Silo Apps: Terminal

Execute powerful command line tools

The Silo Workspace Terminal App gives you a remote host for executing CLI tools over the Silo Managed Attribution network, enabling deeper and more specific analysis. Extend the reach and efficacy with a modern, secure terminal built for OSINT and Cyber Threat Intelligence CLI tools, whether home-built or open source.

We've built a separate and dedicated network category for execution of command line resources, which will allow use of the tool without risking collateral damage to your other Managed Attribution activity.

End User Features and Benefits

- **Secure Execution of Open-Source Tooling**: Enables investigators to run powerful CLI-based OSINT and CTI scripts (e.g., Python tools, scrapers, network analyzers) strictly within Silo's cloud-isolated environment, ensuring that malicious code or compromised repositories never touch the analyst's local machine.
- **Managed Attribution for Command Line:** Extends Silo's managed attribution capabilities to the command line, ensuring that all traffic generated by analysis tools is anonymized and localized to the specific region required, preventing adversaries from fingerprinting the investigator based on non-browser traffic.
- **Enhanced Productivity via Tilix:** Leverages Tilix's robust tiling interface to allow analysts to run simultaneous tasks—such as executing a query in one pane while monitoring logs or referencing documentation in another—optimizing screen real estate and accelerating complex workflows.
- **Consolidated Investigative Workflow**: Eliminates the need for investigators to toggle between a secure cloud browser and insecure local Virtual Machines (VMs) for tool execution. This creates a unified, single-pane-of-glass environment for both web-based and command-line intelligence gathering.

Admin Features and Benefits

- **Managed Tool Deployment:** Allows organizations to standardize and control which command-line tools are available to their team, reducing the "shadow IT" risks associated with analysts installing unvetted software on their own devices.
- **Oversight:** As with all Silo capabilities, administrators maintain visibility over tool usage with user activity logging.

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