Silo Workspace — Protect, mask, and accelerate your investigations

As threats grow more complex, investigators need to engage them securely at the source. Silo Workspace protects infrastructure, masks identity, and accelerates digital investigations beyond the network perimeter. More than 750 organizations worldwide rely on Silo to access, engage, and respond to threats.

Cyber Threat Intelligence - SOC Incident Response - Fraud and Brand Protection - Corporate Security - Financial Crime - PAI and OSINT - Law Enforcement

Silo isolated workspaces place analysts securely and anonymously in-region across the globe. The platform unifies the investigative lifecycle enabling comprehensive content capture and analysis, while maintaining strict policy enforcement and compliance oversight.

Isolated Multi-App Workspaces

Silo Workspace delivers isolated, multi-application environments that let analysts instantly launch region-specific investigative tools while maintaining strong tradecraft and operational security.

- Click-and-go access to region-specific applications with no manual setup
- Secure, non-attributed interaction across web, applications, and services
- Integrated workspace that eliminates the need for custom infrastructure management
- Highly configurable environments adaptable to any investigation type, threat landscape, or geography

Full Scope Platform for Direct Engagement

Global Managed Attribution Network

Silo Workspace's Global Managed Attribution Network preserves digital authenticity by giving investigators precise control over how they appear online, reducing the risk of blocking, exposure, or disinformation during active investigations.

- Operate from 700+ managed endpoints across 32+ countries and 100+ regions
- Blend into local environments using diverse last-mile options, including mobile and regional ISPs
- Precisely control device, network, and geographic attribution to match investigative targets
- Extend reach through native Tor connectivity and secure access to deep and dark web sources

Integrated Capture and Analysis

Silo Workspace unifies content capture, analysis, and collaboration within a single secure environment, enabling investigators to work efficiently without fragmenting tools or data.

- Capture, manipulate, and analyze content across multiple applications and data sources
- Store investigative artifacts in encrypted, cloud-based storage built for secure collaboration
- Preserve evidence and investigative continuity without exporting data to unsecured systems
- Extend workflows through third-party applications and extensions while maintaining centralized control

Enterprise-Grade Policy Enforcement and Audit

Silo Workspace extends security and compliance beyond individual investigators, enabling organizations to enforce governance and regulatory controls without disrupting investigative workflows.

- Centrally provision and revoke web applications, browser extensions, and user access
- Manage credentials and permissions across users and groups with administrative oversight
- Enforce consistent data-handling policies across cloud and local storage environments
- Deliver customizable, click-and-go investigation workspaces with managed fingerprints and geolocation controls

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

FedRAMP · AICPA SOC · PCI DSS Compliant · DFARS Compliant · CSA cloud security alliance® · ISO 27001 · Cybersecurity Maturity Model Compliant · HIPAA Compliance

silo BY AUTHENTIC8

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