silo
By Authentic8

WHITE PAPER
FINANCIAL SERVICES

Guide to Secure Fraud Investigations

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 to 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, including the deep and dark web. The resulting security gap can expose employers to data breaches, regulatory fines, class action, personal liability lawsuits, and significant reputational risks.

Many banks face no-win situations: Block access to suspicious areas of the web in the name of security, relax security on a per-request basis to maintain analyst productivity, or create purpose-built environments that add significant complexity and overhead. 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 white paper examines comprehensive solutions for protecting financial fraud investigation specialists when they go online. To do their job productively, analysts require a purpose-built research platform with these capabilities to keep them anonymous and secure:

- Full isolation of web content
- Access to all parts of the web, including open deep and dark
- Anonymity
- Integrated tools for streamlined access / analyze / capture
- Complete audit and oversight

This white paper explains how and why outsourcing the risk with a compliance-ready, purpose-built research platform has emerged as a viable alternative to DIY investigation platforms.

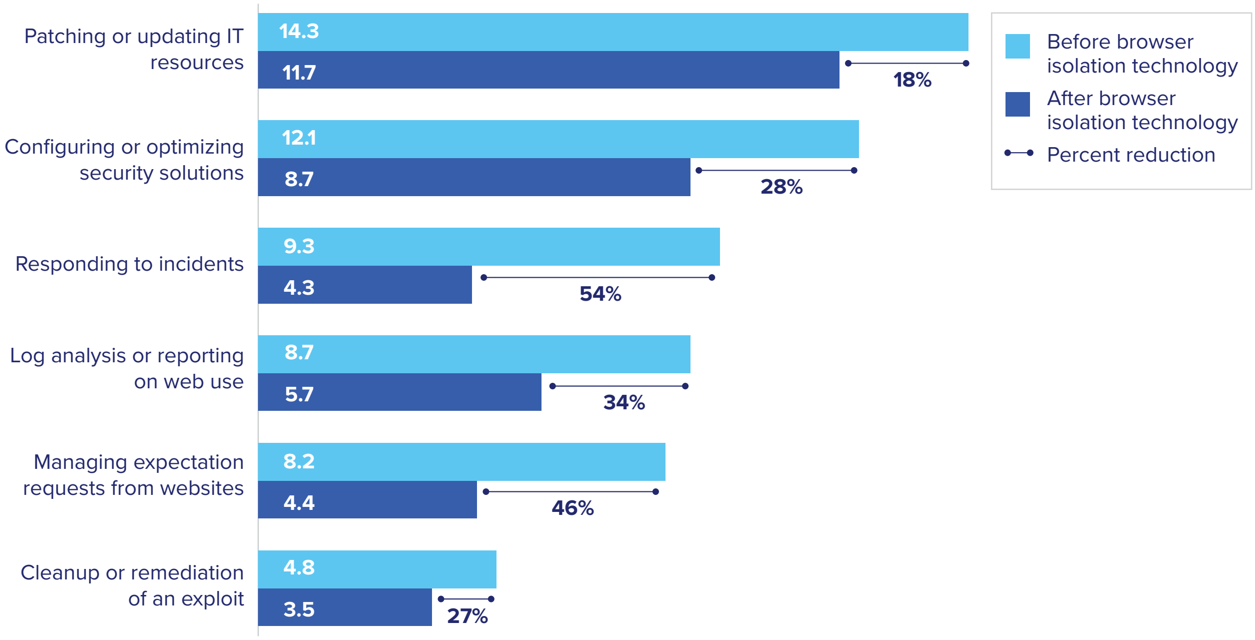
Your Team, In the Trenches – and Exposed

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 web browsing as their primary vehicle 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 investigation 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]

% Reduction in Person-Hours/Month, through the introduction of isolation browser technology.



Investigators rely on IT and security teams 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 both burdensome to use and prone to security breaches.

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 or security—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.

Your Online Activity: Liability for Fraud Research

The basic interaction model of the web has created an environment where a simple page view request can lead to system exploits, data egress and de- anonymization. The IP address disclosed to the world 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.

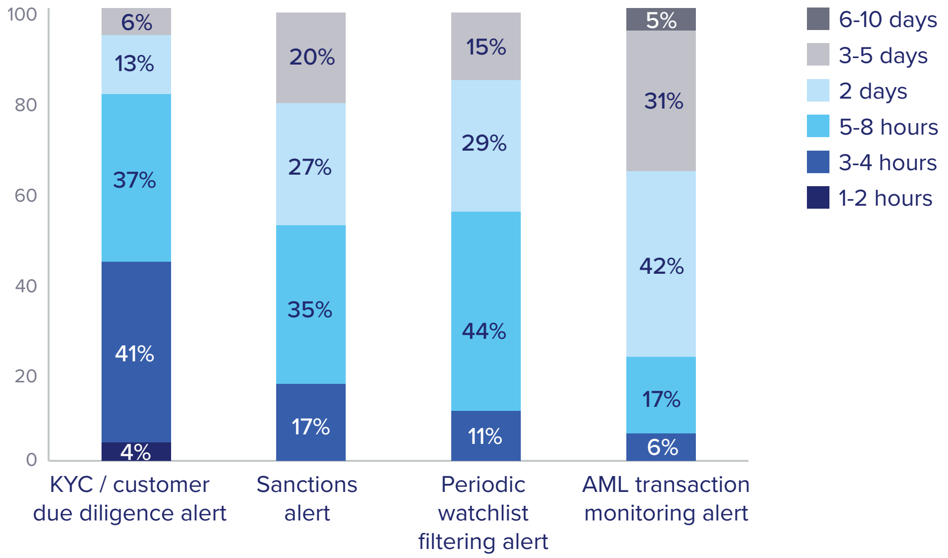
How can CISOs and risk managers address those issues to protect research analysts better and improve overall efficiency of the compliance team in the process?

Which Risks and Threats Are Financial Researchers Facing on the Web?

Analysts must collect hundred s of data points across a wide variety of 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 browsers from caching cookies or the browsing history, but still discloses the organization’s IP address and doesn’t protect the device from web-born 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.

Comparison: Methods to Protect Fraud Investigators Online

	Incognito Mode	Dirty Box	Virtualization	Web Isolation
Remarks	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
Setup & Config	👍👍👍	👎👎	👎👎👎	👍👍👍
Protection from Exploits and Malware	👎👎👎	👍👍	👍👍	👍👍👍
Anonymity	👎👎👎	👎👎	👍👍	👍👍👍
MTTR Impact	👎👎	👎👎	👍	👍👍👍
Maintenance	👍👍👍	👎👎👎	👎👎👎	👍👍👍
Feature Learning Curve	👍👍👍	👎👎👎	👍👍👍	👎
Soft Costs	👍👍👍	👎👎	👎👎👎	👍👍
Hard Costs	👍👍👍	👎	👎👎👎	👍👍👍
Compliance	👎👎👎	👍	👍👍	👍👍👍

Web Isolation for Improved Security and Efficiency

Remote, cloud-based execution of web code, provided as a service offsite by a third-party vendor, enables IT security leaders in financial firms to optimize security and save money. Web isolation shifts the attack surface offsite to a secure cloud container. Each session is a fresh new instance, and 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 web isolation model makes it easy to meet and monitor fraud-relevant compliance requirements:

- Administrators can enforce acceptable use policies, to prevent analyst 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 and support compliance requirement
- Through effectively disconnecting them from the dangers of the web, web isolation 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 Web Isolation Platform

Built on a philosophy of “trust nothing,” Silo separates the things you care about, like apps, data and devices, from the things you cannot trust, like external websites, external users and unmanaged devices.

Silo executes all web code in a secure, isolated, cloud-hosted environment that is managed by policy, to provide protection and oversight. Organizations worldwide use the Silo Web Isolation Platform to:

- Secure data from leaking to compromised endpoints
- Shield web apps from attacks or unauthorized access
- Protect end-user devices from malicious web code
- Deliver true privacy to confound online tracking

Silo for Research: Secure and Anonymous Financial Investigations

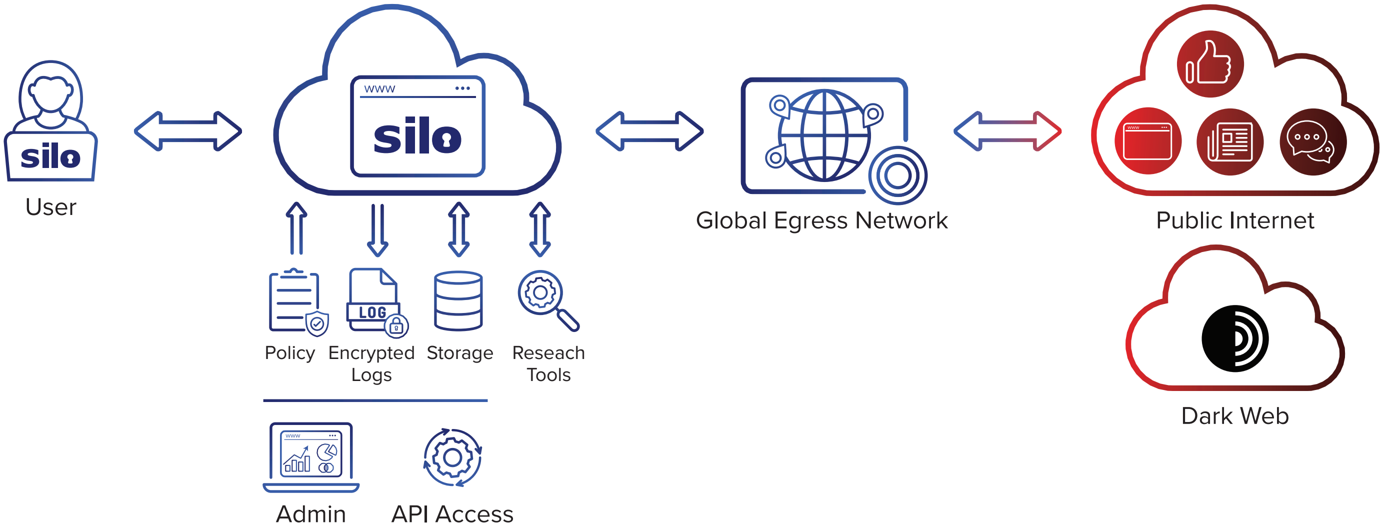
Silo for Research (Toolbox) allows financial investigators to safely, efficiently and anonymously conduct research on the open, deep and dark web.

Silo gives users an on-demand, highly secure and anonymous environment to conduct research, collect evidence and analyze data.

Teams can accomplish their goals without introducing risk to the organization. All analyst activity is logged and encrypted so compliance teams can be sure the tools are being used appropriately.

Primary Benefits

- **Full isolation:** All web code is executed on Silo servers, not end-user devices
- **Managed attribution:** Configure the browser fingerprint and egress location
- **Streamline dark web access:** Provision one-click access to the dark web for anyone
- **Workflow enhancements:** Integrated tools for content capture, analysis and storage
- **Non-repudiable logs:** Encrypted audit logs of all web activity are captured in one place and easily exported
- **Cloud-based solution:** Turn-key, cloud-hosted solution that creates a clean instance every time



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

Conclusion

Deploying a purpose-built, cloud-based research platform 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 for Research, financial institutions can protect end users from malicious web content, remain anonymous, 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, http://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://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey

[6] ACAMS https://risk.lexisnexis.com/global/en/insights-resources/research/the-true-cost-of-aml-compliance-european-survey

[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

silo
By Authentic8

CONNECT WITH US

+1 877-659-6535
www.Authentic8.com

PROTECT THE THINGS YOU CARE ABOUT FROM THE THINGS YOU CANNOT TRUST

Authentic8 enables anyone, anywhere, on any device to experience the web without risk. The Silo Web Isolation Platform by Authentic8 separates the things you care about like apps, data and devices, from the things you cannot trust like public websites, external users and unmanaged devices. Silo executes all web code in a secure, isolated environment that is managed by policy, to provide protection and oversight.

Today, the world’s most at-risk organizations rely on Silo to deliver trust where it otherwise cannot be guaranteed.