DATA SHEET

Secure Application Access

with Silo for Safe Access

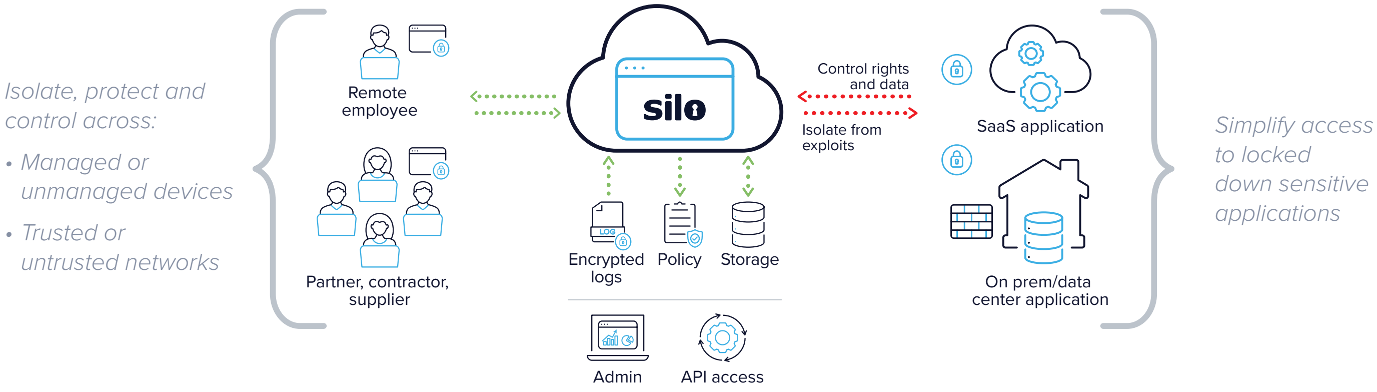
The working world is more distributed than ever, encompassing partners, suppliers, contractors and remote workers. And they need access to your crown jewels: sensitive applications and data. Providing managed corporate laptops for these users isn't practical; so in order to obtain access, they have to use unmanaged and/or personal devices connected across untrusted Wi-Fi, residential broadband and third-party networks.

For IT and the business overall, the security risks couldn't be more significant. And applying traditional security controls (e.g., EDR/MDR, VPN, DLP, CASB) couldn't be more challenging and complex — for IT as well as the users.

Control what you don't own to protect what you do

By turning the browser into a "managed client," regardless of device or network, IT can control what they don't own. This capability enables the business while protecting it from potentially compromised devices coming across unsecured public networks to sensitive SaaS or web applications.

Silo for Safe Access combines application access, authentication, browser isolation, data loss prevention, policy and audit into a centralized browsing platform to enable Zero Trust access integrity.



Isolate, protect and control across:
• Managed or unmanaged devices
• Trusted or untrusted networks
Remote employee
Partner, contractor, supplier
silo
Encrypted logs
Policy
Storage
Admin
API access
Control rights and data
Isolate from exploits
SaaS application
On prem/data center application
Simplify access to locked down sensitive applications

Silo for Safe Access lets you define specific access and user permissions, even when the devices are outside of your control. All policies are enforced in the browser, regardless of the device or the network.

Use Case 1

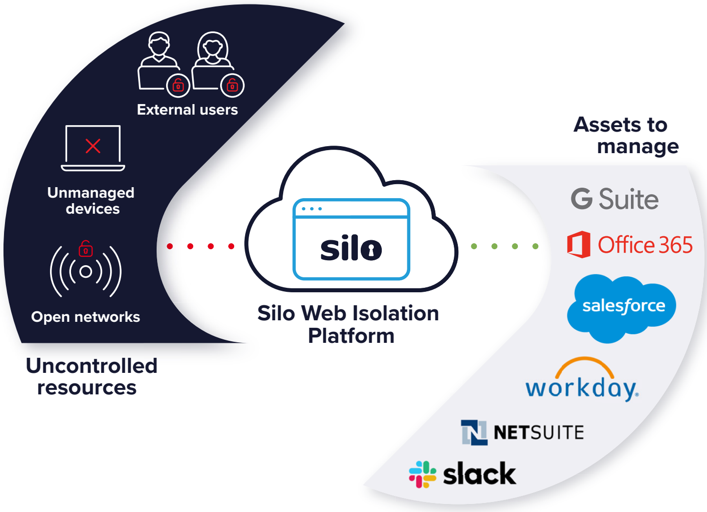
- Secure, auditable access by third parties like contractors, suppliers or partners
- Isolate untrusted endpoints from direct interaction with applications
- Eliminate data exfiltration risks
- Enable or revoke centrally and in real time

Use Case 2

- Secure workspaces for employees to access applications applicable to their role
- Manage diverse permission requirements
- Define and enforce data policies
- Monitor for compliance and abuse

Features and benefits

Silo for Safe Access ensures that an application is entirely air-gapped from local device and browser vulnerabilities; is governed by policies to prevent data leak and misuse; and is wrapped with logging analytics to oversee and audit user actions against the data.



Protection through isolation

- Completely isolate critical apps from device, browser and network vulnerabilities thanks to cloud-based rendering
- Create secure workspaces to lock down a single app or a collection of apps specific to a user's role
- Encrypt data protocols and connections end to end

Management through browser enforcement

- Control sensitive data usage with data transfer policies (e.g., copy/paste and up/download restrictions)
- Provide access without disclosing credentials to individual users
- Fully log user activity on any device or location, encrypted with your key

Simplification through cloud delivery

- Access from any device, any network, any location without the need to install software on endpoints
- Avoid any requirement upfront investment or integration
- Elastically scale from hundreds to thousands of users

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