TAG CYBER

ENTERPRISE BROWSER SECURITY REQUIREMENTS TO COUNTER AI-ENABLED RISKS

DR. EDWARD AMOROSO,
CHRISTOPHER R. WILDER,
TAG CYBER

ENTERPRISE BROWSER SECURITY REQUIREMENTS TO COUNTER AI-ENABLED RISKS

DR. EDWARD AMOROSO
CHRISTOPHER R. WILDER

This report introduces a set of cybersecurity requirements that should be integrated into the enterprise browser and included in major compliance frameworks to counter emerging risks from new artificial intelligence-based tools such as conversational chatbots.

INTRODUCTION

One area where an enterprise browser can effectively address significant challenges for organizations is by leveraging artificial intelligence (AI) advancements to enhance the browsing experience. For example, Microsoft's investment in OpenAI has led to tight integration between their enterprise browser (Edge) and search engine (Bing), providing businesses with a more efficient and intelligent browsing solution. Similarly, Google is expected to pursue a comparable strategy by integrating AI-powered features within its enterprise browser (Chrome) and search engine, further empowering organizations with advanced browsing capabilities.

With such AI-enabled browsing enhancements come the inevitable impacts on cybersecurity. URL redirection, malware delivery, and social engineering attacks are all massive problems for internet users today, so it stands to reason that adding AI tools to the browsing experience will create new and enhanced types of cyber threats. Sadly, this is true for most consequential technology inventions.

This brief note outlines the security features TAG Cyber recommends for inclusion in the enterprise browser to deal with the expanded use of AI tools. We believe that proactively demanding these protection capabilities is wiser than waiting to see what types of threats unfold. The good news is that commercial vendors are available for enterprise security teams who choose to take our advice.

RISKS OF AI-ENABLED BROWSING

The impact of AI-enabled browsing will offer a significantly improved user experience for finding information, personalizing searches and automating various activities and tasks. For example, the introduction of OpenAI's ChatGPT to the Microsoft browsing experience illustrates this intriguing new capability. Google is also working hard to enhance its browsing functionality with chatbot functions.

With AI-enabled browsing comes a set of specific cybersecurity risks, including:

* **Social Engineering** – A user's likelihood of being tricked into sharing sensitive information increases considerably with AI-based tools. The AI algorithms can leverage insights into targeted user behavior to engage in dialogue that will personalize phishing or URL redirection attacks.

* **Malware** – The distribution of malware increases with AI-enabled browsing to trick users into downloading infected software. These tricks include offering phishing links in suggested content and even engaging in dialogue that could cause a user to make bad security decisions during the browsing session.

* **Data Governance and Compliance** - In preventing inappropriate disclosures, organizations must ensure that sensitive or confidential data (i.e., unannounced M&A proposals) is not shared with a general-use AI tool. This can be achieved by using an enterprise browser to define application boundaries, prevent data from being copy/pasted or uploaded, and mask particular keywords or phrases when typed into a conversational chat AI tool.

The full cybersecurity implication of AI-enabled browsing will not be known until this capability is deployed at scale. In advance of this shift, it is prudent for enterprise security teams to take preventive action to avoid threats that are predictable (such as the examples cited above) and perhaps those that are less predictable. The section below suggests that security-enhanced browsers will be an important part of the protection equation.

BENEFITS OF SECURITY-ENHANCED BROWSERS

Broad security requirements for enterprise browsers come in three 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, browsers should be designed to provide reasonable options for individuals or organizations to either remove or avoid using as many existing comparable tools as possible. 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.

Third, browsers should provide so-called last-mile protection for the end-user. This makes sense because the browser provides the most direct interface between the user and any applications being accessed. 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.

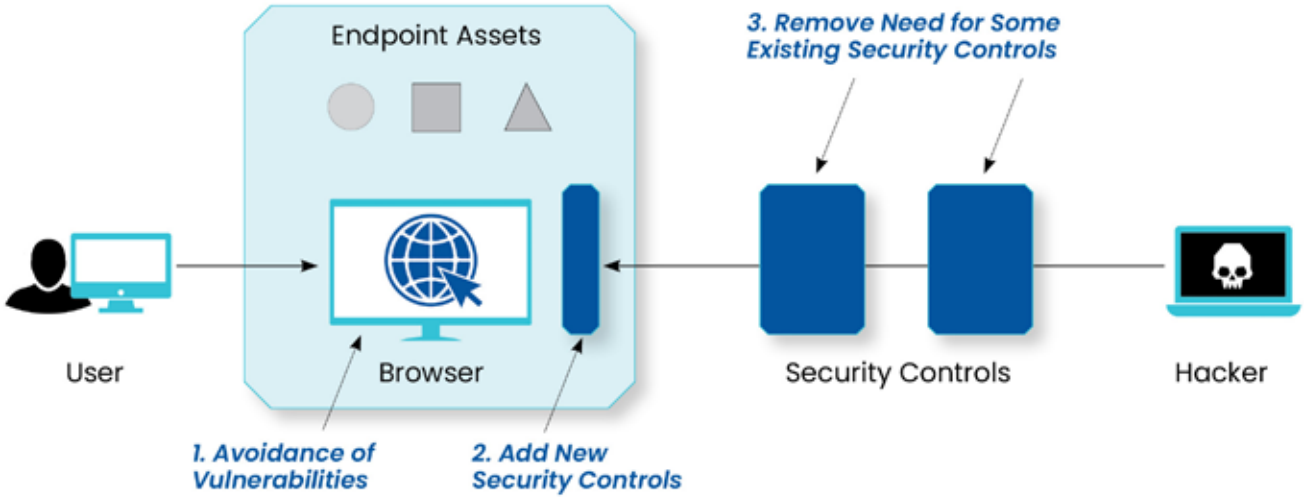

Figure 1. Security Roles for the Browser

The implication of last-mile browser defense is that pre-integration is recommended with existing PC and device controls such as endpoint detection and response (EDR), content disarm and reconstruction (CDR), 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.

Finally, it's an important consideration for organizations embracing conversational AI tools is governing the types of data that are shared. To prevent inappropriate disclosures, sensitive or confidential data (e.g., unannounced M&A proposals) should not be shared with a general-use AI tool. An enterprise browser can define application boundaries and prevent data from being copy/pasted or uploaded. It can also look for keywords or phrases and mask them when typed into a conversational chat AI tool.

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 many programs, especially ones that are highly influenced by formal frameworks, including in highly regulated industries such as financial services, utilities and telecommunications.

A TAG Cyber review of existing popular frameworks, including the NIST Cybersecurity Framework (CSF), Payment Card Industry (PCI) Data Security Standard (DSS), and the 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**. The Chromium security team provides users of its open source project (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 the process 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 to not address these requirements, their inclusion will increase awareness and promote their use.

The specific last-mile browser security requirements we recommend for inclusion in frameworks such as NIST 800-53 and PCI-DSS are summarized below:

- **Data Management** – The browser should include functional controls for where and when users can copy and paste data into or out of applications.
- **Device Posture** – The browser should include means for confirming that device security status is acceptable before granting access.
- **Screen Capture** – The browser should manage whether requested screen captures are allowed or authorized.
- **Browser Extensions** – The browser should include controls for which extensions are considered acceptable for installation.
- **Workflow Support** – The browser should include functional integration with applicable workflow tools in the enterprise.
- **Data Storage** – The browser should include controls for how data are stored and under what types of conditions.
- **Geographic Controls** – The browser should use location as the basis for geo-fencing controls required by an enterprise.

Readers are urged 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 last-mile browser security controls are taken more seriously in the industry, and that this is codified in our major security frameworks.

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

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

Contributors: Dr. Edward Amoroso, Christopher R. Wilder

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.

Copyright © 2023 TAG Cyber LLC. This report may not be reproduced, distributed or shared without TAG Cyber's written permission. The material in this report is composed of the opinions of the TAG Cyber analysts and is not to be interpreted as consisting of factual assertions. All warranties regarding the correctness, usefulness, accuracy or completeness of this report are disclaimed herein.