ANOMALI® silo By Authentic8

PROTECT AND ENHANCE THE ANALYST WORKFLOW

A comprehensive solution for IR and Threat Hunters with Anomali and Authentic8

ANOMALI AND AUTHENTIC8 JOINT SOLUTION FEATURES:

Anomali's intelligence-driven security products provide unmatched threat visibility and accelerated detection. When analysts need to take action based on that intelligence, Authentic8's Silo for Research is the perfect complementary solution, giving the analyst a cloud-based, web isolation platform that benefits the user and the organization:

- **FULL ISOLATION**: All web code is executed on Silo servers, not end-user devices. Potentially unsafe content never touches your assets

- **MANAGED ATTRIBUTION**: Configure the browser fingerprint and egress location. Blend in with the crowd to avoid tipping off your intent.

- **ACCESS OPEN, DEEP or DARK WEB**: One-click access to any destination without tainting your environment. Maintain policy, while providing a secure way for users to interact with any destination

IMMEDIATE TIME-TO-VALUE

Silo provides a research platform for Anomali users that secures the user, device, and organization, while providing advanced OSINT tradecraft tools. Silo eliminates the need to have parallel infrastructure or security policy exceptions to enable analysts to conduct threat research.

- **CLOUD-BASED:** Turn-key, cloud-hosted solution that creates a clean instance every time. Seamless, immediate deployment with on-demand access from anywhere

- **ELIMINATE IT SUPPORT BURDEN:** No more exception approvals or remediation needed

- **COMPLETE AUDIT OVERSIGHT:** Encrypted audit logs of all web activity. Simplify analyst compliance and audit, and improve case documentation

- **WORKFLOW ENHANCEMENTS**: Improve time to insight with integrated OSINT tools

AN ADVANCED ANALYST RESEARCH PLATFORM

Enhance and accelerate the abilities of your analyst team through Silo. Combating sophisticated adversaries requires analysts to be armed with advanced OSINT tradecraft capabilities and managed attribution. Protect your organization and instantly elevate the maturity of your security organization with Silo and Anomali.

ADVANCED OSINT PLATFORM

Secure Global research with embedded OSINT tradecraft

FLEXIBLE DEPLOYMENTS

Fast, scalable cloud-based deployment

IMMEDIATE RESULTS

One-click access into 100% isolation with auditing and policy enforcement

EMPOWER ANALYSTS TO DO MORE

CHALLENGE:

Online research needs can take many forms in a given organization. Increasingly, analysts face common roadblocks to gathering the information they need:

Content can only be accessed from specific geographic location, region, or networks

- Increased CAPTCHA/MFA requests
- Proxy and bot detection algorithms blocking access
- Sensitive research (i.e., dark web) exposes the user and organization to significant risk

SOLUTION:

The world's most at-risk enterprises and government agencies rely on Silo for Research to conduct secure and anonymous online investigations for multiple use cases:

- **Criminal investigations:** Comply with chain-of-custody policy and securely collect evidence on the open, deep, or dark web
- **Cyber threat intelligence:** Access and analyze suspicious or malicious content with 100% isolation from corporate infrastructure
- **Financial investigations:** Keep online fraud investigations anonymous and secure, even on the dark web
- **Open-source intelligence (OSINT):** Disguise identity with a managed attribution platform and global egress network

CUSTOMER BENEFIT:

Ensure your infrastructure security is up-to-date to decrease the chance of being breached, whilst reducing the workload for your SOC team.

FULLY ENABLE REMOTE ANALYSTS ON ANY DEVICE

CHALLENGE:

Home-grown solutions are no longer sufficient for open-source intelligence collection. Using the local computer and network to collect open source content puts OSINT teams and investigators at risk, especially when analysts are remote. In order to minimize that risk, organizations use a variety of tools such as client-side virtualization, VPNs, segregated storage solutions and advanced malware scanning solutions. These are costly to deploy and the complicated IT management requirements create security and attribution gaps.

SOLUTION:

Silo for Research provides one-click access into complete isolation from all web content through a network of cloud-based virtual browsers distributed across geographies. Silo for Research allows full customization of browser parameters including platform, providing key benefits to the organization:

- Auto-deployment of a simpler, stronger and less-expensive security architecture: Replace VPNs, dirty lines, break-inspect, and costly re-image / remediation processes
- Enforce full compliance and audit for each remote user
- Eliminate security risk exceptions

CUSTOMER BENEFIT:

Analyst workflows no longer need to add risk to the organization. Silo helps IT, Security, and Compliance teams across all industries align to solve critical needs.

ANOMALI®