CONTROL AND COMPLIANCE IN REGULATED SECURITIES INVESTMENT FIRMS

THE CCO's BLIND SPOT: WHEN TEAM MEMBERS GO ONLINE

The web is a critical tool for analysts conducting research, accessing online applications, and communicating with business partners. However, for Chief Compliance Officers at regulated entities, managing compliance risks is increasingly difficult as users go online.

Employees may be accessing sensitive client or proprietary firm data from remote locations, sometimes from non-firm-issued hardware, all via the web. In the process, users can inadvertently introduce compromised equipment or files to the firm's network. Compliance officers at regulated entities should look at web-related risk from three angles:

- how users access the web,
- what sites, apps and services they use,
- what users do online.

Where firms still rely on the local browser as their primary tool to access the web, that has created a widening compliance blindspot. Locally installed browsers are based on an outdated architecture [1] and were not designed with oversight and security in mind. How can firms ensure compliance and control when team members go online?

THE BROWSER AS EXPLOIT GATEWAY

Beware of Public WiFi

Whether employees are road warriors, remote workers, or just catching up on emails over the weekend, accessing the web from public "hotspots" at coffee shops, airports, or hotels from a regular browser can pose significant compliance risk for regulated entities. Most users — even IT security professional [2] — won't think twice before connecting to these free public networks.

Because security on these networks is lax or nonexistent, this exposes the firm's hardware, intellectual property, and client data to malware infections and data theft. The same holds true for home networks [3] that team members use to connect with the firm after hours or on the weekend.

> **Whether employees are road warriors, remote workers, or just catching up on emails over the weekend, accessing the web from public "hotspots," from a regular browser can pose significant compliance risk for regulated entities.**

Of growing concern are also Man-in-the-Middle (MitM) attacks, which continue to increase in frequency and sophistication. "Rogue access points" trick victims into connecting to what they think is a legitimate network [4] because the name sounds reputable. WiFi "snooping" and "sniffing" allows attackers to silently monitor everything the user is doing online, capture login credentials, and hijack accounts. If employees have access to sensitive data of their firm or its clients, public access points become a key vulnerability when used with a traditional browser.

[1] Local Browsers: High-risk Holdover From IT's Past - https://www.dropbox.com/s/uktsoawle8ueynh/2018-12-03%20High%20Risk%20Holdover.pdf Authentic8 (2018)

[2] Ryan Orsi: Results of the rogue Access Point experiment at RSA Conference 2017 - https://www.helpnetsecurity.com/2017/02/24/wifi-experiment-rsac-2017/ HelpNet Security (2/24/2017)

[3] *United States Computer Emergency Readiness Team: Home Network Security* - https://www.us-cert.gov/ncas/tips/ST15-002

[4] *Larry Loeb: Rogue WiFi Access Points: Would You Know the Difference?* - https://authentic8.blog/rogue-wifi-access-points-would-you-know-the-difference/ Authentic8 Blog (5/16/2018)

WHY WEB FILTERS FAIL

Navigating the Web’s Danger Zones

Companies typically use domain-level filtering to identify and restrict access to “risky” sites. Research shows that this approach is neither scalable nor effective. More than 1.9B websites were online as of December 2018, with nearly 400 new websites added every minute.[5] 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.

Today, 1 in 13 web requests lead to malware (up from 1 in 20 in 2016) [6]. URL filtering has not stopped or reversed that trend. Instead, it has become an impediment to productivity. Analysts, for example, find sites blocked — such as social media platforms — that may be relevant for research purposes and could provide important insights into consumer habits and trends. Blacklists and whitelists define a narrow sliver of the web, while users spend most of their time in “gray” areas where the majority of risks live.

DRIVING BLIND

The Challenge of Policing Online Behavior

Of particular concern for a growing number of CCOs in regulated firms are social media sites, because every comment posted online by an employee represents a potential compliance violation. The risk associated with employees publicly commenting online extends well beyond social media sites. Infractions are as likely to happen in the comment sections of blogs or industry portals.

Data exfiltration risk also poses a growing problem for compliance officers, because local browsers facilitate unrestricted and unmonitored copy/paste or file transfer from one cloud application to another. Making a bad situation worse is the fact that compliance teams have only limited visibility into a user’s online behavior. While most regulated firms are diligent about archiving email and chat communications, they lack similar records of employee web activity.

> **Managing data exfiltration risk also poses a growing problem for compliance officers, because local browsers facilitate unrestricted and unmonitored copy/paste or file transfer from one cloud application to another.**

REGAIN CONTROL

Silo, the Cloud Browser: Architected for Security

Founded in 2010, Authentic8 pioneered the cloud browser. Each Silo session runs natively in the cloud, hosted in a secure, remote container outside the customer’s IT perimeter. This unique architecture ensures no web-based malicious code, suspicious links or attachments ever touch the local device. Silo also completely mitigates the risk of compromising sensitive data when accessing the internet from a public hotspot. Our patents address the core configurability that organizations need to ensure the browser makes the web available without being compromised — by bad actors or employee mistakes.

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

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

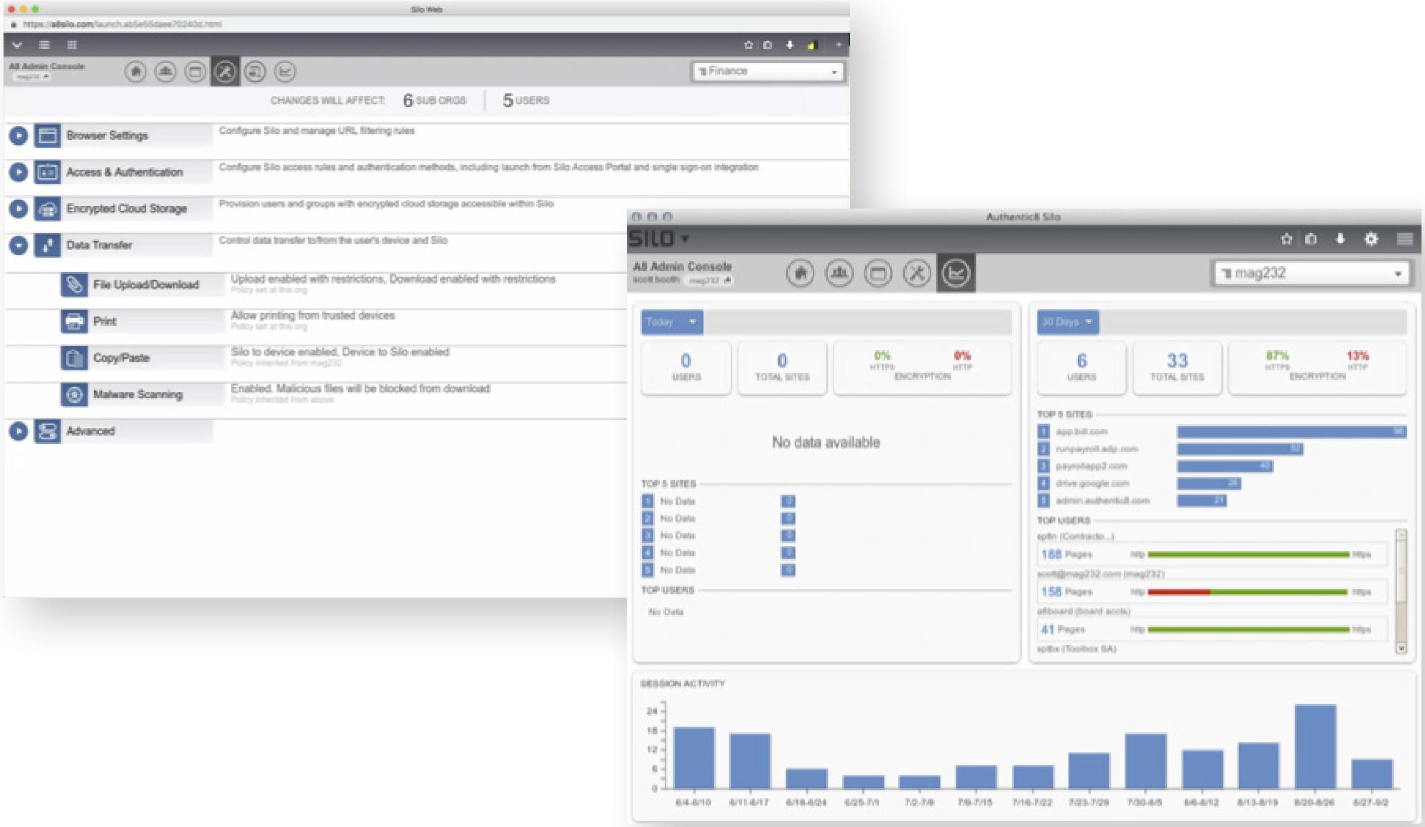
SILO HAS YOUR BACK.

Central Oversight and Compliance Built In

Each Silo session is built with embedded policies defined by IT or the compliance team. They can be set to govern device access, websites, content types, credentials, data operations, and more. The administrative console provides centralized control and overview of activities online, including user management, web app entitlements, and data policies.

All user actions are logged and encrypted, which facilitates compliance reviews and post-issue remediation. Users get a secure, compliant, and personalized browser that allows them to get online and be productive.

Compliance leaders and admins get a centrally managed browser that gives them comprehensive control and visibility over what users do online.



CHANGES WILL AFFECT: 6 SUB ORGS | 5 USERS

Browser Settings	Configure Silo and manage URL filtering rules
Access & Authentication	Configure Silo access rules and authentication methods, including launch from Silo Access Portal and single sign-on integration
Encrypted Cloud Storage	Provision users and groups with encrypted cloud storage accessible within Silo
Data Transfer	Control data transfer to/from the user's device and Silo
File Upload/Download	Upload enabled with restrictions, Download enabled with restrictions Policy set at this org
Print	Allow printing from trusted devices Policy set at this org
Copy/Paste	Silo to device enabled, Device to Silo enabled Policy inherited from mag232
Malware Scanning	Enabled. Malicious files will be blocked from download Policy inherited from above
Advanced	

TRY SILO YOURSELF:

www.authentic8.com

COMPANY HISTORY

Authentic8 was founded in 2010 by the team that built Postini, which was subsequently sold to Google. The firm has deployed Silo to over 100,000 users across 300 organizations, where the technology has been thoroughly tested by the most discerning buyers. Customers include federal agencies and regulators, financial services and law firms, leading cybersecurity technology providers, and IT consulting firms. Authentic8 has headquarters and Federal Operations in California, Washington DC and Berlin Germany