silo

SECURE AML RESEARCH: CRACKING THE EFFICIENCY CODE

Maximum compliance at minimum cost. The problem with protecting BSA/AML teams on the web - and how financial firms are solving it.

Executive Summary

In the financial sector, the in-house specialists tasked with Bank Secrecy Act (BSA) compliance, Anti-Money Laundering (AML) and anti-fraud investigations online are considered most at risk of web-borne exploits and attacks. While protective measures can limit other employees' exposure to web-borne threats, AML analysts and investigators still need to access unknown, uncategorized, and potentially unsafe resources to do their job. The resulting security gap puts their employers at risk of 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. AML analysts will not be productive if IT disconnects their machines from the network because they have been infected. But blocking AML workflows 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.

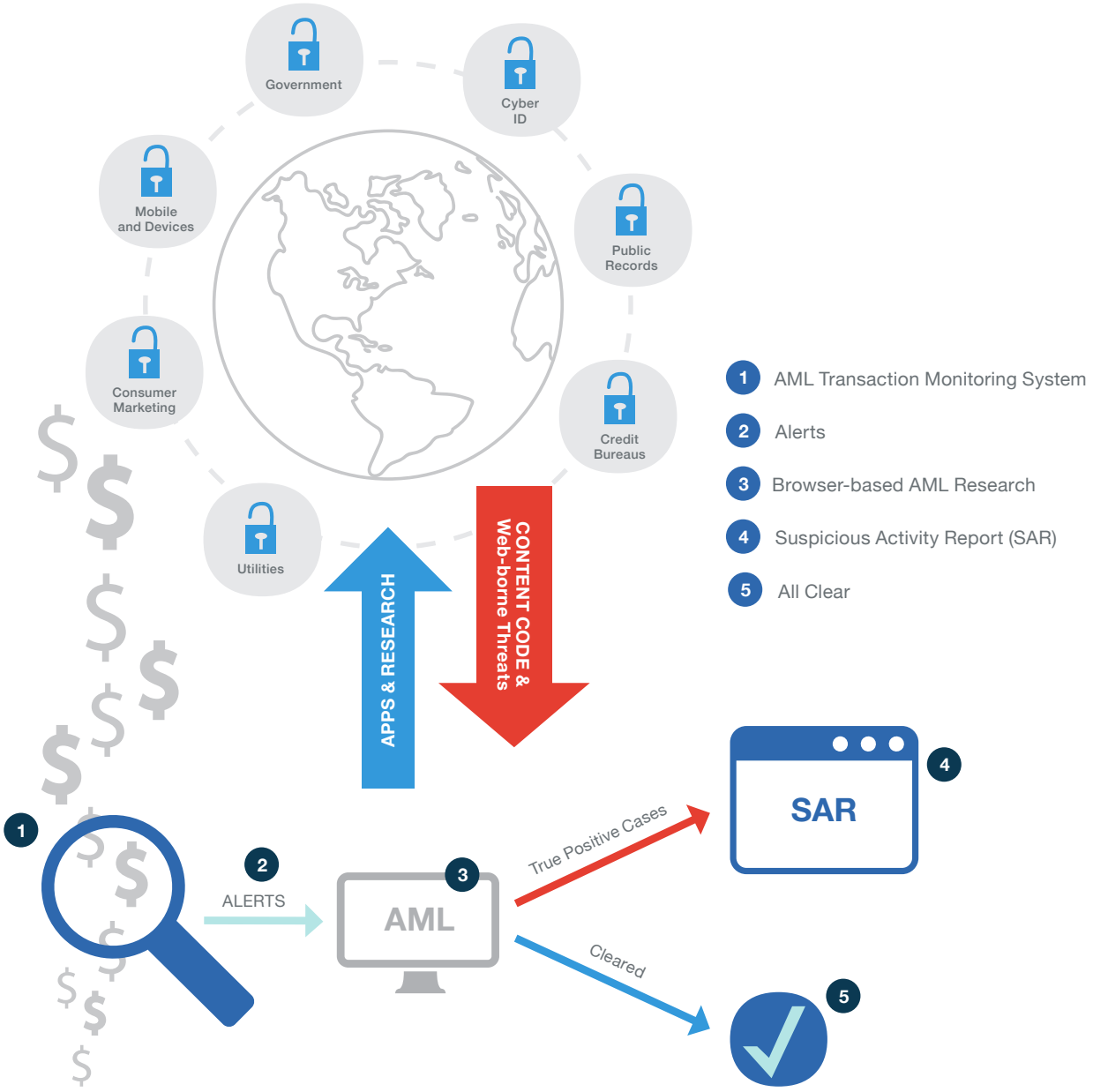
This whitepaper examines a comprehensive solution for protecting BSA/AML specialists when they go online. To do their job productively, analysts require a secure remote browser and these capabilities:

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

This whitepaper explains how and why outsourcing the risk with compliance-ready remote browser isolation has emerged as a viable solution.

Your Team, In the Trenches – and Exposed

The pressure on financial institutions to ensure compliance with federal BSA/AML 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]



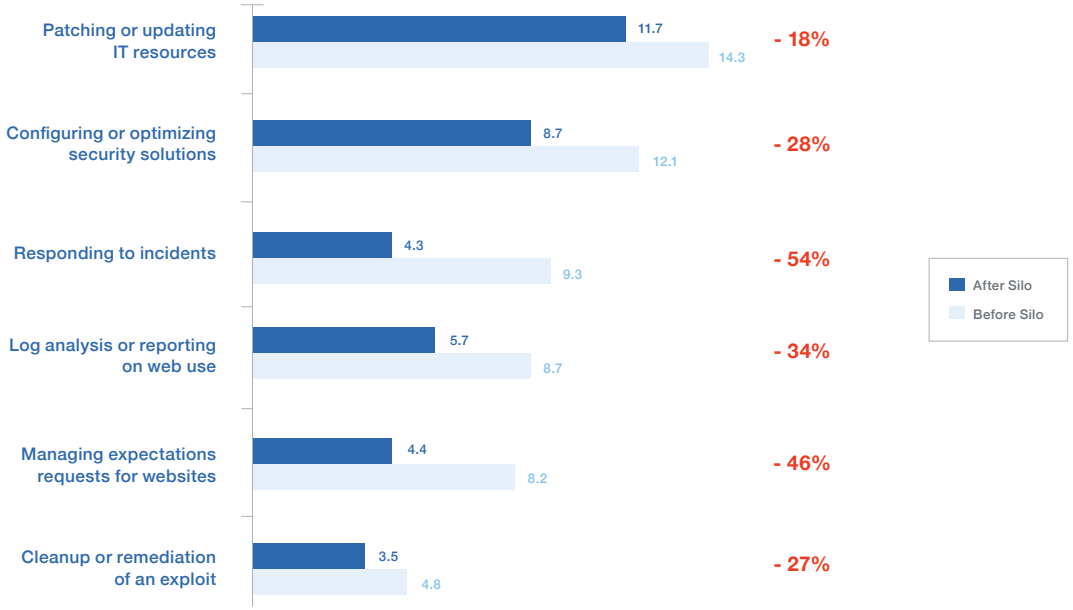
[1] 31 CFR 1010.230 https://www.fdic.gov/regulations/laws/rules/8000-1400.html#fdic8000fra1010.230

[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.

The professionals handling BSA/AML compliance-related tasks use the web browser as their primary research 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 AML teams are still stuck with inefficient and vulnerable tools. Such solutions burden IT with support challenges and oversight requirements that are difficult and costly to manage.

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

% Reduction in Person-Hours/Month, through introduction of Silo the cloud browser



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

BSA/AML specialists 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. AML professionals 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.

[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

The Local Browser: Liability for BSA/AML 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 the BSA/AML analysts better and improve overall efficiency of the compliance team in the process?

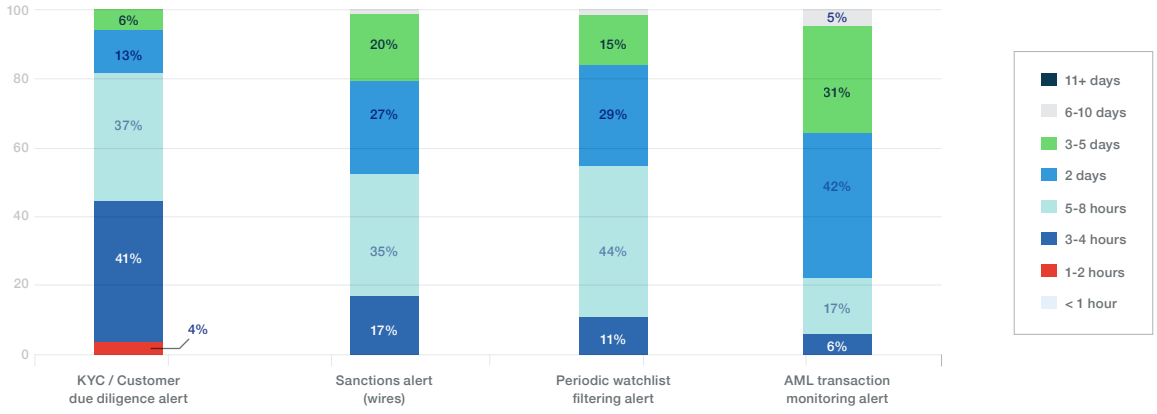
> **"We don't have to spend resources on building new machines, having to spend hours and hours cleaning machines. We probably had one or two viruses that we had to clean up every quarter, so you're talking about several days of work throughout the year, and whatever the rate was per engineer that we have, that's what we would save."**
>
> *— IT Admin at FiServ customer*

Which Risks and Threats Are BSA/AML Researchers Facing on the Web?

According to Forrester Research, BSA/AML 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 AML missions should mitigate the following risks:

[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

- **Risk of Malware Infection:**
  Routine tasks of AML or Anti-fraud investigations, 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:**
  BSA officers/managers and SAR analysts should be able to conduct BDD and EDD 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.

> **"We had a kludgy solution before where we used a virtualized workstation that was still in our environment and we would whitelist. We have various layers of security on our web browsing and we would essentially exempt them from that. There's a lot of overhead in maintaining those virtual workstations."**
>
> *— Sr. IT Admin at FiServ customer*

Traditional Methods: Not Quick. Still Dirty.

Traditional approaches to mitigating the online risks for BSA/AML 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-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 BSA/AML Investigators Online

	INCOGNITO MODE	DIRTY BOX	VIRTUALIZATION	CLOUD BROWSER
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 exploitation and 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	👎👎👎	👍	👍👍	👍👍👍

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 and delivered to the endpoint device over an alternate, non-HTTP protocol. Users get full fidelity access to web content.

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

- Admins 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 research BSA/AML-related web activities and support compliance requirement.

Authentic8 has pioneered the secure remote browser category since 2010 with Silo, its secure cloud "Browser-as-a-Service". With Silo, no web code can touch the local network or machine – only benign, secure pixels.

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

> **"[O]ne of the single most significant ways an enterprise can reduce the ability of web-based attacks on users to cause damage."**
>
> *— Gartner Group*

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. Authentic8 customers have reported MTTR reduction rates of more than 50%.

1. Isolated Client
2. Browser in the cloud
3. Secure offsite storage
4. Onsite network integration
5. IT
6. Sets policy
7. Encrypted logs

Silo: The Compliance-Ready Cloud Browser

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. For BSA/AML analysts, the remote secure browser delivered by Authentic8 provides distinct advantages:

- **Improved security:** The browser runs offsite, 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.
- **Non-attribution:** Users remain anonymous, since the IP of the remote host is the only identifying data exposed to the open web.

Conclusion

Deploying a secure browser in the cloud for their BSA/AML/Anti-fraud teams improves productivity and allows financial institutions to make their online investigations part of a cohesive cybersecurity strategy. It enables them to remove existing hurdles to adequately and effciently access web resources and maximize IT security for their analysts and investigators. With Silo, they can streamline their compliance program and significantly reduce mean time to resolution (MTTR) when researching and filing SARs, while saving money at the same time.

Find out more about Silo, the cloud browser. Try Silo here and connect with one of our financial services specialists:

www.authentic8.com/AML