silo
By Authentic8

GUIDE
REMOTE WORKERS

Rapidly Enabling Remote Workers in Time of Crisis:

A GUIDE FOR CIOs AND CISOs

Introduction

In times of crisis, organizations need to respond quickly. Emergencies like the COVID-19 demand that companies and government agencies switch to remote work literally overnight to ensure operational continuity. But such transition is often challenging and has many limitations:

- When disaster strikes, or authorities issue shelter-in-place orders, there's no time to implement elaborate contingency plans – decisions to transition to remote work need to be made immediately.
- Traditional solutions that require procurement of new equipment and configuration of licenses for each remote worker are time consuming. They often can't be rolled out in time, especially at scale.
- Security teams have the responsibility to protect sensitive data while remote employees work on personal devices and connect using untrusted networks.
- Existing IT solutions that were designed to accommodate on-premise employees are not able to support a sudden surge in the number of teleworkers.

Remote Work Options for Your Workforce

Options for enabling remote workers vary in complexity, time investment, security, and long-term sustainability:

- **Employer-provided equipment with VPN** is a popular choice, but it can be hindered by procurement and supply chain challenges in time of crisis, bandwidth at internet access points, and limited capacity of the existing network infrastructure. While VPN does meet standard security needs, it lacks the ability to control information access at a more granular level, doesn't support detailed endpoint audits, and can be costly to manage and maintain. Devices and organization data remain at risk due to direct connection to untrusted networks.

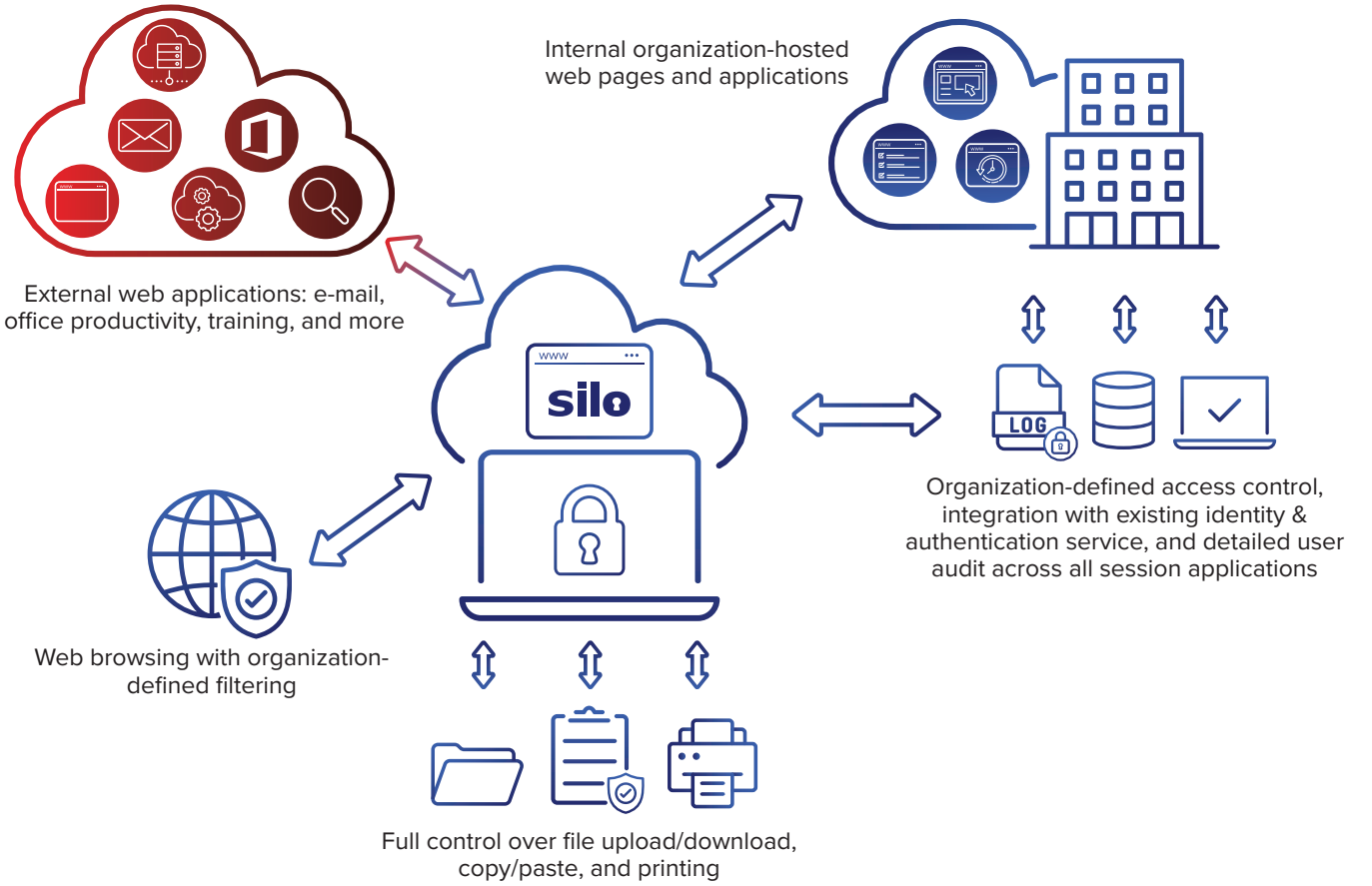
  If you select this option, be alert to unexpected saturation of internet access points or VPN concentrators from web browsing and application access. Be aware that split-tunnel VPNs can exacerbate audit and access control shortcomings, and also lead to theft or unauthorized disclosure of organization data.
- **Employee-owned devices** can help users get up and running quickly, but personal laptops and tablets are much easier to compromise, giving hackers a gateway into the organization's data and applications. And with no ability to monitor unmanaged devices, organizations often remain unaware of a breach until it's too late.

  You can partially mitigate this risk by installing specialized endpoint security solutions on every unmanaged device, such as mobile device management, web-based VPN client, or cloud access security broker (CASB) applications. However, this patchwork of tools still won't guarantee protection against breaches. The additional complexity of licensing, deployment, and managing of all these layers of security often outweighs the benefits, especially in the time when solutions need to be rolled out quickly.
- **Telephone conferences and phone trees** are time-proven collaboration tools. Despite obvious scalability and feature limitations, conferences and phone trees can remain part of a complete solution. In fact, some agencies choose to forward government phones to personal lines at phone.

- **A web isolation solution**, such as Silo Web Isolation Platform, is a modern way to enable your remote workforce while protecting sensitive data. Silo can be accessed via a traditional browser with no additional installation, or it can be installed as an application on a variety of devices – both work-issued and personal –running Windows, Linux and Mac OS, as well as Apple iPads.

  Silo is a web-based solution, so remote workers can be up, running and productive within hours, enjoying full access to web-based applications such as O365, email and web browsing. Employees have access to the productivity apps they need and organizations can maintain security regulations and ensure compliance with company policies.

  Silo isolates the entire remote work session and its sensitive data from the end user device and browser, and also provides protection from untrusted local networks. It offers rapid deployment with an assured zero trust architecture. With Silo, IT can enforce restrictions on copy/paste, printing, and file upload/download, while providing comprehensive user auditing across all web applications.



The Silo Web Isolation Platform provides secure access to web browsing, external web applications, and internal resources, integrated with existing identity services and audit systems

Silo Web Isolation vs. Other Options

	Silo	VPN on Employer-Issued Equipment	Employee-Owned Devices	Cloud Access Security Broker
Rapidly scale	●		●	●
Prevent employer data commingling with personal data or web browsing	●	●		◖
No data resident on device after session end	●			◖
Allow BYOD	●		●	●
Supports 2FA	●	●	●	●
Detailed auditing and logging across web browsing and web-based applications	●	●		◖
Integration with enterprise access control & identity management	●	●		●
Copy/paste protection	●			
File upload/download protection	●			
Printing protection	●			
User-friendly application shortcuts	●			●
Familiar interface requiring no additional user training	●		●	●

BE SURE TO CONSIDER

Security risks of accessing employer-owned data on employee-owned devices, or data transfer outside of IT control

Risks of connecting employer-owned devices to untrusted networks at remote workers' homes, coffee shops, or other locations, outside of your monitoring boundary.

Mixing employer-provided hardware or peripherals (e.g., card readers) for use on personal devices can introduce additional risks and attack vectors

Triage: Enable remote work in hours

During a crisis requiring immediate enablement of remote workers, consider a triage approach – assessing the degrees of urgency of issues to decide which solutions to focus on first. Here are some questions to consider:

- What web-based services are available immediately or can be rapidly deployed for my organization to enable essential communication? Some examples:
  - Outlook Web Access
  - Office 365
  - G Suite
  - Google Apps
  - Collaboration services
  - Web browsing
  - Web-based training
  - Other SAAS
- What existing security services are available to define user roles, groups, and responsibilities? Integrating with existing services can reduce deployment times while providing required access and enforcing consistent security policies.
- What organization-hosted content do remote workers need? Once essential services are available, further integration will provide access to intranet web pages, time reporting solutions, and other on-premises or organization-hosted content.

Staged Approach: From Quick Success to Long-term Sustainment

Quick Wins Within Hours: Remote Web Browsing and Existing Web Applications

Many organizations have full or partial adoption of SaaS web applications, such as web-based email, training, or office productivity. These applications, combined with web browsing, can provide immediate results by delivering essential communication capability through the Silo browser, which isolates employer data from the untrusted user device and enforces restrictions on printing, copy/paste, and file transfer. As a bonus, Silo provides full unified audit for both web browsing and web application access.

Silo can be successfully deployed to organizations in just a few hours, so employees can get productive immediately. Your IT team can get up and running with Silo using Authentic8's self-service guide. When needed, Silo Support and Deployment teams are also here to help.

Integration With Existing Enterprise Services

Once the organization has deployed essential communication and collaboration capabilities to support the crisis, consider leveraging existing security services to maintain pre-existing access control groups, authentication, and identity services. Silo integration with existing enterprise security services will provide additional security value and increased efficiency, saving your security team's valuable time and resources.

Larger organizations typically deploy a variety of authentication, centralization, and control services, many of which can be integrated with Silo for user management, SSO authentication, and log extraction.

Organizations can also define specific access control, web filtering, and other security policies based on user roles. Defining roles and responsibilities and identifying all integration points is the first step for integrating Silo with existing enterprise services. A full enterprise-scale integration depends on the number of integration points that must be configured. In most cases, it can be accomplished in just a couple of days by your internal IT resources.

FULL DETAILS

Full details can be found on the Authentic8 Support Portal:

https://support.authentic8.com/support/solutions/articles/16000046334-deploying-authentic8-silo-for-the-enterprise

Access to Organization-Hosted Applications and Deployment to All Endpoints

Building on initial success, organizations may elect to further deploy and integrate Silo beyond the remote worker use case, and/or allow access to on-premises applications.

Allow Access to Internal Web Applications

Most organizations have internal web-based applications. Since Silo runs on Authentic8 infrastructure outside the organization's network, it cannot directly access internal applications unless specifically configured. There are two methods for enabling internal access:

- **Use an existing SSL VPN portal:** If your organization has one available, this is often the quickest access method since it's likely already configured. Loading the SSL VPN URL into Silo works immediately.

- **Proxy requests for organization-hosted content:** If there isn't a VPN portal available, Authentic8 does have proxy capabilities and is able to proxy requests for specific sites through a known set of IP space. Your network teams will have to make internal resources available to that proxy IP space in order to access through Silo.

Please contact Authentic8 support staff (support@authentic8.com) for further details on accessing internal resources via Authentic8's proxy layer.

Deploying Silo Enterprise-wide, Not Only for Remote Workers

For a large enterprise, this will require orchestration across multiple teams involving project managers, cross-functional IT teams, and dedicated resources from Authentic8's Account Managers and Deployment Teams. These projects are highly dependent on executive sponsorship, budgets, and internal resources available to an organization. From a high-level perspective, here are the teams and considerations likely to be involved.

Pre-Rollout Considerations:

1. Network Proxy
2. Network Capacity
3. Network Firewall
4. Directory Sync
5. Client Distribution
6. SAML, Two-Factor Authentication, and CAC/PIV Configuration
7. Log Extraction and SIEM integration
8. Administrator Training
9. Silo Policy Configuration
10. User Training
11. Phased roll-out

---

1. Network Proxy: To enforce Silo adoption on organization-managed workstations, network edge devices or PAC files will have to be distributed with rules defined to direct non-local traffic into Silo. The most common method of deployment is through the use of a PAC file or other SWG or proxy methods.

TECHNICAL DETAILS:
https://support.authentic8.com/a/solutions/articles/16000026581

2. Network Capacity: Silo is a remote display, thus network performance can impact user experience. The average Silo session consumes 700 Kbps of bandwidth and requires 50 ms of latency for optimal performance but will tolerate up to 150 ms of latency. Your organization's internet access points should be reviewed to ensure adequate bandwidth is available prior to deployment.

TECHNICAL DETAILS:
https://support.authentic8.com/a/solutions/articles/16000042664

3. Network Firewall: Silo establishes an encrypted connection for the remote browsing session using TCP port 443, which is commonly open on most enterprise systems. Administrators are able to extract full audit log data for user activities for integration into an existing SIEM for analysis, with optional log encryption to protect the integrity of audit data.

TECHNICAL DETAILS:
https://support.authentic8.com/a/solutions/articles/16000026587

4. Directory Sync: Silo supports Active Directory synchronization for the creation, deletion, and suspension of user accounts. AD Administrators can control rollout with a combination of OU and Windows Security Groups assignments. This will be the primary method for account management.

TECHNICAL DETAILS:
https://support.authentic8.com/a/solutions/articles/16000033194

5. Client Distribution: Most organizations support Windows 10 and a small contingency of MacOS footprints. It is recommended to use package distribution tools such as SCCM or JAMF to manage and distribute the Silo client binaries.

TECHNICAL DETAILS:
https://support.authentic8.com/support/solutions/articles/16000026518-windows-client-install-instructions-for-enterprise-customers-

6. SAML, Two-Factor Authentication, and CAC/PIV Configuration: Silo supports SAML 2.0 for single sign-on to Silo by federating your logins with your identity provider, as well as two-factor authentication and use of U.S. Government CAC/PIV cards.

TECHNICAL DETAILS:
https://support.authentic8.com/support/solutions/articles/16000035031-saml-sso-for-silo-access
https://support.authentic8.com/support/solutions/articles/16000049229-two-factor-authentication-
https://support.authentic8.com/support/solutions/articles/16000053588-common-access-card-cac-support

7. Log Extraction and SIEM Integration: User activity logs are stored in Authentic8's databases. Those logs can be encrypted with a public key. It is recommended that all customers generate a public encryption key and enable log encryption. Logs can be downloaded through a publicly available API to the customer's premise, decrypted, and loaded into SIEMs or any other log processing system.

TECHNICAL DETAILS:
https://support.authentic8.com/support/solutions/articles/16000027679-authentic8-api-reference-guide

8. Administrator Training: It is recommended that larger organizations identify and train local support staff to be Silo Administrators. Silo supports role-based administration. It is essential to define roles and assign to specific administrators. Determining which roles belong to which administrators will be a requirement. Authentic8 can provide customized administrative support and training materials on a case-by-case basis.

ADMIN GUIDE:
https://support.authentic8.com/a/solutions/articles/16000037250

9. Silo Policy Configuration: Silo supports a rich policy framework that allows for many different use cases. Organizations should configure and apply administrative policies by role or use case. Policies will need to be determined and applied prior to rollout. Below are some examples of policies:

- Data policy
  - Block clipboard access
  - Block all downloads to local endpoint
  - Disallow printing
- URL category filtering
  - Block access to gambling or offensive material
  - Block access to social media sites

10. User Training: Users need to be trained on the differences between using the Silo browser and native browsers. Please review the user guide to set user expectations for performance and user experience.

USER GUIDE:
https://support.authentic8.com/support/solutions/articles/16000035032-silo-access-portal-user-guide

11. Phased Rollout: We recommend a phased rollout by geography and/or user population/department. Consider the following schedule:

- Develop a phased approach for rollout:
  - Distribute licenses to appropriate groups within the organization
  - Develop success criteria for each phase
    - Validate that required policies are in place and enforced
    - Establish user procedures for incorporating user feedback into subsequent phases
  - Select pilot for initial phase
    - Choose users with moderate web usage to minimize business disruption during rollout, while still collecting feedback
    - Select geographic locations with fast network to ensure a smooth user experience
    - Phased traffic migration plan for pilot

  - Phase 1: Dual operation of native browser and Silo browser
  - Phase 2: Block native browsers by policy for internet traffic directing users to Silo browsers for intranet (agency or organization-sponsored) sites and apps
  - Upon successful completion of the pilot phase, develop a timeline for the remaining phased rollout
- Incorporate feedback from the pilot and address technical details and adjust training, as needed

FULL DETAILS

Full details can be found on the Authentic8 Support Portal:

https://support.authentic8.com/support/solutions/articles/16000055331-deploying-authentic8-silo-and-toolbox-for-federal-customers

Conclusion: Enabling Remote Workers Through Web Isolation

- Rapidly enable remote work to ensure continuity of operations.
- Identify which services are currently externally hosted or can be rapidly configured for external access to provide basic communications fast. Some organizations prioritize web-based e-mail and office productivity, such as Outlook Web Access, G Suite and Office 365.
- Customize remote worker roles, application shortcuts, auditing, data transfer policies, web category filtering, and other options in the Silo administration portal.
- Install the Silo application on end-user devices to provide access to employer services while segregating data from the local device and enforcing security policies.
- Direct personnel to use Silo for all employer-related web browsing and web applications, such as Office 365.

silo By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world's most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.