Browsers are the Target: Protect Them with Zero Trust Browser Isolation

Introduction

The internet has unquestionably revolutionized the world over the past 30+ years. The sophistication and ease that web browsers have brought to internet use in particular, have enabled unprecedented productivity gains for individuals and especially for businesses.

Browsers today represent the primary means of interacting with the information and apps we need to do our work and, in the case of web-based email, instant messaging, and collaboration apps, the way we stay connected with fellow employees. On almost every user device, the browser — whether Chrome, Edge, Firefox or others — is open and active whenever the device is, as a primary space where work happens.

Fantastic, right? Except that what was the stuff of futuristic fiction just a few short decades ago has now taken on a dystopian tinge. Today, web browsers are the target of choice for hackers and cybercriminals seeking to do harm to your organization, for profit or kicks.

Why focus attacks on web and email? The simple answer is because it works. Criminals have identified the web and email as the paths of least resistance for delivering ransomware and other forms of malware to endpoints and from there, to the rest of the network.

ericom security by cradlepoint

Table of Contents

> **"Most attacks are delivered via the public internet either through web browsing or emailed links that trick the user into visiting malicious sites. Simply removing (or more strongly, isolating) the browser from the end user's desktop significantly improves enterprise security posture."** [1]
>
> **Neil McDonald,** VP & Distinguished Analyst, Gartner

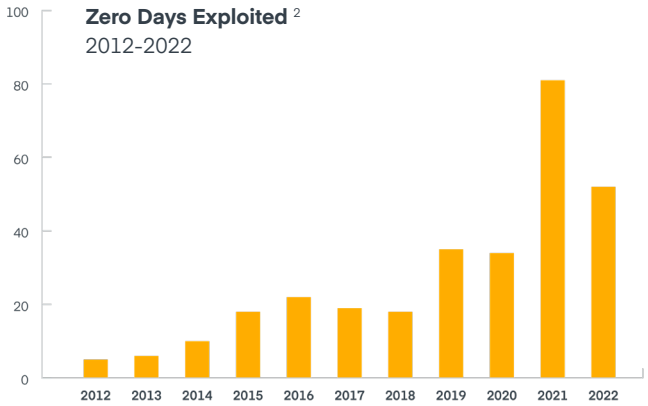
[1] ***Gartner,*** *Network Security Hype Cycle, 2020 June 30, 2020*

Unfortunately, most existing web and email security is no match for today's savvy cybercriminals (which is what keeps these paths attractive.) These solutions are limited by reliance on legacy signature-based security scanning techniques, which attempt to scan and match web and file traffic to known malware variants. If the malware on a site or in an email attachment is a match, it's stopped before reaching the endpoint. But if the scan misses malware, it flows right on through.

40% of web-based malware are zero-day threats

With today's explosion of zero days being exploited in cyberattacks, this approach is doomed to fail. As much as 40% of web-based malware is zero-day threats, which are not "known" to be bad and therefore not caught by signature-based email and web scanning.

A fundamental shift in how we combat malware attacks on vulnerable browsers and webmail is required. One that stops the cat and mouse approach that leaves legitimate users always at risk, and instead stops all malware from entering via these vectors. You read that right — 100% of the threats from the web, stopped. We'll introduce you to how this can be done — a technique called Browser Isolation — but let's first better understand why securing web browsers can be such a challenge.



[2] *Confirmed exploitation of zero-day vulnerabilities in the wild (2012-2022)*

What makes browsers such good targets?

In a word, vulnerabilities. All major browsers — Chrome, Edge, Firefox, and Safari — ship with dozens of vulnerabilities. Their developers play a continual game of "whack-a-mole", spinning out new versions quickly to address security issues. (This is one of the reasons why browser version numbers are so high, with Chrome version numbers exceeding 120!). It's a never-ending struggle with every Patch Tuesday quickly followed by fallout on Exploit Wednesday.

Browsers are particularly sweet targets for attackers who use zero-day malware since almost every desktop computer has at least one browser installed — and many have two or three. When users visit a rogue website, as they often do, malware can exploit vulnerabilities in these browsers. Once they have penetrated the browser, they easily move on to attack systems and networks.

In this context, Windows's lack of a process isolation mechanism is most problematic, since it means that there is no way to segregate the browser from critical system processes. In other words, a security issue in the browser can place the entire operating system at risk.

Malware variants such as WannaCry pose less direct, but still serious threats to browsers, by introducing browser hijackers or other extensions that can be used to harvest account credentials, cookies, and web search history. While the browser is not the primary target of these attacks, it is still in the crosshairs as a rich source of valuable data.

[3] *Windows certainly isn't the only operating system in use. But this white paper focuses on Windows, given its dominance in the consumer market.*

Meticulously patching browsers is absolutely necessary, but never sufficient. With so much malware on the web, it's a given that infections are but a click away. Even if 99% of the devices in an enterprise are secured, it takes just one successful malware attack on a single device to spread mayhem throughout the organization.

These issues make web browsing one of the biggest security risks in an organization. But unlike other risky activities, browsing cannot be banned: It's a clear business need.

High times for hackers

Along with other unfortunate events, 2020 will be remembered for **a seven-fold increase in ransomware attacks** — a trend that has continued to accelerate. Ransomware is present in 62% of incidents committed by organized crime actors and 59% of all financially motivated attacks. And it is most often introduced via email, desktop sharing apps, and web applications. [4]

That shocking growth rate clearly demonstrates the difficulty involved in dealing with this menace. And it's not just numbers that increased, but also the sophistication and aggressiveness of the attacks, which makes them more dangerous than ever before.

Once cybercriminals gain access, their aim is to encrypt as much of a corporate network as possible in order to extort a hefty ransom in order to restore it. This has proven to be a lucrative business for hackers, with many of them taking in hundreds of thousands or even millions of dollars this year. Lured by these paydays, cybercriminals have developed malware that is highly inventive, making it easier than ever to evade legacy signature-based secure web gateways, next-generation firewalls, and anti-virus security controls.

[4] *2023 Verizon Data Breach Investigations Report*

Browser isolation — a Zero Trust approach to web access

As highlighted above, in a recent report, Gartner noted the power of a highly effective web security approach called Remote Browser Isolation (RBI). Gartner was the first analyst firm to put the technology on the map, in a report unambiguously titled "It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing". One need not be a distinguished analyst to understand that unless the browsing experience is cleaned up, myriad security issues put enterprises at risk.

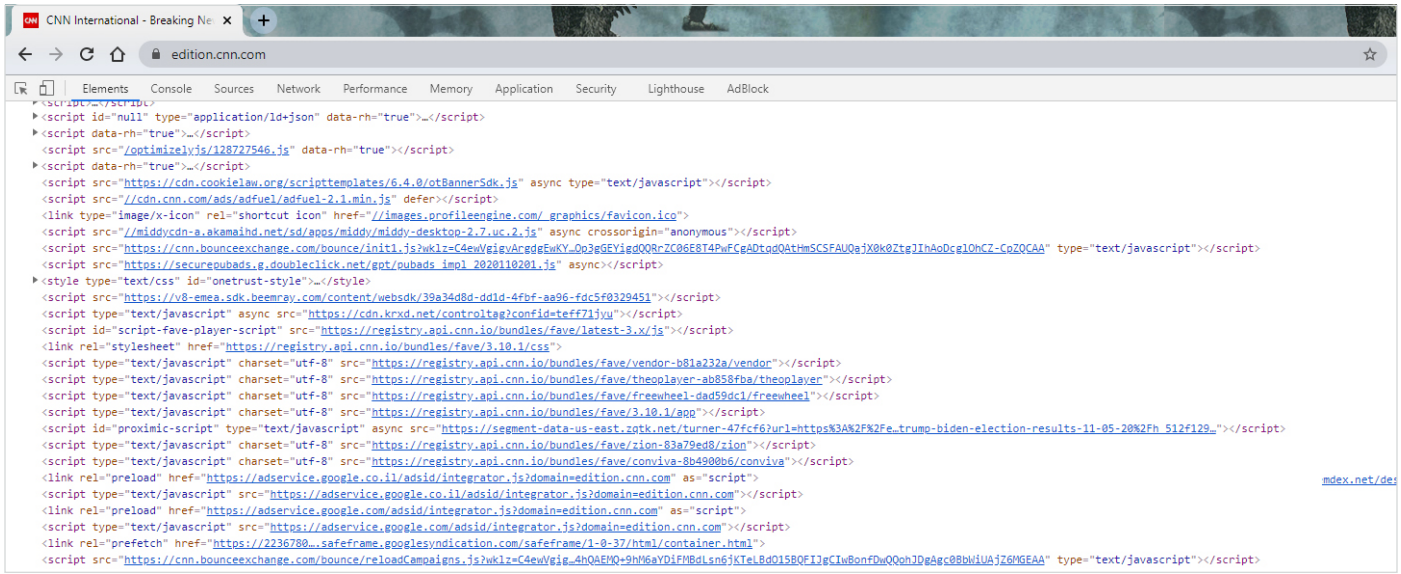
Gartner notes that RBI reduces the impact of browser-based attacks by isolating browsing's "back end" from the user device, as well as from the enterprise network and systems. Isolating browsing makes previously risk-laden web sessions accessible to users in the form of safe web rendering information, free of malware. Items for download such as web docs or e-mail attachments are sanitized fully as they're delivered. And once isolation is no longer needed, remote isolated browsers are simply destroyed, along with all malware generated during the session, and a new one is created for the next browsing session.

The ROI on browser isolation is compelling. Since most attacks originate from the Internet, the mere act of shifting the browsing process off the endpoint and into a safe zone reduces the attack surface. Gartner estimates that firms that isolate browsing will see a 70% reduction in attacks that compromise end user systems.

Browser isolation stops 100% of malware-based attacks delivered via the critical web and email vectors on which cybercriminals focus so much of their efforts. Pragmatic organizations know that attacks are inevitable. What differentiates resilient organizations from others is how well they minimize attack surfaces and how well prepared they are to recover in the aftermath of an attack. Isolation and containment are important as key means to limit the ability of adversaries to wreak havoc.

By operating on the assumption that no web content is safe, isolation brings the concept of Zero Trust security to the internet. In a Zero Trust security world, nothing is implicitly trusted — no user, no device, no application, no destination, no content. Taking this concept to the web, no user can implicitly trust any website. Even sites that might be considered "safe", like the Wall Street Journal, CNN or ESPN, could have advertisements that contain embedded malware. Check the page source of a site like CNN and you'll see all the places where malware can be hidden. And if malware is there, and makes its way into the browser on an unsuspecting user's laptop, it immediately begins to run, exploiting any vulnerability. And then, it is off to the cyberattack races.

Isolation operates on the assumption that every site might have something malicious on it, and takes steps to mitigate against this risk. By running sessions in a remote isolated container, typically in the cloud, anything bad on a website is kept away from an organization's environment. Think of it as a barrier between the endpoint and the insecure frontier of the Internet: The user has the same browser experience, but the risk of attack and malicious infections are eliminated.



Typical websites have dozens of javascripts, style-sheets, fonts, images, advertisements, and so on that can hide malware — which runs once it makes its way onto a device browser.

Browser Isolation...

Eliminates the browser as an attack surface to minimize the enterprise attack service overall.

Prevents credential theft by rendering websites in read-only mode, RBI prevents users from entering IDs, passwords and other credentials on potential phishing sites.

Prevents data loss. Optional controls can be applied to prevent users from uploading information or copying or printing pages. Additionally, isolated web sessions leave no data "footprint" in a browser's cache, which helps reduce the risk that sensitive data from web and cloud-based applications will be lost (especially when these types of apps are accessed via unmanaged devices).

Frees up operation resources by simplifying web access policy management. RBI eliminates the need to define complicated web access policies and adjust them for various users and groups. IT simply identifies sites that violate acceptable use policy (e.g. pornography) and should be blocked; all other sites can be isolated. Enterprise Network Ops and Help Desk resources no longer need to manage a continual flow of requests to unblock web locations for specific users.

Simplifies browser management — Browser isolation means that you no longer have to worry about what version of Firefox, IE or Chrome each employee is using. Just update once and the job is done.

Plays nicely with other solutions — Browser isolation complements existing core security solutions such as secure web gateways (SWGs), next-generation firewalls (NGFWs), intrusion detection (IDS), data loss prevention (DLP), and file integrity monitoring (FIM).

Frees up Incident Response resources — Incident Response personnel are a precious resource and, unfortunately, their plates are typically overflowing. RBI eliminates many of the incidents that now consume their time.

Helps reduce cyber-insurance costs — Firms with effective and formal information security program are often able to negotiate more favorable rates from their cyber-insurance carriers.

Introducing Ericom Web Isolation

Ericom Web Isolation is an enterprise-grade security solution that remotely isolates web traffic from endpoint browsers. Typically deployed as a cloud service within the Ericom Global Cloud platform, Ericom Web Isolation is a clientless solution that leverages remote browser isolation (RBI) and can be easily deployed to quickly secure web and email access for the largest of enterprises.

A major advantage of Ericom Web Isolation is its ability to enhance security without impacting the end user browsing experience. Each web session is rendered remotely in a contained virtual environment, and safely delivers a safe stream of rendering information in real time, for a seamless, native end user browsing experience. Its efficient container-based architecture spins up a new virtual container for every browser tab opened.

Ericom Web Isolation strengthens security without impacting the end user browsing experience.

Malware in active web and email content targets enterprises via endpoint browsers

Ericom Web Security executes web content in a virtual browser in a isolated container. a. Download content b. Execute c. Render

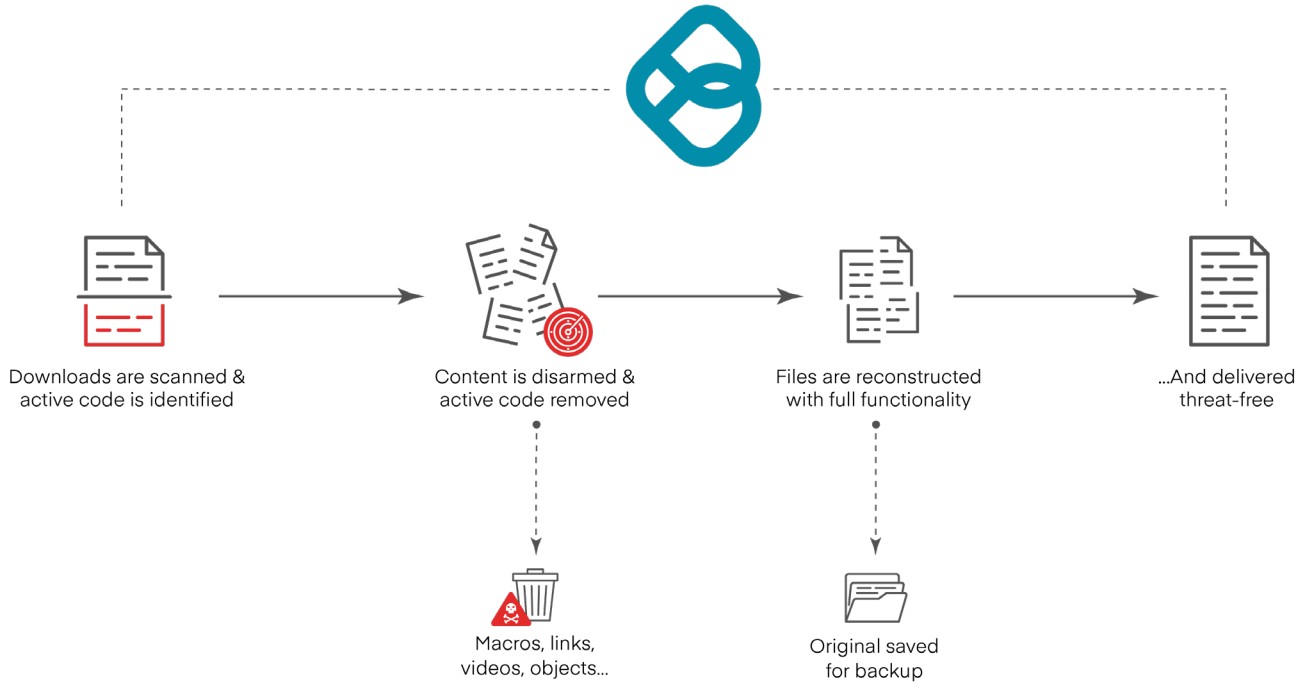
Rendered webpages are sent to endpoints as a safe interactive media stream

Users enjoy secure and seamless browsing in their standard browser

At the end of each session, the remote container is destroyed, preventing attack persistence and drive-by downloads, phishing attempts, and other malware from ever reaching your users or your network.

When used to secure email, Ericom Web Isolation not only prevents malware from malicious phishing sites, but also prevents credential theft by enabling sites launched from links embedded in emails to be launched in read-only mode. Users can see the sites, but are prevented from inadvertently revealing IDs, passwords and other credentials to cybercriminals.

Of course, malware can also make its way onto devices through downloaded content, such as documents on websites or email attachments (e.g., .pdf, .doc, .xls, and .ppt). Ericom Web Isolation has this threat vector covered as well. The solution's Content Disarm and Reconstruction (CDR) capabilities sanitize any documents that may be weaponized, preventing malware from being introduced into the enterprise environment via malicious downloaded content. Files are downloaded to the browsing session container, where they are examined and sanitized of known and unknown threats using data sanitization, vulnerability assessment, and multi-scanning approaches These techniques occur in the background without impacting user browsing experience or file functionality.



Conclusion

Moving web security measures from the local user device to a remote, isolated browser, is a game-changer from a security perspective. This Zero Trust approach to web access effectively quarantines all dangerous content — known or unknown — in a cloud-based container away from the device, yet offers end users the same excellent web and email experience to which they're accustomed. Regardless of whether a user browses to a website infected with ransomware or other malware, or is lured into clicking a link in an email, malware can't get onto their device. Without an initial beachhead in the device browser, malware — such as ransomware — cannot spread to additional devices and apps on the network.

Ericom Web Isolation protects organizations by isolating malware, ransomware and other threats where they can't harm corporate network or user devices. It transparently secures Internet use, including file downloads and phishing sites, while reducing risk, costs and operational burden to IT staff responsible for browsing operations. Ericom Web Isolation harnesses the power of RBI to deliver secure browsing and protect the corporate network and endpoints.

Learn more at **ericom.com** or **contact us**