CONTROL AND COMPLIANCE IN REGULATED SECURITIES INVESTMENT FIRMS

WEB USE: WHAT REGULATORS WANT TO SEE

For buyside and sellside firms, the SEC's Office of Compliance Inspections and Examinations (OCIE) has prioritized [1] "cybersecurity with an emphasis on, among other things, governance and risk assessment, access rights and controls, data loss prevention [...] and incident response."

While these regulated entities have significantly strengthened their compliance policies, their practices reveal alarming gaps when team members access the web. Many firms lack the the tools to monitor, audit, and enforce employee web use policy. Yet regulators expect firms to make a reasonable attempt to ensure oversight and remediate areas of weakness.

Silo, Authentic8's cloud browser, offers a solution empowering compliance teams and IT administrators to regain control over employees' web activities and reduce the risk of compliance violations.

SCRUTINY FROM REGULATORS

What Happens When Team Members Use the Web?

Research analysts and investment managers rely on the web browser as their main tool to gather market intelligence, to access data aggregation tools and web apps, and to communicate via web mail and social media. But the very architecture of the local browser creates oversight and governance challenges for employee web use. Moreover, the browser's inherent security weaknesses leave firms exposed to risks of data breaches and compliance violations online.

The examinations revealed that most firms still have alarming blind spots related to how their teams use the web. OCIE staff observed compliance risks regarding the following issues, among others:

- **No breach response plan:** Fewer than two thirds of advisers and funds had plans for data breach incidents.
- **Lack of remediation:** A number of firms did not appear to fully remediate some of the high risks discovered in penetration tests and vulnerability scans;
- **Missed patches and updates:** Although all advisers and funds had a process in place for ensuring regular system maintenance, critical security updates had not been installed.

HIGH-RISK IT HOLDOVER

Your Web Browser, a Compliance Hurdle?

Compliance risks like these are typical for firms that still use a local browser base to access the internet. This is not coincidental.

While regulated securities investment firms increasingly rely on web apps and the cloud for many critical functions, including threat detection and prevention tools, the local browser remains the last anachronistic holdover from another IT era. At the same time, up to 80 percent of IT security incidents are browser-related, researchers [2] have found.

Traditional browsers remain notoriously difficult to maintain, oversee, patch, and protect against external exploits as well as (intentional or inadvertent) misuse by insiders. Deploying a cloud browser instead, which can be centrally managed, monitored and audited, removes such risks and enables CCOs and IT to implement the recommendations of the OCIE.[3]

PRODUCTIVE WIN-WIN

Managing Risk without Hurting Productivity

Compliance and IT teams face a conundrum: a restrictive web use policy that helps ensure network security and tight policy compliance and oversight can also come at the expense of employee productivity. Employees rely on the web to quickly aggregate actionable market intelligence from widely disparate sources or access office resources from home or a public location without putting their firm at risk.

Firms no longer need to accept a tradeoff between control/governance and risk/productivity. Silo offers a win-win instead of a weak compromise. Employees get access to the web via a secure, compliant, personalized browser. IT gets complete inoculation from the risk of malware, a robust set of administrative controls, and a fully auditable log of user activity, all embedded in a remote cloud browser.

CONTROL AND COMPLIANCE

Silo: A Central Point for Oversight and Governance

Silo, the cloud browser provides a single point of control and granular oversight for IT administrators and compliance officers. With Silo, all web code is processed on a remote host configured for regulatory compliance and data security. No code from the web can reach the local IT infrastructure.

Moreover, Silo's architectural approach simplifies the IT stack, resulting in significant hard and soft cost savings. Customers report an elimination of break-inspect and web filtering gateway infrastructure. The dramatic reduction of web-borne exploits means O-day surface area is minimized or eliminated, resulting in significant endpoint AV savings. Policies embedded in the browser mean network-level log and analysis costs can also be reduced. Beyond these infrastructure savings, our customers report 53% less time responding to security incidents.[4]

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] SEC Office of Compliance Inspections and Examinations Announces 2018 Examination Priorities - https://www.sec.gov/news/press-release/2018-12 (Press Release 2/2018)

[2] Among others, see Verizon Data Breach Investigation Reports 2014-2018 - https://enterprise.verizon.com/resources/reports/dbir/; also Adam Stone: When is the network not really the network? C4ISRNET - https://www.c4isrnet.com/show-reporter/disa-forecast-industry/2018/11/05/when-is-the-network-not-really-the-network-2/ (11/5/2018)

[3] OCIE: Observations from Cybersecurity Examinations - https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf (2017)

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