Silo
By Authentic8

CASE STUDY
US GOVERNMENT/DEFENSE

Shields Up: How a Military Unit Simultaneously Increased Network Access and Decreased Cyber Risk

Whether from a personal privacy or cybersecurity standpoint, military units, federal organizations, commercial organizations, and academic institutions can significantly increase the risks associated with accessing the internet from desktop or mobile devices. With the increased value of publicly available information (PAI), the need to enhance productivity through modern collaboration tools, and the growing need to leverage the internet for both official and personal business, it is becoming increasingly essential to provide responsible access to the broader network — without introducing additional risk.

Introduction

Cybersecurity is mission-critical for the U.S. Government and has become an integral part of the nation's defense. For a military unit based in Virginia charged with securing segments of the Department of Defense Information Network (DoDIN), thoroughly investigating cyber threats requires access to the internet beyond top-level .mil and .gov domains.

For the unit members, access to personal email, social media, and commercial websites to conduct personal business was restricted for security reasons. However, internet access for all unit personnel was considered critical to ensuring personnel readiness, morale, and quality of life. To that end, the unit found several solutions to reduce their network attack surface, minimize risk, and provide all personnel with permissible access to the outside world.

At the same time, the unit is responsible for mitigating network intrusions across the entire military branch. The unit's objective was to reduce the number of cyber incidents and enable a shift in internet access policies to scale across the enterprise network and benefit other military branches more broadly.

The Communications Department Head of the military unit led the efforts to find the optimal solution. After considering internet access kiosks scattered throughout the building, as well as various commercial technology solutions, the team decided to evaluate the Authentic8 Silo for Safe Access (Cloud Browser).

THE STORY

Unit required a secure browsing solution for personal internet access

Personal access using commercial browsers to non-DoD sites was restricted

Unit concerned with significant increase in potential web threats impacting mission

Identified Silo Web Isolation Platform as solution to meet security and operational needs

Silo migrated all external web traffic off unclassified production network

Access to personal email / internet resources provided boost in morale and enhanced productivity

The Challenge

Prior to deployment, personnel were not permitted to access sites that were not related to the mission, which included external webmail and social media websites. Personal electronic devices were prohibited in the workplace due to facility security restrictions. This policy required individuals to leave the secured area when checking personal email, accessing non-whitelisted sites, and visiting websites not directly associated with mission execution.

The unit was also concerned about the rapid adoption of encrypted web data, and the associated difficulty in inspecting the traffic effectively enough. Once the internet usage policy was defined, the unit concerned itself with how best to implement a new technology without incurring an increase in malicious code transiting the network.

The unit was committed to giving personnel the internet access they needed by "transferring the most risk-laden network communications off of the operational platform by leveraging a secure, sandboxed web browsing experience," as the unit's Communications Department Head framed it. The overall objective was to find a solution that would "allow end-users to interact with websites in a familiar way while keeping potentially malicious and un-inspectable traffic from infecting the network." The unit considered Authentic8's Silo remote isolation browser to be the optimal solution for their needs.

The overall objective was to find a solution that would "allow end users to interact with websites in a familiar way while keeping the potentially malicious and un-inspectable traffic from infecting the network."

The Implementation

The unit intended to migrate all external web browsing traffic off the unclassified production network and onto the Silo isolation platform. In what the group affectionately referred to as "Operation SHIELDS UP," the unit rolled out the solution in approximately thirty days. Phase I commenced with the network's web proxy blocking all websites — with a few whitelisted exceptions — that did not have the .gov or .mil top-level domain. All websites requiring Common Access Card (CAC) authorization remained available on the production network. After an initial training session and clear communication of the plan, licenses were deployed, and user

accounts established.

The unit's system administrator stated, "The Silo Web Isolation Platform allows us to grant access to a more diverse array of websites — only blocking those that violate Department of Defense (DoD) acceptable use policy — while ensuring the confidentiality, integrity, and availability of our unclassified production network." The Silo deployment ensured that mission-focused research and analysis did not unintentionally open the network to attack, should analysts venture to the darker places on the internet. Additionally, it enabled the commander to responsibly provide access to external webmail and "quality of life" web services that modern servicemembers deserve.

[Silo] enabled the commander to responsibly provide access to external webmail and "quality of life" web services that modern servicemembers deserved.

The Result

Several years later, the unit continues to keep their "shields up," providing every team member with access to a Silo web browser as the primary means of accessing the internet. Since deployment, there have been zero incidents on the network to mitigate. The unit has since expanded the use of the platform to include Silo for Research (Toolbox) for more in-depth cyber-threat intelligence research, in addition to exploring new user access to Silo, initially focused on remote workers and unit reservists.

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**

Redwood City
333 Twin Dolphin Dr,
Suite 112
Redwood City, CA 94065

San Francisco
555 California St,
Suite 3360
San Francisco, CA 94104

Indianapolis
8888 Keystone Crossing,
Suite 675
Indianapolis, IN 46240

Washington, D.C.
1010 Vermont Ave NW,
Suite 816
Washington, DC 20005