EDITORIAL BRIEF

Using Your Browser as an Auditing Support Tool

Forensic logging activity on the browser when policies are violated can aid cyber investigations and incident response efforts

By Dennis Pike
Enterprise Architect

Traditional cyber audits have drawbacks. They are sometimes painstaking and consume significant time and resources. This is especially true if organizations do not take a targeted approach to the information they log and collect. In such scenarios, the sheer amount of data recorded can make conducting an audit a classic "needle in a haystack" scenario – except that in truth, you're likely to be searching countless digital haystacks.
Audits or less formal examinations of employee activity are typically prompted by triggering events, such as compliance reviews, mandated testing, or the suspicion of illegal behavior. By logging and recording transaction events and other data, anyone reviewing employee activity can get a real-time or historical view of things that have occurred.

Today's organizations have a variety of powerful security controls, yet they typically cannot see what users are doing within their web browser. For example, if a disgruntled worker logs-in and steals business-sensitive data out of a browser screen via copy/paste this will likely never be traced. And it's almost impossible to figure out by conventional means.

Why a Policy-Focused Approach is Imperative

Organizations can capture massive quantities of data, yet their ability to effectively audit that data diminishes as the amount of information recorded grows larger.

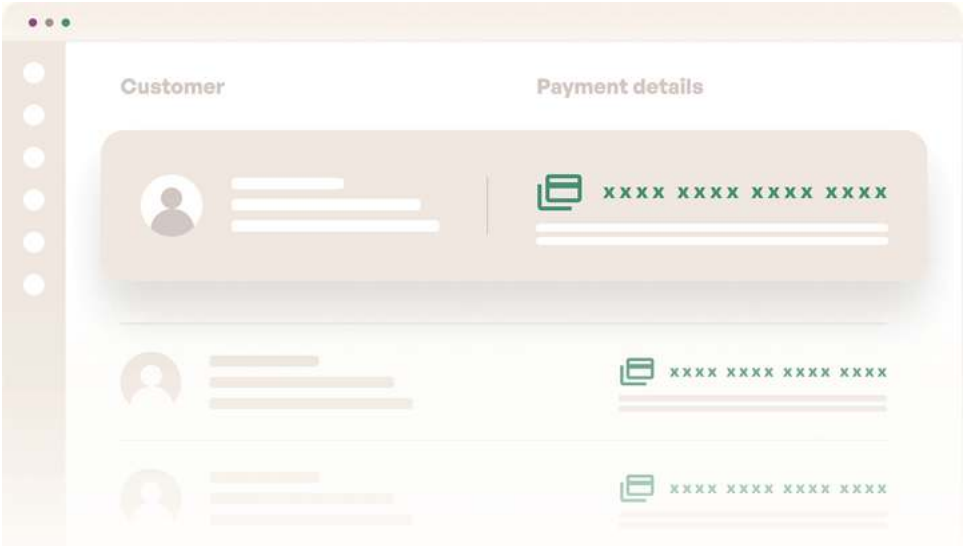
The solution here is straightforward – use the browser as a key resource to set specific policies governing which critical events to capture and the depth at which they are captured.

Once a policy triggers, a browser built with the enterprise in mind can begin to keep a record of all or select user interactions with key parts of the organizational estate.

This surgical approach is critical because compliance practices and mandates can vary wildly by organization, and these mandates come with distinct requirements. One organization's requirements may fall under HIPAA, another under GDPR, or a third may have no regulatory oversight because they're a private company that is not headquartered in a regulated area.

This means requirements for things such as storage, or what types of data you capture, or what you can anonymize will be distinct. Different jurisdictions or regulatory bodies have disparate rules.

Policies are the absolute key to reducing this complexity and helping the organization stay compliant. A browser with such visibility needs policy-driven depth as a critical capability.



Gaining visibility into browser activity – and the ability to record and analyze what happens -- is key to resolving the problem of "last mile" security control.

Island

The Power of Policy-Based Logging at the Browser Level

Analyzing activity at the browser level means you can capture clicks, keystrokes, screenshots, source and destination details including device and user data around any critical application. For example, you can track a source (an employee) who is logged in on a particular device and network. Permissions can be granted based on whether this behavior is authorized, or the policy that you put in place can block them. All these actions can be recorded for future analysis.

The destination shows what the user did or attempted to do. They may have attempted to access a SaaS application, a URL or an internal application that manages sensitive data, all of which is recorded. Ultimately, by taking this approach it also becomes possible to block things such as downloads/uploads, screen prints, screen captures and copy and paste activity on a per destination basis. Every time someone tries to do something that's blocked, the browser records it in a log for future examination. And even in situations where a block wasn't desired, the activity can still be recorded for future needs.

While it may sound like organizations are locking down by implementing these capabilities, the truth is that doing so provides much greater flexibility. Once effective policies are enabled, for example, you can use cloud collaboration applications with greater freedom, knowing that guardrails are in place, while also knowing that users are now aware of these guardrails -- something that should deter inappropriate activity.

One other issue to address is encryption. The widespread adoption of SSL and TLS encryption conceals web content from inspection by network security tools. Logging or auditing becomes almost impossible. The browser is the natural termination point and now it's a much simpler place where inspection, logging, auditing and analysis can take place without the ill-effects of network based-SSL inspection.

Ultimately, by taking this approach it also becomes possible to block things such as downloads/uploads, screen prints, screen captures and copy and paste activity on a per destination basis

This data can be viewed within the Island Management Console via pre-built or custom reports and dashboards. Also, since many enterprise customers use their own in-house and 3rd party tools to make use of log data, there are multiple ways that this data can be exported including Secure Syslog and a Splunk Add-on.

The Takeaway

The browser has historically been something of a cyber-security blind spot. Gaining visibility into browser activity – and the ability to record and analyze what happens -- is key to resolving the problem of "last mile" security control.

While it's possible to record endpoint activity or network traffic with heavy approaches, such tactics are not scalable or workable at the enterprise level. Nor is vacuuming up enormous amount of data without taking a targeted, precision approach. Creating a browser with detailed auditing capabilities and policy-driven controls, however, does the following:

- It gives you last mile visibility
- It allows for granular policies that help you stay compliant
- A browser-based approach makes the process of auditing more efficient
- It allows an organization to operate more freely, knowing that guardrails are present
- It illuminates activities previously unseen in other logging and auditing technologies
- It eliminates the overly complex tooling necessary to see rich audit data in the first place
- It enriches external ecosystems of forensics and logging technologies with a new dimension of data for threat and data protection

These benefits can deliver exceptional value across an organization. The list of who can benefit is long -- auditing committees with fiduciary responsibilities, C-suite executives who need to protect their organizations, general counsel, SOC Analyst and Incident Responders -- and anyone who needs the freedom to work and collaborate in a more flexible and secure fashion.

About Dennis Pike

Dennis Pike was the first Sales Engineer at Island and works with customers to help address their use cases and business needs with Island's unique new technologies. With over 20 years of experience in Information Security, Dennis was most recently a Global Black Belt for Advanced Security Analytics at Microsoft. Prior to Microsoft, Dennis has held various customer-facing technical roles at LogRhythm, Symantec, Blue Coat Systems, Extreme Networks and Sprint. Dennis holds a Bachelor of Science in Systems Engineering from The University of Virginia.

About Island

At Island we are focused on delivering an enterprise browser that enables data protection, access controls and full logging and visibility into all interactions with web-based applications. Our Island Enterprise Browser is built on last mile controls that enforce policy over actions. Island is led by senior executives from the security and technology industry and backed by the world's leading venture funds -- Insights Partners, Sequoia, Cyberstarts, and Stripes. Based in Dallas with operations in Tel Aviv, Island can be reached via email at info@Island.io or (866) 832 7114.