DATA SHEET

The Silo Managed Attribution Network

Security and anonymity are foundational for digital investigations, but they're not the end goal. Analysts are charged with delivering actionable intelligence for the organization, and such a charter requires more of the network they use to access online resources. To provide true insight, analysts need precise access from a specialized Managed Attribution (MA) network with geographically relevant nodes and a variety of network connection types...

...to ensure investigations never link back to the company, and activities blend in with the crowd

...to avoid geo-blocks and to access content as it's being presented locally in foreign regions

...to match the research platform to the context of the investigation to establish and maintain legitimacy

The Silo Managed Attribution Network provides access to 100s of globally distributed, Authentic8 managed end points, ensuring Silo Workspace delivers secure, anonymous and seamless access to surface, deep, and dark web content, right where it's needed.

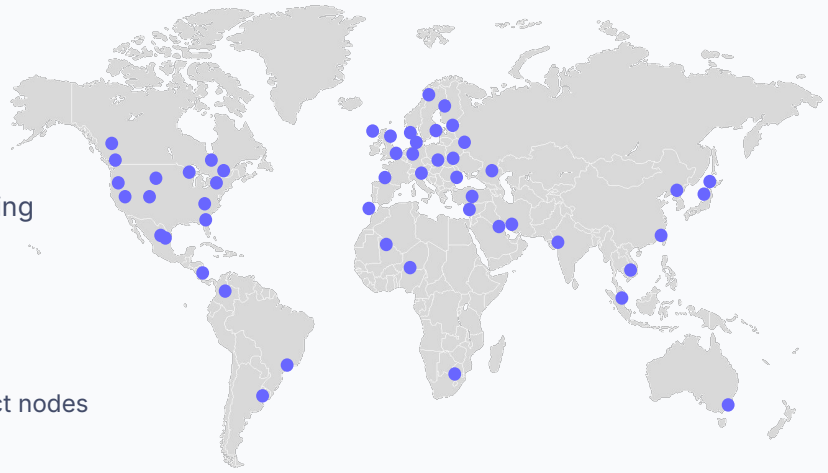
The Silo Managed Attribution Network

The Silo Managed Attribution Network is designed to meet the unique demands of modern digital investigations. This extensive network supports secure and seamless access to surface, deep, and dark web content, ensuring that investigators can operate stealthily and effectively in various geographies and online environments.

700+ Nodes Across **180** Points of Presence

Key Features

- No attribution
- Shared or private nodes
- Geographic and connection variety
- Performance and reputation monitoring
- Continuous rotation and expansion



6 continents

57 country sub-regions

141 state & local regions

90 ISPs

12 Tor interconnect nodes

Non Attribution

The Silo Managed Attribution Network anonymizes connections through multi-layer tunneling in the Silo browser and Authentic8 infrastructure. This prevents traffic from being linked to investigators or their organizations. By ensuring non-attribution, it protects researchers' identities, preserves investigative integrity, and reduces the risk of adversaries tracing activity to its source.

Shared or Private Egress Nodes

Flexibility is a cornerstone of the Silo Managed Attribution Network. Researchers can choose from shared or private nodes based on their operational requirements.

Shared Nodes: These nodes obscure specific user activities by blending them with a larger pool of general crowd traffic. This method offers a higher degree of anonymity, as individual research actions are masked within the broader internet usage patterns.

Private Nodes: These are assigned for exclusive use per mission requirements. Private nodes are particularly useful for operations that require a dedicated, consistent connection source, ensuring that specific research activities remain undisclosed and untraceable.

Geographic and connection variety

The network includes Data Center, ISP, and Mobile nodes, enabling access to geo-blocked content and specialized research. Researchers can select regional egress points. This geographic flexibility supports realistic, location-specific activity simulation and access to restricted content.

Performance and reputation monitoring

Maintaining a high-quality, reputable network is essential for uninterrupted research. Silo Managed Attribution Network ensures this through continuous performance and reputation monitoring via internal audits and third-party services. Proactive oversight quickly resolves IP reputation or geolocation issues, minimizing downtime and ensuring reliable, high-efficiency connectivity for researchers.

Continuous rotation and expansion

To outpace adversaries and meet evolving regional requirements, the network is continuously rotated and expanded. Data Center and ISP IP addresses rotate roughly every 180 days, with no reuse for two years, preventing detection and blocking. Ongoing regional node deployment strengthens resilience, adaptability, and support for customer-specific and emerging research needs.

Egress Node Types

Data Center Egress Node

An endpoint hosted at a data center or cloud provider using IP addresses associated with the hosting provider.
Function: Provides reliable, high-performance access ideal for responsive interaction with web pages and efficient file transfers.
Best use: Suitable for general website research, high-quality service needs such as file transfers and video, or accessing geo-blocked resources within specific regions.

ISP Egress Node

An endpoint using IP addresses associated with regional ISPs providing wired broadband service.
Function: Ensures stable access.
Best use: Ideal for accessing content where social media sites or regionally specific content providers may block data center IPs.

Mobile Egress Node

An endpoint using a wireless network connection provided by carriers offering fixed wireless services.
Function: Expands geographic reach, especially in mobile-centric regions, and provides access to hard-to-reach content. Facilitates blending in with mobile user traffic and accessing dynamic IPs for each session.
Best use: Optimal for accessing platforms that scrutinize data center connections such as social media, forums, etc.

Dark Web Interconnect

A cross-connect into the Tor network through an Authentic8-managed proxy.
Function: Offers integrated dark web access without additional software, ensuring security and anonymity.
When to use: Essential for researching dark web content or accessing dark web forums and marketplaces .

Example Use Cases

The Silo Managed Attribution Network supports a multitude of digital investigation scenarios, providing researchers with the tools needed to navigate complex and sensitive online environments.

Conflict monitoring

For geopolitical analysts, the ability to closely monitor regions experiencing conflict is invaluable. The network's randomized IP allocation and user-specific node assignments enable secure and anonymous tracking of events This ensures that analysts can gather real-time intelligence without raising suspicion or alerting adversaries.

Phishing exploit assessment

Cybersecurity professionals can leverage the network's diverse egress nodes to simulate different user conditions and locations during phishing exploit assessments. This capability ensures comprehensive threat evaluation from multiple external viewpoints, helping organizations to bolster their defenses against sophisticated phishing attacks.

Illicit cryptocurrency transactions

Cryptocurrency transactions on the dark web present unique challenges for financial investigators. The Silo Managed Attribution Network provides a secure means to investigate these activities. By using designated nodes, researchers can trace transactional breadcrumbs and conduct deep-dive analysis into dark web marketplaces, uncovering hidden financial networks and preventing financial crimes.

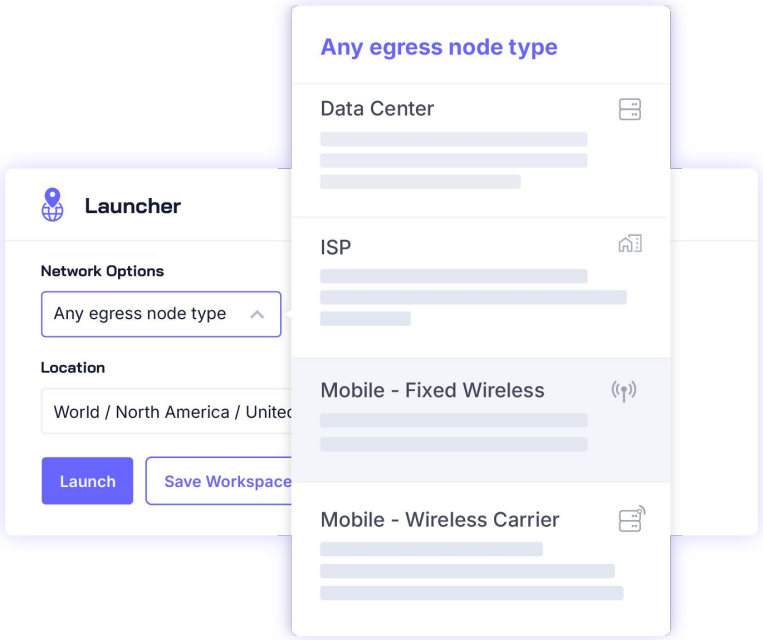
Know Your Customer (KYC) validation

Ensuring regulatory compliance through diligent KYC research requires access to a variety of online platforms, including social media and professional networks. Using ISP and wireless nodes, the network enables compliance officers to discreetly validate customer information across multiple sources, maintaining both thoroughness and confidentiality.

Conclusion

What sets the Silo Managed Attribution Network apart from other solutions is its unparalleled flexibility, extensive geographic coverage, and robust security mechanisms. The network's capacity to adapt to various research scenarios—from geopolitical analysis to financial crime investigation—while preserving investigator anonymity, provides unmatched support for digital investigations.

The continuous rotation and proactive expansion of network nodes ensure that it always stays a step ahead of adversaries.



Ready to modernize your investigation workspace? Schedule a demo today.

Silo Workspace is the digital investigation platform that protects, masks, and accelerates direct engagement at the source. With isolated multi-app workspaces, a global managed attribution network, integrated capture and analysis tooling, and enterprise-grade controls, Silo is your unified workspace to enter the threat environment.

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