BROWSER SECURITY TRENDS 2023

A Guide for CISOs and CIOs

WHITE PAPER
SEPTEMBER
2023

ERMES
BROWSER SECURITY

info@ermes.company | ermes.company

CONTENTS

Abstract ____ 3

Introduction ____ 4

Enterprise Browsers and Security Extensions ____ 5

Predictions ____ 14

Insights for 2023 and Beyond ____ 16

Ermes AI-Driven Solutions for Web Protection ____ 19

Conclusion ____ 20

About ____ 21

ABSTRACT

The modern-day web browser represents the core workspace, key interface, and gateway to many SaaS business apps and web destinations. It has also become the target for multiple types of cyber-attacks while also being the source of much unintentional data leakage in today's corporate environment. Moreover, because the web browser acts as the intersection point between the cloud, web environments, and physical endpoints it is especially attractive to bad actors searching for native vulnerabilities to exploit.

Unfortunately, most commercial browsers have very few built-in security features. Consequently, attacks targeting vulnerabilities in Internet browsers are generally on a steep rise.

The browser threat landscape is highly troublesome for CISOs now facing the challenges of having to provide additional security measures to address the vulnerabilities of commercial web browsers—the main productivity tool for modern day enterprises—while also carefully trying to navigate the existing dichotomy between providing necessary security and maintaining workplace productivity/agility.

To properly address emerging threats to web browsers, CISOs and other security leaders should consider adopting an approach that leverages the use of enterprise browsers and security extensions as a frontline security solution.

According to Gartner, enterprise browsers and extensions provide an alternate, light weight method for delivering many desirable features and benefits. These features and benefits generally fall within four categories: prevention and detection; centralized management; visibility and response; and productivity and collaboration.

Enterprise browser management is expected to grow to widespread adoption by 2030. Web security, workforce productivity, and unmanaged device access use cases are the top drivers for adoption among new entrants.

Researchers at Ermes predict that the need for an enterprise browser security solution will only become more urgent given the democratization and increasing sophistication of web-based attacks and that users have now become the weakest security point.

Ermes also noted that the browser is now the main attack window for both work and private use. In other words, attackers access enterprise data by going after employees' personal information, services and habits. This, in turn, compels security teams to treat all browsing activity as a single, consolidated attack surface.

Lastly, Ermes believes that the proliferation of SaaS apps usage within the enterprise environment will result in more web and cloud-based attacks.

INTRODUCTION

A report released by Gartner in 2020 found that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio. 12% have 46 or more.[1] Similarly, an article in Harvard Business Review (HBR) noted that organizations with 10,000 or more employees typically maintain almost 100 security tools.[2] Given these stupefying numbers, it is no wonder that most CISOs and security leaders are overwhelmed by the volume of security tools required for on-premises infrastructure, cloud infrastructure, and hybrid environments.

Most CISOs would also agree that it has become a colossal challenge to strike the right balance between security and business productivity. To further exacerbate matters, many organizations tend to view security as a business obstacle rather than a facilitator. Some even believe that IT security actually hinders productivity and innovation across the enterprise.

Compounding this already strenuous situation, the web browser—which represents the core workspace, key interface, and gateway to many SaaS business apps[3] and web destinations—has become the target for multiple types of cyber-attacks while also being the source of much unintentional data leakage in today's corporate environment. Moreover, because the web browser acts as the intersection point between the cloud, web environments, and physical endpoints it is especially attractive to bad actors searching for native vulnerabilities to exploit.

To make matters even worse, most commercial browsers have very few built-in security features. Consequently, attacks targeting vulnerabilities in Internet browsers are generally on a steep rise with Google Chrome—the most widely used web browser in the world—followed by Mozilla Firefox, Microsoft Edge, and Safari. All increasingly in the sights of today's sophisticated cyber-attackers.[4]

[1]See "The Top 8 Security and Risk Trends We're Watching," Gartner, November 15, 2021 at https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021. Article references a 2020 CISO Effectiveness Survey from Gartner. It also noted that "[h]aving too many security vendors results in complex security operations and increased security headcount."

[2]See "Where to Focus Your Company's Limited Cybersecurity Budget," Harvard Business Review (HBR), May 23, 2023 at https://hbr.org/2023/05/where-to-focus-your-companys-limited-cybersecurity-budget.

[3]Software as a service (SaaS)—a cloud-based software delivery model that allows end users to access software applications over the internet, frequently requiring the use of a browser—has skyrocketed in growth over the last decade.

[4]See generally "There's Been A Big Rise in Hackers Targeting Google Chrome – Doing This One Thing Can Help Protect You," ZDNet, September 28, 2022 at https://www.zdnet.com/article/theres-been-a-big-rise-in-hackers-targeting-google-chrome-doing-this-one-thing-can-help-protect-you/. Also see "Google Chrome Ranked As the Least Safe Browser: Here's What You Need to Know," Jagran Josh, October 10, 2022 at https://www.jagranjosh.com/general-knowledge/google-chrome-ranked-as-the-least-safe-browser-heres-what-you-need-to-know-1665410343-1.

Put simply, the browser threat landscape is highly troublesome for CISOs now facing the challenges of having to provide additional security measures to address the vulnerabilities of commercial web browsers—the main productivity tool for modern day enterprises—while also carefully trying to navigate the existing dichotomy between providing necessary security and maintaining workplace productivity/agility.

Nonetheless, given all these challenges and conflicting pressures, security leaders still have an affirmative duty to evaluate the architecture of their security stacks and the arsenal of tools currently deployed to ensure that they can fully withstand all growing threats to commercial web browsers in today's riskier environment.

Despite calls for increased productivity and agility, CISOs cannot simply ignore the expanding role that browsers play in modern day enterprises along with the prodigious volume of cyber risks that come along with it. Security stacks must be modulated to effectively address these threats.

To help CISOs and other security leaders effectively address these growing threats, this document explores the key features and benefits of enterprise browsers and security extensions as well as providing predictions and important insights concerning the most prominent browser threats faced by organizations during the first half of 2023.

ENTERPRISE BROWSERS AND SECURITY EXTENSIONS

To properly address the plethora of existing and emerging threats to web browsers, CISOs and other security leaders should adopt an approach that leverages both the use of enterprise browsers and security extensions as a frontline security solution.

In a report recently released by Gartner—***Emerging Tech: Security – The Future of Enterprise Browsers***—Gartner defined an enterprise browser as "a stand-alone web access application with integrated security, centralized policy management, visibility, reporting, productivity, and collaboration tools." Likewise, browser extensions are referred to as "managed agents executed by a browser application to deliver additional security or productivity services."[5]

As a security solution, enterprise browsers and extensions provide an alternate, light-weight method for delivering many desirable features and benefits. According to Gartner, there are four families of key features and benefits a security solution should include:

- Prevention and Detection
- Centralized Management
- Visibility and Response
- Productivity and Collaboration

[5]See "Emerging Tech: Security – The Future of Enterprise Browsers," Gartner, April 14, 2023. Ermes Intelligent Web Protection was recognized by Gartner in this report and a complimentary copy can be downloaded at <Ermes URL download page here>.

PREVENTION AND DETECTION

Modern web pages are complex and dynamic objects—no longer the static web pages comprised of “fixed code” reminiscent of decades ago. Given their complexity and native vulnerabilities, attackers can weaponize a web page through a wide range of malicious activities.

The primary security challenge posed by these dynamic objects or pages is that malicious features only become operational once a web page is rendered by the browser. Also, they cannot be detected by analyzing encrypted network traffic.

An enterprise browser security platform can mitigate web-borne threats by detecting and preventing specific threats and vulnerabilities related to phishing, data loss, web content, and malware.

PHISHING PROTECTION

Any reputable enterprise browser security solution will provide protection from phishing attacks that can cost large enterprises nearly $15 million annually according to a study released by the Ponemon Institute in *The 2021 Cost of Phishing Study.*

Phishing, a type of social engineering attack often used to steal login credentials and credit card numbers, is typically accomplished by disguising compromised web pages and deceiving users as to its legitimacy. These normally involve the use of embedded scripts that leverage autofill and login manager to extract a user’s sensitive information which is then sent to an attacker’s email address.

DATA LOSS PREVENTION

Data loss prevention features for an enterprise browser with security extensions should address the following concerns:

- Information sharing related to the uploading of credit card numbers and other sensitive data.
- Enforcement of data protection policies that restrict or prevent the uploading of data files from managed devices to ungoverned web locations.
- Enforcement of data protection policies that restrict or prevent the sharing of data files to web locations external to the company.
- Enforcement of data protection policies that restrict or prevent screen captures when interacting with a sanctioned app or web page.

An enterprise browser security solution should also address any unauthorized modifications to browser-related features such as the camera, microphone, audio, and video. These are all capable of capturing sensitive corporate data and exfiltrating it to a malicious actor.

WEB CONTENT SECURITY

This feature provides enterprises with the ability to enforce custom policies that govern user navigation through web content filtering. It does so by preventing a user from visiting pre-defined lists of websites (blocklisting) or by limiting a user's access to only certain trusted web categories (allowlisting).

MALWARE PROTECTION

Malware or malicious software installed on a computer or system without a user's consent poses a significant threat when using a browser.

This feature addresses several problems directly related to malware and browser use within an organization. These include:

- Exploitation of browser vulnerabilities that enable attackers to execute code remotely and gain an initial foothold within an on-premises environment.
- Drive-by downloading of malicious files capable of performing a wide range of activities such as opening a backdoor for attackers or executing a ransomware payload.
- Enforcement of data protection policies to restrict or prevent the downloading of data files to unmanaged devices.

CENTRALIZED MANAGEMENT

An enterprise browser allows organizations to manage threats and risks by incorporating a centralized management console for policy enforcement.

DEPLOYMENT

As a security solution, there is a basic requirement that an enterprise browser security solution must have an architecture that can be easily and rapidly deployed through a centralized installation process covering all browser activities.

Additionally, deployment to all managed devices should occur through a centralized installation using group policy or other software distribution utilities.

MONITORING AND ANALYT

When it comes to monitoring, a browser security platform must provide 360-degree visibility into all user activity. This includes all data usage within authorized web apps as well as other non-corporate web destinations. By doing so, it protects users from browsing malicious websites, rogue extensions, and becoming inadvertent victims of phishing attacks. All of which safeguards sensitive corporate data from compromise or loss.

Moreover, these activities must be supported by robust reporting and analytics tools that allow administrators to quickly understand what attacks are threatening their users, perform forensics analysis, and quickly mitigate threats.

POLICY-DRIVEN CONFIGURATIONS

As previously mentioned, centralized deployment and configuration of software on all user devices is a key requirement to distribute security tools and enforce usage.

However, another critical aspect directly related to this, is the ability for administrators to centrally define and programmatically execute policy from security cookbooks. Put another way, security professionals must be able to configure specific pre-defined procedures in the event that security anomalies are detected.

In the context of browsing, administrators must be able to develop and deploy policy from these cookbooks as a direct response to anomalous patterns detected. For example, this might include a user installing multiple border-line extensions or visiting an abnormal number of malicious websites—all of which might be indicative of a compromise to security.

COMPLIANCE REQUIREMENTS

An enterprise browser security solution must ensure compliance with all international privacy regulations and technology frameworks with a comprehensive focus on Zero-Trust, identity, and privacy.

At a minimum this would include compliance with the following standards, legal requirements, and frameworks:

- GDPR
- EU ePrivacy
- CCPA/CPR
- PSD2
- PIPEDA
- LGPD
- PCIDSS
- HIPAA
- Anti-Bribery and Corruption Laws
- ISO 27001
- CIS Controls
- SOC1/2
- IS2700

VISIBILITY AND RESPONSE

Threat actors target browsers because it is both a gateway to the hosting device and to access the sensitive data it stores such as passwords, cookies, and other credentials. To do so, cybercriminals leverage security malpractices along with visibility blind spots.

In order to prevent this risk and ensure that browsers always maintain a sound security posture, there must be extensive visibility into all activities for security professionals to formulate an effective response to a threat. To achieve visibility, an enterprise browser security platform should include continuous security auditing, browser extension control and blocking, and logging with forensics.

CONTINUOUS SECURITY AUDITING

Bad actors seek browsers and extensions with unpatched vulnerabilities to exploit. When successful, this can lead to malicious remote code execution.

A browser security platform can mitigate this through continuous security auditing that includes the following capabilities:

- Scanning for browser and extension versions to detect unpatched vulnerabilities.
- Alerting upon detection of an unpatched browser or extension.
- Acting as a centralized monitoring interface for all browsers in the environment.
- Automatically alerting and enforcing security updates as they are released.
- Auditing credentials used to login for both enterprise and personal services.
- Real-time analysis of user behavior to detect anomalies that may indicate risky activity or potential account compromise.

BROWSER EXTENSION CONTROL AND BLOCKING

Cybercriminals also use malicious browser extensions to achieve various goals such as multi-factor authentication (MFA) bypass, data theft, and malware installation. Additionally, there are borderline extensions out there that ask for multiple permissions that are non-proportional or unrelated to their feature delivery. For example, extensions that provide dark-themed reading for web pages might ask permission for full visibility on web requests.

Unfortunately, there are few tools out there that provide real visibility/governance into the installation of these extensions—which can often occur without even the knowledge of the user. An enterprise browser security platform can mitigate this risk by:

- Scanning for browser extensions that were installed prior to the platform's deployment.
- Detecting malicious extensions, based on their behavior, and removing them.
- Scanning for browser extensions with permissions that are too broad when compared to the features they purport to deliver.
- Scanning for browser extensions that are outdated.
- Enforcing a policy that either prevents the installation of browser extensions altogether or applies real-time analysis to determine if they are safe.

LOGGING AND FORENSICS

An enterprise browser security platform should provide both granular and consistent visibility into all user actions across all web destinations. This should include allowed/unallowed web apps, third-party web services, and other web destinations.

Moreover, it should provide visibility into all installed web extensions while checking for allowed, unallowed, and risky browser plugins.

PRODUCTIVITY AND COLLABORATION

As mentioned earlier in this paper, for many organizations, security is viewed more as a business obstacle, rather than an enabler. Therefore, it is critical that CISOs and security leaders better manage the trade-off between security and agility. In other words, effectively closing the security loop without impacting productivity. To do so, they should choose a browser security solution that focuses on user experience, drives productivity, and respects privacy.

USER EXPERIENCE

An effective browser security platform should not cause a disruption or noticeable change in the browsing experience. In practice this usually falls into two types of usage:

1. Standard browsing when no malicious or risky event is detected.
2. Browsing when a threat is detected and requires mitigation.

In the case of standard browsing when no risk is detected, there should be no difference between a user's browsing experience before the deployment of the security solution and after. To do so, a browser security platform should be compatible with all commercial browsers already in use in the corporate environment. Additionally, the browser security platform should be continuously monitoring and protecting the web session without slowing down or impairing browsing quality.

In the event of browsing when a threat is detected and requires mitigation, the easiest solution in the past has been to terminate the session altogether. However, this is a guaranteed path to disgruntled users and complaints. As these complaints mount, it would likely result in the gradual off-boarding of the solution.

So, instead of terminating a browsing session, when possible, a browser security solution should determine if an equal level of protection can be achieved by merely disabling a specific feature in the visited web page. To do so, a browser security platform should be able to do the following:

- Detect risky components in a web page with high precision (for a full list of these components see the checklist provided later in this paper).
- Employ a wide set of protective actions, from session termination to disabling web page functionalities (for a full list of these actions see the checklist provided later in this paper).
- Determine the least intrusive protective action in respect to the detected risk.

DRIVING PRODUCTIVITY

When it comes to driving productivity, the ideal approach to security is to always keep the business in mind. Accordingly, an effective browser security platform should reduce distractions to users by being ad-free. Also, as indicated earlier, the browser is the main gateway to many apps and productivity services delivered as SaaS nowadays.

USER PRIVACY

Ideally, a browser security platform must shed light on all browsing activity blind spots. However, to do so, might necessarily involve collecting personal information that privacy regulations limit being made visible to anyone that is not authorized. As such, a browser security platform must be able to provide the perfect balance between security and privacy requirements by respecting two fundamental privacy-driven principles:

1. If a risk is detected, it is imperative to send only data related to the risk for further analysis and action without exposing any personally identifiable information (PII) beyond a user's corporate identity.
2. Security teams should be fully enabled to determine the level of PII exposed based on corporate needs, ranging from zero to full disclosure.

PREDICTIONS

Below are some predictions that researchers at Ermes have made concerning the current state of web browser security.

DEMOCRATIZATION AND INCREASING SOPHISTICATION OF WEB-BASED ATTACKS

Due to the recent rise and availability of inexpensive phishing kits in the underground economy, phishing has now become within the reach of less tech-savvy attackers—thus increasing the number of phishers and potential attacks worldwide.

Moreover, we are witnessing the rise of phishing-as-a-service platforms which allow attackers to design their attack campaigns in a few simple clicks.[6] All of this compounded with the increasing complexity of web applications and attacks will almost certainly increase security blind spots.

USER AS THE WEAKEST SECURITY POINT

With the increasing sophistication of attacks targeted at web browsers, it is fundamental to keep users aware of new threats, especially from bad actors leveraging advanced social engineering techniques.

Humans still are and will be the weakest point in the security chain. This requires security teams to implement policies that identify users with a higher risk of being manipulated. Moreover, security teams should adopt more effective tools to increase both user security posture and awareness.

[6]See "New phishing-as-a-Service Platform Lets Cybercriminals Generate Convincing Phishing Pages," The Hacker News, May 13, 2023 at https://thehackernews.com/2023/05/new-phishing-as-service-platform-lets.html.

BROWSER AS THE MAIN ATTACK WINDOW

The unique position of the browser as the default tool for both work and private use will drive more adversaries to turn personal browser usage into an attack vector for accessing work resources. Attackers will try to maliciously access enterprise data by going after the personal browsers of employees.

Because of the dual utility of the browser, security teams are compelled to treat all browsing activity as a single, consolidated attack surface.

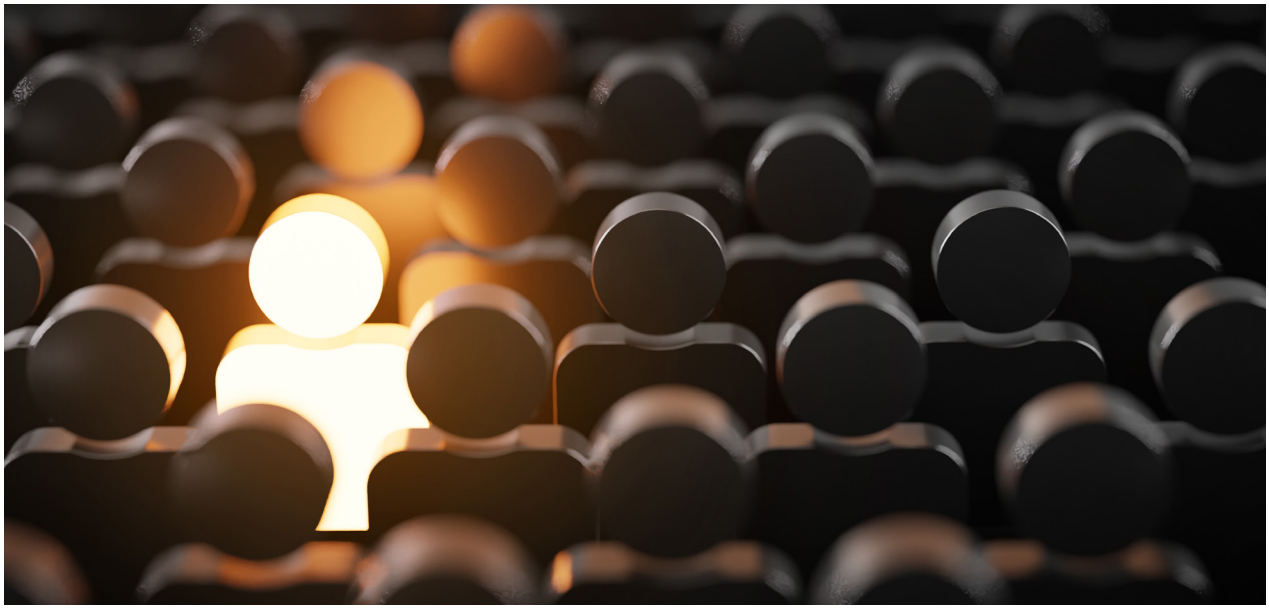
GROWTH OF SAAS ATTACKS

The proliferation of software-as-a-service (SaaS) apps usage within the enterprise environment will decrease the portion of traditional files within it respectively. This will be reflected in the threat landscape as well—more attacks moving from being file execution-oriented to focusing on malicious access to SaaS and web apps. Consequently, the share of web and cloud-based attacks is expected to grow.

INSIGHTS FOR 2023 AND BEYOND

These were some of the most prominent insights, behaviors, and statistics observed by Ermes' researchers during the first half of 2023 that are directly related to the browser threat landscape:

- Millennials and Gen-Z internet users are most likely to fall victim to phishing attacks.[7]
- The average cost of a data breach against an organization is expected to surpass $5 million per incident,[8] for larger enterprises it is already $15 million according to a study released by the Ponemon Institute.
- The use of enterprise credentials with unsanctioned web apps/SaaS is on the rise—in fact the number of corporate credentials with unencrypted passwords posted on the dark web has increased by 429%, leaving organizations vulnerable to various cyber-attacks.[9]
- Continued navigation of risky websites (i.e. pirate streaming) and young domains.
- More downloading of malicious and high-risk browser extensions.
- Surging of HTML smuggling—a highly evasive malware delivery technique that leverages legitimate HTML5 and JavaScript features.[10]
- Risky data and document sharing via unauthorized web apps/SaaS will continue.



[7]See generally "The Latest 2023 Phishing Statistics," AAG, February 6, 2023 at https://aag-it.com/the-latest-phishing-statistics/.

[8]See "Average Cost of Data Breaches to Surpass $5 MN Per Incident in 2023: Report," TechCircle, December 19, 2022 at https://www.techcircle.in/2022/12/19/average-cost-of-data-breaches-to-surpass-5-mn-per-incident-in-2023-report.

[9]See "Number of Corporate Credentials Exposed on the Dark Web Increased by 429%," Help Net Security, October 8, 2020 at https://www.helpnetsecurity.com/2020/10/08/corporate-credentials-dark-web/.

[10]HTML smuggling has been used in banking malware campaigns, notably attacks attributed to DEV-0238 (also known as Mekotio) and DEV-0253 (also known as Ousban). See generally "HTML Smuggling Surges: Highly Evasive Loader Technique Increasingly Used in Banking, Malware, Targeted Attacks," Microsoft, November 11, 2021 at https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/.

CHECKLISTS

Deployment

- [ ] Compatible with most commercial browsers
- [ ] Restarting browser is not required to activate
- [ ] Centralized, automatic, fast, and easy implementation

User Experience

- [ ] Up to 3x faster loading web pages
- [ ] No impairment for users
- [ ] Focus is on page content without distracting ads

Visibility and Logging

- [ ] Issues alerts for web security incidents
- [ ] Provides configurable data collection
- [ ] Integrates with SIEM/SOAR
- [ ] Delivers cyber-threat information for intelligence

Account Protection

- [ ] Blocks use of corporates credentials for unsanctioned web apps
- [ ] Audits use of corporate credentials on the web
- [ ] Prevents usage of personal credentials on corporate web apps

Data Loss Prevention

- [ ] Blocks the upload of unauthorized file categories
- [ ] Prevents cut and paste, screen capture, and page printing

Protection Against Malicious Webpages

- [ ] Stops users from providing credentials to malicious pages
- [ ] Blocks zero-day phishing sites
- [ ] Protects against scam sites and malvertising
- [ ] Intercepts malware by blocking drive-by-download web pages

Security Audit

- [ ] Alerts for risky navigation patterns
- [ ] Identifies users who might be involved in social engineering campaigns
- [ ] Provides awareness pills for users involved in attacks

User Privacy

- [ ] Protects users from rogue tracking services
- [ ] Adjusts for levels of personal data exposure based on corporate needs
- [ ] Prevents users from sharing personally identifiable information on the web

Protection Against Risky Web Extensions

- [ ] Scans for browser extensions
- [ ] Alerts, disables, and removes malicious extensions
- [ ] Enforces extension installation governance policies

Policy-Driven Navigation

- [ ] Allows admin to define categories of websites users-including those who are allowed or not allowed to browse
- [ ] Governs access to productivity services
- [ ] Allows zero-trust browsing policies

ERMES AI-DRIVEN SOLUTIONS FOR WEB PROTECTION

To best serve its customers and organizations that wish to protect against the browser threat landscape, Ermes—recognized by Gartner as one of the best emerging companies in the world when it comes to using AI in cyber-security—has developed a unique early detection system to address threats/attacks targeting web browser use.

We offer a unique solution using 10+ machine learning and deep learning proprietary systems that analyze the actual behavior associated with sophisticated and evolving tactics. Our innovative, AI-driven behavioral web protection solutions overcome the severe limits of traditional solutions for detecting vulnerabilities and contemporary threats emanating from the web.

CONCLUSION

According to Gartner, enterprise browser management is expected to grow to widespread adoption by 2030. Web security, workforce productivity, and unmanaged device access use cases are the top drivers for adoption among new entrants. Enterprise browsers and extensions provide an alternate, light-weight method for delivering many of the features and benefits that existing security technologies provide today.

CISOs and other security leaders might wish to consider the robust enterprise browser security extension developed by Ermes. It acts as a centrally managed agent to deliver additional security services that shield organizations from the browser threat landscape detailed in this paper.

In its most recent report on the subject of browser security, Gartner specifically recognized Ermes for its proprietary enterprise browser security solution, and among all vendors in the report, Ermes is the only one based in the European Union (EU).[11] **This report from Gartner—Emerging Tech: Security – The Future of Enterprise Browsers—can be read here.**

[11]See "Emerging Tech: Security - The Future of Enterprise Browsers," Gartner, April 14, 2023. Ermes Intelligent Web Protection was recognized by Gartner in this report and a complimentary copy can be downloaded at <Ermes URL download page here>.

ABOUT

Ermes - Browser Protection protects companies and employees from contemporary threats that users encounter while surfing the web through the use of artificial intelligence (AI) and deep-learning.

As a leading innovator in web security and data protection, we specialize in modern cyber-threats that elude traditional security systems. This includes attacks that rely on the use of web browsers to breach systems. Our early detection software makes it possible to secure your enterprise from the browser threat landscape.

We look forward to working with you so we can demonstrate the security benefits that our proprietary solutions can provide to your organization.

Ermes Cyber Security SPA.
Corso Bernardino Telesio 29,
10146 Torino, Italy

info@ermes.company

www.ermes.company

ERMES

BROWSER SECURITY

info@ermes.company | ermes.company