



USE CASE

Rapidly Enabling Remote Workers in a Federal Workforce

Introduction

A U.S. Government agency required a secure, easy-to-deploy solution for enabling its remote workforce. They evaluated traditional solutions such as VPNs on government-issued laptops and BYOD policies, as well as the Silo Web Isolation Platform.

The agency selected Authentic8 to enable secure connectivity for remote workers. The Silo Web Isolation Platform by Authentic8 separates the things you care about from the things you cannot trust. A true Zero Trust architecture, Silo isolation enables access to resources while maintaining separation from the user's workstation. A web-based solution, Silo is easy to deploy on any end-user device, and also provides enhanced monitoring and audit of user activity, access control to resources, and trusted isolation that assured protection of U.S. Government

The Challenge

Office 365 is mission critical for the agency, and they were heavily invested in the solution suite for day-to-day operations. Responding to the rapidly emerging COVID-19 Coronavirus outbreak, the agency sought a reliable remote worker solution to ensure continuity of operations.

However, traditional remote working required government-furnished laptops, and was limited by VPN connectivity and the inability to rapidly procure additional devices to support two-factor authentication. Previously, during a major snowstorm requiring employee telework, the VPN solution was overwhelmed by the increased demand and crashed when it was needed most.

Government-furnished equipment procurement could not scale quickly enough so employees would need to use their own devices. Yet a traditional VPN solution cannot secure government information accessed from user-furnished personal devices or enforce restrictions on uploads, downloads, or local file storage.

The agency is now working with Authentic8 to immediately deploy access to Office 365 and policy-compliant web browsing to employees so they can work remotely. Silo is easy to use and can be deployed quickly, and ensures that work data is isolated from unmanaged devices and networks. All while physically isolating users to reduce risk to the workforce from a global pandemic.

THE STORY

Due to the COVID-19 Coronavirus, a U.S. Government agency needed to quickly enable remote workers.


The employees required secure access to policy-compliant web browsing and O365 Suite to continue day-to-day operations while enforcing government security and audit policies.

Silo for Safe Access will allow employees to use unmanaged devices to access O365, while still enforcing security regulations and compliance and audit oversight.

How it works

Silo for Safe Access (Silo Cloud Browser) is a web browsing solution that enables access to untrusted web content — from anywhere, on any device — without introducing risk to your corporate infrastructure.

Silo for Safe Access is built on Authentic8's patented, cloud-based Silo Web Isolation Platform, which executes all web code in a secure, isolated environment that is managed by policy, providing protection and oversight of all web-based activity. Embed security, identity and data policies directly into the browser, giving IT complete control over how the web is used by internal users, and how web apps may be used by external users.



“At a time when flexibility and rapid response were critical, Silo was easy to deploy and use, and it ensured protection of U.S. Government information.”

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 cannot be guaranteed. Try Silo now: www.authentic8.com