The CCO’s blind spot: When team members go online

By John Klassen

John Klassen (jklassen@authentic8.com) is a Product Marketing Manager at Authentic8 in Redwood City, CA, USA.

- linkedin.com/in/johnkklassen

Investment management firms depend on the internet for research, web apps, and communication with business partners, and most firms rely on the web browser as a primary tool for conducting business. This has created a widening compliance blind spot, because locally installed web browsers are notoriously difficult to maintain, secure, and monitor. How can chief compliance officers (CCOs) and IT teams manage the associated risks?

What happens when employees go online? Behind closed doors, many CCOs and IT administrators readily admit they don’t really know. Most compliance teams have only limited visibility into their employees’ online behavior. Though diligent about archiving email and chat communications, their firms lack similar records of employee web activities.

Finding themselves under growing pressure from regulators to ensure compliance and remediate areas of cybersecurity weakness,[1] compliance officers cannot trust that tightening policies and updating compliance handbooks will be sufficient to protect the firm and satisfy examiners.

Control lost, risk increased

Compliance leaders and IT administrators have ample reason to worry. Without
effective governance and granular oversight of employee activities online, regulated firms are facing increasing risks of noncompliant behavior and cybersecurity breaches, mainly in three areas:

- **Social media and online comments/reviews**: Social media sites are of particular concern for a growing number of CCOs. Employees posting public online comments run the risk of violating the Testimonial Rule. This risk extends well beyond the “traditional” social media sites; infractions are as likely to happen on LinkedIn or Facebook as in the comment sections of industry portals or garden-variety investor blogs.

- **Data exfiltration by insiders**: Regular web browsers allow for unrestricted — and unmonitored — copy/paste or file transfer, for example from one cloud storage account or service to another.

- **Remote access and personal devices (BYOD)**: Employees are accessing sensitive data from remote locations like a home office, coffee shop, or airport lounge, often from insufficiently protected hardware, and they can inadvertently compromise the firm’s network in the process.

How did firms lose control and visibility over such critical areas? Industry insiders blame the web browser. The primary tool used by employees in their online activities has become a critical compliance blind spot.

**Blinded by the browser**

The problem: The regular browser wasn’t designed with security and compliance in mind. To make matters worse, it has been plagued by inherent architectural flaws and security vulnerabilities since its inception 30 years ago. Local browsers have become a liability, experts warn. Instead of furthering productivity, they are putting firms at risk of malware attacks, data loss, and compliance violations by insiders. Shutting down the web for employees is hardly a viable solution. But then, what is?

A look at other highly regulated organizations reveals the answer. Major financial institutions, America’s largest law firms, and more than 100 federal agencies are now protecting themselves by deploying a centrally managed and monitored cloud browser to ensure centralized oversight and governance when
employees go online.\[6\]

Regulated investment firms have begun to follow suit. What has prompted this change? One major reason is the ineffectiveness and insecurity of web-filtering tools. Like other single-point solutions aimed at mitigating the inherent problems of the local browser (e.g., antivirus tools), this approach of “blacklisting” or “whitelisting” URLs has proved inefficient as a backstop to prevent compliance or security violations.

Policing the gray zone

Regulated entities have typically used domain-level filtering to identify and restrict access to “risky” websites that could expose the organization to regulatory risks or web-borne exploits. Research shows why this approach is neither scalable nor effective: It has fallen hopelessly behind.

Real-time statistics show that more than 1.9 billion websites were online in January 2019, with nearly 4,000 new websites added every minute.\[7\] Even sites once categorized as “safe” may have fallen into 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 leads to malware (up from 1 in 20 in 2016).\[8\] URL filtering has neither stopped nor reversed that trend. Instead, it has become an impediment to productivity in investment firms. Analysts, for example, frequently find sites blocked, such as social media platforms, that may be relevant for research purposes. Firms have to decide if they allow access to possibly valuable web resources and accept the security risk, or block access and impede productivity by depriving employees of work-relevant web content.

Security researchers estimate that out of more than 50 billion URLs, only 30 billion have been categorized.\[9\] Blacklists and whitelists only define narrow slivers of the web, while users spend most of their time in gray areas where the majority of risks live.

How to regain control…

How are firms addressing this growing problem? Compliance and IT teams have long found themselves in a tough spot. Should they tighten the firm’s web
use policy to shore up network security and compliance? This approach is likely to interrupt time-critical workflows. And that’s only part of the problem.

Another part that IT administrators are all too familiar with is that users will find risky workarounds, such as switching to a personal mobile device or going online from a coffee shop around the corner. What can firms do to enable employees to quickly aggregate actionable market intelligence from disparate sources—or to access office resources from home or a public location—without putting the firm at risk?

Enter the cloud browser. Investment firms are turning to browser isolation in the cloud, because it enables them to regulate and monitor employee activities online without the tradeoff between control/governance and risk/productivity. Instead of adding to the problem, the browser now actually lessens the workload for the compliance team and becomes part of the solution.

How do cloud browsers work? They increase security and oversight by reducing complexity, not adding to it. Each browser session is created from scratch on a centrally managed remote host configured for regulatory compliance and data security. Financial services firms prefer a cloud browser model based on a comprehensive policy framework, which allows the browser to be configured based on the compliance team’s and IT admin’s specific requirements of the particular user and use case. The firm’s network remains insulated from web-borne exploits no matter what websites employees visit, because no code from the web can reach the local device.

...without risky tradeoffs

Deploying a compliance-ready cloud browser has saved their firms both time and money, CCOs report. Resources formerly dedicated to update, patch, configure, and secure locally installed browsers or to post-incident mediation have been freed up for other critical tasks. They no longer worry about blind spots either. Such blind spots are eliminated by a browser that provides instant visibility into individual user activities on the web. Governance and data protection are ensured each time a team member goes online.

With a compliance-ready cloud browser, each session is built with embedded policies as pre-defined by IT or the compliance team. The new browser model enables the firm to exert control without sacrificing productivity:
• 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. Instead of weak compromises, the cloud browser provides a win-win-win-win solution for users, compliance managers, IT admins, and regulatory authorities alike.

Takeaways

• Regulatory pressure has increased, but so has the potential of compliance violations online.

• Firms have lost control and visibility into employee online behavior in critical areas.

• Locally installed web browsers have created a critical blind spot for compliance professionals.

• Point solutions, like the traditional approach of blacklisting and whitelisting web resources, have proved insufficient.

• Cloud browser technology now provides compliance leaders with a central vantage point to manage and monitor employee online activities.

8 Internet Live Stats, Total number of Websites, http://bit.ly/2E8ttTS

This publication is only available to members. To view all documents, please log in or become a member

Become a Member Login