silo
BY AUTHENTIC8

ENHANCING OPERATIONAL SECURITY

WITH MANAGED ATTRIBUTION

The Importance of Managed Attribution

In today's interconnected world, the digital landscape is a battlefield where adversaries constantly seek to exploit any vulnerability. For defense organizations, unmanaged online activities and open-source data collection present significant operational security risks. Every click, search and visit can inadvertently reveal sensitive information about your organization's interests and gaps, providing adversaries with valuable insights. Managed attribution (MA) is an essential tool for protecting web research and maintaining mission security.

Managed attribution refers to the practice of disguising the origin and nature of online activities to prevent adversaries from tracing them back to the organization. It ensures that research and browsing remain anonymous, safeguarding sensitive operations from potential threats. Without MA, adversaries can piece together information about government operations, research and intentions, compromising the security of missions and personnel.

> Our 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.
>
> **DoD Communications Department Head**

Silo for Research: A Comprehensive Solution

Authentic8's Silo for Research offers a proven managed attribution solution designed specifically for defense organizations. Key features include:

Global Points of Presence

Robust IP Address Network

- **Secure:** Authentic8’s unique network of IP addresses are vetted and procured securely, mitigating the risk of adversaries associating online activity with the user organization.
- **Global:** Authentic8 provides users a wide selection of IP address locations to conduct their research. This network includes locations across different regions, ensuring that researchers can access information from various locations around the world without revealing their true origin.
- **Diverse:** The solution includes access to IP addresses from data centers, ISPs, mobile and TOR/dark web. This diversity helps users overcome website blocks and avoid scrutiny, enhancing the ability to gather intelligence from a wide range of sources.

Isolation and Quick Access: Authentic8 Silo is a fully isolated environment, allowing users to conduct research without worrying about malware infections or data leaks. The platform ensures quick and easy access to necessary resources, streamlining the research process while maintaining high security.

Comprehensive audit logs: Authentic8 Silo integrates detailed audit logs of user and administrator actions taken within the platform at scale. Audit logs include user-attributable details, such as URLs visited, cookie and form data, file activity, translations, printing and more. This data can enable tradecraft oversight, insider threat monitoring and other functions.

> If we are not using Silo, sites are going to notice that the traffic is coming from the federal agency’s IP address, especially if we are visiting them again and again. Every hit is being tracked, and all the data on the internet traffic is available for people to purchase.

DoD IT specialist and program manager

Alternatives and Their Disadvantages

While several alternatives to managed attribution exist, they often fall short in terms of security, cost and effectiveness. Here's a look at some common alternatives and their disadvantages:

1. Virtual Desktop Infrastructure (VDI) with Egress from Cloud Provider:

- Limited access to IP addresses in multiple geographic regions or ability to choose a location based on the research target.
- Web traffic from a small number of IP addresses can lead to the association of traffic and eventually expose organizational intent and gaps.
- Cloud provider IP addresses are easily identifiable and may be scrutinized or blocked by certain websites, leading to different treatment or content.
- Lacks integrated, centrally managed audit logs and access controls.

2. Virtual Machine (VM) + Commercial VPN:

- Expensive operation and maintenance.
- Unvetted VPN vendors with unknown security states pose significant risks.
- Typically provide only data center IP addresses, which are easily blocked or scrutinized by online platforms.
- Lacks integrated, centrally managed audit logs and access controls.

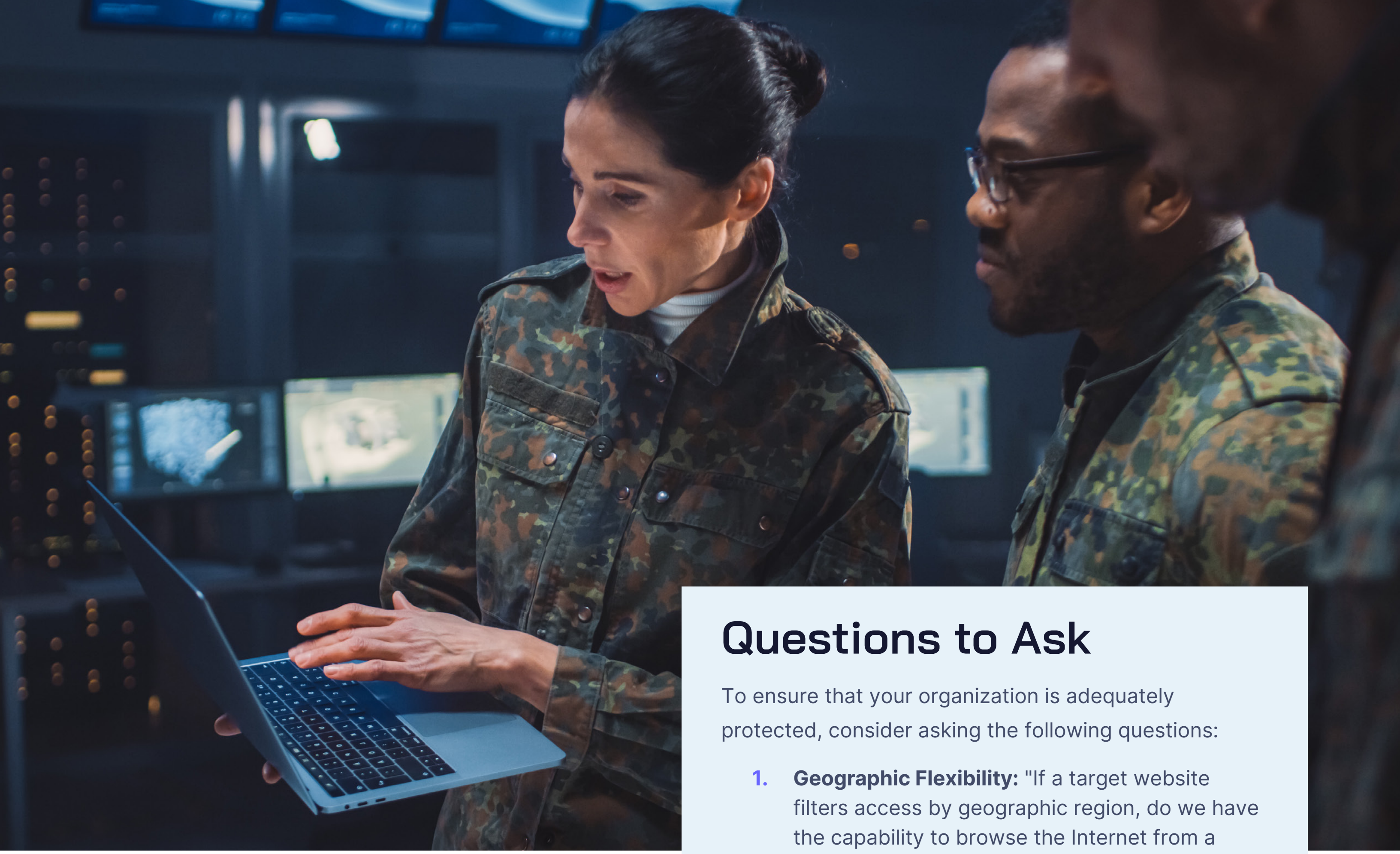
3. Local Browser on Local Endpoint/ Workstation:

- All browsing activity is attributed to the organization, and possibly to the individual, depending on browsing habits.
- Lack of isolation increases the risk of infecting the organization's network with web-based malware.
- Blending research traffic with business traffic makes effective oversight of operational activities extremely challenging.

Accessing a Chinese academic journal

Chinese-controlled websites often block non-regional IP addresses, preventing a government organization from accessing otherwise publicly available academic research.

Using Silo, the organization was able to access the content through a point of presence in located in the region and set up automated recurring collection to capture new journal articles as they were released.



Questions to Ask

To ensure that your organization is adequately protected, consider asking the following questions:

1. **Geographic Flexibility:** "If a target website filters access by geographic region, do we have the capability to browse the Internet from a user-selected region?"
2. **Diverse Points of Presence:** "Do we have access to a wide variety of points of presence, including data centers, ISPs, mobile networks, and TOR/dark web, to avoid scrutiny and bypass website blocks?"
3. **Isolation and Security:** "Are our online activities isolated from our local network and endpoints to prevent malware infections and data leaks?"
4. **Vendor Vetting:** "Are our VPN vendors vetted for security, and do they offer diverse points of presence beyond just data center IP addresses?"
5. **Cloud Provider Risks:** "What measures, such as user-selectable regions, are in place to prevent web traffic from our provider's points of presence from being associated and linked to our organization's activities?"
6. **Local Browser Risks:** "What steps are we taking to ensure that our browsing activities are not easily attributable to our organization or individual users?"

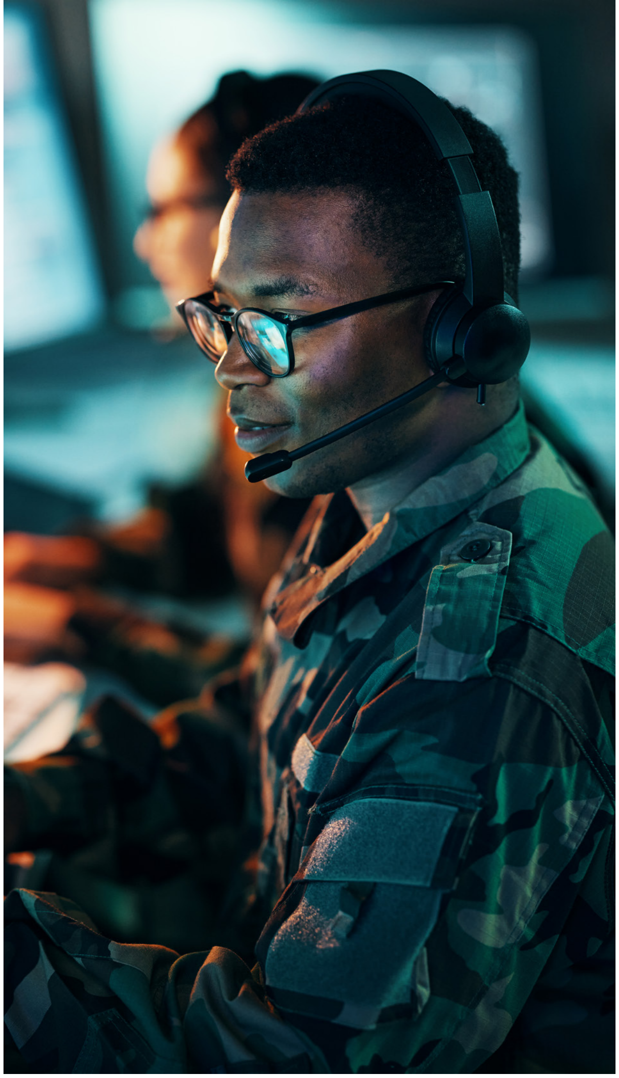
> The Silo Web Isolation Platform allows us to grant access to a more diverse array of websites — only blocking those that violate Department of Defense (DoD) acceptable use policy — while ensuring the confidentiality, integrity, and availability of our unclassified production network.
>
> **DoD Systems Administrator**

Purpose-built managed attribution solution

For defense organizations, protecting online research activities is crucial for maintaining operational security. Managed attribution with Authentic8 Silo for Research provides a comprehensive, rapidly deployable solution, offering diverse points of presence, 100% isolation, and oversight via detailed audit logs. In contrast, alternatives like VMs with commercial VPNs, VDI solutions, and local browsers fall short in terms of security, effectiveness and operational costs. By adopting a trusted, off-the-shelf managed attribution platform, organizations can ensure that their online activities remain secure and anonymous, safeguarding their missions and personnel from adversary exploitation.

Secure your research

Discover how Authentic8 Silo for Research can enhance your operational security. Protect your online activities and secure your mission with our advanced managed attribution solutions.



> When we visit websites, we try to not disclose the agency's IP address; when we are looking at something that's happening in, say, Russia, we don't want the Russian site owners to know that the traffic is coming from the U.S. But any link that you click online can be traced back to you, so we must be careful – because the nature of our investigations demands anonymity.

DoD IT specialist and program manager

Silo for Research is an integrated solution for conducting secure and anonymous web research, evidence collection and data analysis from the surface, deep and dark web. It's 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.

+1 877-659-6535
www.authentic8.com

© Authentic8, Inc. All rights reserved. 06042024

About the authors

MATT ASHBURN
VP of Customer Success
matt@authentic8.com

Matt is the Vice President of Customer Success, focusing on cross-functional strategy and engagement to deliver the best possible experience for Authentic8 customers. Prior to Authentic8, Matt served as a CIA officer focusing on cyber issues, including a detail serving on the National Security Council as the Chief Information Security Officer and Special Advisor to the National Security Advisor, leading technical expertise, risk reduction strategies and policy for national security systems.

At CIA, Matt led the technical direction and coordination to stand up an innovative, unified cybersecurity operations center to fully harness agency authorities, resources and talents to prevent and respond to advanced cyber threats. He also led the detection watch floor of CIA's cyber incident response team, and has been recognized with a national intelligence award and service ribbon from the Director of National Intelligence and the IC CIO Partnership Award.

Prior to CIA, Matt gained additional government and private sector experience focusing on intelligence matters and cybersecurity initiatives. He holds a BS in Electrical Engineering from the University of Virginia and is a graduate of FBI's Intelligence Basic Course at Quantico, VA.

ABEL VANDEGRIFT
Head of Strategic Initiatives & Partnerships
abel@authentic8.com

Abel is the Head of Strategic Initiatives and Partnerships, advising Authentic8’s customer success and sales teams on policy trends, regulatory activities and executive and legislative priorities, as well as supporting strategic industry partnerships. Prior to his role at Authentic8, Abel worked as a government affairs consultant on behalf of clients across the defense, intelligence and cybersecurity sectors.

He is a graduate of the University of Maryland with a BA in Philosophy and earned a Juris Doctor (JD) from George Mason University. Abel is a member of the Maryland Bar.