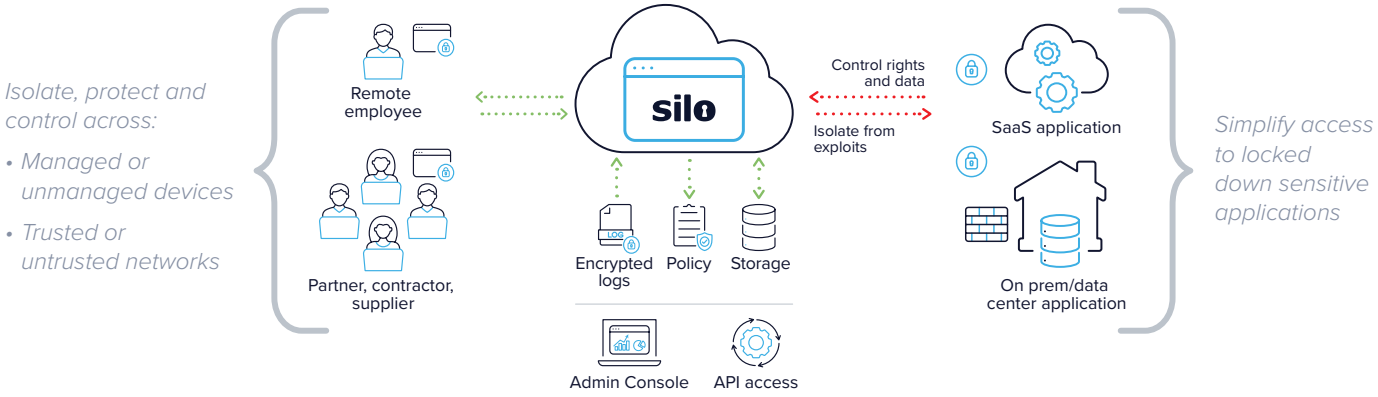
Zero-trust application access

Enabling access to critical web applications for remote workers, third parties and BYOD-enabled users — as well as standard employees — is one of the biggest challenges facing organizations today. Traditional perimeter security tools, including VPNs and VDI, are blunt instruments unable to keep up with a remote-first and web-app filled world. They lack the context-aware security, control and visibility needed for a workforce whose activity constantly shifts across devices, networks and applications.

Isolate and control access to critical application data

How can IT protect the organization from what it does not control? By securely granting access to your most valuable applications through a locked-down, fully isolated cloud environment: this is Silo.

Silo is an elegantly simple cloud solution that centralizes visibility and powers fine-tune control of critical application access and data transfer by any user on any device. Silo combines application access, authentication, browser isolation, data transfer protection, policy and audit into a centralized platform to enable zero-trust access integrity.



Third-party and BYOD use case

Context-aware secure application access and data control

- Seamlessly insert isolation and control into individual app workflows
- Enable external access to both public SaaS and private applications

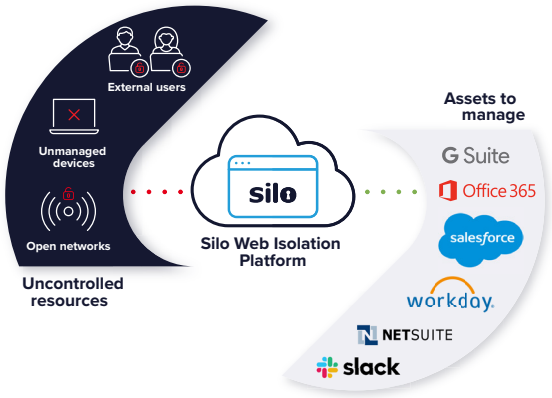
Managed workspace use case

“Always on” secure application workspaces in a single location

- Create a workspace that is segregated from the device and the rest of the web
- Provide a one-stop shop for accessing apps without having to integrate into existing security systems

Features and benefits

Silo 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 always-on or conditional isolation and data protection, you eliminate risk while establishing governance.



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
- Regain visibility into user activities on any public or private web application through detailed logging
- Easily deliver isolated applications to users seamlessly within their local browser or through Silo's purpose-built secure enterprise browser

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