TAG CYBER

WHY ENTERPRISE BROWSERS SHOULD BE INCLUDED IN COMPLIANCE FRAMEWORKS

DR. EDWARD AMOROSO, TAG CYBER

Island

TAG CYBER

WHY ENTERPRISE BROWSERS SHOULD BE INCLUDED IN COMPLIANCE FRAMEWORKS

DR. EDWARD AMOROSO

The emerging availability of commercial browsers with strong security-enhanced features for enterprise warrants inclusion in popular cybersecurity compliance frameworks.

INTRODUCTION

One can make a reasonable case that a browser might be the most important application used in every modern enterprise organization today. And yet, curiously, many security teams do not include the browser as an application in their official inventory. Instead, teams often take browsers for granted, and this can lead to significant lost opportunities to strengthen enterprise cyberdefense.

Recently, our analyst team at TAG Cyber reviewed excellent commercial offerings that include desirable new security features that are embedded into the browser. These features are driven primarily by the needs of the modern enterprise and are consistent with both the cyberthreats experienced by most organizations, and the types of security controls that are considered desirable.

In this brief we make the case that commercially available enterprise browsers are now sufficiently mature that their associated functionality should be included in every cybersecurity framework. We pay particular attention to security features that support the concept of last-mile protection for security endpoints, which complement (or even supplant) many existing enterprise security controls.

BENEFITS OF ENTERPRISE BROWSERS

The types of security requirements enterprise teams should demand from their browsers come in three distinct categories. First, browsers should be free from vulnerabilities. This has been an especially nagging issue since self-propagating malware could no longer rely on open access to target networks through open ports on the firewall. Entry points required exploitable vulnerabilities, so browsers became popular targets. This must therefore be prevented.

Second, creators should design browsers that provide reasonable options for individuals or organizations to either remove or avoid having to use other comparable tools. Consider, for example, that endpoint security has emerged as one of the most expensive line-items for IT and security teams. As such, if the browser can offer cheaper alternatives consistent with budget (or lack thereof), then this is desirable.

Finally, browsers should provide so-called *last-mile protection* for the end-user since the browser provides the most direct interface with the user of any applications. If malware finds its way through the typical gauntlet of controls that exists between a web application and a user, then the browser should provide a final safety net to protect local resources. This is also useful for risks that emerge from careless or unintentional misuse of data.

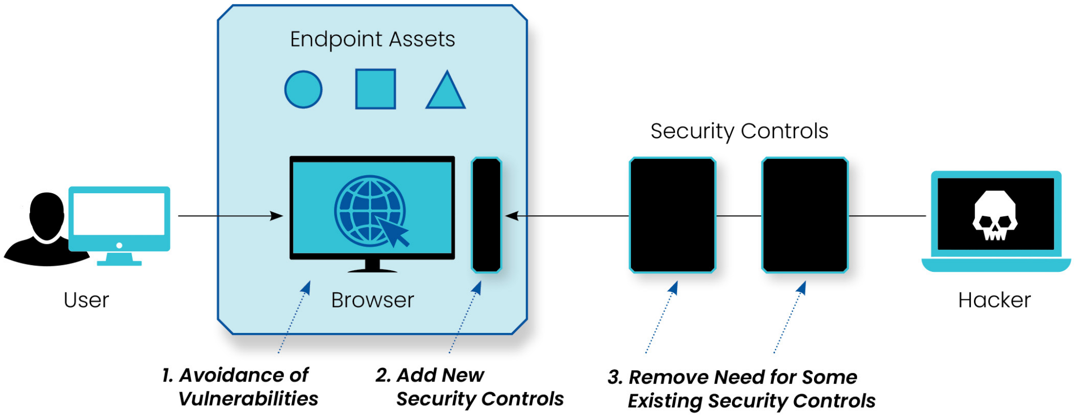
Endpoint Assets
Security Controls
User
Browser
Hacker
1. Avoidance of Vulnerabilities
2. Add New Security Controls
3. Remove Need for Some Existing Security Controls

Figure 1. Security Roles for the Browser

The implication of last-mile browser defense is that we recommend pre-integration with existing PC and device controls such as endpoint detection and response, content disarm and reconstruction, and anti-malware security software. The business opportunities are significant for vendors, certainly, but the real value will come from enterprise teams who will experience better endpoint security.

PROPOSED INCLUSION IN FRAMEWORKS

A significant issue in modern cybersecurity is that the existing popular frameworks dictating the protection control architecture for most enterprise teams are largely silent on last-mile browser security capabilities. This creates a gap in programs, especially ones that are highly influenced by formal frameworks, including in highly regulated industries such as financial services, utilities and telecommunications.

A review of existing popular frameworks,[1] including the NIST Cybersecurity Framework, Payment Card Industry (PCI) Data Security Standard (DSS), and International Standards Organization (ISO) 27000 series confirms this last-mile gap. None of the frameworks includes, for example, copy-and-paste controls for the browser and some barely scratch the surface of browser-based controls.

One excellent resource for information on browser security controls is the Chromium Security website maintained as part of The Chromium Projects.[2] The Chromium security team provides users of its open source (which is the basis for most enterprise offerings) with security features consistent with the following principles: help users safely navigate the web, design for defense in depth, security is a team responsibility, speed matters and be transparent.

Given such excellent resources, our TAG Cyber analyst team urges the purveyors of security frameworks and any other stakeholders to begin to address the standards gap. We believe that a set of simple requirements can be defined that will fit well into modern compliance frameworks. Even if enterprise teams opt not to address these requirements, their inclusion will increase awareness and help promote use where it will be most important.

We summarize the specific last-mile browser security requirements we recommend for inclusion in frameworks such as NIST 800-53 and PCI-DSS:

- ***Data Management.*** The browser should include functional controls for where and when users can copy and paste data, print and save pages into or out of applications.
- ***Device Posture.*** The browser should include means for confirming that device security status is acceptable before granting access.
- ***Developer Tools.*** The browser should govern whether to allow developer tools (e.g., viewing page source) for enterprise applications.
- ***Screen Capture.*** The browser should manage whether to allow or authorize requested screen captures.
- ***Browser Extensions.*** The browser should include controls that consider which extensions are acceptable for installation.
- ***Data Storage.*** The browser should include controls for how data is stored and under what types of conditions.
- ***Geographical Controls.*** The browser should use location as the basis for geo-fencing controls required by an enterprise.

We urge readers to consider improvements to the list presented above, and framework curators will likely have opinions about improved wording, references and other means for presenting the new control statements. Regardless of the implementation process, we hope that the industry starts to take last-mile browser security controls more seriously, and that this is codified in our major security frameworks.

[1] This technical review was performed in late 3Q22 by the TAG Data Research team including Iassen Christov, Carlier Hernandez, Shawn Hopkins, Khanjan Patel and Nick Wainwright.

[2] https://www.chromium.org/Home/chromium-security/

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr. Edward Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by Island. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

Disclaimer: The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. TAG Cyber disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of TAG Cyber's analysts and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

TAG Cyber may provide forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment and opinion on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements considering new information or future events.