LOCAL BROWSERS: HIGH-RISK HOLDOVER FROM IT's PAST

Regulated securities investment firms have outsourced many, if not most, of their critical IT tools. From data aggregation and market analysis software packages, to buy side / sell side trading programs, and to risk management, compliance and IT security solutions, essential functions have migrated to browser-centric web services and cloud apps. The goal: cost savings and increased agility in a highly competitive market.

For successful firms, external IT resources have become essential for conducting business. Regardless of whether web apps are accessed by back-office personnel or the investment team, from the local network or remotely, firms rely on the web browser as their primary tool to view, consume, and manipulate data.

Which functions are most impacted by the move to web services and the cloud[1]? Industry insiders point to the following areas:

- **Infrastructure:** Private, public and hybrid cloud adoption has grown steadily, with alternative investment firms leading the push for a cloud-first strategy.
- **Applications:** Software-as-a-Service (SaaS) has become a quasi-standard for financial applications, ensuring connectivity between global offices.
- **IT Security:** Most firms rely on external cybersecurity expertise and tools to protect their digital assets, due to a dynamically evolving threatscape and the lack of qualified IT security personnel.

CCOs UNDER PRESSURE

More Web Apps. More Cloud. More Complexity.

Decentralized apps hosting a firm's sensitive data in the cloud, accessed by various personnel from different locations, all create new layers of complexity. This puts an extra burden on compliance and IT leaders. One chief concern among Chief Compliance Officers and IT administrators facing this trend: "Loss of control.[2]"

Compliance leaders have good reason to be worried. The pressure from federal and state regulators has been steadily growing over the past two years. By subjecting a whopping 17% of registered investment advisers to OCIE examinations in 2018, the SEC exceeded its own ambitious goal (15%) in this group alone for this year.[3] CCOs, CISOs and CTOs have been put on notice.

PROBLEMATIC LEGACY

The Browser as Compliance Blind Spot

The regular, locally installed browser ironically has become the weakest link in the chain, synonymous with increased risk, loss of control and compliance violations.[4]

Investment firms are increasingly aware that they lack adequate oversight and control to ensure compliance and data protection when their employees and contractors connect to the web.

The reason is simple. The traditional browser was not designed with security and compliance in mind.

An anachronistic holdover[5] from the 1990s rush to the web, the browser's architectural flaws and inherent weaknesses make it notoriously difficult to manage, monitor, and secure against web-borne exploits. This creates a dangerous blind spot for the compliance team and IT.

FALSE SENSE OF SECURITY

How the Web's Gray Zones Put Your Firm at Risk

Every time team members go online to conduct research, check webmail, post on social media platforms, or use cloud storage services, the vulnerabilities of the regular browser leave their firm exposed to the risk of data breaches and compliance violations.

Today, 1 in 13 web requests lead to malware, up from 1 in 20 in 2016.[6] One costly consequence of clinging to the outdated local browser model is that it necessitates IT security point solutions (examples: AV software and Secure Web Gateway devices on the local network) that lull users into a false sense of security.

Many of these tools go back to the same bygone IT era as the browser. They are also likely to introduce additional risks, research shows.[7] The same holds true for URL filtering solutions that aim to mitigate web risks by categorizing sites in "blacklists" and "whitelists".

While blacklists are commonly used to restrict access to "risky" sites, even sites categorized as "safe" by the firm's web filter may expose unsuspecting team members malware via Flash, Java, Visual Basic or other web-based scripts.[8] A cloud storage service that may be whitelisted by the firm for internal use can also be abused by an insider to exfiltrate proprietary information to a personal account with the same service. Firms are blindsided by these incidents because the local browser wasn't designed to handle such gray zones.

READY FOR COMPLIANCE

Silo, the Cloud Browser: Governance and Oversight Built In

As simply shutting the web off for the firm is not an option, how can compliance leaders and IT ensure oversight and security without productivity tradeoffs? Regulated financial services organizations need a solution that empowers them to turn the web from a liability into an asset, without slowing them down.

Silo, the cloud browser built for security, governance, and increased productivity, is used by leading financial institutions and alternative investment firms. As a cloud-based browser, it executes all web code offsite, on a remote host. Only encrypted display information is delivered back to the user. Silo eliminates exposure to web-borne exploits when team members go online, while providing the rich and fast web experience users expect from their browser. Customers report 53% less time spent overall on responding to security incidents.[9]

Silo is in use across the financial services ecosystem

More than 100,000 users across 300 organizations rely on Silo to stay secure and compliant online

Your Peers
More than 65 financial services firms

Your Vendors
Security firms, consulting firms, hardware and software vendors

Your Lawyers
More than 50 firms across AmLaw 100 and Magic Circle

Your Regulators
Key regulatory agencies in Federal and State jurisdictions

OVERSIGHT BUILT IN

Compliance and Control: This Browser That Has Your Back

With Silo, there are no more blind spots when team members go online. This secure cloud browser enables firms to move beyond the minefield of security and regulatory risks associated with the traditional local browser - and improve compliance and productivity at the same time.

Because each Silo session is built with embedded policies pre-defined by the IT or compliance team, oversight, governance and data protection are ensured each time users access the web. Device access, websites, content types, credentials and data operations are centrally managed.

With Silo, all user actions are logged and encrypted, which facilitates compliance review and post-issue remediation. Authentic8's privacy controls fulfill the requirements of the European Union's Data Protection Directive (Directive 95/46/EC) and meet the requirements of the General Data Protection Regulation (GDPR).

Users 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 their firm's activities on the web.

TRY SILO YOURSELF:

www.authentic8.com

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.

[1] Amisha Shah: Outsourcing in the Alternative Investment Management Industry: Navigating Cyber, Legal and Operational Risks - https://www.eci.com/blog/16073-outsourcing-in-the-alternative-investment-management-industry-navigating-cyber-legal-and-operational-risks--webinar-replay.html Eze Castle Blog (10/2018)

[2] ibidem

[3] OCIE tops goal for examining advisers: Visits 17% of firms in FY 2018 - https://www.regcompliancewatch.com/ch/Investment-Adviser/Content/View?id=330433 Regulatory Compliance Watch (11/21/2018)

[4] Isolating the Browser, Not the Business. How financial services firms turn the web from a liability into an asset, while maintaining IT security - https://www.dropbox.com/s/5ls7n72yuhs1z6d/Silo-Isolating-Browser-Not-Business_WP006.pdf Authentic8 Whitepaper

[5] Scott Petry: The Architecture of the Web Is Unsafe for Today's World - https://www.darkreading.com/endpoint/the-architecture-of-the-web-is-unsafe-for-todays-world/a/d-id/1328529 Dark Reading (4/19/2017)

[6] Symantec: Internet Security Threat Report Vol. 23 - http://images.mktgassets.symantec.com/Web/Symantec/{3a70beb8-c55d-4516-98ed-1d0818a42661}_ISTR23_Main-FINAL-APR10.pdf (3/2018) http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf

[7] Xavier de Carné de Carnavalet and Mohammad Mannan: Killed by Proxy: Analyzing Client-end TLS Interception Software - http://users.encs.concordia.ca/~mmannan/publications/ssl-interception-ndss2016.pdf (Research Paper) Concordia University, Montreal, Canada (2016)

[8] Authentic8 Blog: Reliable Sources - for Ransomware Infections - https://authentic8.blog/reliable-sources-for-ransomware-infections/ (3/17/2016)

[9] DISA CRADA https://www.disa.mil/About/CTO/CRADA-Process-Overview and Authentic8 Silo Customer Loyalty Survey (12/2017)