silo

AML INVESTIGATORS:
WHEN ANONYMITY IS PARAMOUNT, CAN YOU TRUST YOUR BROWSER?

BSA/AML SPECIALISTS RISK EXPOSURE

Local browsers put compliance at risk

Financial services firms who violate AML compliance requirements by neglecting to report suspicious transactions risk paying a higher price than ever. Worldwide, regulators impose penalties in the million-dollar range, revoke banking or brokerage licenses, and also bring criminal charges against individual compliance officers.[1]

Enforcement reports show that such entities found themselves under investigation by regulators because their AML programs lacked proper procedures and tools. When AML managers cut corners, core AML requirements - such as accuracy [2] and completeness in reporting suspicious activities - often take a backseat to budget or expediency considerations.

The introduction of FinCEN's Beneficial Ownership Requirements for Legal Entity Customers has increased the pressure on the finance industry. Much of the burden is shouldered by analysts and investigators, due to the additional background research required - most of which is conducted using web resources and apps.

To properly accomplish their mission online, AML specialists rely on the browser as the main tool. Paradoxically it is that same tool that puts BSA/AML compliance at risk.

NO PROTECTION THROUGH "INCOGNITO" MODE

Betrayal by browser: How adversaries get tipped off to AML research

The problem: when BSA/AML compliance managers and analysts access the web, they lack adequate protection online that allows them to conduct their research anonymously and efficiently and also shields them from web-borne exploits.

Instead, they are betrayed by their browser. Many AML analysts are still using a local browser to conduct their research. Due to the inherent security weaknesses of traditional web browsers, this means they risk disclosing their (firm's) identity online. This lack of anonymity is known to invite pinpointed attacks [3] and to potentially tip off the subjects of their investigation.

AML research foiled, SAR never filed - this is how it happens:

"The target/subject/ entity is aware that they are being looked at by someone. That alone might be enough to spook a bad guy and send him running."

—Kevin Sullivan, CAMS, Founder, The AML Training Academy

Using the browser's "incognito" or "private browsing" mode does not provide any protection against compliance violations. One consequence of this common misconception [4] and a lack of proper precautions are inaccurate or contaminated research results. Another is potentially exposing their employer to legal action.

[1] SEC: 1 In the matter of Chardan Capital Markets LLC - https://www.sec.gov/litigation/admin/2018/34-83251.pdf

[2] Accuracy in AML Online Research: How Inaccurate AML Reporting Draws Regulator Scrutiny. https://www.dropbox.com/s/d8y9mqnoll1e8lu/2018-07-06%20AML%20Online%20Research%20-%20How%20Inaccurate%20AML%20Reporting%20Draws%20Regulator%20Scrutiny.pdf

[3] Case Study: Watering Hole Attacks on BSA/AML Compliance Professionals - https://www.dropbox.com/s/9uk1x8y0dqgl6im/2018-05-21%20Watering%20Hole%20Attacks%20on%20BSA-AML%20Compliance%20Professionals.pdf

[4] Your Secrets Are Safe: How Browser's Explanations Impact Misconceptions About Private Browsing Mode. https://www.blaseur.com/papers/www18privatebrowsing.pdf

When filing Suspicious Activity Reports (SARs) on the same platform where they use a local browser, for example, AML specialists may commit a criminal federal offense by unintentionally disclosing a SAR and the identity of its subject to unauthorized third parties online.[4]

Wanted: a browser that empowers AML research in full anonymity, while providing maximum security - without sacrificing speed and efficiency.

SILO: ANONYMITY. SECURITY. EFFICIENCY.

Cloud browser for AML: trusted by banks, FIs and regulators

Leading firms now provide their compliance managers or FIs with a cloud browser to ensure full anonymity and protection from ALL web-borne exploits during KYC, BDD, EDD, negative news research, or in-depth investigations.

Silo, the cloud browser provided as a service on Authentic8 servers, is built fresh from a clean image at the start of each web session. It shields AML researchers and their employers through:

- **Complete anonymity (or managed attribution for in-depth investigations):** Because only Authentic8's IP addresses are used, attribution to AML analysts, networks or organizations becomes impossible. Attempts by adversaries to "browser fingerprint" a site visitor will fail.
- **Disconnect from phishing, malware and download infections:** With Silo, all content is processed offsite, in an isolated cloud container. No code from the web can touch the endpoint. Only visual display information (pixels) is passed back to the user, through an encrypted connection. *This effectively disconnects AML teams from the web's risk zone.*
- **Prevention of data leaks and unlawful disclosure:** Silo keeps malware and spyware off local machines or networks, for example when visiting infected websites while conducting negative news research. BSA/AML team members can safely download and store documents for further inspection in the cloud, and for fast and easy (partial) inclusion when filing a report, using Silo's convenient screenshot and markup tool.

THIS BROWSER HAS YOUR BACK.

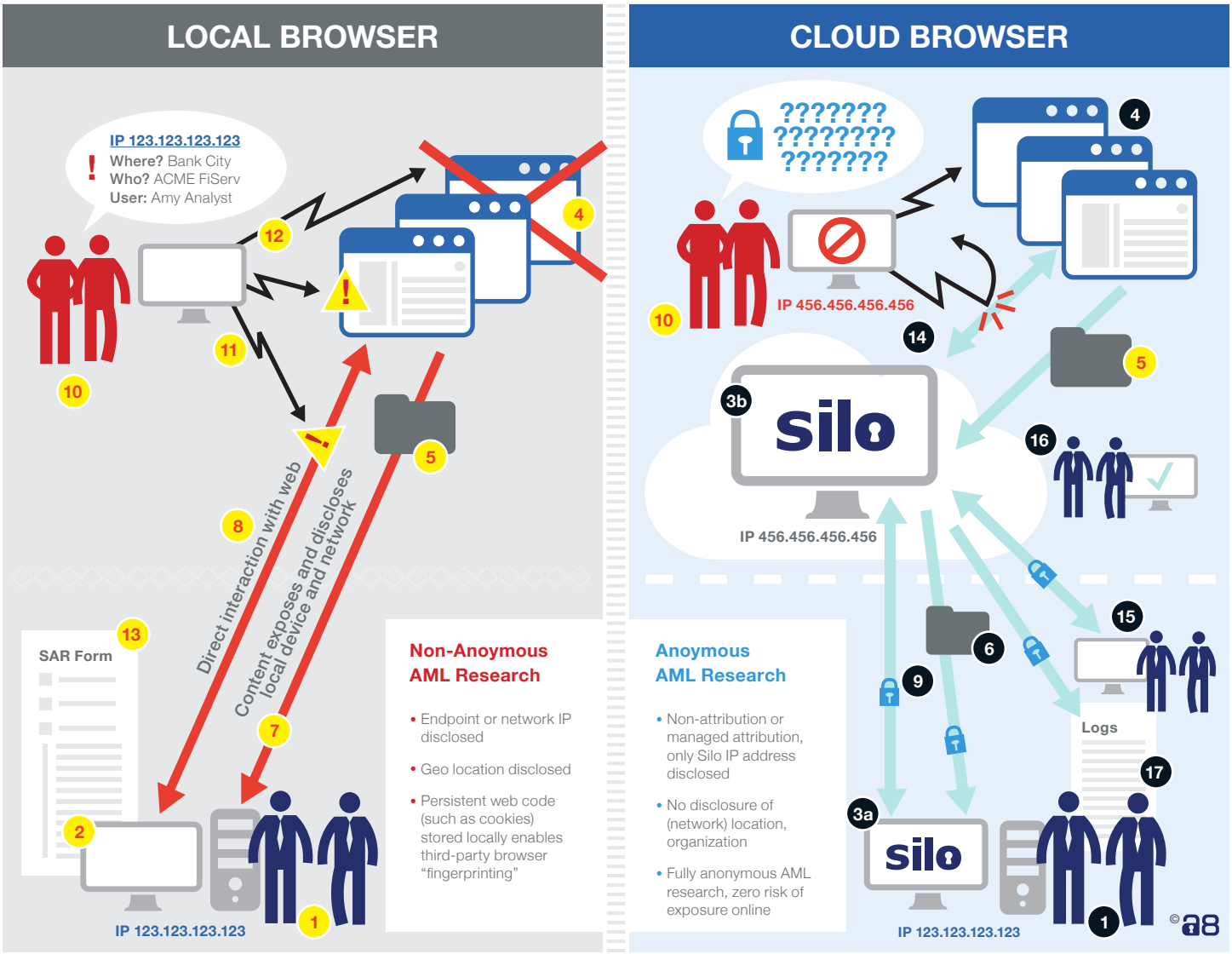
Compliance-friendly auditability and reduced MTTR with Silo

Silo customers report significant productivity improvements for their compliance teams. Silo makes filing SARs faster and allows them to close more cases in less time. Compliance-ready logs enable the firm to easily monitor and audit steps taken during the AML team's online research.

To find out more, connect with our Financial Services team:

www.authentic8.com/AML

[4] See FinCEN, Unauthorized Disclosure of Suspicious Activity Reports - https://www.fincen.gov/resources/statutes-regulations/guidance/unauthorized-disclosure-suspicious-activity-reports



1. AML analysts
2. Local browser
3a. Visual display information (pixels) only
3b. Cloud browser instance
4. Websites & apps
5. File download for inspection, documentation
6. Safe off-site file inspection in the cloud
7. Local file storage & inspection = exposure to malware & spyware
8. IP address disclosed to websites, web content processed locally = exposure to exploits & data leakage
9. Full anonymity & non-attribution through Silo-assigned IP address
10. Adversaries
11. Disclosure of AML analysts' IP/network invites pinpointed attacks
12. Disclosure of ongoing AML research leads to contaminated results became adversaries can alter/delete web resources
13. Risk of SAR (subject) disclosure through data leaks or breaches
14. Silo browser isolation with centrally managed security completely shields local FiServ IT from exploits & de-anonymization attempts
15. IT - policy, integrated credentials management, freed up to focus on other critical security tasks
16. Authentic8 Silo Team — central cloud browser management 24/7 by security professionals
17. Auditability — readily available encrypted logs of AML online activities for IT, compliance managers & regulators

COMPANY HISTORY

Authentic8 is a company with history rooted in another. Postini was founded in 1999 by the Authentic8 co-founder, and the core business and technology team were key Postini personnel. Postini pioneered the idea that a cloud-based service could solve security and compliance problems with email, and back in 1999 this was heresy. But the model won out.

Authentic8 was founded in 2010 around a different idea, but the parallels with Postini are many. The company addresses a real problem with an innovative approach. The thesis is simple: as business apps move to the cloud, the browser becomes more important than ever. Yet it's an unmanageable resource. Silo was conceived to change that.

We have headquarters and Federal Operations in California, Washington DC and Berlin Germany. For further content use web, email or phone (US, International).

www.authentic8.com