CONTROL AND COMPLIANCE IN REGULATED SECURITIES INVESTMENT FIRMS

WEB FILTERING: THE BLACKLIST/WHITELIST FALLACY

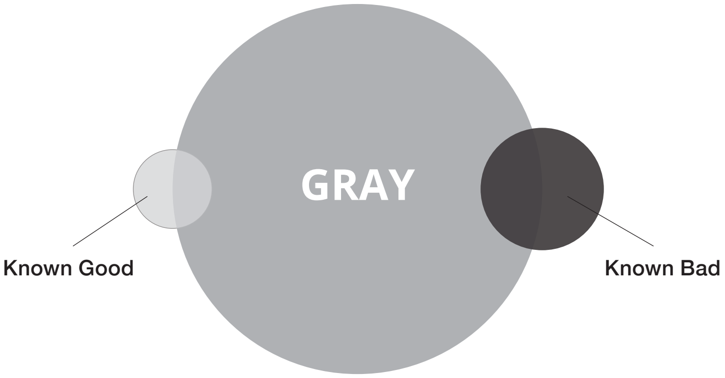
While the pressure is growing from the SEC's Office of Compliance Inspections and Examinations (OCIE) on firms to ensure compliance and remediate areas of cybersecurity weakness, alarming gaps remain.[1] In many firms, employees are still using a locally installed web browser as their primary tool to access sites and apps.[2] This has significantly increased the risk of web-borne exploits, data loss and non-compliant online behavior.

The reason is simple. The regular browser was not designed with security and compliance in mind. Among Chief Compliance Officers and IT administrators, it has become synonymous with loss of control and visibility over employee activities online. This is why many firms now follow the example of major financial services institutions and deploy Silo, Authentic8's secure cloud browser, to ensure centralized oversight and governance when employees go online.

WHY FIRMS FALL BEHIND

Growing Risks in the Web's "Gray Zone"

What has prompted this change? One major reason is the ineffectiveness and insecurity of URL filtering tools. Like other patchwork solutions aimed at mitigating the inherent security weakness of the local browser, they have proved inefficient as a backstop to prevent web-borne exploits.



The problem: Policing web use by blacklisting "bad" and whitelisting "good" web resources merely covers a narrow sliver of today's web. It misses the "gray" areas where users spend most of their time - the danger zones that harbor most critical risks. These risks arise from four sources:

- **The web changes too fast.** More than 1.9B websites (as of 12/2018), with nearly 400 new websites added every minute.[3] Even sites once categorized as "safe" may have fallen in the wrong hands since or are vulnerable to exploits because they run Flash, Java, Visual Basic or other web-based scripts.
- **Approved URLs harbor risk, too.** Today, 1 in 13 web requests lead to malware (up from 1 in 20 in 2016).[4] Millions of website visitors to the New York Times and the BBC, for example, were exposed[5] to ransomware exploit kits distributed via compromised online ads networks.

[1] SEC Office of Compliance Inspections and Examinations Announces 2019 Examination Priorities - https://www.sec.gov/news/press-release/2018-299 (Press Release 12/20/2018)

[2] Corporate Compliance Insights: A Persistent Threat in Financial Services - https://www.corporatecomplianceinsights.com/a-persistent-threat-in-financial-services/ (1/2/2019)

[3] Internet Live Stats - http://www.internetlivestats.com/total-number-of-websites/

© 2019 Authentic8, Inc. All rights reserved.

- **Site functionality evolves, and web filters remain static:** Online comment sections on approved sites, for example, pose additional compliance[6] risks for firms.
- **Web filters often get it wrong:** URL categorization relies on automated heuristic processes. Frequently, such systems mistakenly block access to work-relevant web resources. Defining exceptions for individual employees or whitelisting resources for the firm slows down important processes and puts an extra burden on IT.

NO VISIBILITY
NO CONTROL

The Local Browser, a Compliance Blind Spot

Secure Web Gateway (SWG) solutions and other blacklist/whitelist tools require “compliance vs. productivity” tradeoffs[7] that investment firms can no longer afford, given the growing scrutiny from regulators. At the same time, many compliance teams still don’t have visibility or control over what actually happens when team members enter the web’s growing gray zone.

Local browsers, which are notoriously difficult to manage, secure and monitor, have created this widening blindspot for compliance managers and IT administrators. As a result, their firms run the risk of compliance violations and data breaches every time employees upload a file to a (third-party) cloud storage service, log into webmail from the office or remotely, or (unknowingly) expose the firm to spyware from a website approved for research.

> **Local browsers [...] have created this widening blindspot for compliance managers and IT administrators. As a result, their firms run the risk of compliance violations and data breaches every time employees upload a file to a (third-party) cloud storages service, log into webmail from the office or remotely, or (unknowingly) expose the firm to spyware from a website approved for research.**

REGAIN CONTROL

Silo, the Cloud Browser: Central Oversight and Governance

How can firms maximize security and compliance when employees access the internet, without sacrificing speed and convenience? Leading organizations in the financial services sector found the answer in Silo, the secure cloud browser.

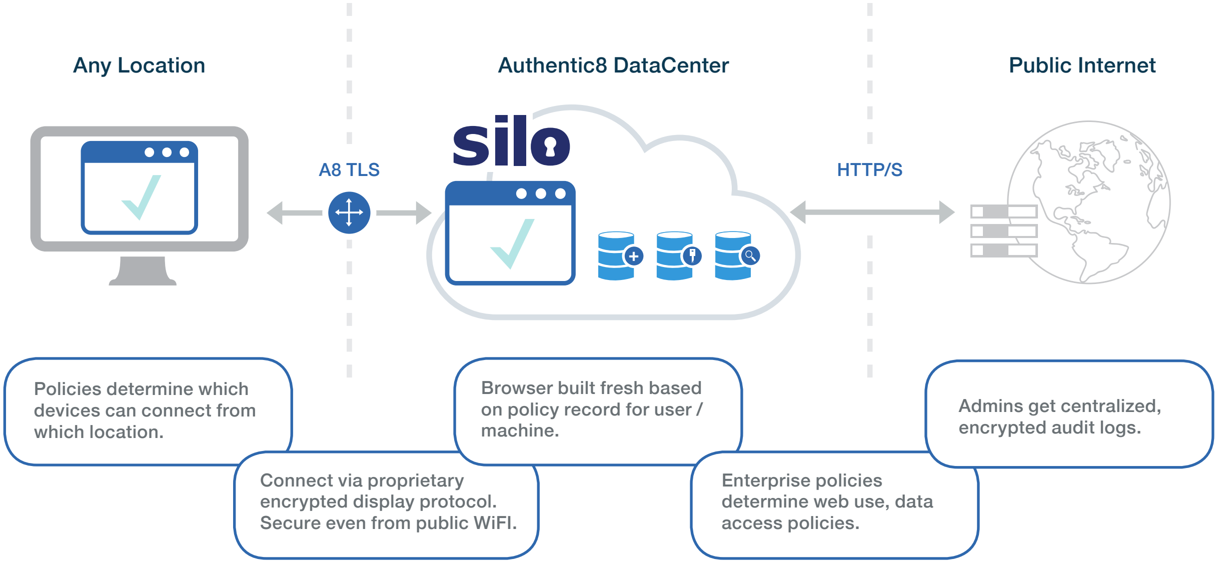
Here’s how it works: With Silo, all web code is processed in the cloud, on a remote host configured for regulatory compliance and data security. Firms remain protected no matter what websites employees visit, because no code from the web can reach the local device. Customers report an elimination of break-inspect and web filtering gateway infrastructure.

[4] Symantec 2018 Internet Security Threat Report - http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf

[5] When URL Filtering Fails, This Browser Has Your Back - https://authentic8.blog/when-url-filtering-fails-this-secure-browser-has-your-back/ (Authentic8 Blog)

[6] SEC Division of Investment Management: Guidance on the Testimonial Rule and Social Media - https://www.sec.gov/investment/im-guidance-2014-04.pdf

[7] Whitepaper: A Cloud Browser Built for Compliance and Control. How Financial Firms Turn the Web from a Liability Into an Asset - https://info.authentic8.com/financial-safe-secure Authentic8 (01/2019)



Policies determine which devices can connect from which location.

Connect via proprietary encrypted display protocol. Secure even from public WiFI.

Browser built fresh based on policy record for user / machine.

Enterprise policies determine web use, data access policies.

Admins get centralized, encrypted audit logs.

Throughout the financial services industry, CCOs and IT are now deploying Silo to maintain oversight and governance when employees go online. No more blind spots or erroneous “site not approved” roadblocks with this browser - with Silo, firms no longer need to accept a tradeoff between control/governance and risk/productivity.

SILO HAS YOUR BACK.

Win-Win-Win for Compliance, Productivity and IT

Because each Silo session is built with embedded policies pre-defined by IT or the compliance team, oversight, governance and data protection are ensured each time employees use the web.

- Research analysts, investment managers and administrative staff get a secure and personalized browser that enables them to leverage the powers of the web without putting the firm at risk.
- CCOs and IT administrators get a compliance-ready browser that is centrally managed and gives them control and oversight over all employee activities on the web.

Device access, websites, content types, credentials and data operations are centrally managed, which prevents IT bottlenecks and minimizes risk when onboarding/offboarding team members. All user actions are logged and encrypted, which makes it easy for regulated entities to “promptly comply” with SEC requests and conduct compliance reviews.

In regulated investment firms, Silo provides a win-win-win solution for users, compliance managers and IT admin alike.

TRY SILO YOURSELF:

www.authentic8.com