silo
By Authentic8

Secure Financial Fraud Investigations in the Cloud

Reduce Cyber Security Risk and Indirect IT Costs Associated with Online Fraud Research

Executive Summary

In the financial sector, the in-house specialists tasked with anti-fraud investigations online are considered most at risk of web-borne exploits and attacks. While protective IT security measures can mitigate some exposure to web-borne threats, fraud analysts and investigators require access to unknown, uncategorized, and potentially unsafe internet locations to do their job. The resulting security gap can expose employers to data breaches, regulatory fines, class action, personal liability lawsuits, and significant reputational risks.

Many banks face a no-win situation: Block access to suspicious areas of the web in the name of security or relax security on a per-request basis to maintain analyst productivity. Fraud analysts will not be productive if IT disconnects their machines from the network because they have been infected. But blocking investigative efforts when analysts access external sources isn't productive either. Sacrificing oversight and governance by providing analysts unsupervised access to a separate network is not an option.

This whitepaper examines comprehensive solutions for protecting financial fraud investigation specialists when they go online. To do their job productively, analysts require a secure remote browser with the following capabilities:

- Anonymous, private, disposable browser environment
- Integrated encrypted storage for capturing files and screenshots without changing workflow
- Central policies for how the web is accessed and the browser features they can access
- Audit logs encrypted with customer-managed keys

This whitepaper explains how and why outsourcing the risk with a compliance-ready, remote browser isolation solution has emerged as a viable alternative to DIY investigation platforms.

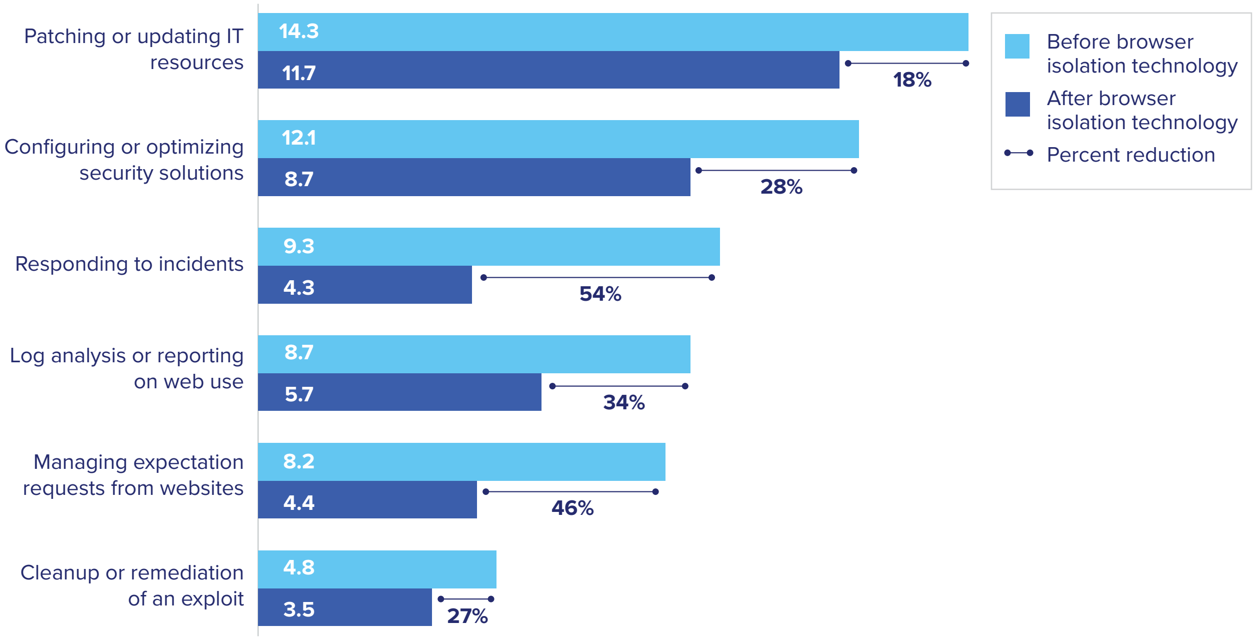
Your Team, In the Trenches – and Exposed

The pressure on financial institutions to ensure compliance with federal regulations is steadily increasing. One example is FinCEN's Beneficial Ownership Requirements for Legal Entity Customers, which went into effect on May 11, 2018.[1] Recent examples show firms suffering reputational damage and facing fines ranging from $70 million to $8.97 billion.[2]

The professionals handling financial compliance-related tasks use the web browser as their primary tool for KYC/CDD/EDD research, transaction monitoring, and compilation of SARs. Paradoxically, while most IT security incidents at financial services firms originate from the web,[3] many teams are still stuck with inefficient and vulnerable tools. Such solutions burden IT with support challenges and oversight requirements that are difficult to deploy and costly to manage.

Hours Per Month IT Typically Devotes to Browser-Related Issues[4]

Includes percent reduction in person-hours/month, through the introduction of browser isolation technology



Investigators rely on IT to provide them with the means to minimize the risk of exposure and prevent compliance violations. Instead, analysts and investigators are often provisioned improvised solutions that are prone to security breaches and result in lower productivity due to malicious code infection.

Research analysts report that those limitations slow down time-critical workflows, thereby limiting the number of cases they are able to investigate and close. According to the Association of Certified Anti-Money Laundering Specialists (ACAMS), 73% of respondents to a 2017 survey stated that AML compliance has negatively impacted their business line productivity.[5]

One bottleneck that has been identified is the browsing environment used by compliance managers and analysts. Online investigators report getting blocked by their bank's web filtering solution from sites that warrant closer inspection. Obtaining exemptions from IT — which often requires filing support tickets with third-party vendors — frequently leads to further delays with the potential of continued risk exposure for the organization.

The Local Browser: Liability for Fraud Research

The basic interaction model of the web has created an environment where a simple page view request from a local browser can lead to system exploits, data egress, and de-anonymization. The IP address disclosed by the browser allows adversaries to identify a user's location and organization. "Digital fingerprints" of a user or group of users can be built from the browser's leaked data, even across different platforms and locations.

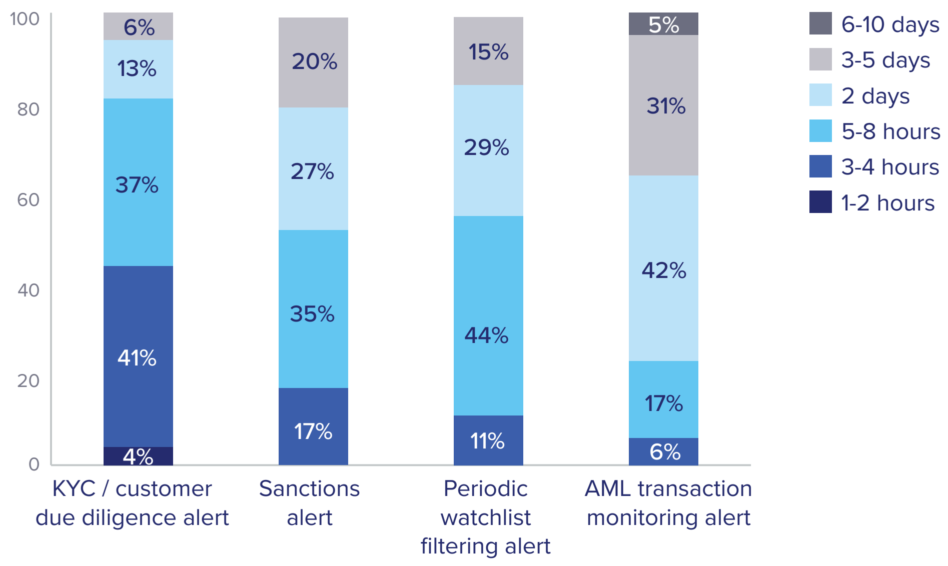
How can CISOs and risk managers address those issues to protect research analysts better and improve overall efficiency of the compliance team in the process?

Which Risks and Threats Are Researchers Facing on the Web?

According to Forrester Research, analysts collect up to 125 data points from on average 20 sources before filing a Suspicious Activity Report (SAR).

This process can take up to eight hours or more, with much of the effort spent on the web or analyzing information that has been downloaded.

Average Time Required to Clear an Alert by Alert Type[6]



Because of the inherent security weakness of the web's architecture,[7] the browsing environments financial institutions select for protecting their missions should mitigate the following risks:

- **Risk of malware infection:** Routine tasks of fraud analysts and investigators — such as "negative news" searches on the open web — can expose the research platform to malware. Files downloaded in the course of compiling SARs can also contain malware.
- **Risk of attribution:** Investigators and analysts should be able to conduct background research as well as in-depth investigations without disclosing their IP address, which could compromise the investigations.
- **Risk of delayed threat response:** Browsing environments with high maintenance and configuration requirements can prevent timely investigations and put the organization at financial and reputational risk.

Traditional Methods: Not Quick. Still Dirty.

Traditional approaches to mitigating the risks for online research specialists vary significantly. They range from basic (and ineffective) methods to more complex (and expensive to maintain) solutions with limited security benefits. All these solutions have been found to increase Mean Time to Resolution (MTTR).

The most basic — and least effective — approach relies on the "incognito" or "private" browser mode that prevents local browsers from caching cookies or the browsing history, but still discloses the organization's IP address and doesn't protect the device from web-borne attacks.

Another common approach involves setting up a "dirty box" or "danger web," a machine or small network not connected to the corporate LAN. The extensive setup and cleanup procedures required for each web session render this approach slow and inefficient.

Some firms deploy Virtual Desktop Integration (VDI) solutions or other virtualization software. While it provides an additional security layer, this solution is known to put a strain on IT budgets, due to the associated hard and soft costs.

Methods to Protect Fraud Investigators Online

INCOGNITO MODE	DIRTY BOX	VIRTUALIZATION	CLOUD BROWSER
• Standard feature of local browsers • Instills false sense of security • High risks of exploit and attribution	• Disconnected from corporate IT • MTTR suffers due to maintenance requirements • Risk of exploit and attribution	• Web code gets filtered before processed locally • High hard and soft costs • Limited risk of exploit and attribution	• Centrally managed offsite • No risk of exploit or attribution • 100% isolation of all web content

A Centrally Managed Cloud Browser for Improved Efficiency

A browser built in the cloud, provided as a service offsite by a third-party vendor, enables IT security leaders in financial firms to optimize security and save money at the same time. Browser isolation shifts the attack surface offsite to a secure cloud container. Each session is built on a fresh instance of the browser. No cookies, trackers, or other cached data persist across sessions.

All web code is executed on a remote host configured for security and data compliance. As code is rendered in the isolated environment, authorized content is converted to an encrypted and interactive display of the page in the cloud. The content is viewed remotely by the endpoint device over a benign, non-HTTP protocol. Users get full fidelity access to web content, without the risk.

Because it enables IT to centrally manage credentials, permissions and policies, the cloud browser model makes it easy to meet and monitor fraud-relevant compliance requirements:

- Administrators can enforce acceptable use policies, to prevent analysts from abusing the tool
- No longer does IT have to manage URL exceptions on a case-by-case base, a process known to introduce additional risks
- While conducting research online, analysts and investigators remain completely anonymous to prevent third parties from identifying them or polluting research results
- Encrypted verbose audit logs allow for internal oversight of investigator or research-related web activities

Through effectively disconnecting them from the dangers of the web, the remote browser allows research teams to quickly access websites and apps as well as examine files online and offline.

Users now can easily capture, annotate, and store web-based research materials at arm's length in the cloud, or download a (sanitized) version of a file for further inspection locally.

Silo: The Compliance-Ready Cloud Browser

Authentic8 has pioneered the secure remote browser category since 2010 with Silo, its secure cloud "Browser-as-a-Service." Authentic8's policy-controlled browser in the cloud was one of the first SaaS solutions to easily overcome compliance concerns in the financial services sector, as more CISOs and compliance officers realized the risks associated with the continued use of local browsers.

Financial service organizations deploy Silo with different policies and points of integration to provide the following advantages.

- **Improved security:** The browser runs in the cloud, on servers managed by Authentic8. Each session is built on a fresh instance of the browser. Web exploits are neutralized outside the organization's IT perimeter.
- **Reduced costs:** The burden of managing the browser shifts to the provider; patching is no longer required, browser versions and approved plugins are all centrally updated. Silo deploys without delay and doesn't require manual cleanup.

- **Centralized governance:** Silo provides management hooks that require only one-time implementation. This model allows for a unified view into all user activity during a web session, for centralized audits and compliance reviews.
- **"Anytime, anywhere" access:** Many organizations are moving to a telework model. Silo enables them to make this move without loss of security or control. Users can perform their functions from anywhere, without eroding security posture or IT's ability to enforce governance and compliance.

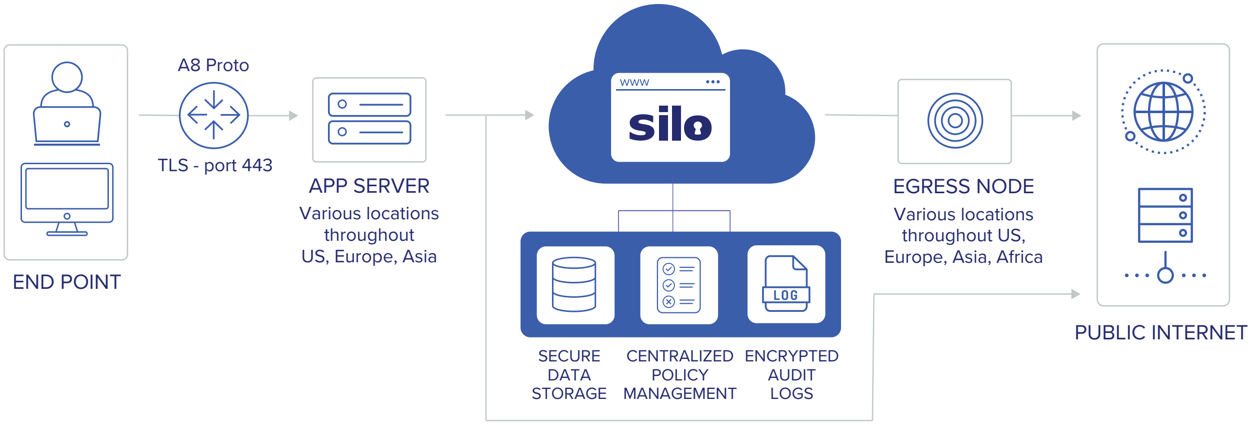
Silo Research Toolbox: Secure Online Fraud Investigations

For dedicated financial fraud research analysts, Silo Research Toolbox provides additional capabilities for carrying out investigations on the open, deep, and dark web. Silo Research Toolbox is a managed attribution and research suite for the Silo cloud browser.

Silo Research Toolbox allows researchers to spoof their true location across different, configurable geo-locations, manipulate their hardware and software fingerprints, and to collect, annotate, and securely store internet-based PAI (Publicly Available Information). Toolbox also includes tools for post-fetch language translation, link tracking, as well as web code and HTTP traffic analysis.

- **Cloud-based investigation platform:** Secure isolation, managed attribution, post-facto language translation, and auditing without the risk of burning online identities or system compromise.
- **Shorten time to intelligence:** Reduce time, costs, and resources needed to deploy, manage, and conduct successful fraud investigations. Capture, annotate, store, and share evidence securely with other members of the team.
- **Investigators stay safe:** Analysts remain anonymous, since the IP in the cloud is the only identifying data exposed to the open web.
- **Streamline IT costs:** Eliminate the need for costly dedicated network infrastructure, IT URL exceptions, and machine re-imaging.
- **Dark Web Research:** Securely and anonymously gather online intelligence from open, deep, or dark web sources.

Silo Research Toolbox deployment scenario with remote egress nodes for increased anonymity


END POINT
A8 Proto
TLS - port 443
APP SERVER
Various locations throughout US, Europe, Asia
www
silo
SECURE DATA STORAGE
CENTRALIZED POLICY MANAGEMENT
LOG
ENCRYPTED AUDIT LOGS
EGRESS NODE
Various locations throughout US, Europe, Asia, Africa
PUBLIC INTERNET

Conclusion

Deploying a secure browser in the cloud for fraud research and investigation teams improves productivity and allows financial institutions to make their online investigations part of a cohesive cybersecurity strategy. It enables firms to remove existing hurdles to adequately and efficiently access web resources and maximize IT security for their analysts and investigators. With Silo and Silo Research Toolbox, financial institutions can protect end users from malicious web content, streamline their compliance programs, and significantly reduce mean time to resolution (MTTR) when researching and filing SARs.

[1] 31 CFR 1010.230, https://www.fdic.gov/regulations/laws/rules/8000-1400.html#fdic8000fra1010.230

[2] Banking Exchange. "Cleaning up money laundering compliance aftermath" Banking Exchange, 28 February 2018, https://www.bankingexchange.com/news-feed/item/7399-cleaning-up-money-laundering-compliance-aftermath.

[3] Verizon. "2018 Data Breach Investigations Report 11th edition." Verizon Enterprise Solutions, https://verizonenterprise.com/DBIR2018

[4] Authentic8 Customer Loyalty Survey performed by Beacon Technology Partners, December 2017

[5] ACAMS: "The True Cost of AML Compliance" Study 2017, https://www.brighttalk.com/webcast/12373/276801

[6] ACAMS https://www.acams.org/aml-training-web-seminars/

[7] Scott Petry: The Architecture of the Web Is Unsafe for Today's World, April 19, 2017, https://www.darkreading.com/endpoint/the-architecture-of-the-web-is-unsafe-for-todays-world

ABOUT | Authentic8 is redefining how enterprises conduct business on the web with the Silo web isolation platform. Silo insulates and isolates all web data and code execution from user endpoints, providing powerful, proactive security while giving users full, interactive access to the web. Silo also embeds security, identity, and data policies directly into browser sessions, giving IT complete control over how the web is used. Commercial enterprises and public sector organizations use Silo solutions to provide secure web access, to control web data, apps, and workflows, and to conduct sensitive online research. Try Silo now at www.authentic8.com.